



Sicherheitslücken schließen

Industrielle Schadsoftware. Dass Computerviren und -würmer auch vor Industrieanlagen keinen Halt machen, sollte spätestens seit Bekanntwerden des Stuxnet-Wurms klar sein. Die eigentliche Gefahr geht heute aber nicht mehr von diesem Wurm selbst aus, sondern von für sehr wahrscheinlich gehaltenen Mutationen. Das Berliner Unternehmen Innominate schafft es, diese Lücke zu schließen.

Joachim Vogl

Der Stuxnet-Wurm hat nach seiner Entdeckung im Juni 2010 weltweit Aufsehen erregt. Er ist der erste öffentlich bekannte und gezielte Angriff auf industrielle Anlagen und wurde vermutlich von zwei Dutzend Entwicklern mit dem Ziel geschrieben, die Leittechnik einer Anlage zur Uran-Anreicherung im Iran zu sabotieren. Die genauen Ziele, Autoren und Auftraggeber sind allerdings bislang unbekannt.

Laut der Phoenix-Contact-Tochter Innominate Security Technologies hat Stuxnet zehntausende von PCs infiziert, windows-basierte Automatisierungssoftware für seine Zwecke missbraucht und manipuliert, um darüber Schadcode in die Steuerungen spezifischer, real existierender Industrieanlagen einzuschleusen. „Während Stuxnet sich noch auf Produkte aus der Siemens-Simatic-Familie und STEP-7-SPS-Projekte mit speziellen Eigenschaften fokussierte, könnten

solche Mutationen auch Komponenten anderer Hersteller erfassen und in ihrer Schadwirkung erheblich weniger wählerisch ausfallen“, vermutet Torsten Rössel, Director Business Development bei Innominate.

Einmal ganz davon abgesehen, dass industriell genutzte PCs häufig nicht mit Antivirus-Software ausgerüstet werden (können), hat Stuxnet auch deutlich gemacht, dass konventionelle Virens Scanner gegen Angriffe dieser Qualität keinen Schutz bieten. Die Analysen von Stuxnet haben rückblickend ergeben, dass der Wurm vor seiner Entdeckung schon mindestens zwölf Monate lange unbemerkt in Umlauf war und während dieser Zeit von Antivirus-Programmen mangels bekannter Signaturen nicht erkannt wurde.

Seit dem ersten Auftreten von Stuxnet haben weltweit insgesamt 22 Siemens-Kunden aus dem industriellen Umfeld von einer Infektion mit dem Trojaner berichtet (Stand: 22. November 2010). In sämtlichen Fällen konnte die Malware entfernt werden und in keinem dieser Fälle kam es laut Siemens während der Infektion zu Auswirkungen auf die Automatisierungslösung.

Aktivitäten des Wurms

Für die Konzeption von Schutzmaßnahmen gegen stuxnetartige Angriffe ist ein grundlegendes Verständnis der Aktivitäten des Wurms unverzichtbar. Er entfaltet seine Schadwirkung in vier Stufen auf verschiedenen Ebenen.

1. Infektion von Windows-PCs: Der Wurm nutzt einen aggressiven Mix von Mechanismen, um sich sowohl auf vernetzte als auch (über USB-Flash-Disks) auf nicht vernetzte Windows-PCs zu verbreiten und diese zu infizieren. Dabei nutzt er insgesamt vier vormals unbekannte Verwundbarkeiten aus, die in mehreren Generationen von Windows-Betriebssystemen vorhanden und durch Security Patches bislang nur teilweise behoben sind. Neben einer Reihe verschlüsselter Dateien, die der Wurm im Verzeichnis %SystemRoot%\inf\ ablegt, installiert Stuxnet dabei die zwei Gerätetreiber %SystemRoot%\system32\drivers\MrxNet.sys und %SystemRoot%\system32\drivers\MrxCLS.sys. Diese Treiber wurden mit geraubten privaten digitalen Schlüsseln der Firmen Realtek und JMicron signiert und enthalten daher Zertifikate, welche von Windows-Systemen als vertrauenswürdig eingestuft werden.

2. Missbrauch und Manipulation von Automatisierungs-Software: Sofern Stuxnet auf einem infizierten PC Installationen von WinCC Visualisierungs- oder Step-7-Projektierungs-Komponenten vorfindet, missbraucht und manipuliert er vorgefundene WinCC-Datenbanken und Step-7-Projekte, um seine weitere Verbreitung und Persistenz auf dem PC zu sichern und in den Projekten erfasste Steuerungen als potenzielle Ziele für Stufe 3 auszuspähen. Ferner benennt Stuxnet



„Die laufende Suche nach Schwachstellen würde das Infektionsrisiko erheblich reduzieren.“

Tino Hildebrand, Siemens

die für die Kommunikation zwischen Simatic-Manager und projektierten S7-Steuerungen zuständige Dynamic Link Library s7otbxdx.dll im Verzeichnis %SystemRoot%\system32\ in s7otbxdx.dll um und legt an ihrer Stelle eine eigene Wrapper-DLL unter dem Namen s7otbxdx.dll im gleichen Verzeichnis an.

3. Einschleusen von Schadcode in Steuerungen: Über eben diese manipulierte Wrapper-DLL wird Stuxnet in die Lage versetzt, letztlich beliebigen Schadcode in die projektierten SPSen einzuschleusen, diese Manipulationen vor dem Projektierer zu verbergen und vor einem erneuten Überschreiben zu schützen. Der von Stuxnet gezielt nur in Steuerungen und Projekte mit ganz spezifischen Eigenschaften konkret eingebrachte Schadcode selbst ist von ausgesprochener Raffinesse und dient nach letzten Erkenntnissen von Experten zur möglichst unbemerkten, dauerhaften Manipulation von Frequenzumrichtern und Turbinensteuerungen, mit dem Ziel der Störung von Prozessen und letztlich der Zerstörung der betroffenen Anlagen. Insbesondere der auf Steuerungen der Modellreihe S7-417 zielende Schadcode kombiniert dabei als sogenannter Man-in-the-Middle-Angriff Denial-of-Control- und Denial-of-View-Techniken in bislang kaum für möglich gehaltener Weise. Das legitime Steuerungsprogramm verliert dabei jede Kontrolle über den Prozess, ohne dass die Steuerung oder das Betriebspersonal auf den HMIs in seinen Leitständen dies bemerken würden. Das Angriffsmuster als solches ist generisch und könnte in Exploit-Werkzeugen wie Metasploit paketiert zur Verfügung gestellt und dann – entgegen oft geäußelter Beschwichtigungen – auch von Personen ohne umfangreiches Insider-Wissen für Angriffe genutzt werden.

4. Kommunikation mit Control&Command-Servern im Internet: Der Wurm versucht von infizierten PCs aus Kontakt zu mehreren Control&Command-Servern im Internet aufzunehmen. Sofern der Kontakt zustande kommt, können sowohl ausgespähte Informationen abgeliefert, als auch neue Instruktionen und Updates für den Wurm selbst und seine schadhafte Nutzlast empfangen und ausgeführt werden. Dies verleiht dem Spionage- und Sabotage-Potential des Wurms eine zusätzliche Dynamik. Kombiniert mit seinen Verbreitungsmechanismen über Peer-to-Peer-Verbindungen und USB-Flash-Disks können diese Effekte mittelbar auch auf Systeme ausstrahlen, die selbst über keine Netzwerk- oder Internet-Verbindung verfügen.

Schadsoftware rechtzeitig erkennen

Aufgrund der generellen Probleme mit dem Einsatz von Antiviren-Software auf industriell genutzten PCs und der rechtzeitigen Bereitstellung von Virensignaturen gewinnen alternative Verfahren zur Integritätssicherung an Bedeu-



„Stuxnet-Mutationen könnten deutlich mehr Schaden anrichten.“

**Torsten Rössel,
Innominate**

tung. So dient das mGuard-CIFS (Common Internet File System, von Windows und anderen Systemen genutztes Filesharing-Protokoll)-Integrity-Monitoring-Verfahren der konfigurierbaren Überwachung von Dateisystemen auf unerwartete Veränderungen von ausführbarem Code. Bei Initialisierung berechnet es eine Baseline von Signaturen für alle zu überwachenden Objekte und überprüft diese anschließend periodisch auf Abweichungen. Das Verfahren funktioniert ohne ständige externe Zuführung von Virensignaturen, ohne das Risiko einer Betriebsunterbrechung durch False Positives, ohne Installation von Software und mit nur moderater Belastung der überwachten PCs unter Nutzung einer mGuard-Security-Appliance. Verdächtige Modifikationen werden zuverlässig erkannt und umgehend per SNMP und E-Mail an Netzwerk-Management-Systeme und zuständige Administratoren gemeldet. In einem vom unabhängigen inIT-Institut für industrielle IT der Hochschule Ostwestfalen-Lippe durchgeführten Test konnte verifiziert werden, dass das mGuard-CIFS-Integrity-Monitoring-Verfahren Infektionen mit Stuxnet lange vor allen Antivirus-Produkten – bereits am Tage Null – als unerwartete Manipulation erkannt und Anwender davor gewarnt hätte. Dabei wurden sowohl die von Stuxnet installierten Gerätetreiber als auch die vorgenommenen Manipulationen an der entscheidenden Sematic-Manager-DLL entdeckt.

Verbreitung eindämmen

Bei der Verbreitung über Netzwerke und entsprechende Schwachstellen im Betriebssystem nutzt Schadsoftware häufig Netzwerkverbindungen, die zum produktiven Betrieb einer Anlage gar nicht erforderlich wären. Durch die Absicherung von Industrie-PCs und Steuerungen oder Gruppen solcher Geräte (Security Zellen) mit mGuard Firewalls lassen sich solche nicht benötigten und unerwünschten Verbindungen zuverlässig blockieren und die Ausbreitung von Schadsoftware in erheblichem Maße eindämmen. Im Falle Stuxnet konnten gesunde Systeme sowohl über bestimmte eingehende als auch

Sicherheit in Industrieanlagen ist nicht als Produkt zu verstehen, sondern vielmehr ein Prozess.

von ihnen ausgehende Verbindungen infiziert werden, befallene Systeme ihre Infektion entsprechend auch über bestimmte aus- und eingehende Verbindungen weiter verbreiten. Daher sollten beim Schutz durch Firewalls sowohl die eingehenden als auch die häufig vernachlässigten ausgehenden Verbindungen soweit als möglich gefiltert werden. Insbesondere der Kontakt über ausgehende Verbindungen zu Control&Command-Servern im Internet und das damit verbundene Potenzial für Spionage und Dynamisierung der Bedrohung kann so unterbunden werden.

Risikobewusstsein schärfen

Sicherheit in Industrieanlagen oder Software-Sicherheit sind nicht als Produkt zu verstehen oder zu erhalten. Sicherheit ist vielmehr ein Prozess, der von den Beteiligten kontinuierlich gelebt werden muss. Siemens setzt neben umfassenden Sicherheitseinrichtungen für Maschinen und Anlagen auch darauf, das Risikobewusstsein von Mitarbeitern zu schärfen. Für Tino Hildebrand, Leiter Marketing & Promotion Sematic HMI der Siemens Division Industry Automation, gehören dazu die Ausbildung der Mitarbeiter und die Schaffung eines tieferen Verständnisses für die Verantwortungen: „Die Erstellung eines IT-Sicherheitskonzepts mit Verhaltensregeln und technischen Maßnahmen ist für jeden Kunden individuell machbar und sinnvoll. Ein Aspekt eines solchen Sicherheitskonzepts könnte die laufende Suche von Schwachstellen und deren Beseitigung sein. Dadurch wird die IT-Sicherheit zu einem festen Bestandteil des sicheren Betriebs einer Anlage – und die bösen Überraschungen auf ein Minimum reduziert.“

webcode www.konstruktion.de/12689

Innominate bietet seine mGuard Security Appliances für den industriellen und produktionsnahen Einsatz in verschiedensten Bauformen an, von integrierbaren und portablen Feldgeräten bis zu Firewall/VPN-Gateways im 19-Zoll-Format.

