

# Keine Chance für Stuxnet & Co!

## Wie sich Industrieanlagen gegen Cyber-Attacken wirksam schützen lassen

■ **Spätestens seit der weltweiten Aufmerksamkeit für den Stuxnet Wurm, der zehntausende von Engineering- und Visualisierungs-PCs befallen und die Steuerungen industrieller Anlagen sabotiert hat, sind die Gefahren durch Schadsoftware und mangelnde IT-Sicherheit in Automatisierungsnetzwerken nicht mehr zu übersehen. Schutz bieten Lösungen für die industrielle Netzwerksicherheit, die unautorisierte Manipulationen und Netzzugriffe von außen verhindern.**

Der Computerwurm Stuxnet hat nach seiner Entdeckung im Juni 2010 weltweit Aufsehen erregt. Diese „Cyber-Attacke“ gilt als der erste gezielte Root Kit-Angriff auf industrielle Anlagen, der öffentlich bekannt wurde. Zehntausende PCs infizierten sich und gaben den schädlichen Programmcode unentdeckt weiter. Die Absicht der Urheber des Computerwurms war es, Windows-basierte Automatisie-

rungssoftware zu manipulieren, um darüber Schadcode in die Steuerungen spezieller industrieller Anlagen einzuschleusen.

Die eigentliche Gefahr geht heute längst nicht mehr von Stuxnet selbst aus. Die Wirkungsweise dieses Wurms wurde hinreichend analysiert und die entsprechenden Signaturen zur Erkennung sind den Herstellern von Antivirensoftware bekannt. Spezialisten für IT-Security sehen aber eine große Gefahr durch Mutationen von Nachahmern.

Während Stuxnet gezielt nur einen spezifischen Typ einer speicherprogrammierbaren Steuerung (SPS) eines Herstellers mit einer sehr genau definierten Konfiguration sabotieren sollte, könnten Mutationen auch Komponenten anderer Hersteller erfassen. Die daraus resultierenden Gefährdungen für das Bedienpersonal und die betroffenen Anlagen könnten erheblich sein.

**Stuxnet-Mutationen sind die eigentliche Gefahr**

Eine Lehre aus der Stuxnet-Attacke ist, dass konventionelle Virens Scanner gegen Angriffe von solcher Qualität routinemäßig keinen Schutz bieten. Die Analysen des Schadcodes haben rückblickend ergeben, dass der Wurm vor seiner Entdeckung bereits mindestens 12 Monate lang unbemerkt in Umlauf war. Während dieser Zeit wurde er von Antivirenprogrammen nicht erkannt, weil es keine Signaturen für ihn gab, die ihn hätten entdecken können.

Um geeignete Schutzmaßnahmen gegen Angriffe des Stuxnet-Wurms und möglicher Mutationen zu entwickeln, ist es notwendig, seine Wirkungsweise zu verstehen. Der Wurm entfaltet seine Schädwirkung in vier Stufen auf verschiedenen Ebenen:

**1. Infektion von Windows-PCs:** Der Wurm nutzt einen Mix von aggressiven Mechanismen, um sich sowohl über Netzwerk-

verbindungen als auch über USB-Memory-Sticks auf Windows-PCs zu verbreiten und diese zu infizieren.

**2. Missbrauch und Manipulation von Automatisierungs-Software:** Sofern Stuxnet auf dem infizierten PC installierte Komponenten des Visualisierungssystems WinCC oder der Engineering-Software Step 7 von Siemens vorfindet, manipuliert er vorgefundene WinCC-Datenbanken und STEP-7-Projekte, um seine weitere Verbreitung und sein Fortbestehen auf dem PC zu sichern. In den Projekten erfasste Steuerungen werden als potenzielle Ziele für Stufe 3 ausgespäht.

**3. Einschleusen von Schadcode in Steuerungen:** Über eine manipulierte Systembibliothek kann Stuxnet beliebigen Schadcode in die projektierten Steuerungen einschleusen, diese Manipulationen vor dem Projektierer verbergen und vor einem erneuten Überschreiben schützen.



*Nach der Stuxnet-Attacke müssen sich auch Betreiber von Industrieanlagen Gedanken über IT-Sicherheit machen*

**4. Kommunikation mit Servern im Internet:** Der Wurm versucht, von infizierten PCs aus Kontakt zu mehreren Servern im Internet aufzunehmen. Kommt der Kontakt zustande, können sowohl ausgespähte Informationen abgeliefert als auch neue Instruktionen und Updates für den Wurm selbst und seine

„digitalen Sprengköpfe“ empfangen und ausgeführt werden. Doch wehrlos stehen die Betreiber von industriellen Anlagen den Cyber-Attacken nicht gegenüber. Innominate, ein Unternehmen der Phoenix Contact-Gruppe, hat mit mGuard eine Technologie mit einer Reihe von Präventions- und Diagnosefunk-

tionen entwickelt, mit denen unautorisierte Netzzugriffe und Veränderungen in Rechnersystemen zuverlässig und zeitnah erkannt werden. Dies erhöht die Sicherheit gegen Stuxnet-artige Angriffe und reduziert die damit verbundenen Risiken.

# Industrieanlagen gegen Cyber-Attacken schützen

## Schadsoftware sofort erkennen: mGuard Integrity Monitoring

Mit dem mGuard CIFS Integrity Monitoring Verfahren (CIFS = Common Internet File System) lassen sich Dateisysteme auf unerwartete Veränderungen von ausführbarem Code konfigurierbar überwachen. In einem vom Institut für industrielle Informationstechnik (inIT) der Hochschule Ostwestfalen-Lippe durchgeführten Test konnte verifiziert werden, dass das mGuard CIFS Integrity Monitoring-Verfahren Infektionen mit Stuxnet lange vor allen Antiviren-Programmen bereits am ersten Tag als unerwartete

Manipulation erkannt und Anwender davor gewarnt hätte.

## Verbreitung eindämmen, Kontakte zu Servern unterbinden: Firewall mGuard

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 mit Firewalls mGuard lassen sich nicht benötigte und unerwünschte Verbindungen zuverlässig blockieren und die Ausbreitung von Schadsoftware eindämmen.

## Authentisierte und autorisierte Projektierung: User Firewall mGuard

Viele der heute eingesetzten Steuerungen beinhalten kaum Schutzfunktionen zur Authentisierung und Autorisierung ihrer Projektierung. Entgegen einer weit verbreiteten Annahme wird zur Programmierung und Manipulation vieler Steuerungen auch keine spezielle oder vom Hersteller autorisierte Projektierungs-Software benötigt.

Die User Firewall mGuard ist ein wirkungsvolles Mittel, um Manipulationen an Steuerungen durch unbefugte Projektierungszugriffe zu verhindern. Der Zugriff auf den Projektierungspport muss dabei zunächst durch Authentisierung eines berechtigten Benutzers an der Firewall freigeschaltet werden.

Die mGuard-basierten Netzwerkkomponenten sind im Produktportfolio von Phoenix Contact im Rahmen der Produktlinie FL Mguard in einer Vielzahl von Bauformen und Ausstattungsvarianten erhältlich.

Somit stehen bereits heute wirkungsvolle Technologien und Produkte zur Verfügung, die Angriffe von Stuxnet & Co zuverlässig abwehren.

