

Post-Stuxnet Industrial Security

Industrielle Schadsoftware am Tage Null erkennen und Risiken eindämmen mit der Innominate mGuard® Technologie

Einleitung

Der Stuxnet Wurm hat nach seiner Entdeckung im Juni 2010 weltweit Aufsehen erregt. Er ist der erste öffentlich bekannte und gezielte Root-Kit Angriff auf industrielle Anlagen. Er hat zehntausende von PCs infiziert, Windows-basierte Automatisierungssoftware für seine Zwecke missbraucht und manipuliert, um darüber schlussendlich Schadcode in die Steuerungen spezifischer, real existierender industrieller Anlagen einzuschleusen. Spätestens seit Stuxnet sind die von Experten seit langem beschworenen Gefahren durch Schadsoftware und mangelnde IT-Sicherheit in Automatisierungsnetzwerken daher nicht mehr zu übersehen. Die eigentliche Gefahr geht dabei längst nicht mehr von Stuxnet selbst aus, sondern von für sehr wahrscheinlich gehaltenen Mutationen durch Nachahmer, die mit den gleichen Basistechniken beliebigen anderen Schadcode in Umlauf bringen könnten. 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.

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 12 Monate lange unbemerkt in Umlauf war und während dieser Zeit von Antivirus-Programmen mangels bekannter Signaturen nicht erkannt wurde.

Schadwirkung in vier Stufen

Für die Konzeption von Schutzmaßnahmen gegen Stuxnet-artige 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 (durch sog. Zero-Day Exploits), 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 JMicon signiert und beinhalten 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- und/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 potentielle Ziele für Stufe 3 auszuspähen.

Ferner benennt Stuxnet die für die Kommunikation zwischen SIMATIC Manager und projektierten S7 Steuerungen zuständige Dynamic Link Library s7otbxdx.dll im Verzeichnis %SystemRoot%\system32\ um in s7otbxdx.dll 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 sog. 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 paketierte zur Verfügung gestellt und dann – entgegen oft geäußerter 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 gar Internet-Verbindung verfügen.

Nutzen der Innominate mGuard Technologie

Die von Innominate entwickelte mGuard Technologie - verfügbar in mGuard-basierten industriellen Network Security Appliances verschiedener Hersteller und auch als embedded Technologie für OEMs – umfasst eine Reihe von präventiven und diagnostischen Funktionen, welche die Sicherheit gegen Stuxnet-artige Angriffe erhöhen und damit verbundene Risiken reduzieren können. Während sich Infektionen mit Schadsoftware aufgrund der Vielfalt der Verbreitungswege dadurch nicht zu 100% aktiv verhindern lassen, geht es dabei insbesondere auch darum, solche Infektionen schnell und zuverlässig zu erkennen und nicht wie im Falle Stuxnet lange Zeit unbemerkt auf Anlagen einwirken zu lassen.

Schadsoftware am Tage Null erkennen: mGuard Integrity Monitoring

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 Bedeutung für den Schutz industrieller Systeme. So dient das **mGuard CIFS Integrity Monitoring** Verfahren (CIFS = Common Internet File System, von Windows u.a. Systemen genutztes Filesharing-Protokoll) 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 ggf. vorgenommenen Manipulationen an der entscheidenden SIMATIC Manager DLL entdeckt.

Verbreitung eindämmen, C&C-Kontakte unterbinden: mGuard Firewall

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 damit in erheblichem Maße eindämmen. Im Falle Stuxnet konnten gesunde Systeme sowohl über bestimmte eingehende als auch 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 Potential für Spionage und Dynamisierung der Bedrohung kann so unterbunden werden.

Authentisierte und autorisierte Projektierung: mGuard User Firewall

Die meisten heute auf dem Markt befindlichen SPSen beinhalten kaum Schutzfunktionen zur Authentisierung und Autorisierung ihrer Projektierung. Entgegen weit verbreiteter Annahme benötigt man zur Programmierung und sonstigen Manipulation der Steuerungen auch keine spezielle oder vom Hersteller offiziell autorisierte Projektierungs-Software. Wer Netzwerkzugriff auf den Projektierungs-Port hat und das richtige Protokoll spricht, ist Herr über die Steuerung. Schutzmaßnahmen erschöpfen sich in der Regel in einer Access Control List (ACL) zur Begrenzung des Projektierungszugriffs auf eine Reihe von IP-Adressen. Eine weitere Überprüfung der Benutzer und Programme, die von diesen IP-Adressen aus zugreifen, und ihrer Berechtigung dazu findet nicht statt.

Perfiderweise nutzt Stuxnet für seinen Angriff auf die Steuerungen aber genau jene Engineering und Visualisierungs-PCs, die zur legitimen Kommunikation mit den Steuerungen vorgesehen sind. Die ACLs laufen hier ebenso wie statische Firewall-Regelwerke ins Leere, da die Zugriffe der Schadsoftware von vermeintlich berechtigten Knoten ausgehen. Hier stellt die **mGuard User Firewall** ein wirkungsvolles Mittel dar, um **Manipulationen an Steuerungen durch unbefugte Projektierungs-Zugriffe zu verhindern**. Der Zugriff auf den Projektierungs-Port muss dabei zunächst durch Authentisierung eines berechtigten Benutzers an der Firewall freigeschaltet werden, die Schadsoftware allein vermag diesen nicht zu erlangen.

Bedenkt man die von Stuxnet vorgenommene Manipulation an der Projektierungs-Software, erkennt man, wie wichtig die **Kombination der hier genannten Techniken** ist: So sollte ein berechtigter Anwender den Zugriff durch die mGuard User Firewall natürlich erst frei schalten, nachdem er sich der Integrität seiner Projektierungs-Umgebung vergewissert hat, wobei ihm das mGuard Integrity Monitoring behilflich ist. Während noch fortschrittlichere Security Technologien wie Application Whitelisting oder Intrusion Prevention eher kommenden Generationen von Automatisierungsgeräten vorbehalten sein werden, eignen sich alle hier vorgestellten Methoden auch zur **Nachrüstung in Bestandsanlagen**.

Innominate Security Technologies AG, Berlin (www.innominate.com)

Stand: 22. November 2010

Quellen

Symantec W32.Stuxnet Dossier, Version 1.3 (November 2010), verfügbar zum Download unter <http://www.symantec.com/business/theme.jsp?themeid=stuxnet>

Langner Communications GmbH, Hamburg, Blog zu Stuxnet verfügbar unter http://www.langner.com/english/?page_id=45