

STUXNET I TORSTEN RÖSSEL, INNOMINATE

Stuxnet ist Geschichte – die Gefahr künftiger Mutationen nicht

„Absolute IT-Sicherheit gibt es nicht, es geht immer um Risiko-Reduktion zu einem angemessenen Kosten-Nutzen Verhältnis.“

Torsten Rössel, Innominate.



Bild: Innominate

SABINE SPINNAKKE, PRODUKTION NR. 6, 2011

Die Auseinandersetzung mit Security-Bedürfnissen industrieller Unternehmen ist für Torsten Rössel, Director Business Development, Innominate, Alltagsgeschäft. Seit Stuxnet stellt sich die Frage ist wirkungsvoller Schutz überhaupt möglich?

Ist Stuxnet noch gefährlich?

Die eigentliche Gefahr liegt inzwischen weniger in Stuxnet selbst, als vielmehr darin, dass sich jeder den Wurm beschaffen und ihn verändern kann. Es reicht also ein wesentlich geringerer Einsatz an Geld und Technologie, um eine vergleichbare Schadsoftware in Umlauf zu bringen.

Mit welchem Ziel?

Denkbar wäre, dass ähnliche Computer-Würmer sich massenhaft verbreiten und insbesondere kleinere, ungeschützte Anlagen, wie beispielsweise Aufzüge in Gebäuden oder Gepäckbänder in Flughäfen, lahmlegen könnten.

Wie ist die Stimmung unter Ihren Kunden?

In der Breite überwiegt die Meinung, der Wurm sei so spezifisch, dass er in der eigenen Anlage keinen Schaden anrichten könne.

Teilen Sie diese Ansicht?

Das ist kurzfristig zutreffend, Stuxnet selbst ist Geschichte. Sich deswegen in Sicherheit zu wiegen, wäre allerdings fatal: Es besteht jetzt die Gefahr eines Proliferationseffekts durch Nachahmer, die wesentlich weniger filigran vorgehen und damit in der Breite Störungen verursachen könnten.

Gibt es wirkungsvolle Schutzmaßnahmen?

Eine organisatorische Maßnahme wäre, die Benutzung von USB-Wechselmedien nicht zuzulassen. Es gab dazu durchaus ernste gemeinte Empfehlungen aus der Security-Szene, nicht benötigte USB-Schnittstellen an PCs mit Epoxidharz zu verschließen. Eine weniger drastische Option wäre, solche USB-Ports softwaretechnisch stillzulegen.

Sind Virens Scanner allein nicht ausreichend?

Der klassische Einsatz von Virens Scannern war im Falle von Stuxnet lange Zeit völlig wirkungslos, da der Wurm vor seiner Entdeckung schon ca. 12 Monate lang unerkannt in Umlauf war und während dieser Zeit folglich keine Virenmuster für ihn existierten.

Wie umgehen Viren die klassischen Schutzprogramme?

Stuxnet hat gleich mehrere Zero Day Exploits (das sind Programmteile zur Ausnutzung bislang nicht bekannter Schwachstellen) für seine Verbreitung genutzt, was Experten extrem ungewöhnlich fanden, da dem Wissen über solche Verwundbarkeiten ein sehr hoher Marktwert nachgesagt wird – man spricht hier von Beträgen bis zu einer halben Million Dollar pro Schwachstelle.

Wie kann man seine Anlage besser schützen?

Die nächste technologische Stufe wären Verfahren, welche die Integrität der von Rechnern ausgeführten Software sicher stellen oder zumindest bemerken, wenn der PC manipuliert wurde. Das sind sogenannte Whitelisting-Verfahren.

Wie funktionieren Whitelisting-Verfahren?

Durch solche Verfahren erweiterte Betriebssysteme lassen die Ausführung von Programmcode nur zu, wenn dieser vorher registriert und signiert worden ist. Derartige Verfahren verhindern also, dass manipulierter Code auf einem Rechner zur Ausführung kommen kann.

Wie sicher ist dies?

Eine Restlücke besteht immer noch, wenn es dem Wurm gelingen würde, das Betriebssystem im laufenden Betrieb im Speicher selber zu manipulieren. Die PCs, die von Stuxnet befallen wurden, waren entweder Engineering-PCs mit denen Steuerungen projektiert wurden oder es waren Visualisierungs-PCs. Was man anstreben sollte ist, die Zugänge zur Programmierung von Steuerungen sehr viel stärker abzuschotten. Die Programmier-Ports sind meist viel zu schwach geschützt, auf den SPSen selbst gibt es in der Regel weder Authentifizierungs- noch Autorisierungs-Funktionen, das hat Stuxnet besonders heimtückisch ausgenutzt. Und die andere Baustelle wäre, den Netzwerkzugriff auf die Programmier-Ports der Steuerungen durch eine vorgeschaltete Firewall zu sichern.

VITA

Der Diplom Mathematiker Torsten Rössel verantwortet bei Innominate (seit 2005) als Director Business Development die Definition neuer Produkte sowie die Bereiche Technical Account Management und Professional Services. Er arbeitet seit über 17 Jahren im Gebiet Internet-Technologien. Seine Karriere startete er in Forschung und Entwicklung der Siemens AG.

Stuxnet: Chronologie eines Bedrohungs-Szenariums

► **Juni 2010:** Der Computerwurm Stuxnet wird entdeckt.
 ► **19. Juli 2010:** Siemens berichtet über die Infektion seiner SCADA-Anlagen. Insgesamt seien weltweit 22 Anlagen infiziert. Schäden hätten jedoch nicht festgestellt werden können.

► **Zwischen August und Dezember 2010** veröffentlicht Microsoft mehrere Patches gegen die verschiedenen Sicherheitslücken.
 ► **September 2010:** Der Iran bestätigt Angriffe durch Stuxnet. Ob der Virus Schaden anrichten konnte oder nicht, wird widersprüchlich kommu-

niziert. Die Nachrichtenagentur Xinhua berichtet von 6 Mio befallenen Computern und fast 1 000 betroffenen Anlagensteuerungen in China. Zur Herkunft des Virus gibt es unterschiedliche Theorien, nachgewiesen werden konnte bislang keine: IT-Sicherheitsspezialisten gehen davon aus,

dass Stuxnet gezielt zur Sabotage iranischer Atomanlagen programmiert wurde. Aufgrund des großen Programmieraufwandes wird von Fachleuten angenommen, dass der Wurm vermutlich von einer staatlichen Organisation stammt. Yossi Melman, israelischer Journalist, hält Israel für den wahr-

scheinlichen Urheber, da der Vertrag des Direktors des israelischen Auslandsgeheimdienstes, Meir Dagan, überraschend verlängert wurde. Zudem hätte Israel den geschätzten Zeitpunkt, bis zu welchem Iran eine Atombombe besitzen soll, überraschend auf das Jahr 2014 nach hinten verschoben.