ONLINE FOCUS

Druck

http://www.focus.de/digital/computer/chip-exklusiv/tid-23248/cyberattacke-industrieanlagen-schuetzen-ist-sehr-aufwendig_aid_653861.html

Cyberattacke

Wie ein Cyber-Wurm die deutsche Industrie bedroht

Donnerstag, 11.08.2011, 11:18 · von Dominik Hoferer

Profi-Hacker warnen: Der Wurm Stuxnet funktioniert wie ein Generalschlüssel für die Anlagen deutscher Unternehmen. Die Industrie unterschätzt das Risiko.

Eben dröhnte noch Krach durch die Produktionsanlage: Die Pressenstampften, Roboter wuchteten Metallplatten durch die Luft. Doch nun herrscht Stille in den Hallen eines Automobilzulieferers. Die Techniker überprüfen hektisch die Wände mit den Steckverbindungen und checken auf dem faktenüberladenen Monitor, ob die Überwachungssoftware einen Grund für den Stopp liefert. Plötzlich nimmt die Maschinenstraße wieder ihren Dienst auf. Ein Szenario, das sich in Industrieanlagen und Lebensmittelfabriken nicht selten ereignet, wie Ralph Langner schildert. Der Experte für Anlagensicherheit berät Firmen aus der Industrie und sichert Produktionsabläufe ab.

Teile von Stuxnet vielleicht bald im Internet

Laut Langner geht im Normalfall niemand von einem Cyberangriff aus, wenn nichts mehr geht. Denn moderne Industrieanlagen sind komplex – und Cyberstörungen schwer zu erkennen. Umso mehr, als sie sich oft auf die gesamte Anlage auswirken. Den Fehler zu finden, ist wie die sprichwörtliche Suche nach der Nadel im Heuhaufen. Böswillige Manipulation vermutet keiner.

Doch seit der Wurm Stuxnet Ende letzten Jahres die iranische Urananreicherungsanlage in Natanz angegriffen hat, ist die Gefahr auch für Industrieanlagen gestiegen, die nichts mit radioaktivem Material zu tun haben. „Stuxnet dient gewissermaßen als Blaupause, wie man Sicherheitsmaßnahmen in der Industrie ausschalten kann“, erklärt Ralph Langner. Der Fachmann für Sicherheit in Industrieanlagen hat sich intensiv mit Stuxnet beschäftigt und seine Funktionsweise analysiert. Seine Prognose: „Die Gefahr, dass Teile von Stuxnet in absehbarer Zeit in einem Tool-Baukasten landen, der frei im Internet zur Verfügung steht, ist hoch.“ Der Experte geht davon aus, dass Hacker dann eine Software-Waffe bauen könnten – und Industrieanlagen angreifen.

*Mit freundlicher Genehmigung von **CHIP**. Dieser Artikel stammt aus der Ausgabe 9/2011 des Computermagazins.*

Deutschland besonders gefährdet

„Würmer können über Dienstleister in die Firmen gelangen“ – Ralph Langner, Experte für Anlagensicherheit Privat

Deutschland ist mit seiner Industriedichte und dem hohen Grad an Automatisierung besonders gefährdet: Es könnte ein beträchtlicher volkswirtschaftlicher Schaden entstehen, wenn Hacker Automobilhersteller über längere Zeit lahmlegen. Zudem könnte ein Angriff auf die Pharmaindustrie – zumindest theoretisch – zu einem Engpass an Medikamenten führen. Darüber hinaus sind flächendeckende und lang anhaltende Stromausfälle denkbare Szenarien. Aber wie soll ein Virus, der es nur auf die Urananreicherungsanlagen im Iran abgesehen hat, etwa in der deutschen

Arzneimittelindustrie Schaden anrichten können? Dazu muss man die Architektur des äußerst komplexen Schädlings verstehen: Würde Stuxnet den Home-PC eines normalen Users befallen, wäre der Schaden gleich null. Kein Phishing, kein Kreditkartenklau, kein Spamversand. Denn dort, wo Stuxnet landet, sucht er nach einer SPS. Das sind Speicherprogrammierbare Steuerungen, die in allen Anlagen dieser Welt verbaut sind. Egal ob in AKW, Chemiewerken oder Stromanlagen – überall steuern diese kleinen Kästchen Motoren und Aufzüge oder regeln die Kühlung von Flüssigkeiten. Aktiv wurde Stuxnet in der Urananreicherungsanlage im Iran.

Laut einem Bericht der New York Times stecken die Geheimdienste der USA und Israels hinter diesem Angriff. Virusanalysten bei Kaspersky sprechen davon, dass weltweit nur zehn Personen über entsprechende Möglichkeiten verfügen. Für die gezielte Attacke benötigt man Geheimdienstinformationen, an die keine private Hackerbande kommt. Der Cyberangriff sollte den Iran daran hindern, eine mutmaßliche Atombombe zu entwickeln. Das konkrete Ziel von Stuxnet war es, Uranzentrifugen zu manipulieren und zu zerstören. Würde der Schädling etwa in einer deutschen Lebensmittelfabrik aufschlagen, entstünde also kein Schaden. Eine beruhigende Nachricht, wenn man bedenkt, dass laut einer McAfee-Studie vom April 2011 knapp 60 Prozent der deutschen Strom, Gas- und Wasserversorger den Wurm auf ihren Systemen entdeckt hatten. Doch gerade diese Zahl schockiert und demonstriert, wie weit sich ein Wurm verbreiten kann. Dass er in absehbarer Zeit aber auch hier Schaden anrichtet, ist nicht unwahrscheinlich, wie der Aufbau der Malware zeigt.

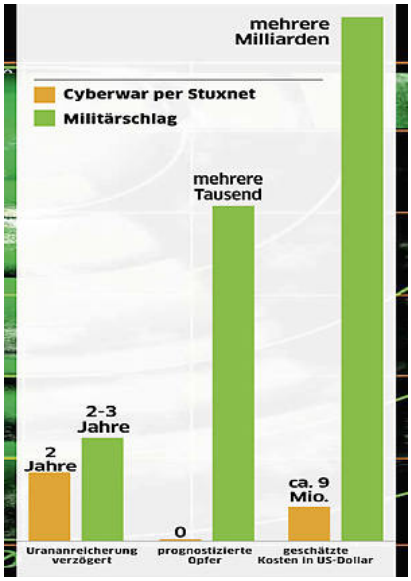
Um tief in das System vorzudringen, mussten sich die Hacker erst einmal Zutritt in das relativ gut gesicherte Netz verschaffen. Dazu entwickelten sie Stuxnet modular (s. Grafik). Ein Teil des Virus knackte Windows-PCs, die als Einfallstor dienten. Sie verbreiteten den Wurm. Eine Hürde bestand darin, dass die Anlage im Iran nicht mit dem World Wide Web verbunden und nur indirekt angreifbar war. Fachleute vermuten, dass ein Mitarbeiter Stuxnet über ein verseuchtes Notebook unbeabsichtigt installiert hat. Ab diesem Zeitpunkt wurde der nächste Teil aktiv, der sich um den Befall der speicherprogrammierbaren Steuerungen kümmert. Sie verbinden digitale Steuerung mit physischer Kraft, sie treiben Pressen, Bohrer und Kühlsysteme an – durch sie werden Cyberangriffe gefährlich. Dieser Teil von Stuxnet ist anlagenspezifisch, nur das Werk im iranischen Natanz ist davon betroffen.

Aber das Modul von Stuxnet, das die Manipulation der Zentrifugen überhaupt möglich macht, nutzt Schwachstellen aus, die es in jeder SPS gibt. Der Sicherheitsforscher Dillon Beresford wollte auf einer Sicherheitskonferenz Mitte Mai Schwachstellen präsentieren, ruderte aber nach Absprache mit SPS-Hersteller Siemens zurück: Siemens hätte es nicht mehr bis zum Vortrag geschafft, die Lücken zu schließen. Doch das ist kein Siemens-Problem, bei allen Firmen gibt es diese Lücken, die das Sicherheitsunternehmen ICS-Cert als „weitreichender und schwerwiegender als alles, womit sie bisher zu tun hatten“ bezeichnete.

Vortrag von Ralph Langner über Stuxnet (Englisch)

Mit Stuxnet sind Industrieanlagen, Strom- und Wasserversorgungssysteme, Zug- und Flugsicherung zu potenziellen Zielen geworden, egal ob Staaten, Terroristengruppen oder Hobbycracker einen Angriff planen. Hochprofessionelle Hacker mit geheimen Infos haben einen Wurm geschaffen, den Nachahmer mit wenig Knowhow ohne großen Aufwand portieren und damit fast jedes Unternehmen angreifen können. Während die Stuxnet-Entwickler sehr viel Arbeit investiert haben, um den Schädling so zu bauen, dass er nur im Iran zuschlägt, ist es deutlich einfacher, einen flächendeckenden Zufallsangriff zu starten. Dafür benötigt man keine tiefen Kenntnisse über das Ziel. Denn laut Langner sind Industrieanlagen so komplex, dass kleinste Änderungen in der Systemlandschaft zu Störfällen führen. Den Schädling könnte man so programmieren, dass sich eine SPS „verschluckt“. Dass dadurch die Anlage zum Erliegen kommt, ist nicht ungewöhnlich. Gewiefte Hacker oder Konkurrenten können auch gezielt die Qualität von Produkten verschlechtern, um die Firma auf diese Weise zu erpressen.

Industrieanlagen schützen ist sehr aufwendig



Cyberwahr – günstig und effektiv CHIP
Digitale Angriffe sind effektiv, und dabei kostengünstiger und unblutiger als ein Militärschlag. Israelische Militärexperten haben geschätzt, wie teuer ein Angriff auf den Iran mit Panzern und Raketen und möglichem Gegenangriff im Vergleich zum Malware-Einsatz wäre. Das Ergebnis zeigt: Stuxnet könnte der Beginn eines Cyberwars gewesen sein, in dem sich Staaten digital bekriegen.

Im Gegensatz zur IT-Welt, in der Sicherheitsupdates, Virenschutz und Firewall Standard sind, gibt es in der Anlagenwelt keinen derartigen Schutz. Die Achillesferse ist das schwache Sicherheitskonzept.

Beim Entwurf von Maschinenstraßen musste man sich noch wenig Gedanken über die Sicherheit der Daten machen, es gab schließlich keine Bedrohung. Hinzu kommt: Man kann Echtzeitsysteme, wie sie in diesen Anlagen vorkommen, nicht mit einem herkömmlichen Virenprogramm schützen. Jahrelang war mangelnde Sicherheit kein Thema – erst durch die Digitalisierung und die Vernetzung entstanden Probleme.

Doch selbst geschlossene Systeme ohne Internetzugang können kompromittiert werden. Peter Pfisterer, der für die TÜV SÜD AG Industrieanlagen testet, sieht einen Großteil der Unternehmen dennoch gut aufgestellt: „Zwar sind sich manche kleine Unternehmen keiner Gefahr bewusst, aber große Betreiber haben hohe Anstrengungen unternommen, Anwendungen abzusichern.“ Anlagenexperte Ralph Langner sieht das anders: „Über gezielt verseuchte Notebooks von externen Dienstleistern mit Wartungsaufgaben können Würmer in die Firmen gelangen.“

Die Konsequenz für den Fachmann ist, dass es schnellstmöglich Vorschriften wie in der Arbeitssicherheit geben muss. Denn ein behördlich vorgeschriebener Grundschutz existiert für die Automatisierung nicht. So etwas ist laut Langner schwierig zu erstellen, in den nächsten Jahren werde es vermutlich kaum große Fortschritte geben. Auch der TÜV mahnt: „Sicherheit ist für die Administratoren eine große Herausforderung. Techniker müssen sauber arbeiten.“ Doch das ist bei komplexen Anlagen nicht einfach, wie das Beispiel vom Beginn zeigt: Die Angestellten haben die Ursache gefunden – ein serielles Kabel, das an einen PC angeschlossen, aber falsch verdrahtet war. Jahrelang ignorierte das System den Fehler. Erst als ein schnellerer Computer seinen Vorgänger ersetzte, verschluckte sich die Steuerung, die Anlage kam zum Stillstand. Also keine Cyberattacke auf die ungeschützten Steuerungseinheiten in dem System – zumindest diesmal.

Fotocredits:

Privat, CHIP

Drucken