IT-Security in der Produktion: Auf der Suche nach Schutz für vernetzte Industrial Control Systems

Industrie 4.0? Aber sicher!

Industrie 4.0 treibt die Vernetzung von Maschinen und Anlagen via Internet voran, und zwar unternehmensübergreifend. Dies eröffnet Wirtschaftsspionen und Cyber-Kriminellen neue Chancen. Wie können sich Unternehmen am besten wappnen?

Die Gefahren für die Produktions-IT nehmen mit der Vernetzung der Systeme zu. Die gängigen Mittel der IT reichen nach Meinung von Experten nicht für ICS-Systeme aus Bild: Innominate

Stuxnet ist immer noch in aller Munde: Mit dem Computerwurm wurden 2010 Atom- und Industrieanlagen zur Urananreicherung im Iran angegriffen – vermutlich von den USA und Israel ausgehend. Das Schadprogramm war speziell für das Scada-System von Siemens, Simatic S7, entwickelt worden und griff außerdem in die Steuerung von Frequenzumrichtern an.

Stuxnet ist sicherlich das prominenteste Beispiel für Angriffe auf Automatisierungs-, Prozesssteuerungs- und -leitsysteme, die unter dem Begriff Industrial Control Systems (ICS) zusammengefasst werden. Daneben gibt es sehr viele andere Möglichkeiten, Maschinen und Anlagen von außen zu attackieren, wie die Top-10-Liste der Bedrohung des BSI (siehe Empfehlungen des BSI) verdeutlicht. Und die Zahl wird in den nächsten Jahren nach Meinung von Experten deutlich steigen durch die Entwicklung hin zu Industrie 4.0.

„Früher waren Produktionssysteme geschlossene Systeme. Im Zeitalter von Industrie 4.0 ist die Vernetzung ein zentrales Element“, sagt Aurelius Wosylus, Director Business Development Embedded Markets beim IT-Security-Anbieter Safenet, Gemering. „Moderne Architekturen öffnen sich immer mehr und werden dadurch auch extern angreifbar. Einzelne Komponenten kommunizieren miteinander ohne ständig überwacht zu werden. Diese offenen Strukturen erschweren das Erkennen von manipulierten Nachrichten. Generell lässt sich sagen: Je komplexer und offener ein System ist, desto vielfältiger sind die potenziellen Angriffsflächen.“

Dem stimmt Jörg Lützenkirchen zu, Sales Engineer bei Norman Data Defense, Düsseldorf: „Industrie 4.0 heißt nichts anderes als Vernetzung. Und Vernetzung verschafft Schadcode jeder Art optimale Verbreitungsmöglichkeiten. Zudem kann die Störung einer einzigen Komponente durch jeden noch so simplen Schadcode eine Kettenreaktion mit unvorhersehbaren Auswirkungen in Gang setzen.“

Hält fehlerfreie Embedded Software für entscheidend: Professor Hartmut Pohl, geschäftsführender Gesellschaft Softscheck Bild: Softscheck

Empfiehlt Partnern, auf Authentizität, Integrität und Vertraulichkeit zu achten: Torsten Rössel, Chief Marketing Officer Innominate Bild: Innominate

Doch für die meisten produzierenden Unternehmen in Deutschland sind Stuxnet und Co. weit weg. Sie wägen sich und ihre Produktion in Sicherheit, da sie überzeugt sind, dass Hersteller wie Siemens aus dem Fall ihre Lehren gezogen haben. Doch dies ist ein Trugschluss. Erst im Januar hat das für die Sicherheit von industriellen Steuerungssystemen zuständige Industrial Control Systems Cyber Emergency Response Team (ICS-Cert) aus den USA erneut vor einem Tool gewarnt, mit dem das Passwort von Simatic S7 geknackt werden kann. Zudem könne es sein, dass der Code auch für Anlagen anderer Hersteller als Siemens angepasst werde. Und im Oktober 2012 hatte das ICS-Cert eine Warnung vor Tools herausgegeben, mit denen Steuerungssysteme von Anbietern wie GE, Rockwell Automation, Schneider Electric und Koyo geknackt werden können. Auch für die Software Codesys des deutschen Herstellers 3S Smart Software Solutions sind bereits solche Werkzeuge aufgetaucht, mit denen auch unerfahrene Angreifer Attacken auf Maschinen und Geräte starten können.

Viele Unternehmen ignorieren solche potenziellen Gefahren aber auch deswegen, weil sie davon ausgehen, dass ihre Systeme (noch) gar nicht an das Internet angeschlossen sind. Doch weit gefehlt: Als größtes offenes Scheunentor, durch das potenzielle Angreifer in die Produktions-IT gelangen können, macht das Bundesamt für Sicherheit in der Informationstechnik (BSI) aktuell die Fernwartungszugänge von Maschinen und Anlagen aus. Diese könnten direkt angegriffen werden, etwa mittels so genannter Brute Force Attacken zum Knacken von Passwörtern. ICS-Anbieter machen es ihnen leicht, denn häufig existieren zum Beispiel Default-Zugänge mit Standardpasswörtern oder sogar fest kodierten Passwörtern.

Ein zweites mögliches Angriffsszenario sind laut BSI indirekte Angriffe über die IT-Systeme des Dienstleisters, für den der externe Zugang geschaffen wurde. Möglich sind dabei

Die Top-10-Bedrohungen

Empfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnologie (BSI) hat die folgenden Top-10-Bedrohungen für Automatisierungs-, Prozesssteuerungs- und -leitsysteme (Industrial Control System, kurz ICS) identifiziert:

- Unberechtigte Nutzung von Fernwartungszugängen
- Online-Angriffe über Office- und Enterprise-Netze
- Angriffe auf eingesetzte Standardkomponenten im ICS-Netz
- (D)DoS-Angriffe
- Menschliches Fehlverhalten und Sabotage
- Einschleusen von Schadcode über Wechseldatenträger und externe Hardware
- Lesen und Schreiben von Nachrichten im ICS-Netz
- Unberechtigter Zugriff auf Ressourcen
- Angriffe auf Netzwerkkomponenten
- Technisches Fehlverhalten und höhere Gewalt

Jörg Lützenkirchen, Norman Data Defense: Security in der Produktion ist eine Frage der Prozesse, und dafür fehlen Standards Bild: Norman

Oliver Winzenried, Vorstand Wibu-Systems: Überprüfbare Sicherheit ist im Industrie-4.0-Zeitalter gefragt Bild: Wibu-Systems

Aurelius Wosylus, Safenet: Durch autonome entkoppelte Subsysteme lassen sich eventuelle Angriffe schnell lokal isolieren Bild: Safenet

Trojaner, die den Zugang direkt auf dem externen Wartungsrechner ausnutzen. Auch kann ein Zertifikat oder ein sonstiges Token gestohlen werden. Und schließlich ist es auch nicht ausgeschlossen, dass Angreifer gestohlene Notebooks verwenden, auf denen eine Software für den externen Zugriff konfiguriert ist.

Doch wie der Gefahr begegnen? Eine vollkommene Abschottung der Produktions-IT nach außen ist im Industrie-4.0-Zeitalter kaum mehr realisierbar, wie das Beispiel der Fernwartungszugänge zeigt. Also müssen Lösungen gefunden werden, die sowohl die IT als auch die Produktion sowie die ICS-Anbieter zufriedenstellen. „Ein branchen- und disziplinübergreifender Diskurs ist notwendig“, stellt Rainer Glatz fest, Geschäftsführer des Fachverbands Software im VDMA und künftiger Leiter der Geschäftsstelle „Plattform Industrie 4.0“, bei der die Branchenverbände VDMA, ZVEI und Bitkom zusammenarbeiten werden – unter anderem im Bereich der Security (siehe Nachgefragt).

Bei einem Expertenworkshop zum Thema Sicherheit in Industrie 4.0 im Januar sei deutlich geworden, „wie unterschiedlich die Problemstellungen von den jeweiligen Sicherheitsexperten gesehen werden und wie hoch teilweise die Sprachbarrieren unter diesen Experten sind“, so Glatz. Beispiele nannte Klaus Bauer, Leiter der Systementwicklung Basistechnologien bei Trumpf Werkzeugmaschinen, Ditzingen: Die Fernzugängen beispielsweise betrachte die IT userzentriert. Das heißt, der User benötigt Zugriffsrechte auf Ressourcen. Bei einem Maschinenbauer wie Trumpf werde das Thema jedoch anlagenzentriert angegangen. Für die IT sei Sicherheit gleichbedeutend mit Datensicherheit, also Security. Maschinebauer hingegen sprechen von Anlagensicherheit, Safety. Bei der Vernetzung empfindet die IT die Maschine als Bedrohung, während für den Maschinenbau das Netzwerk die Bedrohung darstellt. Ganz zu schweigen von den Beschreibungssprachen: Während IT-ler UML oder SYSML reden, nutzt der Maschinenbauer Konstruktionszeichnungen oder ähnliches.

Dennoch ist sich Safenet-Experte Wosylus sicher: „Viele Sicherheitskonzepte lassen sich aus der heute gängigen IT in Industrie 4.0 übertragen. Dazu gehören Authentisierung, abgesicherte Kommunikation und Virtual Private Networks. Die technische Umsetzung muss sich jedoch an den Produktions- und Produktgegebenheiten orientieren.“

Authentizität, Integrität, Vertraulichkeit gewinnen an Bedeutung

Torsten Rössel, Chief Marketing Officer bei Innominate Security Technologies, Berlin, sieht dies ähnlich: „Klassische IT-Schutzziele wie Authentizität, Integrität, Vertraulichkeit und Verfügbarkeit sind und bleiben auch für die industrielle Produktion relevant, ihre Gewichtung wird sich aber verschieben. Während heute die Verfügbarkeit mit deutlichem Abstand höchste Priorität bei Maßnahmen der Cyber-Sicherheit für die Automation genießt, werden die drei anderen Aspekte unter Industrie 4.0 erheblich an Bedeutung gewinnen. Dem Management von Identitäten, Berechtigungen und Vertrauensstellungen – bekannten Aufgabenstellungen der klassischen IT – wird dabei eine Schlüsselrolle zukommen.“

Im Gegensatz dazu plädiert Oliver Winzenried, Vorstand von Wibu-Systems, Karlsruhe, für einen neuen Security-Ansatz: „Ein Automatisierungsprozess in der chemischen Industrie muss 24/7 unterbrechungsfrei laufen und darf nicht unterbrochen werden für Updates oder Virenscans.“ Wenn im Internet der Dinge Sensoren und Geräte mit eingebetteten Softwaresystemen direkt mit dem Internet verbunden seien, müsse man außerdem bedenken: „Ein System muss vertrauenswürdig nur nachgewiesen unveränderte Software aus nachgewiesen berechtigter Herkunft starten und muss sich gegenüber anderen Systemen authentifizieren können.“

Auch Professor Hartmut Pohl, geschäftsführender Gesellschafter von Softscheck, Köln, warnt davor, die etablierten IT-Security-Ansätze einfach in die neue, vernetzte IT-Produktionswelt zu übertragen: „Industrie 4.0 ist ein anspruchsvoller Ansatz. Im Sicherheitsbereich dürfen aber nun nicht die Sicherheitsmaßnahmen des letzten Jahrhunderts eingesetzt werden wie beispielsweise Firewalls, Verschlüsselung, Intrusion Detection oder Protection. Diese Sicherheitsmaßnahmen bewegen sich auf dem Level Security 0.1. Wir brauchen im Sicherheitsbereich neue und vergleichbar anspruchsvolle Ansätze, die nicht nur den Angriffen hinterherlaufen und nur versuchen zu erkennen, ob der Virus nun nicht doch ein Wurm ist.“

Die Experten empfehlen unisono als Basis für den sicheren Einstieg in die Industrie-4.0-Welt die Anwendung des IT-Grundschutzes des BSI mit organisatorischen und technischen Maßnahmen. Doch das Bundesamt selbst ist kritisch genug und plant bereits die Erweiterung dieses etablierten Standards auf ICS.

■ **Sabine Koll**
Journalistin in Böblingen

Nachgefragt

Rainer Glatz, VDMA, wird die neue Geschäftsstelle Industrie 4.0 von Bitkom, VDMA und ZVEI leiten Bild: VDMA

» *Herr Glatz, die drei Branchenverbände Bitkom, VDMA und ZVEI starten im April eine gemeinsame Geschäftsstelle, die sich dem Hypethema Industrie 4.0 widmen wird. Wird auch die Sicherheit von Industrie 4.0 ein Thema sein?*
Sicherheit im Sinne von Security ist eines der zentralen Handlungsfelder in Industrie 4.0. Die Verfügbarkeit nutzbarer Konzepte und Lösungen sind eine unverzichtbare Voraussetzung, dass Industrie 4.0 überhaupt Realität werden kann. Ich gehe davon aus, dass Security in einer eigenen Arbeitsgruppe innerhalb der Plattform Industrie 4.0 behandelt werden wird.

» *Welche Art von Security-Bedrohungen sehen Sie auf die Unternehmen zukommen, wenn sie sich dem Thema Industrie 4.0 öffnen? Wo lauern die Gefahren?*
Security-Bedrohungen gibt es nicht erst, seit wir über Industrie 4.0 sprechen. Bei aller Euphorie um Industrie 4.0 sollten wir die bereits heute bestehenden Bedrohungen ernst nehmen und entsprechende Gegenmaßnahmen ergreifen.

» *Sind die Bedrohungen vergleichbar mit der Büro-IT? Oder ist die Sache noch komplexer?*
Sicherheit für Industrie 4.0 ist wesentlich komplexer, da hochgradig vernetzte Systemstrukturen mit einer Vielzahl von beteiligten Menschen, IT-Systemen, Automatisierungskomponenten und Maschinen betrachtet werden müssen. Zwischen diesen teilweise autonom agierenden technischen Systemkomponenten findet ein reger und oft zeitkritischer Daten- und Informationsaustausch statt – mit einem hohen Anteil an schützenswertem Prozess-Know-how.

» *Haben die Unternehmen heute bereits genügend Maßnahmen getroffen, um die Sicherheit ihrer Produktionssysteme sicherzustellen? Ist ihnen die Brisanz bewusst?*
Insbesondere seit dem Auftreten von Stuxnet ist die Awareness bei unseren Unternehmen enorm gewachsen. Ich glaube, dass sich wie in der klassischen IT-Security auch im industriellen Sektor ein Markt für geeignete Sicherheitsprodukte und -lösungen entwickeln wird. Dies braucht allerdings Zeit und wird maßgeblich davon abhängen, dass sich Investitionen in Sicherheit rechnen beziehungsweise Kunden bereit sind, für Sicherheit Geld in die Hand zu nehmen.

» *Welchen Blickwinkel hatten die einzelnen Verbände bislang auf das Thema Security?*
Der Blickwinkel der einzelnen Verbände wurde selbstverständlich auf die Interessen und Herausforderungen der Verbandsmitglieder ausgerichtet. Dementsprechend reichte das Betrachtungsspektrum von Cloud Security über Embedded Security bis hin zu Industrial Security in Automation und Produktion.

» *Inwiefern kann die Sicherheit von Industrie 4.0 durch die Kooperation von Experten der Fachverbände profitieren?*
Es ist spannend zu sehen, wie unterschiedlich die Problemstellungen von den jeweiligen Sicherheitsexperten gesehen werden und wie hoch teilweise die Sprachbarrieren unter den Experten sind. Sicherheit bei Industrie 4.0 erfordert einen ganzheitlichen Ansatz und hierbei ist ein gemeinsames Verständnis unter der Beteiligten eine zwingende Voraussetzung. sk