Industrie macht in der Produktion die Schotten dicht

Die IT-Branche hat einen neuen Markt entdeckt: Industrie 4.0 – das Internet für die Produktion. Nach dem Büro soll nun auch die Fabrik vernetzt werden. Das Ziel ist eine höhere Effizienz und Effektivität. Mit der stärkeren Vernetzung der Maschinen und Anlagen werden die Fabriken allerdings auch zu einem attraktiven Ziel für Hacker. Mit Kryptografie sorgt die Industrie dafür, dass die Schotten dicht bleiben.

Von Hans Schürmann

Noch gibt es nur wenige Meldungen von Angriffen auf die IT von Produktionsanlagen. Das liegt daran, dass heute noch die Maschinen und Anlagen in den meisten Fabriken zentral und getrennt voneinander gesteuert werden. Doch das wird sich mit Industrie 4.0 ändern. Denn künftig sollen die industriellen Prozesse in der Produktion nicht nur miteinander vernetzt werden, sondern sich in weiten Teilen auch selbst organisieren. „Damit bleiben Störungen und Bedrohungen nicht mehr lokal begrenzt", erläutert Professor Frithjof Klasen, Leiter des Instituts für Automation & Industrial IT am Campus Gummersbach der Fachhochschule Köln, das Problem.

Beim Datentransfer und Informationsfluss zwischen der Büro-IT und Produktions-IT setzen die Anbieter von Automatisierungslösungen auf die bewährten Internetprotokolle, die sogenannte TCP/IP-Kommunikation. Der Einsatz der offenen Standards hat zwar viele Vorteile, es gibt aber einen wesentlichen Knackpunkt: Die Unternehmen übernehmen damit auch die Schwächen der Kommunikationsprotokolle bei der IT-Sicherheit.

Die Einsicht, dass durch die Vernetzung in der Produktions-IT auch die Gefahr von Angriffen steigt, ist nicht neu. Bereits 2005 haben sich Experten mit dem Problem auseinandergesetzt und Sicherheitsregeln für die Steuerung von Fertigungs- und Produktionsanlagen in einer VDI-Richtlinie (2182) definiert. Doch passiert ist bislang nur wenig. Die Umsetzung der empfohlenen Maßnahmen und deren Kombination erfordert den verstärkten Einsatz von finanziellen und personellen Ressourcen. So lange nichts passiert ist, gab es für die Unternehmen keinen Grund in IT-Sicherheit zu investieren", so Klasen.

Einzelne Bereiche absichern

Das wird sich mit der Realisierung von Industrie 4.0 ändern. Allerdings sind sichere IT-Lösungen in der Produktion nicht so einfach zu realisieren, wie in der klassischen Unternehmens-IT. „Das Thema Sicherheit ist in der Automatisierung sehr komplex", sagt Klasen. Was aus Automatisierungssicht als eine sinnvolle Eigenschaft erscheine, werde aus Security-Sicht möglicherweise als Schwachstelle betrachtet, erläutert der Kölner Professor. Am sinnvollsten sei es daher, die Automatisierungsbereiche in Zellen mit unterschiedlichen Sicherheitsstufen einzuteilen und diese nach dem sogenannten Zwiebelmodell der IT-Sicherheit zu schützen: empfindliche Zonen stark und weniger sensible Bereiche kaum oder gar nicht abzuschotten.

Das empfiehlt auch Jürgen Jasperneite, Leiter des Instituts für industrielle Informationstechnik (inIT) an der Hochschule Ostwestfalen-Lippe in Lemgo. „Die Übergänge zu den einzelnen Zonen können mit den Bordmitteln der klassischen IT abgesichert werden – mit Firewalls und Antiviren-Gateways", so der Lemgoer Professor. Das gelte auch für die Vernetzung der Produktionsstätten untereinander. Darüber hinaus empfiehlt der Experte für Industrial-IT die einzelnen Automatisierungskomponenten mit Hilfe von Verschlüsselung direkt zu sichern.

Je Komponente muss sich authentifizieren

Ziel sei es jedoch nicht, die gesamte Kommunikation zu verschlüsseln. „Das ist bei den Echtzeitanforderungen in der Automatisierung und den limitierten Rechenleistungen der Geräte gar nicht möglich", sagt Jasperneite. Es reiche aber in vielen Fällen aus, die Authentizität sicherzustellen. Das heißt, dafür zu sorgen, das nur Informationen akzeptiert werden, die auch tatsächlich von Komponenten kommen, die Teil der Automatisierungslösung sind. „Wir haben in Projekten untersucht, wie sicher die Einzelkomponenten für die Fabrikautomatisierung sind und gesehen, dass derzeit jede Steuerung übernommen werden kann", berichtet Jasperneite. Durch Zusatzfunktionen in der Software, wie eine Authentifizierung der Komponenten, könne man das verhindern.

Allerdings mit Technik alleine, sei die IT-Sicherheit in der Produktion nicht zu erreichen, warnt Peter Schoo. Nur eine Kombination mit organisatorischen Maßnahmen führe zum Ziel, so der Leiter des Department Network Security and Early Warning Systems bei der Fraunhofer Einrichtung für Angewandte und Integrierte Sicherheit (AISEC) in München. Daher sei es ganz wichtig, dass das Personal in Sachen IT-Sicherheit geschult werde. Es gebe zwar inzwischen Produkte, mit denen sicherheitsrelevante IT-Bereiche einer Anlage abgeschottet werden könnten – „doch dazu muss das Know-how bei jedem Anwender vorhanden sein", mahnt der AISEC-Experte. Schließlich werde die Sicherheitstechnik nicht vom Hersteller konfiguriert, sondern von den Mitarbeitern in den Anwenderunternehmen.

„Ohne weiteren Schutz könnte jede Maschinen-Steuerung von Hackern übernommen werden."

Prof. Jürgen Jasperneite,
Leiter des Instituts für industrielle Informationstechnik (inIT)