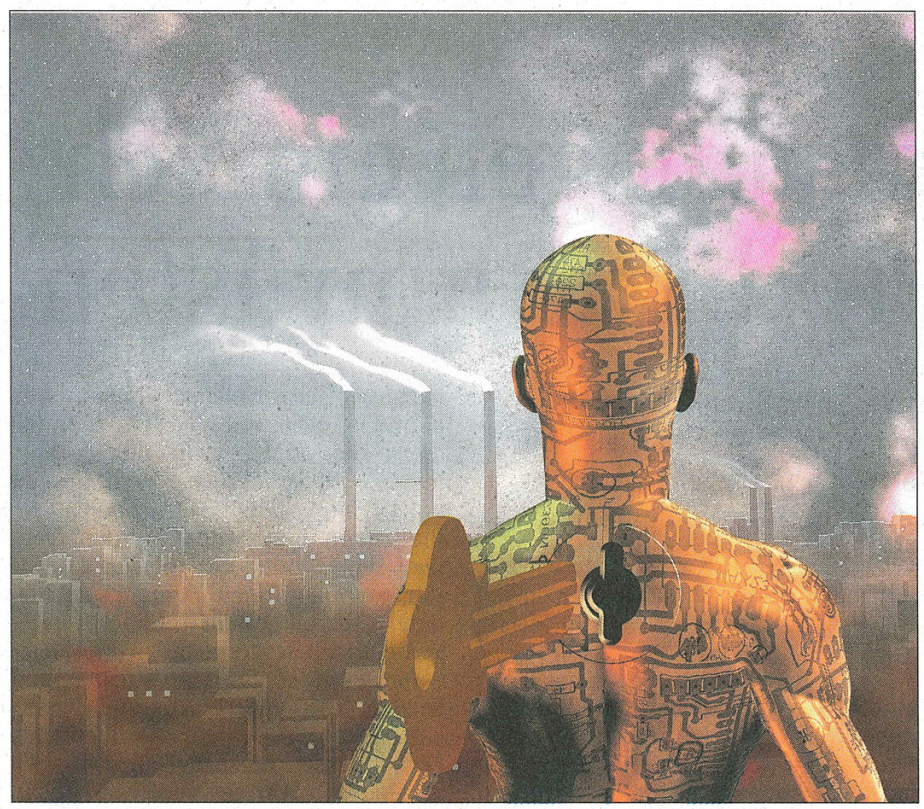
Industrie 4.0 braucht effiziente IT-Sicherheit



Schlüssel zum Erfolg: Soll die Fabrik der Zukunft erfolgreich sein, sind passende Sicherheitsstrategien für die Unternehmens-IT essenziell. Foto: Fotolia

VERNETZUNG: Mit dem Konzept Industrie 4.0 und den die neue „industrielle Revolution" tragenden Cyber Physical Systems will die deutsche Wirtschaft ihre internationale Wettbewerbsfähigkeit sichern und ausbauen. Vieles steht und fällt dabei mit der IT-Infrastruktur in den beteiligten Fabriken und Fertigungsanlagen und deren Schutz.

VDI nachrichten, Düsseldorf, 23. 11. 12, ciu

Mehr Produktivität und höhere Flexibilität durch dezentrale, hochgradig vernetzte Systeme, das ist das Ziel der geistigen Väter von Industrie 4.0. Das bedeutet: Maschinen, Sensoren und Aktoren werden miteinander vernetzt sein und über das „Internet der Dinge" ihre Daten austauschen. Vom ERP-System für die Auftragssteuerung über die Scada-Rechner der Steuerungs- und Betriebsleitebene bis zum Sensor auf der Feldebene werden alle Systeme und Subsysteme eine Internetadresse besitzen und von außen zugänglich sein.

Statusmeldungen, Anforderungen von Rohstoffen, Steuerbefehle, Konstruktionsdaten, Informationen über Energieverbrauch, Wartungsstand und Ausschussquoten von Anlagen, all das wird in einem wesentlich höheren Maß als heute in den Netzen zirkulieren und verteilt in der „Cloud" gespeichert werden, so die Vision der Vordenker. Viele dieser Daten sind wettbewerbsrelevant.

Mit dieser neuen Dimension der Vernetzung gilt es die Sicherheitsrisiken neu zu bewerten. Spionage- und Sabotage-Programme wie Stuxnet oder Flame vermitteln eine Vorstellung davon, wie hoch im Extremfall das Schadenspotenzial in der Produktionsinfrastruktur bei Angriffen durch Hacker sein kann. Diese Attacken konnten bereits bei einem relativ niedrigen Vernetzungsgrad ihrer Ziele Erfolge verbuchen.

In einem Szenario nach der Blaupause von Industrie 4.0 dürften sich Angriffspunkte und Schadenspotenzial multiplizieren. „Bei einer hochgradig autonomen Kommunikation ergeben sich ganz neue Bedrohungsszenarien", sagt Rainer Glatz, Geschäftsführer des Fachverbandes Software im Verband Deutscher Maschinen- und Anlagenbau (VDMA). Allerdings haben gerade die Branchen, die am meisten von Ansätzen wie Industrie 4.0 profitieren könnten, nämlich die Maschinen- und Anlagenbauer, noch nicht in ausreichendem Maß Konzepte entwickelt, wie dieser Bedrohung zu begegnen wäre. „Für sie ist diese Situation ja auch etwas vollkommen Neues", schiebt Glatz gleich nach. Im Vergleich zur kommerziellen IT hinke die Produktions-IT sicherheitstechnisch um mehrere Jahre hinterher, schätzt er.

Auch Hartmut Pohl, Professor für Informationssicherheit an der Hochschule Rhein-Sieg und Geschäftsführender Gesellschafter der IT-Sicherheitsberatung SoftScheck, sieht Handlungsbedarf, soll die angepeilte vierte industrielle Revolution nicht im Cyber-Fiasko enden. Die ISO 27001, welche die Anforderungen an IT-Sicherheitsmanagementsysteme unter Berücksichtigung der Risiken spezifiziert, werde noch nicht vollständig umgesetzt und reiche dafür auch nicht aus, kritisiert der Experte. „Die Fertigungsindustrie denkt häufig noch analog", sagt Pohl, „sie betrachtet speicherprogrammierbare Steuerungen als nicht manipulierbar. Tatsächlich sind spezielle Sicherheitstests der Software unverzichtbar."

Da ist einmal die Technik. In einer Landschaft, in welcher Sensoren, eingebettete Steuerungsrechner, Aktoren, Netzwerkprotokolle und andere Elemente echtzeitfähig sein müssen, benötige man andere Internetstrukturen, sagt Wolfgang Dorst, als Bereichsleiter Software beim Branchenverband Bitkom unter anderem für das Thema Cyber Physical Systems (CPS) zuständig. Gefragt sind hier vor allem Techniken, die die geringen Latenzzeiten von Steuerungssystemen mit den Anforderungen einer erhöhten Sicherheit unter einen Hut bringen.

Natürlich sollten die in der betrieblichen IT etablierten Techniken wie Firewalls, Verschlüsselung, Virenscanner oder Signaturchecks auch in der Prozess- und Produktions-IT Einzug halten. Aber das wird kaum ausreichen, um die Sicherheit zu gewährleisten. Dorst: „Industrie 4.0 erfordert eine ganzheitliche Herangehensweise auf allen Ebenen."

Auch auf der organisatorischen Schiene müsse sich in den Unternehmen einiges ändern. Vor allem müssten die Verantwortlichen für die zurzeit noch separat agierenden Sparten der Unternehmens-IT und der Produktions-IT zur Schaffung eines ganzheitlichen Sicherheitsmanagements zusammenarbeiten. „Keine der beiden Seiten kann ein modernes, umfassendes Sicherheitskonzept alleine erstellen – der betrieblichen IT fehlt häufig das Know-how für die Prozesse in der Fertigung, und die Produktions-IT kennt oftmals die neuesten Entwicklungen bei der Sicherheitstechnik nicht gut genug", analysiert Dorst.

Ein übergreifendes IT-Sicherheitskonzept müsste in den Betrieben auf der Geschäftsleitungsebene initiiert und von dort nachgehalten werden, präzisiert Holger Junker, Referatsleiter Cyber-Sicherheit in kritischen IT-Systemen im Bundesamt für Sicherheit in der Informationstechnik. „Man muss sich darüber im Klaren sein, dass IT-Sicherheit kein Produkt ist, sondern ein sinnvolles Zusammenspiel von Maßnahmen."

CHRISTOPH HAMMERSCHMIDT

Zehn Hauptbedrohungen gegen industrielle IT

Das Bundesamt für Sicherheit in der Informationstechnik hat eine Aufstellung der häufigsten Bedrohungsarten für die IT-Infrastruktur in der Industrie (Industrial Control Systems – ICS) zusammengetragen. Deren Definition ist in vielen Bereichen deckungsgleich mit derjenigen von Cyber Physical Systems (CPS):

- Unberechtigte Nutzung von Fernwartungs-Zugängen;
- Online-Angriffe über Unternehmensnetze;
- Angriffe auf eingesetzte Standardkomponenten im ICS-Netz;
- Denial of Service-Angriffe (setzen digitale Dienste außer Betrieb);
- menschliches Fehlverhalten und Sabotage;
- Einschleusen von Schadcodes über Wechseldatenträger und / oder externe Hardware;
- Mitlesen und Einschreiben von Steuerbefehlen im ICS-Netz;
- unberechtigter Zugriff auf Ressourcen;
- Angriffe auf Netzwerkkomponenten;
- technische Defekte und höhere Gewalt.

ch