Stufensystem für die Sicherheit

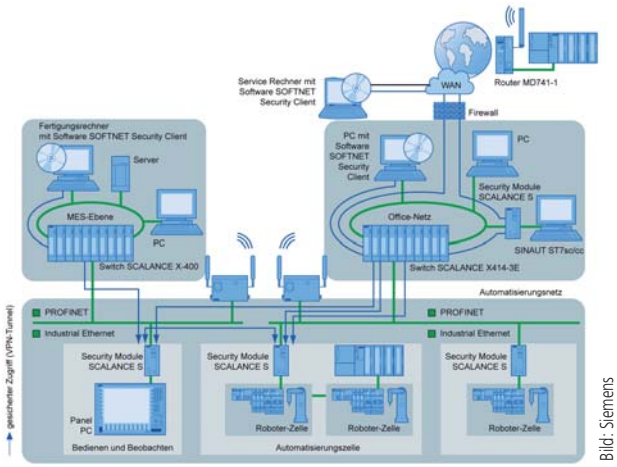

Bild: Siemens

Seit dem Auftreten von Stuxnet häufen sich Mitteilungen zur Anfälligkeit von Automatisierungssystemen für derartige Angriffe. Doch eine Absicherung der Automationsebene alleine genügt nicht - in der Regel sind zusätzliche Maßnahmen erforderlich, um bestimmte Angriffe abzuwehren. Inzwischen stehen bewährte und wirksame Konzepte bereit, um einen entsprechend sicheren Betrieb von Industrieanlagen zu unterstützen.

Die öffentliche Diskussion differenziert meist nicht ausreichend zwischen dem notwendigen Beheben von Produktschwachstellen auf der einen und der Einrichtung von Schutzmaßnahmen gegen Schadsoftware auf der anderen Seite. Auf Seiten der Automationshersteller werden seit Jahren Schwachstellentests für seine Standardprodukte durchgeführt und Geräte entsprechend optimiert – dies bezeichnet man als Härten. Jedoch kann diese Absicherung allein keinen umfassenden Schutz vor Cyberangriffen gewährleisten. Hierfür sind in der Regel zusätzliche Maßnahmen wie sichere Authentifizierung, Zugangskontrolle oder Verschlüsselung erforderlich. Diese Kombination aus passiver Sicherheit und aktiven Maßnahmen ist in der IT schon Usus: So werden regelmäßig durch Windows-Patches Schwachstellen bereinigt, für einen umfassenden Schutz gegen Viren oder unberechtigte kommen zusätzliche Schutzmaßnahmen zum Einsatz, etwa Virenscanner und Firewalls. Beim Design heutiger Automatisierungsprodukte und -protokolle standen bisher Performance und Funktionalität im Vordergrund. Security-Aspekte wurden kaum berücksichtigt, da entsprechende Anforderungen in der Industrie erst in den letzten Jahren zunehmen. Daher verfügen die meisten Automatisierungssysteme und -protokolle nur über begrenzte Sicherheitsfunktionalitäten. Um ein gutes Schutzniveau zu erreichen, ist ein umfassendes Security-Konzept aber unabdingbar, das unterschiedlichen Bedrohungen auf unterschiedliche Weise und auf verschiedenen Ebenen begegnet. Es bedarf also einer mehrschichtige Strategie oder 'Defence in Depth', die mehrere Hürden für potenzielle Angreifer aufbaut. Dazu gehören physikalische Security-Maßnahmen, IT-Sicherheit und Netzwerkzugangsschutz sowie Zugriffskontrolle und Applikationssicherheit auf allen Endgeräten.

Zellenschutz als Königsweg

Der physikalische Zugangsschutz und die Einrichtung entsprechender Security-Prozesse und -Richtlinien liegt in der Verantwortung der Betreiber. Herstellerfirmen können jedoch im Bereich der Netzwerk- und Endgeräte-Security unterstützen, indem sie geeignete Produkte zur Verfügung stellen. Im Bereich der industriellen Netzwerksicherheit hat sich das Zellenschutzkonzept bewährt. Dabei werden Teile eines Netzwerkes von einer verteilten Security-Anwendung geschützt und dadurch das Netz bei Einsatz mehrerer Module sicherheitstechnisch segmentiert. Somit sind Geräte im geschützten Netzsegment, der 'Zelle', vor unbefugten Zugriffen sicher. Auch die Kommunikation zwischen den Zellen ist geschützt. Scalance S von Siemens ist solch eine Security Appliance, die Zugriffe mittels Firewall-Mechanismen kontrollieren sowie den Datenverkehr mittels Virtual Private Network (VPN) verschlüsseln kann. Ein geschütztes Netzsegment bietet auch den Vorteil, dass Echtzeitkommunikation innerhalb des Sicherheitsbereichs unbeeinflusst von rechenintensiven Sicherheitsanwendungen stattfindet und dennoch geschützt wird. Vergleichbares gilt auch für Safety-Applikationen wie Profisafe, die aber eine ausreichende Performance benötigen. Sonst kann die Anlage leicht in den funktional sicheren Zustand gezwungen werden kann, worunter die Verfügbarkeit leidet. Das Zellenschutzkonzept bietet den Ausweg aus dem Dilemma, einerseits genügend Leistung zur Verfügung haben zu müssen und andererseits ausreichenden Schutz zu gewährleisten. Zukünftig wird Siemens sein Security-Produktportfolio erweitern und damit auch die Einsatzmöglichkeiten des Zellenschutzkonzeptes. Die Security-Funktionalitäten 'Firewall' und 'VPN' werden etwa in die Kommunikationsprozessoren (CP) der Steuerung Simatic S7 integriert. Damit können auch Endgeräte wie PC und andere Steuerungen geschützt werden. Zur Unterstützung der Anwender bietet das Unternehmen außerdem auch Security-Dienstleistungen an, die je nach Bedarf Schwachstellenanalyse, Erstellung, Implementierung und Überprüfung von Schutzkonzepten umfassen können. Werden solche Security-Maßnahmen und -Konzepte konsequent umgesetzt, lassen sich Automatisierungsanlagen auch heute mit einem vernünftigen Grad an Sicherheit betreiben. ■

Der Autor Franz Köbinger ist System Manager für Security im Bereich Industrial Communication bei der Siemens AG Industry Sector in Nürnberg.

www.siemens.de

Auszug aus IT&Production, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 12/2011.