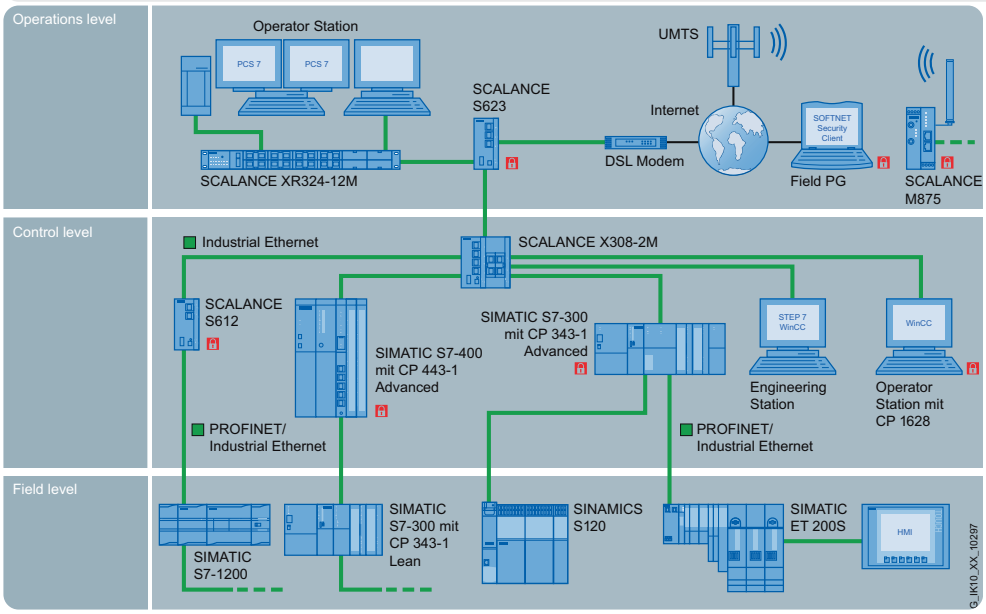

Bild 1: Beim Zellenschutzkonzept werden Netzwerke mittels Security-Modulen segmentiert. Das Bild zeigt eine Erweiterung des Zellenschutzkonzeptes durch Security-Kommunikationsprozessoren (CP) für Simatic-Steuerungen und PCs.

Wie sicher sind industrielle Anlagen?

Seit die Schadsoftware namens Stuxnet letztes Jahr in Erscheinung trat, wurde immer häufiger über Security-Vorfälle und die Anfälligkeit von Automatisierungssystemen für derartige Angriffe berichtet. Dabei wird häufig der Eindruck erweckt, die Ursachen seien nur Schwachstellen innerhalb der Systeme; man müsse diese einfach beseitigen, um solche Angriffe zu verhindern. Das allein reicht jedoch nicht aus. Neben der Behebung von Schwachstellen in den Systemen sind zusätzliche aktive Security-Maßnahmen erforderlich, um bestimmte Angriffe abzuwehren. In anderen IT-Umfeldern, etwa dem Office-Bereich, ist dies längst bekannt und akzeptiert.

Siemens führt bereits seit Jahren Schwachstellentests für Standardprodukte durch und optimiert die Geräte entsprechend - diesen Vorgang bezeichnet man als Härten. Jedoch kann die Behebung von Schwachstellen allein keinen Schutz vor bestimmten Cyberangriffen gewährleisten. Zusätzliche Sicherheitsfunktionalitäten sind erforderlich, z.B. sichere Authentifizierung, Zugangskontrolle oder Verschlüsselung. Diese können nur durch aktive Schutzmaßnahmen bzw. mit speziellen Security-Produkten zur Verfügung gestellt werden. Ein Beispiel aus der IT: Bei PCs werden regelmäßig durch Windows-Patches Schwachstellen bereinigt. Dies allein stellt keinen ausreichenden Schutz gegen Bedrohungen wie Viren oder unberechtigte Zugriffe dar. Hierfür sind zusätzliche Schutzmaßnahmen zu installieren, etwa Virenscanner und Firewall. Das ist die erwähnte Kombination aus passiver Sicherheit und aktiven Maßnahmen.

Security-Konzepte sind gefragt

Um ein gutes Schutzniveau zu erreichen, ist ein umfassendes Security-Konzept unabdingbar, das unterschiedlichen Bedrohungen auf unterschiedliche Weise und auf verschiedenen Ebenen begegnet. Es bedarf also einer mehrschichtigen Strategie, die mehrere Hürden für potenzielle Angreifer aufbaut. Dazu gehören physikalische Security-Maßnahmen, IT-Sicherheit und Netzwerkzugangsschutz sowie Zugriffskontrolle und Applikationssicherheit auf allen Endgeräten. Der physikalische Zugangsschutz und die Einrichtung entsprechender Security-Prozesse und -Richtlinien liegt in der Verantwortung der Anlagenbetreiber. Herstellerfirmen können jedoch im Bereich der Netzwerk- und Endgerätesecurity unterstützen, indem sie geeignete Produkte zur Verfügung stellen.

Geschützter Bereich

Im Bereich der industriellen Netzwerksicherheit hat sich das Zellenschutzkonzept bewährt. Es besteht darin, dass Teile eines Netzwerkes von einer Security Appliance geschützt werden. Dadurch wird das Netz sicherheitstechnisch segmentiert. Somit sind alle Geräte im geschützten Netzsegment vor unbefugten Zugriffen sicher und die Kommunikation zwischen den Zellen ist geschützt. Scalance S von Siemens ist solch eine Security Appliance und kann Zugriffe mittels Firewall-Mechanismen kontrollieren sowie den Datenverkehr mittels Virtual Private Network (VPN) verschlüsseln. VPN bietet auch noch die Möglichkeit der sicheren Authentifizierung und ist damit in der Lage, z.B. auch Replay-Attacken abzuwehren. Dieses geschützte Netzsegment (oder Zelle) bietet auch noch den Vorteil, dass Echtzeitkommunikation unbeeinflusst von performanceintensiven Security-Mechanismen ist und dennoch geschützt wird.

Produkte unterstützen Zellschutzkonzept

Zukünftig wird Siemens das Security-Produktportfolio und die Einsatzmöglichkeiten des Zellenschutzkonzeptes erweitern. Die Security-Funktionalitäten 'Firewall' und 'VPN' werden auch in die CPs der Steuerung Simatic S7 (CP 443-1 Advanced und CP 343-1 Advanced) sowie den CP für Industrie-PCs CP 1628 integriert. Damit können auch Endgeräte wie PCs und die Steuerungen S7-400 und S7-300 geschützt werden. ■

www.siemens.de

Autor: Dipl.-Ing. Franz Köbinger, Security Manager für Industrial Communication, Industry Sector, Industry Automation Division, Siemens AG