Security-Konzept für industrielle Anlagen

Die fünf Kernelemente sicherer Automatisierungsnetzwerke

Die Ethernet-basierte Kommunikation nimmt im Automatisierungsumfeld eine zentrale Rolle ein und Industrial Ethernet wird auch zunehmend im Feldbereich eingesetzt. Die Vorteile davon liegen klar auf der Hand: Neben der Nutzung offener und standardisierter IT-Technologien wie z.B. Wireless LAN oder Webserver ist damit auch eine durchgängige Vernetzung realisierbar. Allerdings steigt somit auch die Gefahr von Zugriffsverletzungen und durch sogenannte Malware, sodass damit einhergehend auch das Gefährdungspotenzial für die Automationsnetze neu bewertet und Sicherheitskonzepte entsprechend umgesetzt werden müssen.

IT-Security in Büro-IT-Netzwerken ist längst kein besonderes Thema mehr: nicht, weil es nicht wichtig wäre, sondern weil es dort bereits zum Standard geworden ist. Sicherheits-Patches und -Updates, Verschlüsselung, Passwörter usw. gehören hier schon lange zum Alltag. Ganz anders sieht die Situation aber im Automatisierungsumfeld aus. Automatisierungsnetze abzusichern stellt eine große Herausforderung dar, da dies mit anderen wichtigen Anforderungen wie 'Performance' und 'Usability' kollidiert. Die Zusatzkosten spielen dabei natürlich auch eine wichtige Rolle. Hinzukommt, dass die Absicherung eines Netzwerkes ständige Aufmerksamkeit erfordert und es nicht mit dem einmaligen Einrichten getan ist. Gleichwohl führt kein Weg daran vorbei, sich dem Thema 'Security' in der Automatisierung bzw. industriellen Anlagen widmen zu müssen. Durchgängige Vernetzung und die Nutzung offener IT-Standards sind nicht nur der Garant, sondern in den meisten Fällen auch die Voraussetzung für die Wettbewerbsfähigkeit. Und dass die Gefährdungen real sind, zeigen deutlich die häufiger gewordenen Meldungen in den Medien über Sicherheitsvorfälle. Auch in der nationalen sowie internationalen Normung und Standardisierung wird das schwierigere Thema 'Industrial Security' adressiert und stellt zunehmende Anforderungen an Automatisierungssysteme und -anlagen. Besonderes Augenmerk liegt hierbei auf der Absicherung kritischer Infrastrukturen. Stellen Sicherheitsvorfälle in Produktionsanlagen im Wesentlichen 'nur' – wenn auch teils große – monetäre Verluste dar, kommt bei den kritischen Infrastrukturen auch noch das öffentliche Interesse hinzu. Denn hier kann durch Störungen ja sogar die Bevölkerung in Mitleidenschaft gezogen werden. Wie können

nun die Gefahrenpotenziale signifikant minimiert und hinreichende, aber auch bezahlbare Sicherheit in der industriellen Automation erreicht werden? Ein Allheilmittel oder ein Patentrezept, das immer anwendbar ist, gibt es nicht, da jede Anlage individuelle Randbedingungen, Gefährdungen und Schutzziele besitzt. Aber es gibt bewährte Vorgehensweisen. Beispielsweise eine überschaubare Anzahl von Eckpunkten für ein effizientes Security-Konzept, die betrachtet werden müssen, da einzelne Sicherheitsmaßnahmen alleine lückenhaft und damit unzureichend sind und nur ein Gesamtkonzept optimalen Schutz bieten kann. Für den sicheren Betrieb ist der Betreiber zuständig, aber Hersteller wie beispielsweise Siemens können dabei unterstützen, indem entsprechende Beratungsleistung und 'sichere' Produkte und Komponenten zur Verfügung gestellt werden. Die fünf Kernelemente eines Industrial-Security-Konzeptes, wie Siemens es anbietet, sind in Bild 1 dargestellt.

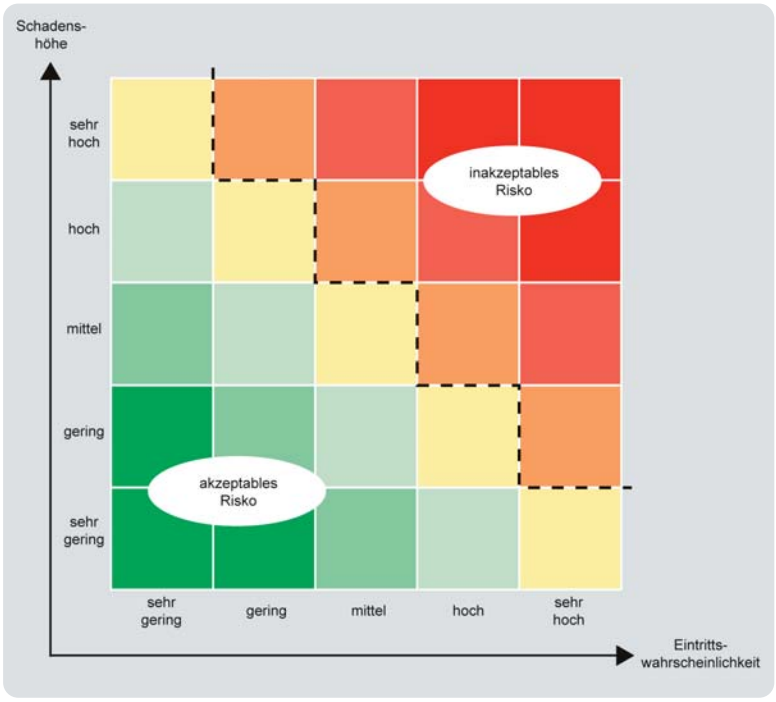

Bild 2: Entscheidungstabelle zur Bewertung von Risiken nach einer anlagenspezifischen Risikoanalyse, die regelmäßig überprüft werden sollte.

1. Security Management

An erster Stelle und am wichtigsten ist die Etablierung eines Security-Prozesses bzw. Security-Managements. Um fundiert entscheiden zu können, welche Maßnahmen letztendlich getroffen werden müssen, ist zunächst zu analysieren, welche Risiken konkret bestehen, die nicht toleriert werden können. Hierbei spielen sowohl die Eintrittswahrscheinlichkeit eines Risikos als auch die mögliche Schadenshöhe eine Rolle. Werden Risikoanalyse und Ermittlung der Schutzziele vernachlässigt oder gar nicht durchgeführt, ist die Gefahr groß, dass unpassende, zu teure oder wirkungslose Maßnahmen getroffen werden und Schwachstellen nicht erkannt und nicht behoben werden (Bild 2). Aus der Risikoanalyse ergeben sich dann Schutzziele, die als Basis für konkrete Maßnahmen dienen und zwar sowohl organisatorische als auch technische Maßnahmen, die sich ergänzen müssen. Die Maßnahmen müssen nach der Implementierung überprüft werden. Von Zeit zu Zeit oder wenn sich Änderungen ergeben haben, muss das Risiko erneut bewertet werden, da sich ja die Bedrohungslage mittlerweile geändert haben könnte. Dann beginnt der Prozess wieder von vorne (Bild 3).

Zum Security-Management gehören zudem folgende Elemente:

- Das Schaffen eines grundsätzlichen Security-Verständnisses bei allen Mitarbeitern (Security Awareness)
- Das Festlegen von Verantwortlichkeiten
- Die Definition von gefährdeten Prozessen und Abhilfemaßnahmen
- Das Erarbeiten von Notfallplänen, z.B.: Was tun bei Anlagenstillstand durch Schadsoftware?

2. Sicherung der Schnittstellen zwischen Unternehmens- und Anlagennetz

Dieses Element ist erforderlich, wenn eine Netzwerkverbindung zwischen Unternehmens- und Anlagennetzwerk vorhanden ist. Dies fällt vor allem in die Verantwortlichkeit der IT-

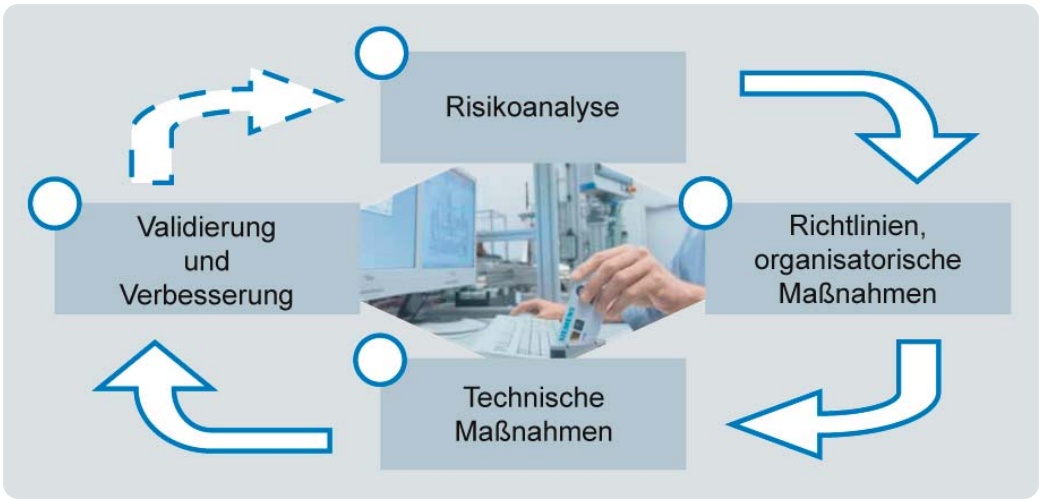

Bild 3: Die vier kontinuierlich durchzuführenden Schritte des Security-Management-Prozesses

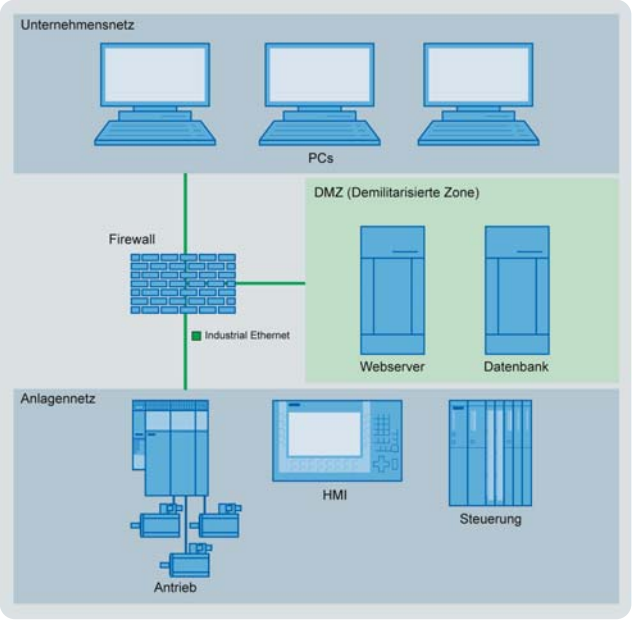

Bild 4: Einsatz einer 'Demilitarisierten Zone' für den Datenaustausch zwischen Unternehmens- und Anlagennetz.

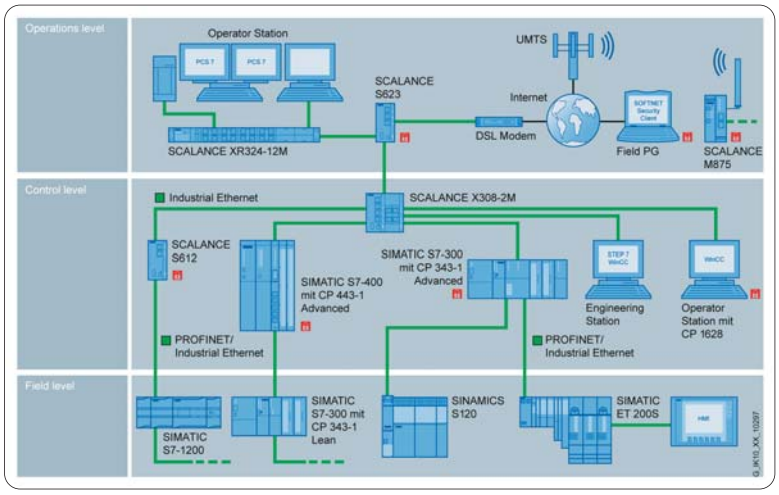

Bild 5: Realisierung des Zellenschutzkonzepts mit Hilfe von Security Appliances Scalance-S- und Simatic-S7- und PC-Kommunikationsbaugruppen von Siemens, jeweils mit integrierter Security-Funktion (siehe Schlosssymbol).

Abteilung, da es in erster Linie um die Definitionen geht, welche Zugriffe aus dem Unternehmensnetz in das Anlagennetz zulässig sind und was datentechnisch in umgekehrter Richtung übertragen werden darf. Diese Definitionen sind in Regeln und Zugriffsrechte zu übersetzen, die es mit technischen Maßnahmen umzusetzen gilt. An erster Stelle stehen hier 'Network Intrusion Detection'-Systeme (NIDS) und Firewalls, welche Eindringversuche in das Gesamtnetzwerk erkennen und den Datenverkehr in beide Richtungen regeln. Und auch das Einrichten einer sogenannten Demilitarisierten Zone (DMZ) ist möglich, in der beide Teilnetzwerke Daten miteinander austauschen können, ohne eine direkte Verbindung miteinander zu haben (Bild 4).

3. Schutz PC-basierter Systeme im Anlagennetz

Ebenso wie PC-Systeme in Büros gegen Schadsoftware zu schützen sind und mögliche Lücken im Betriebssystem oder in Anwendersoftware durch Updates mit Patches geschlossen werden müssen, bedürfen auch PCs und PC-basierte Steuerungssysteme im Anlagennetz entsprechender Schutzmaßnahmen. Auch können hier viele der im Büroumfeld bewährten Schutzsysteme eingesetzt werden. Zu den bekanntesten Maßnahmen gehört hierbei der Einsatz eines regelmäßig zu aktualisierenden Virenscanners. Allerdings ist zu bedenken, dass Virenscanner nur einen Teil der Viren erkennen kann (ca. 70 bis 80%) und gegen neue Viren, für die noch kein Pattern zur Verfügung steht machtlos ist. Auch kann im Automatisierungsumfeld nicht immer zeitnah aktualisiert werden, wenn kein Wartungsfenster zur Verfügung steht, z.B. bei 24/7-Betrieb. Daher ist der Einsatz von sogenannter Whitelisting-Software (siehe Kasten) eine gute Alternative zu Virenscannern. Whitelisting arbeitet mit sogenannten Positivlisten, in denen der Benutzer festlegen kann, welche Prozesse bzw. Programme auf dem Rechner laufen dürfen. Versucht dann ein Benutzer oder eine Schadsoftware ein neues Programm zu installieren, so gelingt zwar eventuell noch die Installation, aber der für den Betrieb notwendige Prozess wird nicht ausgeführt und das Programm kann nicht gestartet werden und somit auch keinen Schaden anrichten. Hersteller von Industriesoftware können hierbei den Anwender unterstützen, indem sie ihre Software auf Verträglichkeit mit Virenscannern oder Whitelisting-Software testen.

Whitelisting

Ob Personen, Unternehmen oder Programme: Eine Weiße Liste – oder auch Positivliste – bezeichnet eine Sammlung gleicher Elemente, die als vertrauenswürdig eingestuft werden. Whitelisting für PCs sorgt dafür, dass nur erwünschte Programme ausgeführt werden können.

4. Schutz der Steuerungsebene

Dass man PCs und Netzwerke gegen Bedrohungen schützen kann und muss, ist hinlänglich bekannt. Doch welche Maßnahmen kann man zum Schutz meist herstellerspezifischer, proprietärer Systeme ergreifen? Wie schützt man speicherprogrammierbare Steuerungen (SPS) und Operator Stations, die entweder kein kommerzielles Betriebssystem oder eine ältere Version nutzen, da sie über viele Jahre und sogar Jahrzehnte im Einsatz sind? Hier ist der Einsatz von Sicherheitssoftware Dritter nicht möglich und Zugriff auf die Systemfunktionen der Geräte ist meist gar nicht oder nur eingeschränkt möglich. Daher sind bei diesem Schritt die Hersteller von Automatisierungshardware gefragt, entsprechende Sicherheitsmechanismen zu implementieren und den Anwendern anlagenspezifische Einstellmöglichkeiten zur Verfügung zu stellen. Die Anwender hingegen sind dazu aufgefordert, das Vorhandensein solcher Mechanismen bei den Herstellern zu hinterfragen und diese auch zu aktivieren, so Einstellungsmöglichkeiten angeboten werden. Wichtig ist zunächst aber eine grundsätzliche Robustheit der Systeme in Bezug auf die Beeinflussung vor allem durch fehlerhafte Datentelegramme und größere, unerwünschte Datenströme. Die Hersteller müssen dafür sorgen, dass Geräte auf mögliche Schwachstellen getestet und durch bestimmte Maßnahmen wie 'Secure Coding' entspre-

chend ‘gehärtet’ werden. Ähnlich wie bei PC-basierten Systemen sollten sich auch bei SPS- und HMI-Systemen ungenutzte Dienste (z.B. ein nicht benötigter Webserver), Protokolle (z.B. SNMP, wenn kein Netzwerkmanagement gewünscht ist) und sogar nicht verwendete Schnittstellen (z.B. freier RJ45-Port) deaktivieren lassen. Werden beispielsweise die von Siemens-Steuerungen zur Verfügung gestellten Funktionen wie Passwortschutz, Bausteinverschlüsselung und Kopierschutz genutzt, ist ein weiterer essenzieller Baustein zur Absicherung des Anlagennetzwerks gelegt.

5. Netzwerksicherheit

Das fünfte Element eines industriellen Security-Konzeptes betrifft die Netzwerksicherheit. Dies ist ein wesentlicher Schritt hin zu einer ‘sicheren’ Anlage, da es um nichts weniger als die Sicherung der Datenübertragung und den Zugang zum Netzwerk geht. Die wenigsten Automatisierungsgeräte verfügen derzeit über Security-Funktionen, mit denen die Kommunikation gegen Spionage oder Manipulation durch Verschlüsselung gesichert werden kann bzw. durch die die Kommunikationspartner sicher authentifiziert werden können. Das wird sich aufgrund der langen Lebenszyklen von Automatisierungsanlagen und ihren Geräten auch so schnell nicht ändern. Obwohl zunehmend mehr Geräte herstellerseitig damit ausgestattet werden, wird es wohl weiterhin Geräte geben, die aufgrund von Kostenoptimierung oder anderen Gründen über keine derartigen Security-Funktionen verfügen. Hinzu kommt, dass in manchen Fällen Echtzeitanforderungen bestehen, die den Einsatz Performance-intensiver Security-Funktionen wie Verschlüsselung oder sichere Authentifizierung zumindest derzeit nicht erlauben.

Netzsegmentierung und Zellenschutz

Zur Lösung dieses Dilemmas hat sich das sogenannte Zellenschutzkonzept bewährt. Die Idee ist einfach: Man verwendet eine ‘Security Appliance, das heißt, eine speziell ‘gehärtete’ Netzkomponente, die über Security-Funktionen wie Firewall und Virtual Private Network (VPN) verfügt. Diese Security Appliances, auch Security Modules genannt, übernehmen den Schutz der Automatisierungsgeräte, indem sie vorgeschaltet werden und zu den jeweils geschützten Geräten den einzigen Zugang bilden. Der geschützte Bereich wird auch Zelle genannt und entspricht einem Netzsegment, meist einem eigenen Subnetz. Dadurch wird das Netzwerk sicherheitstechnisch segmentiert. Die Firewall kann nun den Zugriff auf die Zelle kontrollieren, wobei festgelegt werden kann, welche Netzteilnehmer miteinander und ggf. auch mit welchen Protokollen kommunizieren dürfen. Damit können nicht nur unbefugte Zugriffe unterbunden, sondern auch die Netzlast reduziert werden, da nicht jede Kommunikation, z.B. Broadcasts (Meldungen an alle Netzteilnehmer) passieren dürfen. Die Security Modules können auch miteinander gesicherte VPN-Kanäle aufbauen, sodass die Kommunikation von und zu Zellen verschlüsselt und sicher authentifiziert werden kann. Damit ist die Datenübertragung gegen Manipulation und Spionage geschützt. Neben der Security Appliance ‘Scalance S’ wird der Automatisierungsausrüster Siemens zukünftig diese Sicherheitsfunktionen auch in Kommunikationsprozessoren für Simatic-S7-Steuerungen und PCs anbieten. Die Vorteile liegen auf der Hand: Ein Security Module kann mehrere andere Geräte schützen, man muss diese Funktionen also nicht in jedes Gerät einbauen und administrieren. Innerhalb der Zelle bleibt Echtzeitkommunikation, wie z.B. Profinet-I/O-Kommunikation, unbeeinflusst von Performance-intensiven Security-Funktionen und dennoch ist der Zugriff auf die Zelle geschützt (Bild 5).

Für eine sichere Automatisierung

Die effektive Umsetzung eines Industrial-Security-Konzeptes erfordert sowohl die Mitwirkung der Hersteller, als auch der Anwender und Betreiber von Automatisierungstechnik. Zudem sind auch Standardisierungs- und Normungsgremien gefragt, entsprechende Regeln vorzugeben, Standard-Lösungen zu entwickeln und Maßnahmen aufzeigen. Mit dem bereits heute angebotenen ‘Industrial-Security-Konzept’ und den erwähnten Security-Produkten vom Automatisierungshersteller Siemens liegt jetzt ein solch umfassender Ansatz vor, der Unternehmen aus sämtlichen Industriebranchen in fünf Schritten einen Weg hin zum sicheren Anlagennetzwerk bietet. ■

www.siemens.com/industrialsecurity

Autor: Dipl.-Ing. Franz Köbinger, System Manager für Security im Bereich Industrial Communication, Siemens AG, Industry Sector, Nürnberg.