Automatisierungsanlagen gegen Angriffe sichern

Autor(en): **Brändle, Markus / Naedele, Martin**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **98 (2007)**

Heft 7

PDF erstellt am: **13.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-857431

Automatisierungsanlagen gegen Angriffe sichern

Pragmatische Massnahmen gegen elektronische Angriffe

Sei es der Servicelaptop, ein USB-Stick oder der Remote Access über das Internet: Moderne Automatisierungsanlagen sind immer stärker mit der Umwelt verknüpft und so denselben Viren und Angriffen ausgesetzt, die man aus der Bürowelt kennt. Deshalb müssen die Anlagen ähnlich wie Büronetzwerke mit Firewalls, Virenscannern und demilitarisierten Zonen geschützt werden.

Markus Brändle, Martin Naedele

Automatisierungssysteme sind heute häufig nicht mehr isoliert und auf Verbindungen mit den Sensoren und Aktoren der Produktionsanlage beschränkt. Um den Forderungen des Marktes nach immer schnelleren Reaktionszeiten bei immer niedrigeren Betriebskosten folgen zu können, ist eine enge Vernetzung der Produktion mit den betrieblichen Steuerfunktionen, Supply-Chain-Partnern und externen Wartungsdienstleistern notwendig. Diese vertikale Integration zwischen Automatisierungssystem, betrieblichen Informationssystemen wie ERP und SCM und externen Netzwerken führt dazu, dass heute vielfach ein direkter Datenaustausch zwischen öffentlichen und halböffentlichen Netzen wie dem Internet oder einem Intranet und dem Automatisierungssystem stattfindet. Zusammen mit der immer stärkeren Verwendung von «Internet-Technologie», der TCP/IP-Protokollsuite, schafft dies ein Potenzial für elektronische Angriffe auf das Automatisierungssystem.

Tatsächlich sind in den letzten Jahren einige Angriffe auf Automatisierungssysteme bekannt geworden, wobei es sich hauptsächlich um ungezielte Seiteneffekte von Wurmepidemien und anderen Ausbreitungen von Schadsoftware im Internet handelte. Im Herbst 2006 wurde jedoch von US-Regierungsstellen bestätigt, dass es bereits in verschiedenen Ländern Erpressungsversuche gegenüber Wasser- und Stromversorgungsunternehmungen gegeben hat, bei denen die Erpresser einen Angriff auf Leitsysteme angedroht haben.

IT-Sicherheit ist also nicht mehr nur ein Thema für die Büroinformationstechnik, auch der Automatisierungsfachmann muss sich mit dieser Thematik auseinandersetzen. Dieser Beitrag zeigt einige pragmatische Möglichkeiten auf, wie Automatisierungsanlagen gegen elektronische Angriffe gesichert werden können.

Einfallswege und Barrieren

Um ein IT-System zu kompromittieren, muss der Angreifer in irgendeiner Weise Zugang zum System erhalten respektive ein Programm in das System einschleusen. Dies kann direkt über eine bestehende Netzwerkverbindung erfolgen oder indirekt über einen Datenträger, der an das Netzwerk angeschlossen wird. Wie in der Einleitung beschrieben, sind Automatisierungssysteme einerseits mit öffentlichen oder halböffentlichen Netzwerken verbunden, um Betriebsdaten, Statusinformationen oder Produktionsaufträge auszutauschen, oder anderer-

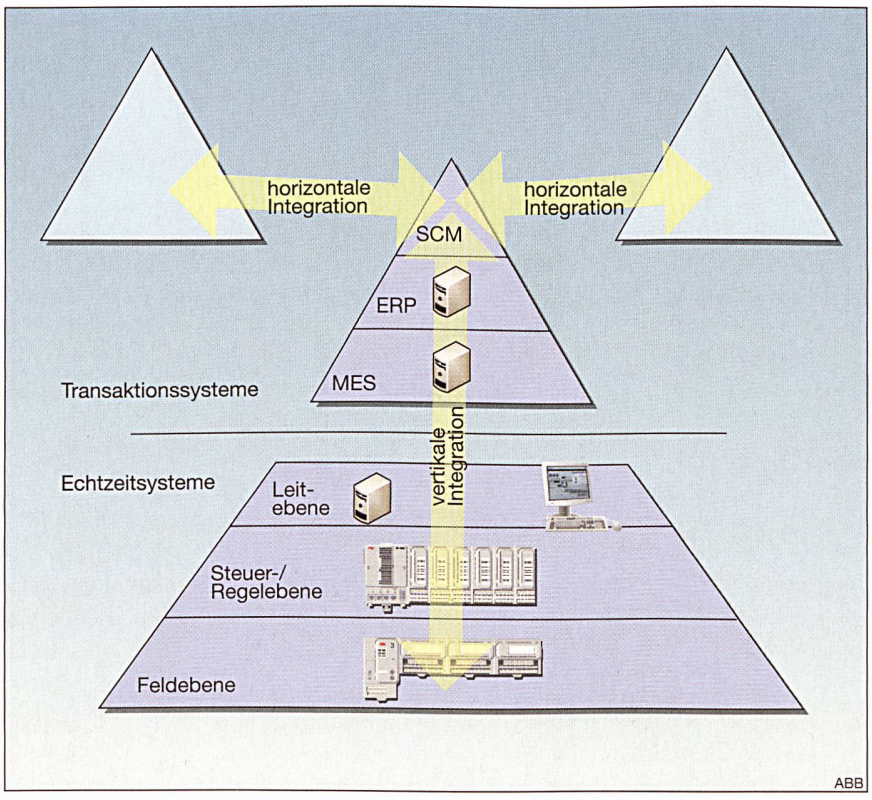

Bild 1 Automatisierungshierarchien, vertikale Integration, horizontale Vernetzung zwischen Unternehmen

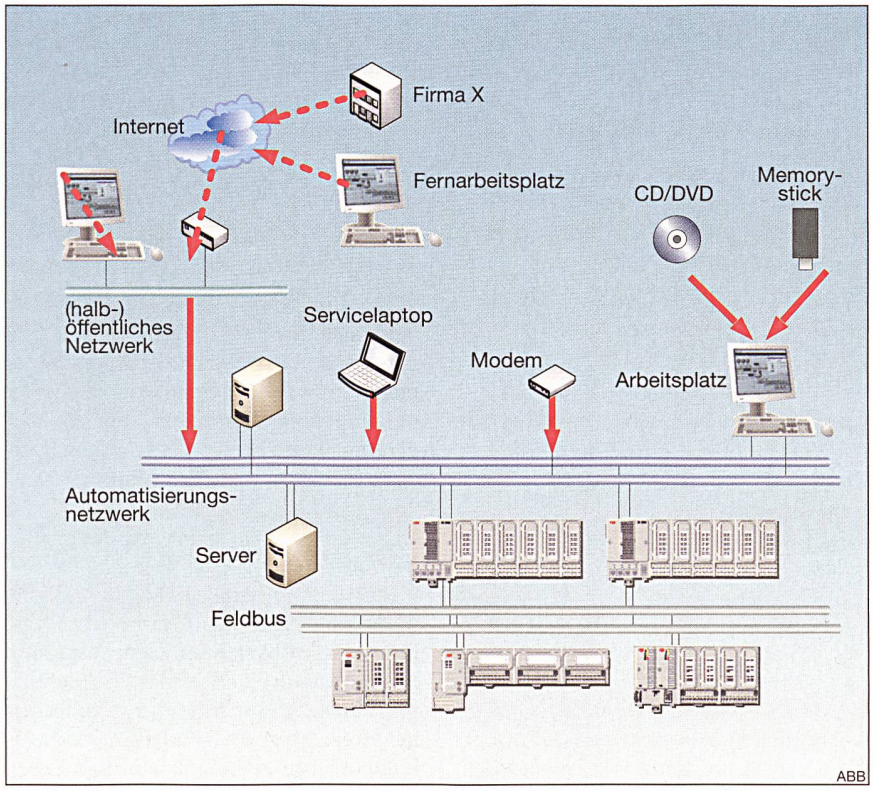

Bild 2 Einfallswege ins Automatisierungssystem

seits, um einem externen Benutzer direkten, interaktiven Zugriff auf das Leitsystem zu geben. Dieser Fall ist vor allem für die Diagnose und die Behebung von Betriebsproblemen oder für die Veränderung von Konfigurationseinstellungen und Steuerprogrammen von Bedeutung. Diese Verbindungen zu externen Netzwerken bieten jedoch nicht nur legitimen Benutzern Zugang zum Automatisierungssystem, sondern stellen auch mögliche Einfallswege für Angreifer dar. Dies gilt nicht nur für statische Verbindungen von Netzwerken, wie beim Zusammenschluss zweier Netzwerke über einen Router, sondern auch für Verbindungen, die dynamisch erstellt werden, wie bei der Benutzung eines Modems zur Einwahl ins Automatisierungsnetzwerk.

Bei der zweiten Art von Angriffen werden bösartige Programme über Datenträger ins Netzwerk eingeschleust. Dabei kann zwischen passiven Datenträgern wie CDs und DVDs, aktiven Datenträgern wie einem kompromittierten Servicelaptop und Zwischenformen wie Memorysticks, die beim Verbinden mit einem Computer automatisch Programme starten, unterschieden werden.

Eine Sicherheitsarchitektur sollte so ausgelegt sein, dass alle relevanten Einfallswege für elektronische Angriffe blockiert werden. Noch besser ist, wenn man im Sinne der tiefengestaffelten Verteidigung jeweils mehrere unabhängige Mechanismen vorsieht und das Automatisierungssystem in einzeln schütz- und nutzbare Zonen unterteilt.

Netzwerksicherheitszonen

Die Netzwerkarchitektur eines Automatisierungssystems sollte dem etablierten Konzept von Sicherheitszonen folgen.

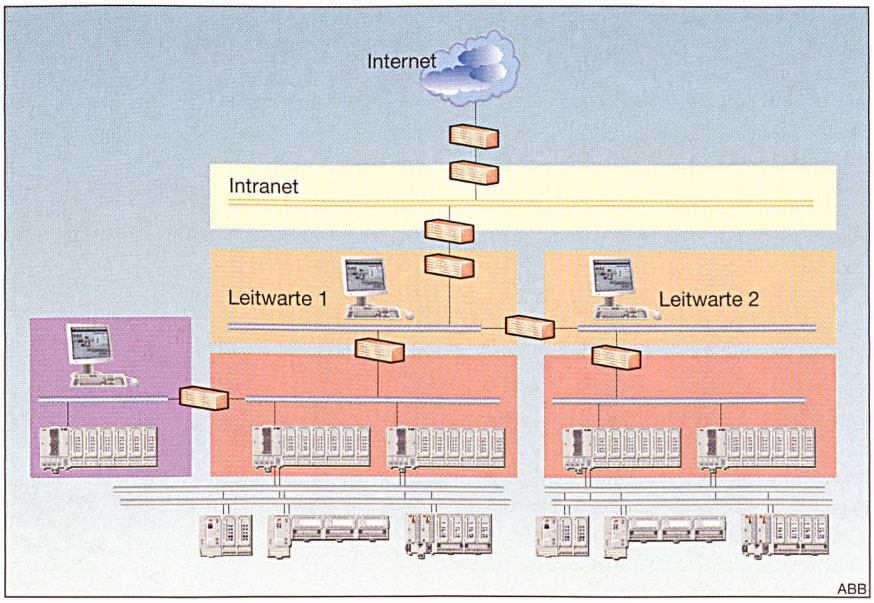

Bild 3 Zonen und Zugriffsrechte zwischen den Zonen

Der Einsatz von Firewalls mit strikten Regelsätzen zwischen den verschiedenen Netzwerken ist ein absolutes Muss, auch zwischen Intranet und Leitsystem. Zusätzlich sollten mehrere Sicherheitszonen definiert werden, die ebenfalls durch Firewalls getrennt sind und Zugriff nur von direkten Nachbarn zulassen. Eine demilitarisierte Zone (DMZ) zwischen Geschäftsnetzwerk und Automatisierungssystem sollte eine Minimalanforderung darstellen, bei höheren Sicherheitsanforderungen sollte die Verwendung unterschiedlicher Firewallprodukte in Betracht gezogen werden, um auch bei zeitweisem Ausfall der Schutzwirkung eines Firewalls durch Fehlkonfiguration oder Entdeckung einer neuen Schwachstelle noch eine Trennung zwischen Automatisierungsnetz und externen Netzen zu erreichen.

Terminalserver-Kaskade

Der interaktive Fernzugriff auf ein Automatisierungssystem, zum Beispiel für die Fehlerdiagnose, verbindet einen Client-Computer mit der Anlage. Der Client-Computer befindet sich dabei ausserhalb des Anlagennetzwerks, und für seine Konfiguration und sein Sicherheitsniveau ist meist eine andere Organisation oder gar Firma verantwortlich. Auch wenn es heute über das recht neue Konzept des Network Access Control (NAC) möglich ist, gewisse Sicherheitsprüfungen auf einem Client-Rechner durchzuführen, bevor die Verbindung vollständig freigegeben wird, so sind diese Verfahren doch noch nicht reif und sicher genug für den industriellen Einsatz.

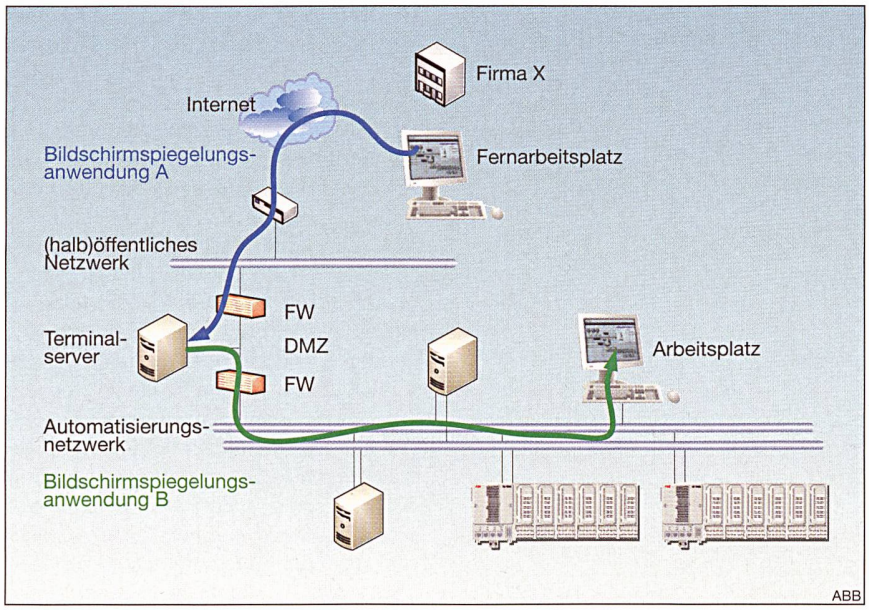

Bild 4 Interaktiver Fernzugriff auf ein Automatisierungssystem mit zwischengeschaltetem Terminalserver

Eine sicherere Lösung ist es, den Client nicht direkt mit dem Automatisierungssystem zu verbinden, sondern in einer DMZ einen weiteren Terminalserver dazwischenzuschalten. Für die Verbindungen zwischen Client und Terminalserver sowie Terminalserver und Automatisierungssystem sollten unterschiedliche Desktop-Mirroring-Anwendungen (z.B. Remote Desktop, PC Anywhere, VNC) verwendet werden. Der Terminalserver-Rechner sollte zudem einzig als Durchgangsstation dienen und keine speziellen Automatisierungsanwendungen ausführen. Dies ermöglicht der IT-Abteilung, den Rechner jeweils auf dem sicherheitstechnisch neuesten Stand (Patching, Antivirus, Host-IDS) zu halten, ohne Rücksicht auf andere Anwendungen nehmen zu müssen.

Die Automatisierungsverantwortlichen haben mit dieser Lösung die Gewähr, dass nur ein einziger externer Rechner mit bekannter und akzeptiert sicherer Konfiguration direkt mit dem Automatisierungssystem verbunden wird.

Datenfluss nur von innen nach aussen

Ziel der vertikalen Vernetzung des Automatisierungssystems ist der Austausch von Daten zwischen der Anlagensteuerung und den geschäftlichen Informationssystemen. In einfachster Form könnte dies realisiert werden, indem Rechner im Firmennetzwerk Befehle und Daten direkt an das Automatisierungssystem schicken. Vom Sicherheitsstandpunkt her gesehen, ist es nicht optimal, solche Datenflüsse zuzulassen. Denn um die Bearbeitung unzulässiger oder bösartiger Befehle und Daten zu verhindern, müssten alle aus der Sicht der Anlage eingehenden Verbindungswünsche auf Anwendungsebene inspiziert werden, bevor sie im Automatisierungssystem weiterverarbeitet werden. Eine solche Filterung ist schwer durchzuführen und zu automatisieren. Darüber hinaus können auch legitime Verbindungsanforderungen in zu grosser Zahl die Verfügbarkeit der Anlagensteuerung gefährden.

Eine sicherere Alternative ist die Zwischenspeicherung externer Anfragen auf einem Rechner in der DMZ. Das Automatisierungssystem kann dann Daten und Befehle von dort abholen, wenn genügend freie Rechenkapazität für die Bearbeitung zur Verfügung steht. Eine noch bessere Isolation erreicht man, wenn das Automatisierungssystem keinerlei Anfragen oder Daten von aussen annimmt, sondern nur in regelmässigen Abständen alle potenziell interessanten Daten vom Leitsystem auf den Zwischenspeicherrechner in der DMZ kopiert.

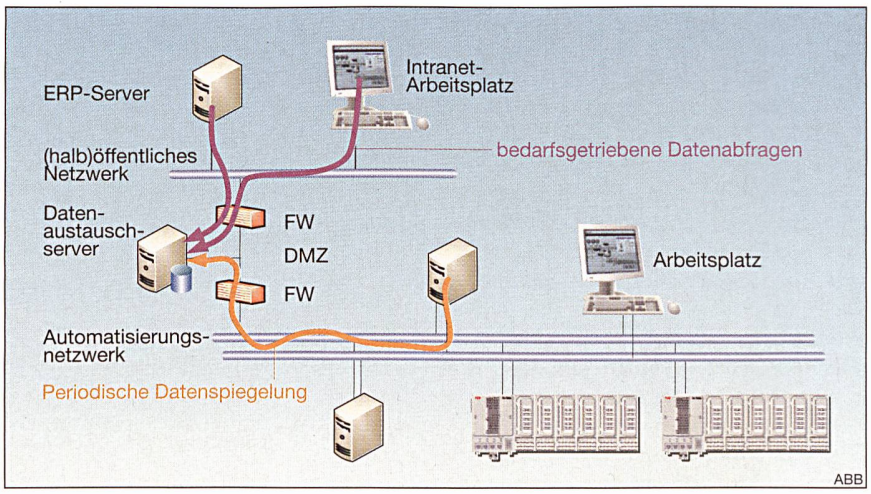

Bild 5 Sichere Datenflussarchitektur zwischen öffentlichen und geschützten Netzen

Prüfung passiver Datenträger

Datenträger wie CDs, DVDs und die verschiedenen Arten von Speicherkarten können Viren und andere Schadsoftware (Malware) von infizierten externen Systemen auf die Automatisierungsrechner übertragen. Eine neue Art von Schadsoftware, deren mögliche negative Konsequenzen den Benutzern oft nicht klar ist, stellen auch die heute von der Musikindustrie immer stärker verwendeten Kopierschutzprogramme (Digital Rights Management, DRM) auf Musikmedien dar. So installierte Ende 2005 Sony beim Abspielen einiger seiner Musik-CDs eine verborgene Anwendung, einen sogenannten Rootkit [1]. Das Benutzen des CD-Laufwerks eines Leitrechners zum Hören von Musik während der Arbeit könnte deshalb fatale Auswirkungen haben. Einerseits könnte sich das so installierte Rootkit negativ auf Automatisierungsanwendungen auswirken, andererseits öffnen Rootkits oftmals neue Einfallswege für andere Angriffe, zum Beispiel wenn sie Netzwerkverbindungen zulassen.

Um Ansteckungen mit Malware jeder Art zu vermeiden, ist ein disziplinierter Umgang mit mobilen Datenträgern notwendig. Das bedeutet, dass Datenträger nur im Rahmen eines genau definierten und von allen Beteiligten befolgten Prozesses in das Automatisierungssystem eingebracht werden dürfen und dass technische Mittel zur Erkennung von infizier-

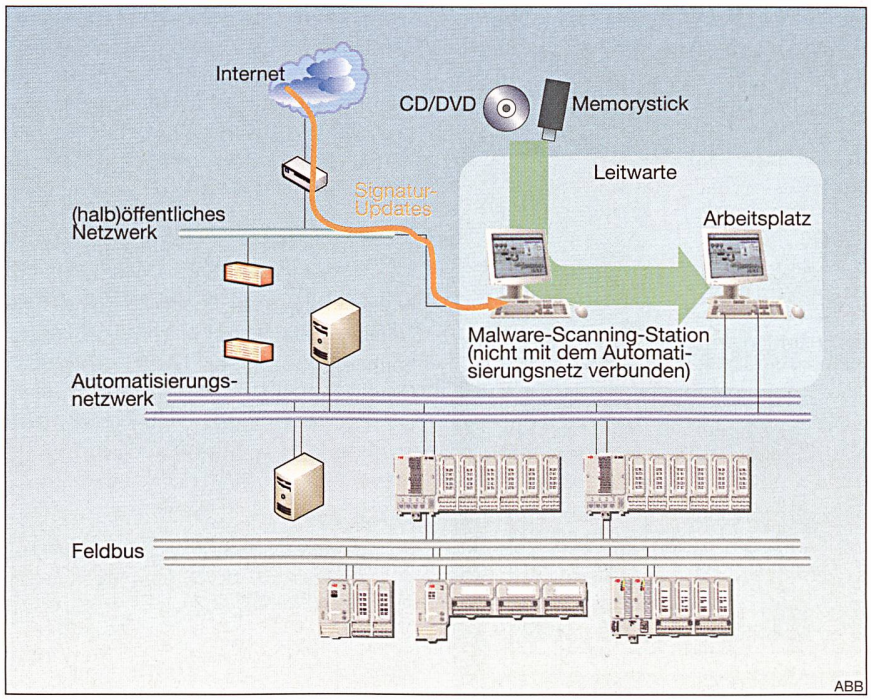

Bild 6 Automatisierungssystem mit Scanning-Station, die an das Intranet/Internet, nicht aber an das Automatisierungsnetzwerk angeschlossen ist

ten Medien zur Verfügung stehen sollten. Teil der Behandlung jedes eingebrachten Datenträgers sollte die eingehende Untersuchung (Scan) mit mehreren Anti-Virus- und Anti-Spyware-Anwendungen sein. Soweit möglich sollte zudem der Inhalt autorisierter Datenträger vom Absender digital signiert werden. Der Empfänger kann dann durch Verifikation der Signatur sicherstellen, dass der Inhalt des Datenträgers nicht verändert wurde. Die Untersuchung des Datenträgers sollte auf einem separaten Rechner erfolgen, der nicht Teil des Automatisierungssystems und auch nicht an dessen Netzwerk angeschlossen ist. Aus Gründen der Usability und um zu verhindern, dass der Scan aus Bequemlichkeit übergangen wird, ist es sinnvoll, den Scanning-Computer in der Nähe der erwarteten Verwendung externer Datenträger, also der Leitwarte oder dem Serverraum, zu platzieren.

Die Einhaltung der Vorschriften kann durch technische Massnahmen wie Schlösser, Demontage der Leseeinheiten oder deren Verriegelung durch entsprechende Software unterstützt werden. Ein perfekter Schutz ist nur durch derartige technische Massnahmen aber nicht zu erreichen. Dies unter anderem auch, weil Schnittstellen wie USB einerseits dem Anschluss von Speichermedien dienen, andererseits für notwendige Peripherieeinheiten wie Maus und Tastatur gebraucht werden.

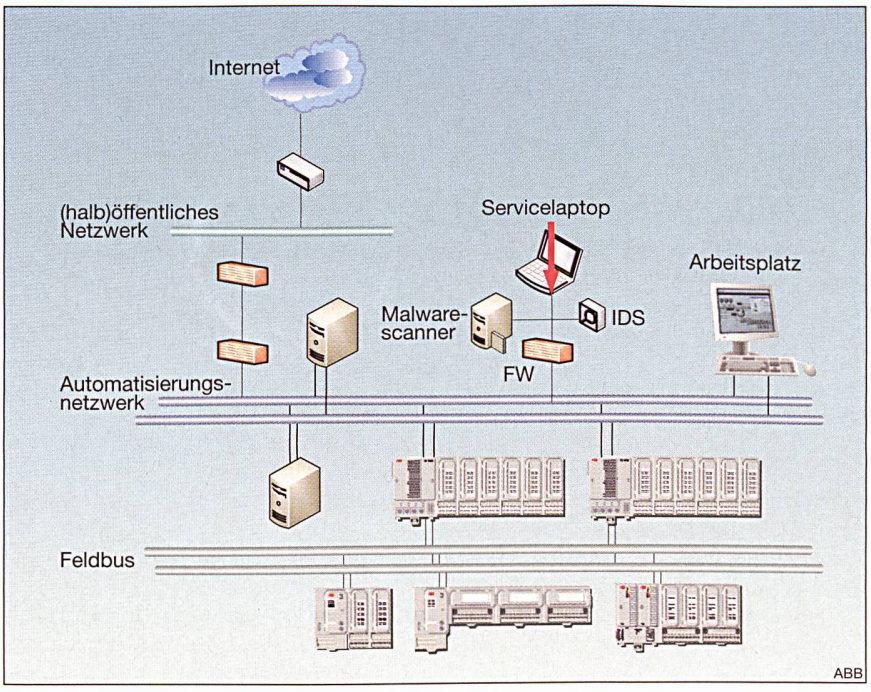

Bild 7 Automatisierungssystem mit Anschlusszone für Servicelaptop

Umgang mit Laptops

Für das Engineering von Automatisierungskomponenten werden vielfach tragbare PCs verwendet. Im Idealfall sollten solche Laptops oder zumindest die Festplatten, die die «Persönlichkeit» des Computers verkörpern, nur innerhalb einer bestimmten Automatisierungsanlage verwendet und nie an andere Netze angeschlossen werden. In der Praxis ist dies selten realistisch, insbesondere wenn Engineering- und Wartungsdienstleistungen von externen Firmen erbracht werden, die mehrere Kunden betreuen. Zusätzlich verwenden Servicetechniker denselben Rechner oftmals für geschäftliche und private Kommunikation und schliessen ihn dazu an die verschiedensten externen Netze an, zum Beispiel im Hotel oder am Flughafen. Ist der Anschluss eines solchen «unreinen» Laptops an das Automatisierungsnetzwerk notwendig, so sollte dies nur an speziellen Anschaltpunkten geschehen. Diese sollten gegenüber dem Automatisierungsnetzwerk mit einem strikt konfigurierten Firewall abgeschottet sein und den Verkehr vom und zum Servicerechner mittels Malware-Scannern und Intrusion-Detection/Protection-Systemen (IDS/IPS) überwachen und für eventuelle spätere forensische Untersuchungen aufzeichnen.

Weitere Sicherheitsmassnahmen im industriellen Umfeld

Bisher wurde in diesem Beitrag beschrieben, wie gängige Sicherheitsmechanismen aus der Büroinformationstechnik verwendet werden können, um die wichtigsten Einfallspfade in ein Automatisierungssystem zu schützen. Diese Beschreibung muss aufgrund des hier gegebenen Raumes naturgemäss recht oberflächlich und pauschal bleiben. Die

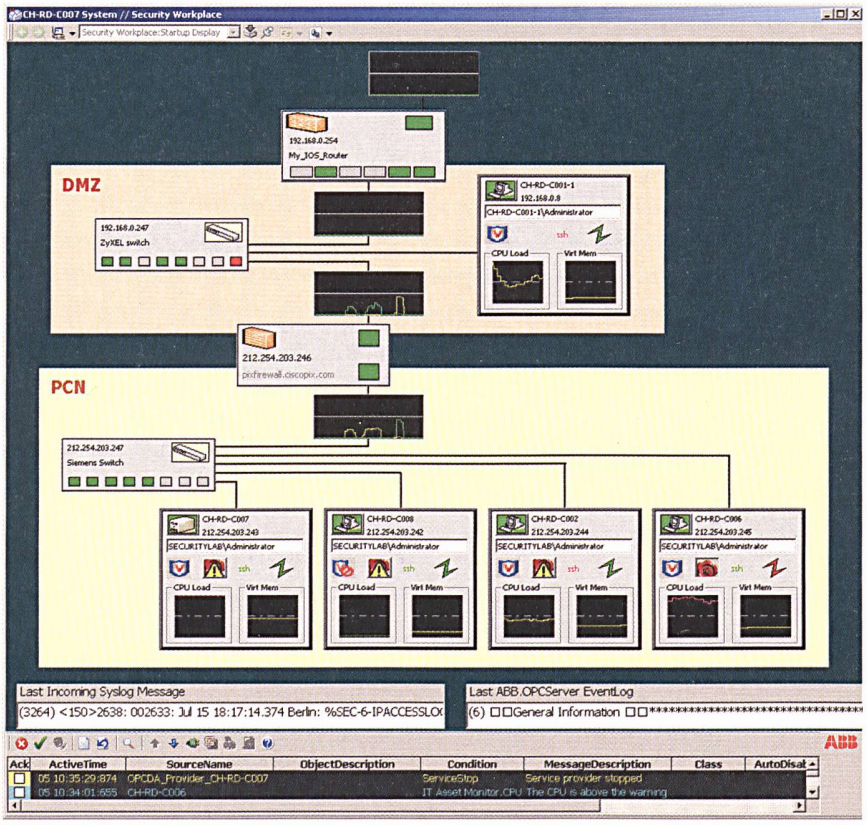

Bild 8 Bildschirmfoto des im ABB-Forschungszentrum entwickelten Prototypen für einen «Security Workplace» als Teil eines Leitsystems

Implementierung und kontinuierliche Pflege der hier genannten Massnahmen kann zwar das Sicherheitsniveau einer Anlage beträchtlich verbessern, dennoch ist für jede Anlage eine genaue Analyse der schützenswerten Güter und der auf sie anwendbaren Schutzziele, eine detaillierte Bedrohungsmodellierung und daraus resultierend eine individuelle Sicherheitsarchitektur wünschenswert. Es gibt inzwischen eine Reihe spezialisierter Beratungsfirmen, nicht zuletzt die Beratungsabteilungen der Automatisierungshersteller, die die Anlagenbetreiber hierbei unterstützen können. Eine VDE-Richtlinie (VDI/VDE 2182) zum systematischen Vorgehen bei der Sicherung einer industriellen Anlage wird zurzeit in Deutschland vom VDE/GMA-Fachausschuss 5.22 erarbeitet und soll noch 2007 verabschiedet werden.

Über die bisher beschriebenen Massnahmen hinaus sind noch weitere, auch automatisierungsspezifische Sicherheitsmassnahmen möglich, die den sicheren Betrieb einer industriellen Anlage erleichtern und den dazu notwendigen Kostenaufwand verringern. Am ABB-Forschungszentrum in Baden wurde zum Beispiel das Konzept eines «Security Workplace» entwickelt, der sicherheitsrelevante Systemparameter innerhalb des Leitsystems in einer dem Prozessbediener vertrauten Form (Prozessbilder, Trendkurven) visualisiert. Dies ermöglicht auch dem Anlagenbedienpersonal, ohne IT-Sicherheitsexpertise möglicherweise sicherheitskritische Anomalien im Systemverhalten frühzeitig zu entdecken und Gegenmassnahmen einzuleiten.

IT-Sicherheit ist wichtig, aber auch machbar

IT-Sicherheit ist heute ein wichtiger Aspekt bei der Auslegung und dem Betrieb von Automatisierungssystemen. Entgegen der insbesondere im nordamerikanischen Raum verbreiteten Panikmache ist es heute sehr wohl möglich, industrielle Anlagen adäquat gegen elektronische Angriffe zu sichern. Die beschriebenen Konzepte können dabei als Ausgangspunkt dienen. Jeder Anlagenbetreiber muss sich jedoch bewusst sein, dass sein Automatisierungssystem nur dann sicher bleibt, wenn über die anfängliche Investition in Sicherheitshard- und -software auch während des Betriebs kontinuierlich personelle und finanzielle Ressourcen für Betrieb und Anpassung der Sicherheitsmassnahmen bereitgestellt werden.

Referenzen

[1] Sony BMGs Kopierschutz mit Rootkit-Funktionen, Heise News 11/2005, http://www.heise.de/newsticker/meldung/65602.

Weiterführende Literatur

D. Dzung, M. Naedele, T. von Hoff, M. Crevatin: Security for industrial communication systems, Proceedings of the IEEE, Vol. 93 (6), Juni 2005, S. 1152–1177.

M. Naedele, R. Vahldieck: Malware protection for industrial automation systems, ABB Review 3/2005, S. 74–78.

M. Naedele: Addressing IT Security for Critical Control Systems, 40th Hawaii Int. Conf. on System Sciences (HICSS-40), Hawaii, Januar 2007.

Angaben zu den Autoren

Dr. **Markus Brändle** (GSEC) arbeitet am ABB-Forschungszentrum in Baden als Scientist im Team für Softwarearchitektur und ist verantwortlich für Forschungsaktivitäten zur IT-Sicherheit in Automatisierungssystemen für die Energieübertragung und -verteilung. Dr. Brändle ist aktives Mitglied von ISA-SP99.
ABB Schweiz AG, 5405 Baden,
markus.braendle@ch.abb.com

Dr. **Martin Naedele** (GSNA, GCFW) arbeitet am ABB-Forschungszentrum in Baden als Senior Principal Scientist im Bereich Softwarearchitektur und koordiniert die ABB-Forschung zur IT-Sicherheit für industrielle Systeme weltweit. Dr. Naedele beschäftigt sich seit mehr als 10 Jahren mit Sicherheitsfragen in der Informationstechnik und ist in mehreren internationalen Normungsgremien und Fachausschüssen aktiv.
ABB Schweiz AG, 5405 Baden,
martin.naedele@ch.abb.com

Résumé

Protection des installations d'automatisation contre les attaques

Des mesures pragmatiques contre les attaques électroniques. Qu'il s'agisse de l'ordinateur portable du service externe, d'un stick mémoire USB ou de l'accès à distance par internet: les installations modernes d'automatisation sont de plus en plus intégrés à leur environnement et de ce fait exposés à leurs virus et attaques, bien connus du monde bureautique. Aussi ces installations doivent-elles être protégées, comme les réseaux de bureau, par des pare-feu, scanners à virus et zones démilitarisées.