ECKHARD EBERLE:
„Durch eine steigende Vernetzung ist die Anzahl der Schnittstellen gewachsen, die potenzielle Angriffspunkte bieten. Anwender und Hersteller müssen nun gemeinsam dafür Sorge tragen, dass daraus kein Schaden entsteht", fordert der CEO Industrial Automation Systems der Siemens-Division Industry Automation.

„Viele Anlagen sind nur unzureichend geschützt“

Eckard Eberle im Interview mit atp edition

Automatisierungsanlagen werden immer stärker vernetzt. Und mit dem Trend zu offenen Systemen haben Standard-Technologien aus der Bürowelt Einzug gehalten – das schafft neue Einfallstore für Angriffe auf die IT. atp edition sprach darüber mit mit Eckard Eberle, CEO Industrial Automation Systems, Siemens-Division Industry Automation. Der Informationssicherheit widmen sich auch alle Hauptbeiträge dieser Ausgabe der atp edition.

atp: Herr Eberle, wo steht die IT-Security für die Automatisierungstechnik heute? Wie gut geschützt sind die Anlagen?
ECKARD EBERLE: IT-Security in der Automatisierung hat in den letzten zwei Jahren enorm an Bedeutung gewonnen. In der Pre-Stuxnet-Ära war IT-Security bei dem Großteil unserer Kunden hauptsächlich in der Office-Welt ein Thema. Im Vordergrund stand dort ganz klar die Datensicherheit. Seit Stuxnet wissen wir, dass auch industrielle Automatisierungsnetze Ziel von Angriffen sein können. Aus unserer Sicht sind noch viele Anlagen unzureichend geschützt. Viel zu oft wird den potenziellen Bedrohungen auf Anwenderseite nicht die notwendige Aufmerksamkeit gewidmet. Wir spüren aber ganz klar, dass dieses Thema für Anwender und Hersteller immer wichtiger wird.

atp: Worüber reden wir, wenn wir heute von Industrial Security in der Prozess- oder Fertigungsautomatisierung sprechen – wie lautet Ihre Definition?
ECKARD EBERLE: Industrial Security in der Prozess- oder Fertigungsautomatisierung umfasst alle – einschließlich datentechnischer – Maßnahmen, die Manipulation von Abläufen in Prozessen der Industrie und Infrastruktur sowie den Verlust des geistigen Eigentums verhindern sowie Schäden an Umwelt, Reputation und Finanzen vermeiden helfen sollen. Dabei kann niemand 100-prozentige Sicherheit garantieren. Industrial Security muss als Prozess gelebt und als Management-Aufgabe verstanden werden.

atp: Wo liegen die größten Herausforderungen?
ECKARD EBERLE: Industrieanlagenbetreiber wurden 2010 vom Stuxnet-Angriff überrascht. Die wenigsten Anlagenbetreiber hatten es bis zu diesem Zeitpunkt für möglich gehalten, dass industrielle Anlagen durch gezielte Angriffe über Datennetze attackiert werden. Noch ist es eine große Herausforderung, dafür ein Bewusstsein zu schaffen und die Notwendigkeit von Schutzmechanismen überall zu verankern. Denn oft geschieht solch ein Angriff unbemerkt und das konkrete Schadensausmaß ist nicht direkt erkennbar.

atp: Geht es eher um Hardware, um Software oder um die Psychologie der Anwender?
ECKARD EBERLE: Es geht um alle drei Faktoren. Industrial Security darf nicht mit einem Produkt oder gar einem Tool verwechselt werden, das einfach per Katalog gekauft werden kann. Genauso wenig reichen umfangreiche Listen von Vorschriften aus, die für sich genommen zwar alle richtig und gut sind, aber erst dann wirken, wenn diese auch gelebt werden.

atp: Können Sie dafür ein Beispiel nennen?
ECKARD EBERLE: Ein hochentwickeltes Sicherheitskonzept ist machtlos, wenn ein Mitarbeiter einen USB-Stick am Netz anschließt und dieses infiziert. In einem solchen Fall können Hard- und Software-Mechanismen die Ausbreitung eines etwaigen Virus zwar eindämmen, aber nicht verhindern. Nur eine umfassende Security-Strategie hilft, präventiv Angriffen entgegen zu wirken. Hier stehen Richtlinien und Schulungen der Mitarbeiter an erster Stelle. Dieses Vorgehen ist sehr effizient, und es lässt sich schon viel mit geregelten Prozessen und Richtlinien erreichen.

atp: Existiert bereits eine allgemein anerkannte und verbindliche Definition der Schutzziele?
ECKARD EBERLE: Sicherlich gibt es allgemeine Schutzziele wie in der ISA 99 beschrieben oder allgemein die Verhinderung von Umweltschäden und der Gefahr für Leib und Leben oder des Verlusts von geistigem Eigentum. Doch im Kern muss man sich darum bemühen, dass kein unkontrollierter Zugriff auf Anlagen und Produktionsprozesse möglich ist. Gerade in diesem Bereich haben wir in den letzten Jahren im Bereich Safety-Automatisierung viele Erfahrungen gemacht, die wir auf den Security-Bereich übertragen können.

atp: Immer komplexere Produkte und Produktionskonstellationen erfordern eine immer weiter gehende Vernetzung mit immer neuen Schnittstellen, die wiederum potenzielle Einfallstore für Angreifer sind. Wie lässt sich diese Gefahr bannen?
ECKARD EBERLE: Diese Gefahren lassen sich durch Security-Strategien reduzieren. Das fängt bei der Systemhärtung an, wobei zum Beispiel ungenutzte USB-Ports abgeschaltet werden oder LAN-Anschlüsse hardwareseitig blockiert werden. Dies führt weiter über eine konsequente Umsetzung von Sicherheitsmaßnahmen, etwa der Netzwerksegmentierung und dem Aufbau sicherer Auto-

Bilder: Siemens

matisierungszellen, hin zu Einzelmaßnahmen wie Anti-Virus-Programmen und Whitelisting-Software auf PC-basierten Systemen oder auch zu definierten Security-Richtlinien für die Mitarbeiter. Die Hersteller sind natürlich angehalten, immer effizientere Sicherheitsfunktionen in ihren Produkten zu integrieren. Wir arbeiten stetig an der kontinuierlichen Verbesserung unserer Produkte im Bereich der Industrial Security.

atp: Eine absolute Abschottung scheint oft unmöglich; zwischen der Produktion und der Außenwelt kann man zwar Schleusen aufbauen – aber irgendwann muss doch ein Mitarbeiter mit Laptop oder Datenträger Kontakt zur Produktionssteuerung aufbauen. Wie lässt sich ausschließen, dass auf diesem Weg Angriffe erfolgen?
ECKARD EBERLE: Es gibt Verfahren, um Systeme zu härten und somit dieser Art von Angriffen zu begegnen. So lässt sich zum Beispiel die Kommunikation zwischen HMI/Steuerung und Engineering-Station mit einem Passwort absichern. Ebenso lassen sich die Bausteine im PLC-Programm vor unautorisiertem Zugriff schützen. Will ein Service-Mitarbeiter aus der Ferne auf die Anlage zugreifen, steht ein sicherer VPN-Tunnel einschließlich Passwortabfrage bereit.
Wenn ein Mitarbeiter – etwa in einem Servicefall – per Laptop oder Datenträger an die Anlage muss, sollte gewährleistet sein, dass sowohl auf PC-Systemen wie auch auf Servicegeräten ein entsprechender Virenschutz vorhanden ist.

atp: Zunehmend werden unternehmensweite Systeme wie ERP mit der Produktionsebene vernetzt. Wie lässt sich das unter Security-Aspekten verantworten?
ECKARD EBERLE: Systeme wie ERP oder DCS lassen sich einfach in ein Sicherheitskonzept integrieren. Gerade bei ERP-Systemen kann man auf das breite Angebot der IT-Sicherheit zurückgreifen und auf Basis Front und Back Firewall mit einer DMZ (demilitarised Zone) für umfassenden Schutz sorgen. Die einzelnen Zonen des Netzwerkes können auf diese Weise voneinander getrennt werden, was die Sicherheit wesentlich erhöht.

atp: Auch unter dem Dach der digitalen Fabrik soll eine zunehmende Vernetzung und Datendurchgängigkeit realisiert werden – lässt sich das sicherheitstechnisch beherrschen?
ECKARD EBERLE: Die Beherrschung der digitalen Fabrik unter Sicherheitsgesichtspunkten ist machbar, wie wir beispielhaft in unserem Werk in Amberg zeigen. Es wird sicher noch einige Jahre in Anspruch nehmen, bis dieser visionäre Ansatz flächendeckend anzutreffen ist. Wir untersuchen dort das Zusammenspiel von digitalem Engineering und Produktion seit einiger Zeit sehr erfolgreich. Sicherheitstechnisch lässt sich ein hochkomplexes Gebilde nur durch konsequente Umsetzung von übergreifenden Security-Maßnahmen beherrschen. Das heißt: Hersteller und Anwender müssen effizient zusammenarbeiten. Gerade auf Anwenderseite ist eine Kooperation von IT und Automatisierung sehr wichtig.

atp: Schaffen der Einsatz von Wireless-Technologien und von immer mehr mobilen Endgeräten neue Risiken?
ECKARD EBERLE: Wir empfehlen unseren Kunden, auf industriell erprobte Lösungen zurück zugreifen, wenn eine mobile Lösung gewünscht ist. Diese lassen etwa die Bedienung einer Maschine nicht zu, wenn sich das Endgerät außerhalb des definierten Bedienbereichs befindet. Wireless-Technologien an sich bieten eine ausreichende Sicherheit, da aktuelle Verschlüsselungsmechanismen nutzbar sind.

atp: Wer ist für ausreichende IT-Security verantwortlich: der Hersteller oder der Anwender?
ECKARD EBERLE: Für eine ausreichende Sicherheit können nur beide Parteien gemeinsam sorgen. Auf der einen Seite steht der Hersteller, der mit seinen Produkten die Grundlage für die Umsetzung einer konsequenten Sicherheitsstrategie schafft. Auf der anderen Seite steht der Anwender, der durch den konsequenten Einsatz der Produkte sowie ihrer Sicherheitsfunktionen und die Umsetzung von Sicherheitsrichtlinien ein umfassendes Konzept erstellen kann. Eine 100-prozentige Sicherheit ist allerdings nicht realisierbar. Sicherheit ist ein Prozess, der, einmal eingeführt, einer kontinuierlichen Überwachung und Erneuerung bedarf. Wir helfen unseren Kunden dabei mit Dienstleistungen im Security-Umfeld wie dem Security Assessment, um Sicherheitsrisiken und Strategien zusammen mit dem Kunden zu definieren und zu implementieren.

atp: Welche Managementebene beim Anwender sollte aus Sicht eines Herstellers das Thema IT-Security verantworten, um die besten Erfolge zu erzielen?
ECKARD EBERLE: Nach unserer Auffassung liegt die Aufgabe, für das Bewusstsein des Themas Industrial Security in einem Unternehmen zu sorgen, in der obersten Managementebene. Die Erfahrung zeigt, dass sich IT-Abteilung und Automatisierungsabteilung im Bereich Security nicht immer einig sind. Bei IT-Security innerhalb der Prozess- und Fertigungsindustrie gelten verschärfte Anforderungen an die jeweilige Lösung. Während in der Office-IT-Security die Datensicherheit im Vordergrund steht, besitzt in der Industrial Security die Verfügbarkeit der Anlage die höchste Priorität. Es ist Aufgabe des oberen Managements, diese Differenzen im Vorfeld auszuräumen.

atp: Wie verhalten sich funktionale Sicherheit und IT-Security zu einander: ergänzen sie sich, bedingen sie sich, behindern sie sich ...?
ECKARD EBERLE: Ganz klar: Funktionale Sicherheit und IT-Security ergänzen sich. IT-Security schützt gegen Cyber-Angriffe auf das Automatisierungssystem. Funktionale Sicherheit kann hier bis zu einem gewissen Maße auch hilfreich sein, dient aber in erster Linie zur Absicherung gegen zufällige Fehler im System.

atp: Es existiert ein „Dschungel" domänenspezifischer Standards für IT-Security in der Automatisierung.

Reichen diese aus? Sind es zu viele? Besteht Harmonisierungsbedarf?

ECKARD EBERLE: Aus heutiger Sicht existieren noch viele verschiedene Standards. Bislang gibt es noch keine international gültige Norm. Daher versuchen Hersteller zusammen mit unabhängigen Partnern, wie den CERT-Organisationen, deren Entwicklung und Harmonisierung weiter voran zu treiben.

atp: Standardisierung erlaubt einerseits, Systeme mit höherer Sicherheit zu entwickeln, weil mehr Unternehmen Know-how einbringen. Das erhöht zwar den Aufwand für potenzielle Angreifer – aber wenn ein Angreifer die Systeme „geknackt" hat, gewinnt er direkt Zugang zu allen Unternehmen, die diese Technologie einsetzen. Schafft die Standardisierung also größere Sicherheit oder größere Gefahren?

ECKARD EBERLE: Gemeinsam mit den Anwendern haben die Hersteller von Automatisierungsprodukten die Offenheit ihrer Systeme vorangetrieben. Dies war auch immer wieder von den Anwendern gefordert worden, um mit offenen Systemen Produktivität zu erhöhen. Standard-Technologien aus der Bürowelt, wie Microsoft-Technologien, Internet-Kommunikation oder Ethernet-Kommunikationsnetze, haben daher Einzug in die automatisierte Industrieproduktion und Infrastruktur gehalten. Durch eine steigende Vernetzung ist die Anzahl der Schnittstellen gewachsen, die potenzielle Angriffspunkte bieten. Anwender und Hersteller müssen nun gemeinsam dafür Sorge tragen, dass daraus kein Schaden entsteht.

„SICHERHEIT IST EIN PROZESS, der, einmal eingeführt, einer kontinuierlichen Überwachung und Erneuerung bedarf", hebt Eckard Eberle hervor.

atp: Kann die Security in der Automatisierung von den Sicherheitsbemühungen der nichtindustriellen IT profitieren?

ECKARD EBERLE: Bei der Standardisierung von IT-Komponenten spielen auch die Sicherheitsexperten, die sich zunehmend dem Industrieautomatisierungsumfeld widmen, eine nicht zu unterschätzende Rolle. Meist aus dem IT-Umfeld stammend, tragen sie mit ihren Analysen dazu bei, dass die Automatisierungshersteller ihre Produkte hinsichtlich IT-Verwundbarkeiten optimieren können. Für Siemens ist das Thema wichtig und wir nehmen die Hinweise dieser Experten sehr ernst. Wir veröffentlichen regelmäßig Updates und arbeiten stetig an der kontinuierlichen Verbesserung unserer Produkte in diesem Bereich.

atp: Was erwarten Sie von Microsoft mit Blick auf IT-Security? Wird dieses Betriebssystem angesichts der Bedrohungen auch künftig eine Rolle in der Automatisierung spielen?

ECKARD EBERLE: Microsoft hat gerade in den letzten Jahren einiges im Bereich Security geleistet. Wir sehen Microsoft auch in Zukunft als starken Partner in der Automatisierung. Die Erfahrung zeigt, dass eine kooperative Partnerschaft auf diesem Gebiet Früchte trägt.

Die Fragen stellten Leon Urbas und Gerd Scholz