Cyber-Bedrohung für Prozessanlagen

Kommunikation braucht Security – Security braucht Kommunikation

Die Fabrik der Zukunft vernetzt die intelligenten Systeme des gesamten Unternehmens untereinander sowie nach innen und außen mit dem Ziel, möglichst viele Informationen digital nutzbar zu machen. Das beginnt bei den Maschinen, Sensoren und Feldgeräte in den Produktionsanlagen, geht über Enterprise-Resource-Planning (ERP), Marketing, Vertrieb und Einkauf entlang der Wertschöpfungskette bis zu den IT-Systeme der Lieferanten, Kunden und Servicepartner.

Dieser Entwicklung zur „Industrie 4.0“ wird sich kaum ein Unternehmen entziehen können, denn die zu erreichenden Effizienz- und Effektivitätssteigerungen müssen genutzt werden, wenn das Unternehmen nicht seine Wettbewerbsfähigkeit verlieren will. Die durch die Informationstechnik beschleunigte Globalisierung treibt ohne Frage den Wettbewerb um Ressourcen, Märkte und politische Einflussbereiche voran.

Es wäre aber naiv anzunehmen, die neu gewonnenen digital vernetzten Technologien würden nicht auch für Auseinandersetzungen in der Wirtschaft, Gesellschaft und Politik ausgenutzt werden. Im Gegenteil ist zu beobachten, dass Wirtschaft und Verwaltung zunehmend von sehr versierten IT-Angriffen betroffen sind, die mit großem Ressourceneinsatz und großer Professionalität ausgeführt werden.

Cyber Security muss systematisch in Steuerungen und Softwarelösungen hinein entwickelt werden.

Dr. Alexander Horch, HIMA

Sprengstoffgürtel ade

Cyber-Angriffe auf Unternehmen, Verwaltungen und Privatnutzer kommen jeden Tag vor. Solche Angriffe sind meist nur schwer zu erkennen und abzuwehren. Deshalb verlaufen viele Angriffe erfolgreich: Die Angreifer werden zum einen immer professioneller und treffen zum anderen auf Rahmenbedingungen, die sie zu ihrem Vorteil zu nutzen wissen.

Für erfolgreiche Cyber-Angriffe braucht man heute vielfach nicht mehr als einen PC und einen Internetanschluss. Diesen eher kleinen Investitionen stehen die vielfältigen Möglichkeiten gegenüber, durch kriminelle Handlungen Geld zu verdienen, vertrauliche Informationen zu erlangen oder Sabotageakte durchzuführen.

Entsprechende Angriffswerkzeuge und -methoden sind einfach und kostengünstig verfügbar. Es existiert ein funktionierender globaler Markt, auf dem Schadsoftware eingekauft oder als Dienstleistung beauftragt werden kann. Sowohl gut organisierte Gruppen als auch Einzelpersonen bieten auf diesen kriminellen Online-Marktplätzen ihre Fähigkeiten und Dienstleistungen an.

Die besonderen Randbedingungen des Internets machen es als Angriffsplattform besonders attraktiv. Die Vernetzung von Informationstechnik ermöglicht Angriffe aus der Distanz von nahezu jedem Ort der Welt und zu jedem Zeitpunkt auf immer mehr Ziele. Ein Angreifer muss sich dadurch keinen unmittelbaren Risiken vor Ort aussetzen. Das dezentral und offen gestaltete Internet bietet ihm zugleich vielfältige Tarnungsmöglichkeiten, die das Risiko, entdeckt zu werden, gering machen. Zudem erschweren Unterschiede in den nationalen Regularien die Maßnahmen der Strafverfolgung. Dadurch erschließen sich insbesondere auch terroristischen Attacken neue gefahrbringende Möglichkeiten.

Die zunehmende Komplexität der Technik und oftmals fehlendes Sicherheitsbewusstsein führen oft zu unzureichend abgesicherten Systemen und erhöhen damit die Erfolgsaussichten für Cyber-Angriffe. Darüber hinaus erleichtert der oft sorglose Informationsaustausch über das Internet im privaten Bereich, der „Always-On“-Status mobiler Systeme und der Trend zu BYOD – „Bring your own Device“ in die Arbeitswelt den Zugriff auf schützenswerte Firmeninformationen.

Der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT Sicherheit in Deutschland zeigt eindringlich viele der Risiken und tatsächlich erfolgte schwerwiegende Attacken im industriellen Bereich sowie Lösungsansätze auf.

Cyber Security im Fokus

Bei diesen Randbedingungen lag es nahe, dass sich im Programm des von VDI/VDE GMA, NAMUR und ZVEI fachlich getragenen Kongresses „Automation 2016“ in Baden-Baden unter dem Motto „Secure & reliable in the digital world“ eine Vielzahl der Vorträge der Cyber Security widmete: Die visionären Möglichkeiten der umfassenden Vernetzung bergen eben auch Sicherheitsrisiken.

Weitgehender Konsens besteht darin, dass die Schutzziele in der Automatisierungstechnik grundsätzlich die gleichen sind, die auch für klassische IT-Systeme gelten, dass jedoch die Bewertung deutlich unterschiedlich ist. Diese Schutzziele im Einzelnen sind

- Verfügbarkeit: Daten und Funktionen des Systems können zum definierten Zeitpunkt genutzt werden;
- Integrität: Daten und Funktionen des Systems können nicht unbemerkt durch Unberechtigte manipuliert werden;
- Vertraulichkeit: Unberechtigte können nicht auf Daten und Funktionen des Systems lesend zugreifen;
- Authentizität: Sicherstellung der eindeutigen Identifizierbarkeit von Personen und Systemen sowie der Herkunft der übertragenen Daten;
- Nicht-Abstreitbarkeit: Beweisbarkeit, dass die Erzeugung bzw. der Erhalt von Informationen (und Auslösung einer Aktion) durch eine Person erfolgte;
- Überprüfbarkeit: Eindeutige Nachvollziehbarkeit der Aktionen bis zu ihrem Ursprung.

Für Systeme der industriellen Automatisierung stehen Verfügbarkeit und Integrität unter Echtzeit-Bedingungen an erster Stelle, während im Controlling, der Forschung oder im HR-Bereich in der Regel die Vertraulichkeit die höchste Priorität hat.

Je nach Anwendung kann jedoch auch in den industriellen Anlagen der Schutz der Vertraulichkeit zu einem wichtigen Ziel werden. In besonderen Fällen, wie z.B. dem Einsatz in der pharmazeutischen Produktion, spielen auch Nicht-Abstreitbarkeit, Authentizität und Überprüfbarkeit eine große Rolle.

Echtzeit und Security

Produktionsanlagen erfordern die permanente Verfügbarkeit aller relevanten Messdaten in Echtzeit, also unter deterministischen Bedingungen. Je nach Prozess kann die zulässige Latenzzeit zwischen wenigen Mikrosekunden (z.B. in einer Verpackungsmaschine für Pharmaprodukte) bis zu einigen Sekunden (z.B. für die Temperaturregelung in einem großen Reaktor) liegen. Dementsprechend steht für die Datenübertragung und evtl. notwendige Verschlüsselungen mehr oder weniger viel Zeit zur Verfügung.

Auch wenn die neue Welt der digitalen Automation dynamisch, lose gekoppelt und flexibel erscheint, um auf alle Anforderungen reagieren zu können, erfordert doch die Realität einen differenzierten Umgang. Darauf wies Prof. Jörg Wollert, FH Aachen, Embedded Systems und Mechatronik in seinem Vortrag auf der Automation 2016 hin: Eine Steigerung der Leistung von Anlagen ist nur mit hohen und höchsten Reaktionszeiten der Automatisierungssysteme zu meistern. Im Gegenzug erfordert die Anbindung an die IT-Welt Sicherheitskonzepte nach dem Stand der Technik. Die Reaktion auf Nachrichten innerhalb weniger Mikrosekunden ist technisch realisierbar, aber nicht gleichzeitig mit einer effektiven Verschlüsselung.

Echtzeit und Security sind also divergierende Anforderungen in der Automatisierungstechnik. Unter den Randbedingungen von Industrie 4.0 ist sowohl die Abstraktion von Industrie 4.0-Komponenten für einen standardisierten Informationsaustausch als auch eine sichere Echtzeit-Kommunikation für höchste Qualität und kürzeste Bearbeitungszeiten zwingend notwendig. Aktuell ist das nur mit einem hierarchischen Konzept zu lösen. Verschärft werden diese Herausforderungen durch die hohen Anforderungen an die Datensicherheit.

Products, People und Processes müssen miteinander in Gleichklang gebracht werden.

Erwin Kruschitz, Anapur

Safety und Security

Hat man vor gut 10 Jahren – also in der Phase, in der die Bedeutung der Cyber Security in der Automatisierung selbst Fachleuten noch ins Bewusstsein gerückt werden musste – sich mit Cyber Security noch deutlich von Functional Safety differenziert, so weiß man heute, dass Safety ohne Security nicht möglich ist. Insbesondere für sicherheitsgerichtete Systeme spielt Security eine ganz zentrale Rolle, da diese die letzte Front vor einer möglichen Katastrophe darstellen. Entsprechend äußert sich auch Dr. Alexander Horch, Entwicklungsleiter bei HIMA: „Für wirkungsvolle Cyber Security in der Prozessindustrie reicht es nicht aus, ein vorhandenes Produkt im Nachhinein durch zusätzliche Software-Funktionalität zu verbessern. Jede Lösung zur funktionalen Sicherheit muss von Beginn an im Sinne der Cyber Security durchdacht und entworfen werden.“

Zum Erreichen von SIL 3-Levels in der Funktionalen Sicherheit müssen Hardware und Software normenkonform aufwändig zertifiziert werden. Regelmäßige Änderungen und Updates wie bei PC-Anwendungen wären hier nicht realistisch. Dazu meint Horch: „Die jahrzehntelange Erfahrung als Safety-Spezialist in der Prozessindustrie hilft uns, die entsprechenden Normen effizient in Technologie umzusetzen und Cybersecurity

▶ Fortsetzung auf **Seite 19**

Zertifiziertes „Defense in Depth“-Schutzkonzept

Um Industrieanlagen umfassend vor Cyber-Angriffen von innen und außen zu schützen, muss auf allen Ebenen gleichzeitig angesetzt werden – von der Betriebs- bis zur Feldebene, von der Zutrittskontrolle bis zum Kopierschutz. Zu diesem Zweck setzt Siemens auf die tiefengestaffelte Verteidigung – „Defense in Depth“ – als übergreifendes Schutzkonzept, nach den Empfehlungen der IEC 62443 Normenreihe, dem führenden Standard für Security in der industriellen Automatisierung.

Dazu hat Siemens jetzt als erstes Unternehmen eine auf IEC 62443-4-1 basierende TÜV Süd-Zertifizierung für den übergreifenden Entwicklungsprozess von Produkten der Automatisierungs- und Antriebstechnik, einschließlich der Industriesoftware, an sieben Entwicklungsstandorten in Deutschland erhalten. An diesen Standorten werden unter anderem Simatic S7-Industriesteuerungen, Industrie-PCs, HMI Geräte zum Bedienen und Beobachten und Sinamics-Antriebe bis zur Engineering-Software TIA (Totally Integrated Automation)-Portal entwickelt.

Die internationale Normenreihe IEC 62443 legt die Security Maßnahmen für industrielle Automatisierungssysteme fest, wobei Teil 4-1 der Norm die Anforderungen an den Entwicklungsprozess des Herstellers beschreibt. Das TÜV Süd-Zertifikat basiert auf dem Standard IEC 62443-4-1 (Secure Product Development Lifecycle Requirements, Draft 3 Edition 10, 01.2016) mit Security-relevanten Aspekten wie Fähigkeiten und Expertise, Sicherheit von Komponenten Dritter, Prozess- und Qualitätssicherung, sichere Architektur und sicheres Design, Schwachstellen-Handhabung bis zum Sicherheits-Update-, -Patch- und -Änderungs-Management.

Als führender Automatisierungs- und Software-Anbieter für die Industrie verbessert Siemens kontinuierlich seine Produkte und Lösungen hinsichtlich industrieller Sicherheit. Hierzu gehört auch die auf IEC 62443-4-1-basierte Zertifizierung.

Mit dieser Zertifizierung dokumentiert Siemens seinen „Security by Design“-Ansatz für Automatisierungsprodukte und bietet Integratoren und Betreiber transparenten Einblick in die IT-Security-Maßnahmen für die Konzeption und den Betrieb von Automatisierungsprozessen und -anlagen mit „Defense in Depth“-Schutzkonzept. (vo) ■

◀ Fortsetzung von **Seite 18**

systematisch in unsere Steuerungen und Softwarelösungen hinein zu entwickeln.“ Deshalb sind die HIMA-Lösungen so konzipiert, dass sie nicht gepatcht werden müssen. Firmware und Applikationssoftware sind nicht öffentlich und beruhen zu 100 % auf firmeninternen Entwicklungen, bei denen Funktionalitäten der Cybersecurity gezielt berücksichtigt wurden. Standard-Software, die bekannte (und unbekannte) Sicherheitslücken aufweist, wird nicht verwendet. Dies ist ein signifikanter Unterschied zu allgemeingültigen Prozessleitsystemen.

Für Hochrisikoanwendungen wie Notabschaltsysteme auf Bohrinseln oder Hochdrucküberwachungen geht es aber auch ganz ohne Software: Bei bestimmten Sicherheitssteuerungen für die höchste Sicherheitsstufe nach IEC 61508 (SIL 4) wird die Sicherheitslogik durch feste Verdrahtung programmiert und funktioniert komplett softwarefrei. Damit ist eine Kompromittierung durch Cyber-Angriffe schlichtweg nicht möglich. Festverdrahtete Sicherheitssteuerungen sind heute aber nur in speziellen Anwendungen ökonomisch sinnvoll, da Engineering und Flexibilität mit programmierbaren Systemen deutlich effizienter sind.

Fit für Security

Das magische Dreieck zum Sicherstellen eines zufriedenstellenden Security Ergebnisses wird oft durch die drei ‚P‘ symbolisiert: „Products“, „People“ und „Processes“ müssen miteinander in Gleichklang gebracht werden.

Produkte für Industrie 4.0 und die digital vernetzte Welt müssen „secure by design“ und „secure by default“ sein, betont Erwin Kruschitz, Vorstand von Anapur und Mitglied des NAMUR AK 4.18: „Damit ist gemeint, dass ein Anwender bereits „nach dem Auspacken“ ein Produkt in Händen halten soll, das sicher ist und nicht erst durch weitere Maßnahmen

Cybersicherheit erfordert nachhaltige Aktivitäten über den gesamten Lebenszyklus der Anlage.

Konstantin Rogalas, Honeywell Industrial Cyber Security

sicher gemacht werden muss. Dies wird so auch in der NAMUR Empfehlung NE153 „Automation Security 2020“ manifestiert.“

Die Zusammenarbeit von Personen, Abteilungen und Organisationen ist laut Kruschitz bei einem Querschnittsthema wie der Cyber Security der Erfolgsfaktor Nummer 1. Die Arbeitsergebnisse des NAMUR AK 4.18 wurden deshalb auch gemeinsam mit dem BSI und dem ZVEI Fachverband Automation erstellt und abgestimmt. Durch die Mitarbeit bei der ISA99/IEC62443 erfolgt die Abstimmung mit internationalen Normungsgremien. Regelmäßige Treffen mit dem VCI und VDE und Austausch auf europäischer Ebene mit ENISA (European Union Agency for Network and Information Security) und anderen Anwenderverbänden (EEMUA England, EXERA Frankreich, WIB Niederlande) stehen gleichfalls auf dem Programm, um diese Security-Konzepte global abzustimmen.

Planung und technische Überwachung

Die Bedeutung der drei Hauptkomponenten Menschen, Prozesse und Technologie für die Sicherheit innerhalb eines Industriebetriebs betont auch Konstantin Rogalas, Business Leader Europe, Honeywell Industrial Cyber Security. Damit ein Sicherheitsprogramm erfolgreich ist, müssen diese drei Elemente in der Sicherheitsstrategie berücksichtigt werden. Dazu gehören Mitarbeiterschulungen zum Sicherheitsbewusstsein (die Komponente „Menschen“), die Erstellung von Reaktionsplänen nach Vorfällen (die Komponente „Prozesse“) und der Einsatz der richtigen Tools für die Sicherheit leittechnischer Netzwerke sowie der richtigen Software hinsichtlich Virenschutz/Application White Listing/Sicherheitsmanagement (die Komponente „Technologie“). Cybersicherheit, so sagt Rogalas, erforderte nachhaltige Aktivitäten über den gesamten Lebenszyklus der Anlage, eingebettet in die organisatorischen Abläufe des Unternehmens: „Verbesserungen der Sicherheit erfordern Planung. Es ist relativ einfach, technische Sicherheitsanpassungen vorzunehmen, aber die Organisation muss sich entsprechend mit entwickeln, dabei aber risikobewusst und handhabbar bleiben. Die hierzu notwendige Zeit sollte nicht unterschätzt werden.“

Erschwerend kommt bei den meisten Automationsnetzwerken hinzu, dass ihre Struktur ein System von Sub-Systemen darstellt mit umfangreichen Abhängigkeiten, die von kritischer Bedeutung für die fortlaufende Produktion und die Sicherheit in der Anlage sind. Die Überwachung der Cybersicherheit ist deswegen hier viel komplexer als in reinen IT-Netzwerken und erfordert die Korrelation von Daten und Alarmen aus mehreren Systemen verschiedener Hersteller. Internationale Informationen und Richtlinien zur industriellen Cybersicherheit müssen berücksichtigt werden, um effektiven Schutz gegen Angreifer mit detailliertem Fachwissen zu den eingesetzten Industriesteuerungen und Produktionsprozessen zu bieten.

OT und IT zusammenbringen

Prozessanlagen unterliegen den aktuellen Trends bzgl. zunehmender Vernetzung, großen Datenmengen und die Verwendung offener Standards, die man mit den Schlagwörtern „Industrie 4.0“, „Digitalisierung“ oder „digitale Fabrik“ verbindet. Das Ziel einer effektiveren, wettbewerbsfähigeren und flexibleren Produktion lässt sich anderweitig auch kaum erreichen. Die Schattenseite dieser Entwicklung ist die zunehmende Verwundbarkeit dieser Systeme gegenüber Cyberangriffen.

Die neue Bedrohungslage erfordert ein grundlegendes Umdenken in Bezug auf Informations- und Zugriffsschutz, sowie das Vorgehen bei der Etablierung von industriellen Sicherheitskonzepten. Auch wenn man eine 100 %ige Sicherheit nicht erreichen kann, gibt durchaus Mittel und Wege das Risiko auf ein vertretbares Maß zu reduzieren, meint Franz Köbinger, Siemens Process Automation: „Hierfür ist ein umfassendes Sicherheitskonzept erforderlich, das sowohl den verschiedenartigen Angriffen, als auch den professionellen Charakter der Angriffe Rechnung trägt und das Zusammenwirken der beteiligten Akteure, d.h. den Betreibern, Integratoren und Herstellern von Automatisierungssystemen erfordert.“

Die veränderte Bedrohungslage erfordert ein grundlegendes Umdenken in Bezug auf Informations- und Zugriffsschutz.

Franz Köbinger, Siemens, Process Industries and Drives Division

Die Lösung kann ein Defense in Depth Konzept sein, das Prozessanlagen sowohl rundum als auch in die Tiefe schützt und auf Anlagensicherheit (z.B. physikalischer Zugangsschutz, organisatorische Maßnahmen), Netzwerksicherheit (z.B. Absicherung der Netzwerkzugänge, DMZ, sichere Fernwartung und Kommunikation) und Systemintegrität (z.B. Endgeräteschutz, Integritätsschutz für Daten) basiert – entsprechend den Empfehlungen der IEC 62443, dem führenden Standard für Security in der industriellen Automatisierung.

Große Einigkeit besteht bei den Experten, dass die Zusammenarbeit von IT und OT und das gegenseitige Verständnis der Schlüssel für reibungslos funktionierende Anlagen mit einer hinreichenden Cyber Security ist. Das ist auch Ziel der Tagung „IMI 2016 – IT meets Industry“ am 27. – 28. September 2016 in Frankenthal, die IT und Industrie an einen Tisch bringt, um die Chancen der Vernetzung von IT und Automation für den optimalen Betrieb von industriellen Produktionsanlagen zu nutzen und gleichzeitig die dem gegenüber stehenden komplexen Risiken zu minimieren.

Dr. Volker Oestreich, CHEManager

Secure Remote Maintenance

Die neue Fernwartungslösung von B&R steht im Einklang mit gängigen IT- und Sicherheitsrichtlinien. Sie ermöglicht Servicetechnikern den Zugriff auf Maschinen von jedem Ort der Welt. Dazu wird eine zertifikatgesicherte und verschlüsselte VPN-Verbindung zwischen dem Site Manager an der Maschine und einem Gateway hergestellt, welches typischerweise im Service-Center des Maschinenbauers steht. Dort können Zugriffsberechtigungen für bis zu 10.000 Maschinen hinterlegt werden; ein umfangreiches Maschinen-Pool-Management lässt sich einfach einrichten.

Der Site Manager verfügt über integrierte digitale Ein- und Ausgänge. Ein Schlüsselschalter kann angeschlossen werden, um Wartungszugriffe erst nach Betätigung des Schalters zu ermöglichen. Vor unerwünschten Zugriffen von Dritten schützt eine integrierte Firewall. Um Sicherheitskonflikte mit werksseitigen Firewalls zu vermeiden, läuft die Kommunikation in das Internet über firewallverträgliche, verschlüsselte Web-Protokolle. Es müssen keine zusätzlichen Ports geöffnet werden.

Über die sichere VPN-Verbindung können alle Wartungs- und Diagnosefunktionen des B&R-Systems genutzt werden. Dazu wird der Site Manager einfach über die Automatisierungssoftware Automation Studio parametriert. Wo eine Anbindung über LAN oder WLAN nicht möglich oder erwünscht ist, kann die VPN-Verbindung via GPRS- und UMTS-Mobilfunk aufgebaut werden. (vo) ■