1

Bild: © Texelart - Fotolia.com

PROFI-GUIDE		
Branche	Anlagenbau	●
	Chemie	● ● ●
	Pharma	● ● ●
	Ausrüster	
Funktion	Planer	● ●
	Betreiber	● ● ●
	Einkäufer	
	Manager	● ●

ENTSCHEIDER-FACTS

Für Betreiber

- Sabotage- und Spionage-Angriffe auf Industrieanlagen nehmen zu: IT-gestützte Produktions- und Steuerungsprozesse benötigen deshalb besonderen Schutz.
- Security für Leitsysteme folgt den Maßnahmen der klassischen IT-Security im Office-Umfeld nur mit Verzögerung.
- Segmentieren der Netzwerke, Separieren der Leitsysteme, Abschotten der Prozesse, Sichern der Schnittstellen und intelligentes Patch-Management sind geeignete Lösungsansätze.

IT-Management und Sicherheit

Angriff auf das Herz der Anlage

Der Autor:

Steffen Stripf,
Head of Business
Development Exco

Dass Industrieanlagen Ziele von Cyberkriminalität sind, ist spätestens seit Stuxnet bekannt: Das Schadprogramm sabotierte 2010 die Steuerungsprozesse in iranischen Atomanlagen. Auch andere Industrieanlagen wie Kraftwerke und Chemiefabriken wurden weltweit – vermutlich über USB-Speichermedien – mit dem Schädling infiziert. Doch nicht nur Betriebe, die für eine funktionierende Infrastruktur wichtig sind, befinden sich im Visier von Hackern & Co. „Wirtschaftsspionage und Konkurrenzausspähung sind eine permanente Bedrohung für die deutsche Wirtschaft", verkündete Dr. Burkhard Even, Abteilungsleiter für Spionageabwehr im Bundesamt für Verfassungsschutz, auf einer gemeinsamen Tagung von Verfassungsschutz und der Arbeitsgemeinschaft für Sicherheit der Wirtschaft im Juni 2013. Bedroht, so der Verfassungsschützer, seien „vor allem technologieorientierte und innovative mittelständische Unternehmen, die das Rückgrat der deutschen Wirtschaft bilden."

Zunehmende Vernetzung

Unabhängig von der Größe und Art der Anlage gilt bei Automatisierungsprozessen grundsätzlich das 24/7/365-Prinzip; ständige Verfügbarkeit und kontinuierliche Sicherheit der Produktionsqualität sind die Grundlage für Erfolg. Dabei hat die IT-Unterstützung beim Überwachen und Steuern komplexer physikalischer Prozesse in den letzten Jahren kontinuierlich zugenommen, wie auch die Vernetzung in Produktionsanla-

gen mit standardisierter industrieller IT. Sicherheitslücken bedeuten in diesem Umfeld ein wachsendes Risiko für Produktionsstandorte. Als Folge der fehlenden Härtung der Systeme droht das zufällige Übertragen von Schadsoftware aus dem klassischen Office-IT-Umfeld ins Produktionsumfeld. Aber auch gezielte Angriffe auf eingesetzte Technologien sind möglich, um in den Besitz wettbewerbsrelevanter Daten zu gelangen und Wirtschaftsspionage auf der einen Seite zu betreiben oder Sabotageangriffe einzuleiten, die zum Ausfall von Anlagen führen können.

Offener Zugang in das Herz der Anlage

Viren, Würmer und Schadprogramme haben häufig leichten Zugang in die Leit- und Automatisierungssysteme von Industrieanlagen. Über offene USB-Schnittstellen sowie den Anschluss mobiler Geräte und Datenträger können sie den unmittelbaren Weg in das Herz der Anlage finden. Auch nicht sichere Verbindungen ins Internet ermöglichen das Eindringen von außen in die interne Produktionsleittechnik. Fehlende Netzwerksegmentierungen erleichtern zusätzlich den Weg der Schädlinge in die Steuerungsprozesse. Oft findet die Übertragung ungewollt und unbemerkt statt. Der freundliche und kompetente Servicetechniker, der im Jahresverlauf eine Vielzahl von Produktionsnetzwerken wartet, oder auch der loyale Mitarbeiter, der über den eigenen USB-Stick Produktionsdaten, Rezepturen, Protokolle oder Datenbanken kopiert, können – ohne es zu wissen – Multiplikatoren von Schadprogrammen sein. Die Möglichkeiten, in die Leittechnik einzugreifen, sind vielfältig.

Branchenspezifische Normen erst im Entstehen

Universelle und leicht umzusetzende Empfehlungen für die IT-Sicherheit in Industrieprozessen und wichtige Regelwerke sind derzeit erst im Aufbau. Auf der Basis der internationalen Norm ISO 27001, dem Standardwerk für Informationssicherheitsmanagementsysteme, entstehen zurzeit weitere branchenspezifische Normen. Software-Hersteller, Anlagenbetreiber und Industriezweige definieren so die Standards für das Regelwerk IEC 62443. Unter dem Schlagwort „Security for Industrial Process Measurement and Control“ wird diese internationale Normenreihe über die „IT-Sicherheit für industrielle Leitsysteme – Netz- und Systemschutz“ zurzeit eingeführt. Die Reihe übernimmt wesentliche Inhalte der amerikanischen ISA-99-Norm. Relevant ist die IEC 62443-Reihe für allgemeine Anlagen der industriellen Automatisierungstechnik, aber auch in Anlagen kritischer Infrastrukturen, die von essentieller Bedeutung für die Gesellschaft sind. Diese sind einem besonders hohen Bedrohungsrisiko ausgesetzt. Verschiedene Security Assurance Levels beschreiben unterschiedlich hohe Angriffspotenziale: Die Sicherheitsstufe 1 umfasst die Verteidigung vor zufälligen und ungewollten Eingriffen ins System (SAL 1). Die zweite Stufe befasst sich mit absichtlichen Angriffen, die mit einfachen Methoden und wenig ausgeprägter Motivation erfolgen (SAL 2). SAL 3 setzt voraus, dass der Angreifer über hinreichende Kenntnisse, Motivation und Mittel verfügt, um gezielt in industriellen Anlagen Schaden anzurichten. Bei kritischen Anlagen, die zum Erhalt der Infrastruktur notwendig sind, beispielsweise Wasserwerke, Energieunternehmen oder Verkehrsleitsys-

Umfassende Konzepte der Sicherung erfordern eine klare Definition der Gefahrenstellen und eine konsequent umgesetzte Sicherungsstrategie, angelehnt an die spezifischen Industrie-Normen

1: Die Prozessindustrie ist vermehrt Opfer von Sabotage und Spionage

2: Über USB-Speichermedien kann Schadsoftware in Systeme eindringen

Bild: © Texelart - Fotolia.com

3

3: Firewalls und andere Maßnahmen sollen vor unautorisierten Zugriffen schützen

teme, beschreibt SAL 4 die Bedrohung durch Angreifer, die mit erheblichen Mitteln und hoher Motivation vorgehen.

Notwendige Schutzmaßnahmen ergreifen

Umfassende Konzepte der Sicherung erfordern eine klare Definition der Gefahrenstellen und eine konsequent umgesetzte Sicherungsstrategie, angelehnt an die spezifischen Industrie-Normen. Bei Bestandsaufnahmen vor Ort weisen offene USB-Schnittstellen, der Einsatz von externen Notebooks und Datenträgern, die Kopplung von Office- und Produktions-IT, Verbindungen zum Internet und veraltete Absicherungen der Fernwartungszugänge auf häufige Gefahrenquellen hin. Patch-Management-Strategien, die einen effektiven Schutz durch systematische und geregelte Software-Update-Prozesse bieten sollten, setzen Betreiber in der Praxis oftmals nur mangelhaft um. Auch versorgen sie produktiv betriebene Server und Rechner bewusst nicht mit aktuellen Patches. Dies geschieht nicht nur aus Nachlässigkeit, sondern oft unter der Annahme, dass Server und Rechner durch die Abkopplung vom Internet ausreichend geschützt seien und durch fehlende aktuelle Security Patches kein Risiko entstünde. Hinzu kommt, dass die Systeme bei Inbetriebnahme der Anlagen aufgesetzt werden. Jeder Patch ist ein Eingriff in ein bestehendes und funktionierendes System. Deshalb müsste für qualifizierte Prozesse ein Änderungswesen etabliert werden, damit spätere Änderungen dokumentiert sind. Während Software-Hersteller also kontinuierlich Verbesserungen einführen und Sicherheitslücken in ihren Programmen schließen, finden die Aktualisierungen durch das unvollständige Patch-Management nicht immer ihren Weg in die Prozesse und Anlagen.

My Server is my castle

Grundlegende Lösungsansätze finden sich im Sichern der (USB-)Schnittstellen, dem Bereitstellen firmeneigener Notebooks für externe Servicetechniker, dem Installieren von Scanning-Stationen bis hin zu Zellenschutz-Konzepten. Unternehmen können ein mehrstufiges System einrichten, das es – ähnlich wie beim mittelalterlichen Burgenbau – den Anlagenbetreibern ermöglicht, ihr Innerstes zu schützen. Wie die feindlichen Ritter müssen Angreifer verschiedene Wälle überwinden. Im Anlagenbereich heißt das: Anlagensicherheit, Netzwerksicherheit sowie logischen und physischen Zugriffschutz müssen Hacker erst einmal überwinden, bevor sie Schaden anrichten können. Die Kontrolle des physischen Zugangs von nicht autorisierten Personen zu kritischen Komponenten ist die Ausgangsbasis für eine effektive Anlagensicherheit. In puncto Netzwerksicherheit gilt es, das Gesamtsystem zu schützen. Die in der gängigen Office-Umgebung bekannten Firewalls verhindern unberechtigte Zugriffe von außen. Ähnlich müssen Firmen auch Produktionsnetzwerke abschotten; das Schließen von Kommunikationsports und unsicheren Fernwartungszugänge ist unerlässlich.

Herausforderung Industrie 4.0

Die Industrial-IT benötigt darüber hinaus ein segmentiertes Zellenschutzkonzept mit mehrstufigen Hierarchien, so dass verschiedene Zonen bestimmten Sicherheitsanforderungen zuzuordnen sind. Das Segmentieren der Netzwerke und Separieren der Leitsysteme erfolgt nach prozessorientierten Überlegungen, bei denen Produkte und Prozesse logisch gegliedert betrachtet werden. Nach dem Need-to-know-Prinzip werden Zugänge intelligent und bedarfsgerecht geöffnet, also nur dann, wenn dies zum Erfüllen einer konkreten Aufgabe notwendig ist. Intelligente Softwarelösungen ermöglichen einen kontrollierten und sicheren Umgang mit USB-Speichermedien sowie das revisionssichere und dokumentierte Update von Produktionssystem-Software über ein entsprechendes Patch-Management. Aufgrund des Zusammenwachsens von Produktionsanlagen und IT-Komponenten innerhalb der Industrie-4.0-Konzepte wird IT-Sicherheit im Umfeld von Produktion und Fertigung noch mehr als heute zur strategischen Herausforderung für Anlagenhersteller, Systempartner und Betreiber. ●

Einen Link zum Unternehmen sowie weitere Beiträge zum Thema IT-Security finden Sie unter www.chemie-technik.de/1311ct602 – oder den QR-Code einscannen!