Die zunehmende Vernetzung in der Produktion öffnet **neue Einfallstore für IT-Angriffe**. Um Industrie 4.0 zum Erfolg zu machen, ist daher ein neues Bewusstsein notwendig. Statt auf klassische Schutzmechanismen vor Internet-Attacken zurückzugreifen, müssen für Industrieanlagen neue Methoden erfunden werden. Dazu ist es notwendig, sich in die Rolle des Angreifers zu versetzen.

Text: **Ulrich Hottelet**

Sicherheit 1.0

„Das Thema Sicherheit wird für die Industrie 4.0 total unterschätzt. Man vertraut auf die klassischen Gegenmittel gegen Internet-Risiken. Wir müssen aber etwas Neues machen, statt auf kalten Kaffee wie Firewalls, Identitätsmanagement und Intrusion Detection zu setzen." Professor Hartmut Pohl, Geschäftsführer der Sicherheitsberatung softScheck, spricht Klartext. Der eindringliche Mahner ist Sprecher des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik.

Denn die Herausforderungen sind enorm. Nicht nur die inzwischen schon traditionell zu nennenden Internet-Risiken wie Viren oder Trojaner bedrohen die zunehmend via Internet vernetzten Produktionsanlagen, sondern auch neuartige und auf industrielle Steuerungssysteme (ICS) maßgeschneiderte Attacken à la Stuxnet, Duqu und andere Nachfolger. Da sie unbekannte Sicherheitslücken ausnutzen, können sie von Systemen, die darauf spezialisiert sind, Angriffe zu erkennen, nicht identifiziert werden. Auch wenn mittelständische Unternehmer einwenden, solch ausgeklügelte und gezielte Angriffe würden sich bei ihnen nicht rentieren: Die sich aus der Komplexität der Vernetzung von industriellen Steuerungen mit der IT und dem Internet ergebenden Risiken sind gravierend. Die Einfallstore werden größer. Es wird sich oft um eine Hypervernetzung über Abteilungs-, Unternehmens- und sogar Ländergrenzen hinaus handeln. Daraus ergeben sich technische, organisatorische und rechtliche Herausforderungen neuer Art.

Top 10 der Bedrohungen

„Industrie 4.0 wird sich nur durchsetzen, wenn die gesamte Wertschöpfungskette der produzierenden Industrien auch hohe Sicherheitsanforderungen erfüllt", betont Professor Dieter Wegener, Technologiechef des Sektors Industrie bei ▷

Illustration: Christoph Kienzle

Illustration: Frank von Grafenstein

Siemens. Der Konzern bezeichnet sich als weltweit einzigen Anbieter einer kompletten Angebotspalette für Industrieautomatisierung und -software, mit der sich heute die ganze Wertschöpfungskette der Industrie 3.0 abbilden lässt.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinen Analysen zur Cyber-Sicherheit in Zusammenarbeit mit Experten aus Maschinenbau und IT-Industrie die wichtigsten Bedrohungen in einer Top 10-Liste zusammengestellt, denen industrielle Steuerungssysteme derzeit ausgesetzt sind. Die kriminellen Motive hinter diesen Manipulationsversuchen sind oft Wirtschaftsspionage, Produktpiraterie und der Diebstahl von Know-how. Auch die organisierte Kriminalität setzt zunehmend auf Betrugsmaschen und Erpressungsmethoden online. Dr. Thomas Kaufmann, Leiter der Automatisierungstechnik bei Infineon Technologies, präzisiert das Szenario: „Angriffe auf Netzwerkkomponenten, industrielle Kontrollsysteme wie SCADA und Produktionssteuerungen werden möglich."

Lebenszyklen beachten

Damit nicht genug: Die Lebenszyklen von IT-Komponenten (drei bis fünf Jahre) und industriellen Produktionsanlagen (teilweise Jahrzehnte) sind deutlich verschieden. Das zeigt sich zum Beispiel bei Software-Aktualisierungen. Während Microsoft einen monatlichen „Patch Tuesday" hat, nimmt die Autoindustrie Änderungen möglichst nur zum geschäftlich ruhigen Jahresende vor. Denn für das produzierende Gewerbe hat die Verfügbarkeit stets höchste Priorität.
Von entscheidender Bedeutung für die Abwehr ist nach einstimmiger Ansicht von Fachleuten das Prinzip „Security by design", wobei Sicherheitsanforderungen mit Beginn der Produktentwicklung berücksichtigt werden. „Wenn man neue Systeme entwickelt, muss die entsprechende Sicherheitsarchitektur mitbedacht werden", fordert Dirk Seewald, Vorstand von Innominate Security Technologies, einem Hersteller von Netzwerksicherheitsgeräten für den Einsatz in Industrieumgebungen und Anbieter von Fernwartungslösungen über das Internet. Derzeit entwickelt die Industrie solche Konzepte. Doch ist es eine besondere Herausforderung, Techniken aus der IT in die industrielle Fertigungswelt zu übertragen. „Bei hochspezialisierten eingebetteten Systemen sind Rechenleistung und Speicher begrenzt. Eine der Schlüsselherausforderungen besteht darin, trotz dieser Limitierungen moderne Sicherheitstechniken umzusetzen, die in der Verschlüsselungsstärke den einschlägigen Empfehlungen, zum Beispiel des BSI, entsprechen", sagte Seewald. Professor Wegener von Siemens setzt den Akzent etwas anders: „Security by design ist enorm wichtig, aber alleine nicht für den Markterfolg ausreichend." IT-Sicherheit sei in der Industrie keine Produkteigenschaft, sondern die Sicherheitskonzepte müssten von den Errichtern und Betreibern industrieller Anlagen fortwährend ausgebaut werden.

Ein stärkeres Augenmerk auf Software-Sicherheit fordert Kaufmann von Infineon: „Bisher lag der Schwerpunkt auf Funktionalität." Geeignete Schutztechnologien seien beispielsweise TPM-Chips zur Authentifizierung. Neben aller Technik sei auch der Mensch gefordert. Hierfür muss die Sensibilität der Mitarbeiter durch Schulungen geschärft werden. Ähnlich argumentiert Wegener von Siemens: „Sicherheit ist kein Produkt, das man von der Stange kaufen kann, sondern eine ständige Managementaufgabe, die dafür verantwortlich ist, dass die richtigen sicherheitsrelevanten Produkte und Verfahren zum Einsatz kommen." Ein Schlüsselelement auf dem Weg zu integrierten Welten aus Büro-, Produktions- und Infrastrukturnetzen und durchgängigen Konzepten sieht Siemens in internationalen Standards. Der Konzern arbeitet in den entsprechenden Gremien mit an Standards für Management-, System-, Komponenten- und Kommunikations-Sicherheit. Auch der ZVEI tritt für internationale Normen und Standards ein, um den Zugang zu Märkten in aller Welt zu erleichtern. „Wir benennen die Experten der Elektroindustrie in alle wichtigen Normenkomitees und unterstützen damit die Erarbeitung hochwertiger Standards", ergänzt Haimo Huhle, Leiter der Abteilung Technisches Recht und Standardisierung im ZVEI.
Einigkeit besteht unter den Fachleuten, dass die Frage, mit welchen Protokollen in der Fabrik der Zukunft kommuniziert wird, nicht kriegsentscheidend ist. „Die unterschiedlichen Anforderungen produzierender Industrien werden dafür sorgen, dass wir verstärkt branchenspezifische Ausprägungen von Protokollen und Netzwerktechniken sehen werden", sagte Wegener. Sicherheit sei ein „Schlüsselelement" bei den Netzwerkprotokollen. Neben dem IP-Protokoll gehören für Anwendungen OPC UA sowie industrielle Protokolle und zum Beispiel das echtzeitfähige Ethernet zu wichtigen Standards für die Industrie der vierten Dimension. Die Protokolle zu implementieren, ist eine neue Herausforderung, insbesondere wenn altbewährte Anlagen mit neuen internetfähigen Produkten ergänzt werden. „Es kommt auf die Implementierung an. Die Protokolle müssen sorgfältiger geschrieben werden, als das heute üblich ist", kritisiert Pohl.
Die Sicherheit der Zukunft fußt also auf vielen Säulen, nicht auf der einen großen Lösung. Viele Experten bestätigen noch großes Forschungs- und Entwicklungspotenzial. Die Verbändeplattform zu Industrie 4.0, die BITKOM, VDMA und ZVEI gemeinsam gegründet haben (→ Seite 40), will denn hier auch einen inhaltlichen Schwerpunkt setzen. ■

Die Frage, welche Protokolle für die Kommunikation verwendet werden, ist für die Sicherheit nicht entscheidend.

IMPRESSUM

HERAUSGEBER
ZVEI-Services GmbH
Patricia Siegler (Geschäftsführerin, verantwortlich für Anzeigen)
Thorsten Meier (Chefredakteur)
Lyoner Straße 9, 60528 Frankfurt am Main
Telefon +49 69 6302-316
E-Mail: zsg@zvei-services.de
www.zvei-services.de
ZSG ist eine 100-prozentige Servicegesellschaft des
ZVEI – Zentralverband Elektrotechnik- und Elektronikindustrie e.V.

ANSPRECHPARTNER ZVEI E.V.
Thorsten Meier (Chefredakteur), meier@zvei.org
Nadine Novak (CvD, Anzeigenberatung), novak@zvei.org
www.zvei.org

VERLAG, KONZEPT UND REALISIERUNG
PICS publish-industry Corporate Services GmbH, München
Projektleitung: Julia Rinklin, j.rinklin@publish-industry.net
Inhalt: Johannes Winterhagen
Art-Direktion: Rose Pistola GmbH

DRUCK
Firmengruppe APPL, sellier druck GmbH, Freising

PERSONENVERZEICHNIS

	Seite
Bent, Roland, Geschäftsführer, Phoenix Contact	31
Denner, Dr. Volkmar, Vorsitzender der Geschäftsführung, Bosch	16
Dumitrescu, Dr. Roman, Geschäftsführer, it's OWL	31
Heinemann, Dr. Christopher, Geschäftsführer, Manufactum	34
Helmrich, Klaus, Technikvorstand, Siemens / Vizepräsident ZVEI	15, 34
Hohwieler, Eckhard, Fraunhofer IPK	18
Hüther, Prof. Dr. Michael, Direktor, Institut der deutschen Wirtschaft	33
Huhle, Haimo, Leiter Abteilung Technisches Recht und Standardisierung, ZVEI	27
Kagermann, Prof. Dr. Henning, Präsident, acatech	14
Kaufmann, Dr. Thomas, Leiter Automatisierungstechnik, Infineon	26
Kienzle, Dr. Stefan, Direktor Konzernforschung, Daimler	22
Köhler, Dr. Peter, Vorstandssprecher, Weidmüller / ZVEI-Vorstand	31
Kohlmann, Roger, Geschäftsführer, BDEW	45
Kröger, Harald, Leiter Entwicklung e-Drive Pkw, Daimler	44
Kurz, Dr. Constanze, Vorstandsmitglied, IG Metall	32
Loh, Friedhelm, Präsident, ZVEI	3, 44
Lukas, Prof. Dr. Wolf-Dieter, Abteilungsleiter, BMBF	13, 30
Mittelbach, Dr. Klaus, Vorsitzender der Geschäftsführung, ZVEI	41
Pohl, Prof. Hartmut, Geschäftsführer, softScheck	24
Ramesohl, Dr. Ingo, Bosch	45
Rauen, Hartmut, Mitglied der Geschäftsführung, VDMA	41
Rösler, Dr. Philipp, Minister, BMWi	30
Rohleder, Dr. Bernhard, Hauptgeschäftsführer, BITKOM	40
Seewald, Dirk, Vorstand, Innominate Security Technologies	17, 26
Terwiesch, Dr. Peter, Vorstandsvorsitzender, ABB / ZVEI-Vorstand	22
Wahlster, Prof. Dr. Wolfgang, Vorsitzender der Geschäftsführung, DFKI	13
Wegener, Dieter, Technologiechef des Sektors Industrie, Siemens	24
Wittenstein, Dr. Manfred, Vorstandsvorsitzender, Wittenstein	16
Ziesemer, Michael, COO, Endress+Hauser Gruppe / Vizepräsident ZVEI	42
Zinkann, Dr. Reinhard, Geschäftsführer, Miele / ZVEI-Vorstand	46

DOWNLOAD & BESTELLUNG
Sie können die Ausgabe von AMPERE über den QR-Code downloaden oder unter novak@zvei.org bestellen.
QR-Code Reader im App Store herunterladen und Code mit Ihrem Smartphone scannen.

ISSN-Nummer 2196-2561
Postvertriebskennzeichen 84617

www.zvei.org/ampere