www.vdma.org

VDMA Nachrichten

11 | 14

• SONDERDRUCK • SONDERDRUCK • SONDERDRUCK • SONDERDRUCK •

Industrial Security – die unangreifbare Maschine

im blickpunkt → SEITE 18

Security in der Produktion – Vernetzung sicher nutzen

Liebe Mitglieder und Leser,

die Implementierung von Industrie 4.0 ist ein wesentlicher Schritt zur Digitalisierung von Industrieunternehmen. Damit verbinden sich auch viele Erwartungen. Diese lassen sich jedoch nicht zum Nulltarif realisieren. Die Basis dafür ist die Standardisierung von IT-Infrastrukturen von Unternehmen. Ein Kulturwandel muss erfolgen, der diese offene, vertrauensvolle Zusammenarbeit ermöglicht. Der kritischste Punkt ist aber das Thema Security in der Produktion – die Industrial Security.

Durch die Verknüpfung von heute nicht vernetzten Prozessen lässt sich die Effektivität von Industrieunternehmen dramatisch steigern. Entscheidungen werden auf Basis aller benötigten Informationen getroffen und können schnell umgesetzt werden. Da alle benötigten Informationen immer in Echtzeit verfügbar sind, wird die Fertigung flexibler. Sogar „Losgröße eins“ lässt sich mit angemessenen Kosten realisieren. Der Informations- und Datenfluss entlang des Produktlebenszyklus ist gewährleistet, er spart Kosten und hebt neue Servicepotenziale durch Nutzung von Wissen aus früheren Phasen. Der Datenaustausch zwischen Fertigungen unterschiedlicher Unternehmen funktioniert reibungslos.

Ist schon heute die Sicherheit von elektronisch abgelegten Daten und Informationen ein sicherheitsrelevantes Thema, so wird diese potenzielle Schwachstelle künftig „Mission critical“. Durch die vollständige Vernetzung werden alle wertvollen Daten und Informationen zugänglich gemacht. Genau dies ist die Basis für den beschriebenen Nutzen.

Dies stellt aber gleichzeitig ein hohes Risiko dar, wenn von den Unternehmen keine angemessenen Vorkehrungen zum Schutz dieser Daten vor Missbrauch und Diebstahl getroffen werden. Doch dies geht oft über die Möglichkeiten einzelner Unternehmen hinaus. Daher ist eine Zusammenarbeit mit Partnerunternehmen, die zum Thema „Industrial Security“ spezialisiert sind, unumgänglich. Aber auch die vertrauensvolle Zusammenarbeit von Industrieunternehmen mit staatlichen Stellen, wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI), ist nötig. Nur so gibt es eine Chance, den ständigen Wettlauf mit Angreifern auf unsere Sicherheitssysteme zu bestehen.

Ihr

Dr. Reinhold Achatz
Head of Corporate Function Technology, Innovation & Sustainability
ThyssenKrupp AG

Foto: ThyssenKrupp, 3alexd / Getty, Artur Marciniec / Fotolia (Titelbild)

„Unternehmen müssen angemessene Vorkehrungen zum Schutz ihrer Daten treffen. Eine vertrauensvolle Zusammenarbeit ist dabei unumgänglich.“

Dr. Reinhold Achatz
ThyssenKrupp

Industrial Security: Die unangreifbare Maschine

Sicherheit in Produktion und Automation hat in den letzten Jahren immer mehr an Bedeutung gewonnen. „Industrial Security“ ist einer der wichtigsten Bausteine für den Erfolg von Industrie 4.0. Maschinen- und Anlagenbauer schützen sich vor unliebsamen Angriffen mit intelligenten Lösungen „Made in Germany“.

Fotos: Monkey Business; beermedia.de / Fotolia

➔ Produktionsstillstand, über Wochen hinweg, wegen eines Hackerangriffs – das klingt wie ein Fernseh-Krimi, ist aber bereits Realität: Die Zahlen der aktuellen VDMA-Studie „Status Quo der Security in der Produktion und Automation" belegen: Ganze 29 Prozent der Unternehmen sind von Produktionsausfällen durch Security-Vorkommnisse betroffen.

Steht die Produktion, geht bares Geld verloren. Schlimmer wird es noch, wenn kritische Infrastrukturen, wie Kommunikationsnetze, Krankenhäuser oder Energieversorger ausfallen. Dann stehen mit jeder Minute eines Systemausfalls Menschenleben auf dem Spiel. Der Schutz von Produktions- und Fertigungssystemen sollte daher im Interesse jedes Unternehmens sein. Nicht zuletzt durch den Stuxnet-Angriff hat sich die öffentliche Wahrnehmung der im Fachjargon sogenannten „Industrial Security" verbessert. Im Blickpunkt ist Industrial Security als ein Prozess zu verstehen, der Maschinen und Anlagen schützen soll vor:

- ➔ Ausfall
- ➔ Know-how-Abfluss
- ➔ Spionage und
- ➔ Manipulation

Die Schutzziele können auch mit dem VIVA-Begriff definiert werden: Verfügbarkeit (V), Integrität (I), Vertraulichkeit (V) und Authentizität (A).

Kleine Lücke – System ausgehebelt

Angreifer auf Unternehmen agieren aus ganz unterschiedlichen Gründen. Sie haben den Vorteil, mit nur einer Lücke das komplette Schutzsystem auszuhebeln. Je nach Angriffsziel und Absicht haben es Unternehmen dabei mit Wettbewerbern, Mitarbeitern, fremden Staaten, organisierter Kriminalität oder Aktivisten zu tun.

Wo der Maschinen- und Anlagenbau hinsichtlich der Industrial Security steht, beantwortet die „VDMA-Studie ➔

Status Quo der Security in Produktion und Automation 2013/14“, die Unternehmen auch praxisnahe Handlungsempfehlungen gibt.

Anwendbarkeit von Normen

Zudem wurde 2014 die vom Bundesministerium für Wirtschaft und Energie geförderte Studie des Normenausschusses Maschinenbau zu „Vergleich und Bewertung von nationalen und internationalen Normen und Standards für Automations- und Produktionssicherheit“ herausgegeben. Untersucht wurde, inwieweit sich die ISO 27001 (Informationssicherheit), die VDI-Richtlinie 2182 (Informationssicherheit in der industriellen Automatisierung) und IEC 62443 (Industrielle Kommunikationsnetze – IT-Sicherheit für Netze und Systeme) im deutschen Maschinen- und Anlagenbau anwenden lassen.

„Bei einer kleinen Lücke können Angreifer das gesamte Schutzsystem aushebeln.“

Steffen Zimmermann
VDMA

Ergebnis der Studie ist die Empfehlung, ein spezifisches Framework für Security in Maschinen und Anlagen zu entwickeln – eine Empfehlung, die der VDMA zügig aufgreifen wird.

Anforderungsprofil definieren

Nicht zuletzt durch das für 2015 angekündigte IT-Sicherheitsgesetz besteht Handlungsbedarf für ein von der Industrie gestaltetes Anforderungsprofil für sichere Maschinen und Anlagen im Sinne der Industrial Security, das auch weltweiten Ansprüchen gerecht wird. Zudem müssen im Sinne einer nationalen Strategie für die industrielle Zukunft (Industrie 4.0) Security-Konzepte neu erarbeitet werden. Denn ohne den Schutz von Daten und Know-how in den unternehmensübergreifenden Produktions- und Kommunikationsprozessen wird Industrie 4.0 undenkbar.

Im Rahmen der „Plattform Industrie 4.0“ erarbeitet die „Arbeitsgruppe 4 – Sicherheit vernetzter Systeme“ ebendiese Security-Konzepte. Dabei gilt es, für Industrie 4.0 den automatisierten Datenaustausch vernetzter Produktionssysteme sicher und zuverlässig zu gestalten, die eindeutige Identifizierung der Prozessakteure zu kontrollieren und das Know-how von Produkten, Verfahren, Maschinen und Anlagen zu schützen. Im VDMA greift das neue „Forum Industrie 4.0“ die Security-Aktivitäten der Plattform branchenspezifisch auf.

Oft mangelt es an Zeit und Know-how

Viele Unternehmen stehen heute noch vor dem Problem, dass es keinen Verantwortlichen für Industrial Security gibt. An Zeit und Know-how fehlt es häufig. Der VDMA-Arbeitskreis „Security in Produktion und Automation“, in dem sowohl Betreiber als auch Hersteller und Integratoren vertreten sind, veröffentlicht daher zur sps ipc drives den „Fragenkatalog Industrial Security“. Der Fragenkatalog richtet sich an Fach- und Führungskräfte von Unternehmen, die Security in der Fertigung ihres Unternehmens etablieren oder verbessern wollen. Er liefert Fragestellungen, die ein strukturiertes, systematisches Vorgehen zur Ermittlung und damit zur Verbesserung des aktuellen Stands der Security im Produktionsbereich ermöglichen. Der Fragenkatalog unterstützt zudem den einfachen Einstieg in das Thema Security und führt bei regelmäßiger Anwendung in kleinen, überschaubaren Schritten an Standards der Industrial Security heran. Der Aufwand kann dabei je nach Bedarf und Kapazität selbst gewählt werden.

Sollte weiterer Bedarf bestehen, die Geschäftsführung für das Thema zu sensibilisieren, sind zwei Dinge empfehlenswert: Erstens ein Besuch durch das Referat Wirtschaftsschutz im Bundesamt für Verfassungsschutz. Die Kollegen wissen aus erster Hand, was den „Hidden Champions“ bei fehlender Security passieren kann. Die zweite Empfehlung ist „Blackout“ von Marc Elsberg, ein beängstigend realistischer und fundiert geschriebener Security-Thriller. ■

TERMINE

Praxisnahe VDMA-Veranstaltungen zu Embedded Security finden im Herbst auf den Messen Medica und sps ipc drives statt.

13. November 2014
Fachforum Security in medizintechnischen Systemen von 14:30 bis 16:00 Uhr, Halle 12, Stand E36, Medica, Düsseldorf

26. November 2014
Podiumsdiskussion zu den Themen Reverse Engineering, Hardwareverschlüsselung & Co. von 13:00 bis 14:00 Uhr, VDMA-Forum in Halle 3, Stand 3-618, sps ipc drives, Nürnberg

STECKBRIEF

Steffen Zimmermann

Zuständig im VDMA für:
Produktpiraterie, Know-how-Schutz, Informationssicherheit, Industrial Security sowie die Arbeitsgemeinschaft Protect-ing.

Ausbildung / Studium:
Diplom-Wirtschaftsinformatiker, CISSP (Certified Informations Systems Security Professional)

AUTOR
Steffen Zimmermann
VDMA Informatik
Telefon +49 69 6603-1978
steffen.zimmermann@vdma.org

LINK
pks.vdma.org/security

BSI

Hilfe für industrielle Cyber-Sicherheit

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet zahlreiche kostenlose Informationen zur Cyber-Sicherheit im Kontext industrieller Anlagen. Im Folgenden ist eine Übersicht.

Foto: Gstudio Group / Fotolia

„Ganz gleich, wie viele technische Maßnahmen etabliert werden, es bleibt immer der Mensch als Fehlerquelle."

Jens Mehrfeld
BSI

→ Cyber-Sicherheit rückt immer stärker in das Bewusstsein von Unternehmen. Eine steigende Anzahl von Vorfällen hat in jüngster Vergangenheit dazu beigetragen. Es stellt sich die Frage, wie sich Unternehmen schützen können. Auf keinen Fall besteht Anlass, davor zu resignieren.

ICS-Security-Kompendium

Dieses Grundlagenwerk zum Thema Industrial Control System (ICS) gliedert sich in zwei Teile. Der erste Teil wurde bereits 2013 veröffentlicht und richtet sich an Betreiber von ICS, um Experten aus der IT-Sicherheit und der Industrieautomation eine gemeinsame Basis zu schaffen. Dazu sollen beide Seiten für Anforderungen der jeweils anderen sensibilisiert werden. Um das zu erreichen, erhalten sie Informationen zum Aufbau und zu speziellen Rahmenbedingungen. Auf der anderen Seite gibt es eine Übersicht zu Bedrohungen aus der IT. Passend dazu werden Maßnahmen und Best-Practices vorgestellt, wie diesen Bedrohungen begegnet werden kann. Darüber hinaus gibt es eine Übersicht existierender Standards von IT-Sicherheit und es wird eine Vorgehensweise zur Auditierung der IT-Sicherheit beschrieben..

Der zweite Teil, der zur sps ipc drives 2014 vorgestellt werden soll, richtet sich an Hersteller und Integratoren von ICS-Komponenten und Anlagen. Es werden Anforderungen an Geräte und Dokumentation erläutert. Dies soll Betreiber unterstützen. Zur Gewährleistung werden zu unterschiedlichen Themen Fragen geliefert, die den Herstellern beim Test der IT-Sicherheit hilfreich sind.

Light and Right Security ICS

Dieses Werkzeug erleichtert kleinen und mittleren Unternehmen aus dem Umfeld industrieller Steuerungsanlagen den Einstieg in die Cyber-Sicherheit. Es bietet eine fragengeleitete Selbsteinschätzung des aktuellen Stands der Cyber-Sicherheit und gibt Empfehlungen, welche Maßnahmen in welchen Bereichen als Nächstes umgesetzt werden sollten. Alle Maßnahmen sind entsprechenden Teilen der Normen und Vorgehensweisen IT-Grundschutz, ISO 27001, IEC 62443 und BSI-ICS-Security-Kompendium zugeordnet, was den Übergang zur Nutzung eines ganzheitlichen Managementsystems für Informationssicherheit erleichtert.

Allianz für Cyber-Sicherheit

Die Allianz für Cyber-Sicherheit ist eine Plattform, in der sich Unternehmen zu

Sicherheitsfragen austauschen können. Grundsätzlich ist Kooperation der Schlüssel zum Erfolg. Nur durch gemeinsame Anstrengungen von Industrie, Staat sowie Lehre und Forschung ist es möglich, die erforderlichen Rahmenbedingungen für Cyber-Sicherheit zu schaffen. Die Allianz für Cyber-Sicherheit baut hierfür eine umfangreiche Wissensbasis auf und unterstützt den Informations- und Erfahrungsaustausch zwischen den Teilnehmern.

Es gibt im Rahmen der Allianz bereits eine Reihe von Empfehlungen für den Themenkomplex ICS. Dazu zählen insbesondere die „ICS Top 10 Bedrohungen und Gegenmaßnahmen“, die die kritischsten Bedrohungen und mögliche Gegenmaßnahmen in prägnanter Weise oder auch Informationen zum Thema „Innentäter“ aufzeigen.

Zusätzlich werden mit der monatlich erscheinenden „BSI IT-Sicherheitslage“ des IT-Lagezentrums im BSI Statistiken, Hintergrundinformationen und Analysen zu aktuellen Themen und Vorfällen zur Verfügung gestellt.

Awareness Toolkit

Neben den technisch orientierten Hilfsmitteln wird mit dem Awareness Toolkit der Mitarbeiter angesprochen. Ganz gleich, wie viele technische Maßnahmen etabliert werden, es bleibt immer der Mensch als Fehlerquelle. Der hinsichtlich IT-Sicherheit informierte und sensibilisierte Mitarbeiter ist daher wichtiger als jede technische Sicherheitsmaßnahme. Insbesondere ist der sicherheitsbewusste Umgang mit IT- und Produktionssystemen durch keine technischen Maßnahmen vollständig zu ersetzen.

Da für eine umfangreiche Planung einer Sensibilisierungskampagne häufig keine Mittel zur Verfügung stehen, wird ein kooperativer Ansatz verfolgt. Hierzu wird eine Auswahl an Materialien bereitgestellt, die in verschiedenen Lernformen verwendet werden können – praktisch wie ein Werkzeugkasten mit unterschiedlichen Materialien oder Werkzeugen – daher die Bezeichnung „ICS Security Awareness Toolkit“. Sämtliche dieser Materialien werden kostenfrei zur Verwendung im eigenen Unternehmen bereitgestellt. Eine Anpassung an das firmeneigene Corporate Design ist möglich. Gerade wegen dieser vorgefertigten und anpassbaren multimedialen Darreichungen und des schlanken Ansatzes ist somit ein Awareness-Programm mit geringen Kosten umsetzbar. Die Anwender sind dabei aufgerufen, eigene Erfahrungen einzubringen. ■

AUTOR
Jens Mehrfeld
Referent beim Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn

INFO
Das BSI steht auf der sps ipc drives vom 25. bis 27. November 2014 in Nürnberg am Stand 2-419 für Fragen zur Verfügung.

LINKS
www.bsi.bund.de/ICS-Security-Kompendium
www.allianz-fuer-cybersicherheit.de

Foto: Maksim Kabakou / Fotolia

Die Experten der Office IT haben eine beachtliche Lernkurve bezüglich der bislang fremden Fertigungs- und Produktionsanforderungen durchlaufen.

BOSCH REXROTH

Alle Beteiligten sind gefordert

Industrial Security ist eine mehrdimensionale Aufgabe unter Einbeziehung der Organisation, der Prozesse und der Technologie. Security-Aspekte müssen in der Produktentstehungsphase, der Integration und im Betrieb berücksichtigt werden.

→ Der Trend zur Vernetzung ist auch bei Maschinen und Anlagen unumkehrbar. Nur durch die immer engere Verknüpfung mit der Unternehmens-IT können Betreiber ihre Fertigung zukunftssicher aufstellen. So ist die Verbindung mit dem Internet eine Voraussetzung für kosteneffiziente Fernwartungskonzepte. Damit gewinnt aber auch der Schutz gegen Angriffe von außen und Manipulationen von innen an Bedeutung.

Das aus der VDI-Richtlinie 2182 bekannte Vorgehensmodell für Informationssicherheit in der industriellen Automatisierung (Verzahnung der Komponentenhersteller sowie der Maschinenbauer und der Betreiber) war die Basis für eine systematische Auseinandersetzung bei der Bosch Rexroth AG in Lohr am Main.

Absolutes Neuland für alle

Die größte Herausforderung dabei war und ist, dass für alle Beteiligten im Sinne der VDI 2182 das Thema Industrial Security absolutes Neuland ist. Zudem handelt es sich nicht um ein Feature, das einen funktionalen Fortschritt oder messbaren Umsatz oder Rendite bringt. Last but not least ist Industrial Security mit erheblichen Auswirkungen und Folgekosten verbunden.

Weitere positiv zu nennende Hilfsmittel waren und sind in diesem Sinne auch die Unterlagen, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung stellt – insbesondere das ICS-Security-Kompendium, welches eine Einführung und einen Überblick zum Thema bietet, sowie „Light and Right Security“ (LARS), das bei der Risikoerfassung und -analyse benutzt werden kann (siehe dazu Seite 22).

Konkrete Schritte im Umfeld haben die Robert Bosch GmbH, Stuttgart und die Bosch Rexroth AG, Lohr am Main in Anlehnung an die VDI 2182 umgesetzt. Im organisatorischen Umfeld wurden bekannte Strukturen aus dem Office-Umfeld entsprechend den besonderen Rahmenbedingungen des Produktionsumfelds angepasst und umgesetzt. Verantwortliche für Werke und Werksbereiche wurden definiert, die nach ent-

sprechenden Schulungen speziell mit dem Thema Industrial Security befasst und dafür verantwortlich sind. Sie sind die Basis einer Struktur, die sich bis in die Leitungsebene fortsetzt. Anzumerken ist in diesem Zusammenhang sicherlich auch die Tatsache, dass die Experten der Office IT eine nicht zu unterschätzende Lernkurve bezüglich der bislang fremden Fertigungs- und Produktionsanforderungen durchlaufen haben. Diese konnte insbesondere auch bei der Umsetzung der notwendigen Maßnahmen bei der Ablösung von Windows XP erfolgreich bewiesen werden.

Im Bereich des Einkaufs für Maschinen und Investitionsgüter für Produktion und Fertigung wurden Fragebögen und Listen entwickelt, um allgemeine IT- und auch spezielle Industrial-Security-Themen bei Lieferanten zu erfragen und gegebenenfalls auch einzufordern. Diese fließen mittlerweile als Entscheidungskriterium für Investitionen maßgeblich mit ein.

Service durch das Netz nutzen

Im Betriebsumfeld wurden Themen wie die Eliminierung von Default-Passwörtern und die Nutzung von gesicherten Protokollen (OPC-UA) genauso auf die Tagesordnung gesetzt wie der sichere Einsatz einer WLAN-Vernetzung, Fernwartung und von Service-Portalen. Hinzu kommen konkrete Projekte, die sich mit den Themen Einsatz von Whitelisting, Virus-Scanstations und VPN-Technologien beschäftigen. Hierbei spielt insbesondere der zunehmende Wunsch und die Forderung von Integratoren eine Rolle, Service-Dienstleistungen durch das Internet zu nutzen.

All diese Themen werden in koordinierten Gremien besonders unter dem Aspekt Industrial Security betrachtet und möglichst standardisiert und standortübergreifend geregelt und gehandhabt.

„Der Stellenwert von Industrial Security wird noch weiter zunehmen."

Michael Jochem
Bosch Rexroth

Leitfaden zum Thema

Unterstützung zur Handhabung von Rexroth-Komponenten liefert ein Industrial-Security-Leitfaden. Er vereinfacht Konfiguration, Inbetriebnahme und sicheren Betrieb innerhalb der existierenden Netzwerke. Erster Ansprechpartner ist der zuständige Vertriebsmitarbeiter.

Die vorwiegende Nutzung von standardisierten Protokollen mit integrierten Security-Funktionen wie OPC-UA kann einen deutlichen Sicherheitgewinn bringen. Das BSI beabsichtigt im Rahmen einer Sicherheitsanalyse, OPC-UA zu untersuchen.

Die beschriebenen Maßnahmen und Mittel bilden das Fundament. Klar ist, dass der Stellenwert von Industrial Security – getrieben durch Vernetzung und Industrie 4.0 – noch weiter zunehmen wird. Zukünftige nationale und internationale Standards werden in diesem Sinne das Handeln prägen. ■

PROFIL

Bosch Rexroth AG, Lohr am Main
Das Unternehmen bietet seinen Kunden Hydraulik, elektrische Antriebe und Steuerungen, Getriebetechnik sowie Linear- und Montagetechnik aus einer Hand. Es ist in mehr als 80 Ländern präsent. Umsatz: 5,7 Milliarden Euro, Mitarbeiter: 36 700

LINK
www.boschrexroth.com

AUTOREN
Michael Jochem
Director Sales Product Management

Heinz-Uwe Gernhard
Development Embedded Firmware,
beide bei der Bosch Rexroth AG, Lohr am Main

HOMAG

Herausforderung Anlagen-Security

Bei der Sicherheit von Anlagen gilt es, Besonderheiten zu beachten. Bei der Homag Group AG geht es im Wesentlichen um Elemente einer modernen Möbelproduktion.

Foto: Homag

Heute weiß vermutlich noch niemand, welche Security-Risiken es bei modernen Anlagen gibt.

➔ Die Anlagen der Homag Group AG aus Schopfloch bestehen in der Regel aus einem Verbund von einzelnen Bearbeitungsmaschinen und Handlings-Einrichtungen. Diese sind sowohl untereinander verbunden (mechanisch, elektrisch, datentechnisch) als auch an das Firmenumfeld, etwa das Firmennetzwerk, angebunden. Prinzipiell hat man bei diesen Anlagen dieselben Security-Themen wie in der metallverarbeitenden Industrie. Dennoch gibt es in der Möbelindustrie ein paar zusätzliche Herausforderungen, die beachtet werden müssen.

Jede Einzelmaschine des Gesamtprojekts ist zunächst eine in sich abgeschlossene Einheit. Eine einzelne Maschine kann man recht gut absichern. Man muss dafür sorgen, dass keine offenen Schnittstellen nach außen vorhanden sind. Dies mag zwar im einen oder anderen Fall gewisse Einschränkungen mit sich bringen, aber es ist realisierbar.

Etwas anders verhält es sich bei Anlagen. Hier werden Schnittstellen selbstverständlich benötigt, um die einzelnen Anlagenteile miteinander zu verbinden. Damit ergibt sich zwangsläufig eine Möglichkeit, um solch eine Einheit von extern „angreifen" zu können. Neben diesen meist datentechnischen Schnittstellen müssen in einer Gesamtbetrachtung auch weitere Schnittstellen, etwa zum Bediener oder Service-Mitarbeiter, im Auge behalten werden.

Herausforderung für den Betreiber …

Das Thema Security wird im Produktionsumfeld der hier betrachteten meist mittelständischen Möbelindustrie bisher nur wenig beachtet. Die IT kümmert sich zwar um die Netzwerksicherheit, aber dies hört am RJ45-Stecker des Ethernetkabels an der Maschine meistens auf. Die Produktionsmitarbeiter und auch die Verantwortlichen haben dagegen meist nichts einzuwenden, denn sie fühlen sich so freier und nicht durch die IT „gegängelt". Auf der anderen Seite kann die IT gut mit diesem Zustand leben, denn die Fertigungsanlagen und ihre Prozesse stehen nicht im Fokus der IT und insofern existiert dort zum Teil zu wenig Know-how darüber.

„Ein System für Security wie die EG-Maschinenrichtlinie für Safety wäre gut."

Ernst Esslinger
Homag

Derzeit wird der Handlungsbedarf von keiner Seite erkannt, da bisher keine gravierenden Daten-Missbrauchsfälle in diesem Industriezweig passiert sind. Dort, wo schon einmal etwas passiert ist, wurden entsprechende Verbesserungsmaßnahmen eingeleitet. Diese behinderten aber teilweise die tägliche Arbeit so sehr, dass sie sehr schnell wieder aufgeweicht werden mussten.

Die Herausforderung für die Geschäftsführung der Anlagenbetreiber besteht zunächst darin, das Thema Industrial Security mehr in den Fokus der einzelnen Abteilungen zu rücken. Denn eigentlich ist jedem klar, dass ein potenzielles Risiko besteht und dass dieses im Extremfall durchaus existenzgefährdend sein kann. Allerdings fühlt sich auch die Geschäftsführung oft nicht kompetent genug, um die richtigen Maßnahmen einleiten zu können. Es gibt zwar Beratungsunternehmen, die auf die potenziellen Gefahren aufmerksam machen. Es wird diesen jedoch oft unter-

stellt, dass sie das Thema überspitzt darstellen, um mehr Geld zu verdienen.

... wenn die Anlage in China steht

Prinzipiell macht es keinen Unterschied, wo auf der Welt solch eine Anlage steht. Datensicherheit lässt sich in Zeiten der weltweiten Vernetzung nicht auf einzelne Länder eingrenzen. So wie es zum Thema Safety unterschiedliche Ansichten in den verschiedenen Regionen der Welt gibt, so wird auch das Thema Security unterschiedlich wahrgenommen. In der Möbelindustrie nimmt aber vor allem in den Konzernen in China die Sensibilität für dieses Thema zu – deutlicher als beim Thema Safety.

Schutz der Servicedaten

Die derzeitigen Zugänge von den Serviceabteilungen der Maschinen-/Anlagenlieferanten zu den Maschinen/Anlagen der Kunden erfolgen meist über einen Ethernet-Netzwerkzugang mit TCP/IP. Ganz selten sind in in der Möbelindustrie noch Modems anzutreffen, und wenn, dann vor allem bei älteren Maschinen.

Die Netzwerkverbindung wird dabei meist über einen VPN-Tunnel über das Internet aufgebaut. Dies wird allgemein als sicher betrachtet. Es ist jedoch nur schwer zu überwachen, wer diese Verbindung aufbaut und ob er dazu berechtigt ist. Mit den aus der Netzwerktechnik bekannten Methoden wie dem Einbau von Firewalls versucht man zwar, dies abzusichern, aber eine hundertprozentige Sicherheit bringt auch das nicht. Wenn der Servicemitarbeiter mit seinem Laptop vor Ort ist, dann versagen diese Mechanismen meist vollständig, denn er hängt sich eben irgendwo in das Anlagennetz und hat so ungehinderten Zugang. Dieser Zugang über Fernservice oder vor Ort ist aber in der Regel erforderlich, um überhaupt erfolgreich die Servicetätigkeit durchführen zu können.

In jedem Fall sind die eigentlichen Dateninhalte bisher überhaupt nicht abgesichert. Die gesamte Servicetätigkeit funktioniert derzeit nur, weil eine Vertrauensbasis vom Maschinen-/Anlagenbetreiber zum Maschinen-/Anlagenhersteller existiert. Dies ist aber nichts Neues. Sie war schon immer notwendig, auch wenn der Servicemitarbeiter direkt vor Ort ist und die Maschine bedient.

Was noch fehlt

Derzeit weiß vermutlich niemand genau, welche Risiken es hinsichtlich der Industrial Security überhaupt gibt. Eine umfangreiche Analyse wäre notwendig. Zur Abwehr identifizierter Gefahren müssen Geräte, Modelle und Vorgehensweisen entwickelt werden. Im Sinne eines sicheren Betriebs wäre ein ähnliches System wünschenswert, wie es die EG-Maschinenrichtlinie für Safety bereits heute bietet. Für all dies ist aber noch umfangreiche Forschungsarbeit zu leisten und es wird noch Jahre dauern. ■

PROFIL

Homag Group AG, Schopfloch

Das Maschinenbauunternehmen ist Innovations- und Weltmarktführer in der holzbearbeitenden Industrie und im Handwerk. Auf seinen Hightech-Maschinen und -Anlagen produzieren die Kunden Wohn- und Büromöbel, Küchen, Parkett- und Laminatfußböden, Fenster, Türen, Treppen sowie komplette Holzsystemhäuser. Umsatz 2013: 789 Millionen Euro, Mitarbeiter weltweit: rund 5 500

LINK

www.homag.com

AUTOR

Ernst Esslinger

Leiter IT-Engineering bei der Homag Group AG, Schopfloch

Foto: Ion Popa, Julien Eichinger / Fotolia

KOLBUS

Fernwartung ja, aber sicher muss sie sein

Remote-Service-Lösungen vernetzen Anlagen über das Internet. Wie Anwender dies sicher umsetzen können, zeigt die Praxis.

→ Maschinen- und Anlagenbauer setzen heute vor allem moderne Breitband-Internet-Verbindungen ein, die mithilfe von „Virtual Private Networks“ (VPN) sowie Firewall-Technik gesichert werden. Maschinenkomponenten können immer einfacher durch vorhandene Ethernetschnittstellen eingebunden werden. Diese tiefe vertikale Integration bis in die Prozessebene birgt neben den positiven Aspekten auch die Gefahr von Missbrauch und Störungen durch unbefugte Dritte. Daher ist für die Vernetzung von Anlagen über das Internet ein entsprechendes Sicherheitskonzept unabdingbar.

24-Stunden-Service

Als Hersteller von Buchbindemaschinen bietet die Kolbus GmbH & Co. KG aus Rahden ihren Kunden eine Remote-Support-Option an. Kunden erhalten rund um die Uhr Unterstützung von Kolbus-Experten. Mit Aktivierung der Online-Verbindung durch den Kunden hat der Techniker die Möglichkeit, direkt auf die Anlage zuzugreifen. Um den Remote Service gegenüber dem Kunden auch heute gut vermarkten zu können, wurden weitere Mehrwertdienste integriert.

Kolbus setzt eine javabasierte Client-Server-Lösung ein, die eine 256 Bit Advanced-Encryption-Standard- (AES-) verschlüsselte SSL-VPN-Verbindung zwischen Hersteller und Kunde realisiert. Die Pilotinstallation erfolgte bei Kolbus im Jahr 2006. Bis heute wurden weltweit über 320 Anlagen mit Remote Service in Betrieb genommen. Der Trend zeigt eine verstärkte Nutzung solcher Hilfsmittel. Allein im vergangenen Jahr wurden über 50 Anlagen mit Remote-Service-Unterstützung aktiv geschaltet. Aktuell nutzen insgesamt mehr als 150 Kunden mit 960 Maschinen den Remote-Support.

„Die Nutzung von Remote-Service-Lösungen hat bei den Kunden enorm zugenommen.“

Fabian Duffert
Kolbus

Funktionsprinzip VPN-Lösung

Die VPN-Lösung besteht aus einem Site Control Server, einem zentralen VPN-Gateway-Server und entsprechenden VPN-Clients. Über eine Bedienoberfläche kann eine Supportanfrage abgeschickt werden. Dadurch baut die Site Control über einen definierten Port eine ausgehende verschlüsselte VPN-Verbindung mit dem Central Server auf. Die Site Control ist über das lokale Netzwerk an die Maschinen und Anlagen angebunden. Beim Maschinenprogramm trennt Kolbus strikt die zeitkritische Prozesskommunikation und die Anlagenvernetzung für den Remote-Zugriff.

Der Central Server ist Sammelstelle für Serviceanfragen und über eine feste Domain-Adresse ansprechbar. Er hält die zum Verbindungsaufbau notwendigen offenen Ports bereit, die mit entsprechender Firewalltechnik überwacht werden. Darüber hinaus weist der Central Server die Kommunikationskanäle zwischen den Site Controls und den VPN-Clients zu. Die über den VPN-Client angemeldeten Techniker werden bei Bedarf mittels eines Reverse-Proxy-Mechanismus auf die Kunden-Site-Control weitergeleitet und können so auf die am Site Control angeschlossenen Maschinen und Anlagen zugreifen. Durch den Kommunikationsaufbau mit dem Central Server benötigen sowohl die Site Control als auch der Client nur einen ausgehenden Internetport.

Der Client wird sowohl vom Techniker zur Einwahl auf dem Zentralserver als auch vom Kunden für die lokale Verbindung zum Site Control eingesetzt. Da die VPN-Lösung modular aufgebaut ist, ermöglicht sie neben der Remote-Service-Infrastruktur auch die Einbindung zusätzlicher Applikationen wie Maintenance, Condition Monitoring, Parts Agent und ein integriertes Conference

PROFIL

Kolbus GmbH & Co. KG, Rahden
Das Unternehmen entwickelt, produziert und vermarktet Maschinen und Anlagen für die industrielle Druckweiterverarbeitung und Packmittelproduktion.

LINK
www.kolbus.de

Center. Die Rechteverwaltung erfolgt über ein Rollenkonzept, wodurch eine sehr feine Gliederung der Benutzerrechte möglich ist und Zulieferer eingebunden werden können.

Neben den in der Software integrierten Kommunikationsmöglichkeiten können spezielle Programme über VPN getunnelt werden. Dabei werden die für das Programm notwendigen Kommunikationsprotokolle von der Software in das Tunnelprotokoll (SSH) eingebettet und verschlüsselt übertragen. Die Software der Gegenstelle extrahiert die Protokolle wieder und leitet sie über das lokale Netzwerk an das Zielsystem. Die Tunnelports werden dabei nicht wie bei anderen VPN-Lösungen standardmäßig geöffnet, sondern abhängig von den gestarteten Tunnelverbindungen dynamisch bereitgestellt (Instant VPN).

Sicherheitsanforderungen definieren

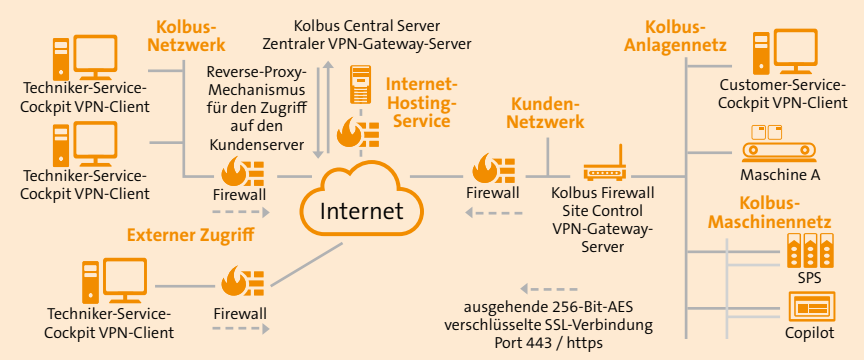
Jedes Unternehmen muss bei der Auswahl einer passenden Remote-Service-Lösung frühzeitig eigene Anforderungen an das System definieren. Dabei sollten die Sicherheitsaspekte und Herausforderungen sowohl beim Betreiber als auch beim Kunden berücksichtigt werden.

Bei Kolbus-Kunden gibt es verschiedene IT-Policies, die für die Anbindung der Site Control in das Kundennetzwerk beziehungsweise für den Internetzugriff zu berücksichtigen sind. Dabei akzeptieren die Kunden keine speziellen Konfigurationen der Firewalls. Sie wollen die volle Kontrolle über den Zugriff und die Freischaltung. Die Abwehr von unautorisiertem Zugriff und der damit verbundene Know-how-Schutz spielen hierbei eine wichtige Rolle.

Bisher ist es Kolbus immer gelungen, das bestehende IT-Konzept mit den vom Kunden geforderten Sicherheitsrichtlinien in Einklang zu bringen. Ziel ist es nun, die bestehende VPN-Infrastruktur Kunden im gewissen Maße zur Verfügung zu stellen, damit diese über mobile Endgeräte jederzeit Informationen über ihre Produktion auf Kolbus-Maschinen abrufen können. Das heißt, der Kunde könnte weltweit live, etwa via Smartphone, auf Produktionszahlen zugreifen. ■

AUFBAU DES REMOTE-SERVICE-NETZWERKS

Internetsicherheit: Der Central Server ist der zentrale Verbindungspunkt, der die zum Verbindungsaufbau notwendigen Ports bereithält.



Quelle: Kolbus

AUTOR
Fabian Duffert
Entwicklungsingenieur für Serviceprodukte bei der Kolbus GmbH & Co. KG, Rahden

WIBU-SYSTEMS

Embedded Security

Kunden der Wibu-Systems AG, Karlsruhe, schützen ihr Know-how gegen unterschiedliche Angriffe und auf verschiedenen Ebenen – einfach, erweiterbar und erfolgreich.

Fotos: Wibu-Systems

Intelligente Schutzkonzepte erfüllen unterschiedliche Anforderungen und arbeiten unauffällig wie der USB-Stick (rechts) in der Orion-Maschine.

➔ Immer stärker bestimmt die zur Maschine gehörende Embedded Software deren Funktionsweise. So legen CAD- und CAM-Software eines niederländischen Kunden der Wibu-Systems AG fest, wie Blechteile gestanzt, lasergeschnitten oder gebogen werden. Mithilfe präventiver Lösungen schützt das Unternehmen sein Software-Know-how.

Software verschlüsseln

Die Niederländer schützen ihr Know-how vor unterschiedlichen Angriffsarten. Das Verhindern einer Kopie oder Installation ist für die Niederländer nicht ausreichend. Daher verschlüsseln sie ihre Software. Diese Software kann zwar kopiert werden, wird in einer nachgebauten Maschine aber nicht funktionieren – sie kann nicht entschlüsselt werden.

In der Software stecken zudem mathematische Algorithmen, damit etwa Zeichnungen eingelesen und für die Produktion vorbereitet werden. Damit diese Algorithmen nicht in die Hände Dritter gelangen, werden sie verschlüsselt gespeichert. So kann der Programmablauf nicht analysiert (debuggt) werden. Lediglich der aktuell benötigte Teil des ausführbaren Programmcodes wird während der Laufzeit entschlüsselt. Das Know-how im verschlüsselten Teil bleibt also weiterhin geheim.

„Kopierte Software kann in einer nachgebauten Maschine nicht funktionieren."

Oliver Winzenried
Wibu-Systems

Darüber hinaus signieren die Niederländer Programmcode und Produktionsdaten digital. Bei Prüfung der Echtheit der digitalen Signatur kontrolliert das Schutzsystem, ob der Code und die Daten von einem berechtigten Herausgeber kommen und nicht manipuliert wurden.

Nachahmer aussperren

Bevor der Wibu-Systems-Kunde seine Generation an Laserschneidegeräten mit einer neuartigen Touchscreen-Steuerung auf den Markt brachte, wollte er sein Expertenwissen vor Reverse-Engineering schützen und Hacken verhindern. Nachahmer sollten ausgesperrt werden. Das Schutzkonzept sollte unauffällig in den Maschinen arbeiten, deren Leistung aufrechterhalten, komplexe und Routine-Eingaben von Schneideparametern ermöglichen. Zudem sollte es so flexibel sein, dass beim globalen Vertrieb jederzeit Funktionen modular freigeschaltet werden können.

Die neue Lösung wurde in der Programmiersprache C# entwickelt und besteht aus kleineren sowie komplexeren Anwendungen. Die Niederländer verschlüsseln die einzelnen Funktionen der Orion-Maschine und schalten die neuen Funktionen frei. Auch nachträglich gekaufte Funktionen können per Remote-Update freigeschaltet werden. Um die vorhandenen, vielseitigen Sicherheitsmechanismen einzusetzen, nutzen die Entwickler eine einheitliche Lösung.

Mehr Produktivität und Wachstum

Seit dem Jahr 2011 verschlüsselt der niederländische Weltmarktführer die Software der Orion-Maschinen, was zu gesteigerter Produktivität und schnellerem Wachstum geführt hat. Besonders wichtig ist, dass das Unternehmen bisher keine Hacks identifizieren konnte und die Ausfallrate der Schutzhardware beim weltweiten Einsatz nur 0,1 Prozent beträgt. Das aufgebaute Floating-Lizenzmodell führt zu verbesserter Betriebseffizienz und optimiertem Management-Workflow.

Ein USB-Stick von Wibu-Systems erfüllt im Prozess verschiedene Schutzbedürfnisse und erlaubt die Freischaltung weiterer Funktionen. Zudem ragt der USB-Stick nur vier Millimeter aus der USB-Schnittstelle im Innern der Orion-Maschine heraus.

Das Herz der Ver- und Entschlüsselung ist ein Smartcard-Chip, der sich in jeder Schutzhardware befindet, etwa im Reisepass oder in der Gesundheitskarte. Der USB-Stick benutzt moderne und sichere Algorithmen: die symmetrische Verschlüsselung mit Advanced Encryption Standard (128-Bit-Schlüssel) und die asymmetrische Verschlüsselung Elliptic Curve Cryptography (224-Bit-Schlüssel).

Produktion und Dokumente schützen

Wie die Technologie weitere Schutzanforderungen erfüllt, verdeutlicht der Einsatz bei einem deutschen Textilmaschinenbauer. Dieser verschlüsselt ebenfalls sein Know-how in der Software, um es vor Reverse-Engineering, Nachbau und gegen Manipulation zu schützen und Maschinenfunktionen flexibel freizuschalten.

Wird ein Betreiber einer Stickmaschine mit der Produktion von T-Shirts beauftragt, bekommt er Original-Daten. Die Gefahr ist, dass er ohne Wissen des Auftraggebers in Nacht- oder Sonderschichten weitere T-Shirts in hochwertiger Qualität produziert und auf eigene Rechnung auf den Markt bringt. Die Ziele des Auftraggebers sind, das Stickmotiv vor Kopieren und unberechtigtem Einsatz zu schützen und die erlaubten Produktionsstückzahlen festzulegen, was technisch über einen Zähler erfolgt.

Innenleben und Funktionsweise einer Stickmaschine werden in Serviceunterlagen und technischen Zeichnungen dargestellt. Solche wertvollen Informationen helfen Produktpiraten, Entwicklungskosten zu sparen, die eigene Maschine zu verbessern oder die ganze Stickmaschine nachzubauen und als eigenes Produkt zu vermarkten. Die Plug-ins des USB-Sticks, den auch die Niederländer nutzen, erlauben das Erstellen geschützter Dokumente und Berechtigten das Lesen – wahlweise zeitlich oder funktionell begrenzt. ■

PROFIL

Wibu-Systems AG, Karlsruhe

Das 1989 gegründete Unternehmen bietet Lösungen für Kopier- und Know-how-Schutz, Software-Lizenzierung und Security für Embedded, SPS und PC Systems sowie Clouds. Die Karlsruher haben Töchter in den USA und in China sowie Büros in Europa. Mitarbeiter weltweit: über 100

LINK

www.wibu.com

AUTOR

Oliver Winzenried

Vorstand bei der Wibu-Systems AG, Karlsruhe, sowie Vorsitzender des Vorstands der VDMA-Arbeitsgemeinschaft Produkt- und Know-how-Schutz

INFO

Wibu-Systems ist vom 25. bis 27. November 2014 auf der sps ipc drives in Nürnberg in Halle 7, Stand 660 vertreten.

SECURITY BY DESIGN

Schlagwort oder interdisziplinäre Herausforderung?

Der Begriff „Security by Design“ wird regelmäßig als Umsetzungsstrategie für die IT-Security in Produkten genannt. Was muss man darunter verstehen, was muss dabei beachtet werden?

Foto: Siemens

Sicherheit ist ein Dauerthema: Die Bedrohungen verändern sich mit neuen technischen Möglichkeiten.

➔ Der Begriff entstand in den 1990er-Jahren, als IT-Security im Rahmen von Standardisierungsaktivitäten in der Telekommunikation (3GPP, ATM-Forum, ITU-T H323, ...) als integraler Teil definiert wurde. Man wollte einerseits Datenverschlüsselung und (starke) Authentifikation performanceoptimiert durchführen und andererseits diese Funktionen unabhängig von teuren Zusatzgeräten in Standardprodukten anbieten können. Inzwischen spricht man auch von Privacy by Design und Safety by Design, wenn entsprechende Funktionen integraler Bestandteil einer Systemarchitektur sein sollen.

Bedrohungs- und Risikoanalysen

Ziel ist es zunächst, Security-Funktionen als integrierten Teil eines Produktes beziehungsweise einer Lösung zu realisieren. Neben einer klaren Verankerung von Security in den betroffenen Standards, und zwar von Anfang an, ergeben sich Konsequenzen für Hersteller und Betreiber von Anlagen. So sind umfassende Ergänzungen zu den bestehenden Prozessen erforderlich.

„Ziel ist es, Security-Funktionen als integrierten Teil eines Produktes zu realisieren.“

Dirk Gebert
Siemens

Die bestehenden Entwicklungsprozesse müssen angepasst werden. Um Security Requirements dort zielgerichtet einzubringen, sind zunächst Bedrohungs- und Risikoanalysen erforderlich, die insbesondere die entsprechenden Anwendungsfälle des späteren Produktes in Betracht ziehen. Schutzziele von Sicherheitsmaßnahmen für ein Produkt orientieren sich an den schützenswerten Assets der betroffenen Hersteller, Integratoren und Betreiber und gegebenenfalls an (oft länderspezifischen) regulatorischen Vorgaben von Behörden, etwa wenn Einsatzszenarien im Rahmen kritischer Infrastrukturen zu erwarten sind.

Nach Identifikation der zu schützenden Assets wird eine Bedrohungs- und Risikoanalyse durchgeführt. Anhand der identifizierten Risiken werden Sicherheitsmaßnahmen ausgewählt. Hier spielen auch wirtschaftliche Aspekte eine wichtige Rolle. Security-Maßnahmen werden nämlich nur dann im Markt akzeptiert, wenn sie zum Geschäftsmodell der Zielarchitektur passen und die damit verbundenen finanziellen Aufwände tragbar sind. Typische Schutzziele sind:

- ➔ Know-how-Schutz für Hersteller, Anlagenbauer und Betreiber
- ➔ Integrität der Produktfunktionen
- ➔ Absicherung von Safety-Mechanismen (gegen beabsichtigte Störungen)
- ➔ Absicherung der Produktqualität gegen beabsichtigte Einflüsse
- ➔ Verfügbarkeit von Produktions-Ressourcen (in Anwendungsumgebung)

Bei der Auswahl kryptografischer Komponenten müssen Exportrichtlinien und die damit verbundenen Prozesse beachtet werden. Wenn Produkte mit integ-

Schwachstellen ermitteln: Erfahrungen aus Qualitätstests müssen in den Design-Prozess einfließen.

Foto: beermedia.de / Fotolia

rierter Sicherheit in vielen verschiedenen Bereichen eingesetzt werden sollen, kann dies zu einer Bandbreite von zu implementierenden Maßnahmen (Profilen) führen, um verschiedene Sicherheitsniveaus zu unterstützen.

Auswahlkriterien

Weitere Auswahlkriterien für Security-Mechanismen sind zum Beispiel:

- Benutzerfreundlichkeit: Security-Funktionen sollen möglichst transparent und einfach in Betrieb zu nehmen sein („Plug-and-Operate" für Security)
- Security-Konsistenz in der Gesamtarchitektur: Die gesamte Sicherheit einer Kette (Gesamtsystem) ist nicht besser als ihr schwächstes Glied. Daher ist ein sinnvolles Sicherheitsniveau im Gesamtsystem anzustreben und abzustimmen.
- Migrationsfähigkeit der Lösung: Da eine gewünschte Sicherheitsstufe für eine Gesamtsicherheit in den wenigsten Fällen mit einer einzelnen Maßnahme erreicht werden kann, sind sinnvolle Migrationsstrategien zur sukzessiven Erhöhung des Sicherheitsniveaus erforderlich. Lösungen müssen an vorhandene Infrastrukturen für Security-Managementfunktionen anpassbar sein.
- Kosteneffizienz steht über allem, insbesondere ist die Betrachtung von Folgekosten durch erforderliche Management-Prozesse und -Infrastrukturen notwendig.

Während der Implementierungs- und Testphase können zusätzlich zu den gewohnten Qualitätsmaßnahmen Zertifizierungsprozesse erforderlich werden, deren Aufwände stark von den beabsichtigten Sicherheitsniveaus abhängen. Im Einzelfall können der zeitliche und zusätzliche Kosten-Aufwand beträchtlich sein.

Neben der prozessmäßigen Bewältigung von expliziten Sicherheitsfunktionen an sich ist eine sichere Implementierung von softwarebasierten Anwendungen im Sinne der Softwarequalität zu gewährleisten. Damit ist „Secure Design" ein wichtiger Teil von Security by Design: Für die konsequente Umsetzung sind Schulungen der beteiligten Ingenieure und zielgerichtete Qualitätstests der Ergebnisse bezüglich Schwachstellen erforderlich. Erfahrungen aus den Qualitätstests müssen ausgewertet werde und in den Design-Prozess einfließen.

„Security by Design kann nicht auf einzelne Funktionen beschränkt werden."

Dr. Pierre Kobes
Siemens

Kein „Einmal-Thema"

Ein konsequentes „Security by Design" betrifft natürlich auch Anlagenbauer und Betreiber. Für Security-Management-Funktionen und -Prozesse (Key Management, Audit-Funktionen, Event Handling) müssen Infrastrukturen und Personal mit entsprechender Ausbildung bereitgestellt werden. User-Guidelines, die vonseiten der Hersteller von Produkten und Lösungen zur Verfügung gestellt werden, müssen in die Prozesse integriert werden. Awareness-Schulungen des beteiligten Personals zur Stärkung des Sicherheitsbewusstseins erleichtern das Verständnis für die Maßnahmen und fördern die Qualität der Umsetzung.

Sicherheit ist kein „Einmal-Thema": Die Bedrohungslage verändert sich mit neuen technischen Möglichkeiten für potenzielle Angreifer oder mit der Entdeckung und Veröffentlichung von Schwachstellen in Standardprodukten und -Komponenten. Hersteller und Betreiber müssen darauf mit Patches und Updates reagieren können, Möglichkeiten für das Einbringen von neuen Security-Versionen müssen identifiziert und prozessmäßig eingeplant werden. Die Kosten für Security sind sowohl auf Hersteller- wie auch auf Betreiberseite nicht unerheblich, daher muss in allen beteiligten Prozessen ein Over-Engineering konsequent vermieden werden.

Insgesamt ist festzustellen, dass „Security by Design" nicht auf einzelne Funktionen beschränkt betrachtet werden kann. Ziel ist stets die Realisierung einer übergreifenden Security-Architektur. Dabei sind die Gesamtarchitektur der Anwendungsumgebung und alle Prozesse im Rahmen von Standardisierung, Entwicklung, Produktion und Management zu betrachten. ■

PROFIL

Siemens AG, Corporate Technology (CT), München

Die Siemens-Zentralabteilung CT wirkt mit ihren weltweit über 1600 Forschern als internationales Netzwerk der Kompetenzen und weltweit als Partner für Technologie und Innovationen. CT trägt durch weltweite F&E-Aktivitäten zur Zukunftssicherung des Unternehmens bei.

LINK

www.siemens.com/corporate-technology

AUTOR

Dr. Wolfgang Klasen
Head of Research Group bei der Siemens AG, Corporate Technology, Research & Technology Center, München

FORSCHUNG

Industrielle Fernwartung absichern

Das vom BMBF geförderte Forschungsprojekt „Sibase“ entwickelt einen „Sicherheitsbaukasten für sichere eingebettete Systeme“. IT-Sicherheitsspezialisten versprechen sich einiges davon.

„Es kann nicht das eine Sicherheitsprodukt als Silver Bullet geben, das alle Probleme löst.“

Alexander von Gernler
genua

➔ Herkömmliche industrielle Fernwartung basiert auf der Vermittlung sicherer definierter Kommunikationskanäle zwischen Fernwarter und gewarteter Anlage. Sie wird derzeit mittels zugangsbeschränkter VPN-Verbindungen und einiger Zusatzlogik in den Produkten verschiedener Hersteller realisiert. Neue Herausforderungen für Fernwartung können auf Basis neuer Technologien wie der Separierung mittels Microkernel angegangen werden.

Aus Dornröschenschlaf erwacht

Aus Sicht eines Sicherheitsherstellers sind die IT-Landschaften bei Industriekunden zum einen über die Jahre gewachsen, zum anderen heterogen und divers, weil sie jeweils unterschiedlichen Aufgaben und Ansprüchen genügen müssen. Der Zweck solcher Installationen ist es, zu funktionieren, und nicht durch überlegene Architektur zu glänzen. Allerdings halten viele dieser Netze einem genaueren Blick mit der Sicherheitsbrille nicht stand. Das wurde lange nicht als Problem wahrgenommen: Vor dem Auftreten des Computerwurms Stuxnet im Jahr 2010 wiegten sich die meisten Anlagenbetreiber noch in einem sicherheitstechnischen Dornröschenschlaf. Seit der Stunde null ist ein Verzicht auf eine Sicherheitsbetrachtung jedoch nicht mehr zu verantworten. Es gibt hier und da noch geistige Hintertüren wie eine vorgebliche Netztrennung oder sogenannte „Air Gaps“. Letztere wurden schon vor einigen Jahren als Mythen entzaubert.

Weil die vorliegenden Infrastrukturen gewachsen sind und es sich um Anlagen im laufenden Betrieb handelt, ist ein radikaler Neuansatz, das Netz noch einmal auf der grünen Wiese neu aufzu-

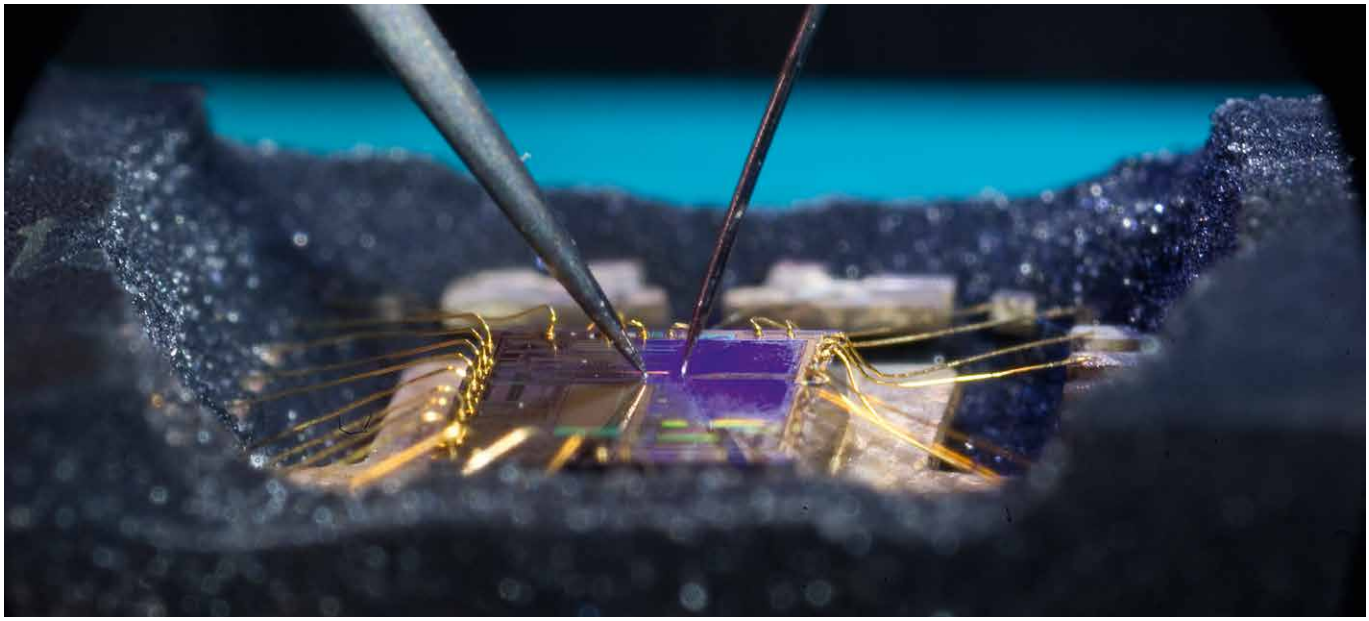


Foto: Fraunhofer Aisec

Durch die Einbettung von hochkomplexen, miteinander vernetzten Systemen werden zukünftige Produkte zunehmend intelligent.

bauen, bereits ausgeschlossen: Die Betreiber werden die bestehende Installation aus guten Gründen nicht über den Haufen werfen wollen und können. Gleichzeitig folgt aus der Verschiedenartigkeit der Netze über die verschiedenen Industriekunden hinweg auch die Erkenntnis, dass es nicht das eine Sicherheitsprodukt als Silver Bullet geben kann, das alle Probleme löst: Zum einen gibt es viele verschiedene Einsatzgebiete für solche Systeme. Zum anderen gibt es in den bestehenden Anlagen eine Vielzahl von Architekturen, Bussen, Plattformen und Protokollen, die unterstützt werden müssten. Eine Lösung, die alle Anforderungen abdecken würde, wäre aufwendig und teuer. Kaum ein Kunde würde für solch ein multifunktionales System viel Geld ausgeben, wenn im konkreten Anwendungsfall nur ein Bruchteil der Features benötigt wird.

„Wir gewinnen Know-how, das wir in unsere Produkte einfließen lassen."

A. von Gernler
genua

Drei Jahre Forschung

Dieses Problem haben Wissenschaft und Hersteller erkannt und sind die Lösung gemeinsam angegangen: Es wurde ein Konsortium gebildet, das im August 2013 mit Förderung des Bundesministeriums für Bildung und Forschung (BMBF) die Arbeit aufgenommen hat. Das Projektkürzel Sibase steht für „Sicherheitsbaukasten für sichere eingebettete Systeme". Das Vorhaben ist auf drei Jahre angelegt und wird von mehreren schwergewichtigen Partnern betrieben.

Um am Ende der drei Jahre mit nachweisbaren Ergebnissen aus dem Projekt gehen zu können, hat sich das Konsortium der Erstellung von vier repräsentativen Demonstratoren verschrieben, die in einem jeweils anderen Bereich die Anwendbarkeit des Sicherheitsbaukastens zeigen sollen. Für den Demonstrator zur industriellen Fernwartung ist der IT-Sicherheitsspezialist genua mbH aus Kirchheim federführend zuständig. Hier sollen bestehende Konzepte aus der bisherigen bewährten Fernwartungslösung der Firma weiter verbessert und mittels Microkernel-Technologie auf ein noch höheres Sicherheitsniveau gehoben werden.

Was wird also neu entwickelt? Hierzu muss man wissen, dass die bisherige Lösung mit einem Rendezvous-Server als neutralem Treffpunkt außerhalb sensibler Netzbereiche bereits einen soliden Ansatz darstellt, der unter anderem garantiert,

- dass ein Fernwarter sich nur dann einwählen kann, wenn dies von innen erlaubt wird,
- dass er sich nur auf diejenige Maschine verbinden kann, die er warten soll,
- dass der Rest des Netzes im Moment der Wartung für den Fernwarter gesperrt wird,
- dass seine Sitzung aufgezeichnet werden kann.

Tasks überwachen wichtige Parameter

Allerdings war beim bisherigen Fernwartungskonzept für jedes Abfragen von Daten der Maschine eine Fernwartungsverbindung nötig. In Zukunft soll es dem Fernwarter auch möglich sein, kleine Tasks auf der Fernwartungs-Appliance zu installieren, die sich regelmäßig mit der Maschine verbindet. Beim nächsten regulären Fernwartungsfenster können die Daten dann bequem abgeholt werden, ohne dass in der Zwischenzeit eine ständige Verbindung nötig wäre.

Klein und robust: Die Hardware soll alle Funktionalitäten unterbringen.

Foto: genua

Auch das Einbeziehen von Tasks mehrerer Stakeholder (zum Beispiel Vertreter verschiedener Firmen wie Hersteller, Wartungstechniker, Betreiber, Messbehörden) ist mit diesem Konzept möglich. Allerdings darf gerade hier die Sicherheit nicht auf der Strecke bleiben: Damit die Tasks sich untereinander weder beeinflussen noch sehen können, sind im Vergleich zum früheren Konzept deutliche Änderungen am eingesetzten Betriebssystem notwendig – ein sogenannter Microkernel kommt zum Einsatz, der die verschiedenen Belange hart voneinander separiert. Für den einzelnen Benutzer ändert sich hingegen nichts.

All die genannte Funktionalität möchte genua auf einer kleinen, robusten, passiv gekühlten Hardware unterbringen, die industriellen Formfaktoren und Schienenmontagen genügt. Dies ist anspruchsvoll genug, um die Teilnahme an einem Projekt wie Sibase zu rechtfertigen, an dessen Ende ein funktionierender Prototyp dieser Hardware stehen soll. Aber auch bereits während des noch laufenden Vorhabens kann genua Know-how gewinnen und in seine bestehenden Produkte einfließen lassen. ■

PROFIL

genua mbH, Kirchheim
Das Leistungsspektrum des deutschen Spezialisten für IT-Sicherheit umfasst Firewalls, Hochsicherheits-Gateways, Mobile-Security-Lösungen, Fernwartungs- und VPN-Systeme, fortlaufendes System-Management sowie ein umfangreiches Dienstleistungsangebot. Mitarbeiter: über 180

LINK
www.genua.de

AUTOR
Alexander von Gernler
Technischer Botschafter bei der genua mbH, Kirchheim

LINK
www.sibase.de

Foto: Style Media & Design / Fotolia

APPS

Neue Technologie sicher einsetzen

Der Einsatz von Apps in der Produktion bringt nicht per se nur Nutzen. Aus diesem Grund sollten die Verantwortlichen hier genauer hinschauen, bevor sie eine Entscheidung treffen.

„Der Einsatz von Apps in der Produktion sollte generell einer Sicherheitsbewertung unterzogen werden."

Wolfgang Straßer
@-yet

→ Genaues Hinschauen ist nötig, aber keinesfalls nur bezüglich der Optimierung der Prozesse, sondern ebenso hinsichtlich der möglichen Risiken. Denn die allgemeine Sicherheitslage war, so die Meinung der meisten Sicherheitsexperten, noch nie so bedenklich wie heute.

Fakt ist: Apps können mittlerweile nicht mehr als Hype oder Spielerei abgetan werden, denn sie sind längst bestens etabliert – und das keinesfalls nur im privaten, sondern auch im beruflichen Umfeld – bis in die Produktion. Für die zügig erfolgte Verbreitung gibt es gute Gründe, denn mittels eines dediziert auf einen bestimmten Anwendungszweck zugeschnittenen Stücks Software lassen sich Flexibilität und Effizienz innerhalb von Arbeits- und Produktionsabläufen mittlerweile nachweislich steigern.

Folglich werden die möglichen Einsatzszenarien zunehmend vielfältig – von der Regelung der Maschinenbelegung bis hin zu Wartung, Diagnose und Reparatur der Fertigungsanlagen. Ebenso ausschlaggebend für den hohen Verbreitungsgrad ist, dass mit einem mobilen Endgerät die komfortable Steuerung von jedem beliebigen Standort, auch außerhalb der Werkshalle, vorgenommen werden kann. Fazit: Das Konzept ist unter dem Gesichtspunkt der Arbeitserleichterung und ebenso unter Kosten-/Nutzenaspekten aus den Fabrikhallen nicht mehr wegzudenken.

Einsatzszenarien und Gefahrenquellen

Doch in dem Maße, in dem Apps sich als besonders hilfreich erweisen, steigt auch das daraus resultierende Risikopotenzial für das Unternehmen. Zum Beispiel bietet es sich im Service-Umfeld an, über die im Mobiltelefon eingebaute Kamera im Zusammenspiel mit den verschiedenen Sensoren sowie dem Online-Zugriff auf Konstruktionspläne effizientere Arbeitsbedingungen für Mitarbeiter vor Ort zu schaffen – aber ebenso schafft dies gute Bedingungen für Werkspionage.

Auch in der Personaleinsatzplanung bieten sich vielfältige Möglichkeiten. So ist es aufgrund des mobilen Zugriffs zukünftig realisierbar, dass bei einem Alarm der richtige Mitarbeiter reagiert, ohne vor Ort sein zu müssen.

Bei innovativen Technologieansätzen gibt es nicht nur positive Aspekte – generell ist deren Implementierung im Unternehmen immer mit neuen Risiken verbunden. Der Einsatz von Apps verlangt

hierbei jedoch ein zusätzliches Umdenken. Denn bislang lag im Sinne der Unternehmenssicherheit der Fokus darauf, sich vor Malware zu schützen, die die Schwachstellen von Applikationen und – vor allem in der Produktion – der Infrastruktur ausnutzt.

Technische Schwachstellen

Mit Apps sind Anwendungen im Unternehmensnetzwerk integriert, über die unmittelbar ein Angriff gestartet werden kann – nicht zuletzt, weil sie teilweise unsauber oder schlecht programmiert sind. Das vermehrte Aufkommen fehlerbehafteter Apps resultiert insbesondere daraus, dass seitens der Anbieter meist keine Kriterienkataloge bezüglich Sicherheitsanforderungen vorgegeben werden und eine Abnahme lediglich formal nach funktionalen Eigenschaften erfolgt.

„Im geschäftlichen Umfeld sollten per se keine Gratis-Apps genutzt werden."

Wolfgang Straßer
@-yet

Steht auch in der unternehmensinternen Konzeption Nutzerfreundlichkeit an erster und Sicherheit an hinterer Stelle, dann ergeben sich aus der Kombination von mobilen Endgeräten mit Apps weitere Angriffspunkte. Zum Beispiel die Übernahme von Schnittstellen wie WLAN oder Bluetooth, was unter anderem ein Auslesen von abgespeicherten Daten oder die Übernahme des ganzen Systems ermöglicht sowie eben die „Fremdsteuerung" durch unsichere Apps.

Das Kernproblem beim Einsatz mobiler Geräte liegt in dem grundsätzlich unsicheren Gesamtpaket. Die allermeisten Smartphones und Tablets, egal ob es sich um Android, IOS oder windowsbasierte Systeme handelt, sind als unsicher und leicht hackbar einzustufen – sowohl über kabellose Zugriffe (GSM, WLAN), aber vor allem auch bei direktem Zugriff.

Eine zusätzliche Gefahr besteht darin, dass so ein Gerät leicht verloren geht. Kommen dann noch unsichere Apps hinzu, können sich hier Schwachstellen ergeben, die große Sicherheitsprobleme hervorrufen. Datendiebstahl ist dabei noch der geringste Schaden, bedeutend schwerer wiegen Manipulationsmöglichkeiten von Steuerungen.

Erste Hilfe für mehr Sicherheit

Im geschäftlichen Umfeld sollten per se keine Gratis-Apps genutzt werden, auch wenn es wirklich gute kostenlose Software gibt. Ein Konzeptansatz, um für Unternehmen einen bedenkenloseren Einsatz von Apps zu gewährleisten, sind sogenannte Reputationssysteme. Dabei etablieren Hersteller eigene App-Stores und verkaufen dort nur Programme, die vor der offiziellen Freigabe umfassend analysiert worden sind. Ebenso gilt es, von Beginn an sicherzustellen, dass jede Aktualisierung nicht nur durchgeführt, sondern auch stets einer erneuten Überprüfung unterzogen wird. Im Prinzip müsste die Einführung von Apps – wie bei der Implementierung von klassischer Software – gegen die spezifischen Sicherheitsanforderungen im Unternehmen getestet werden.

Doch nicht nur mit den Apps, auch mit diversen Mobiltelefonen bewegen sich Unternehmen nach wie vor auf unsicherem Terrain: Denn die meisten Endgeräte sind per se über ihr Betriebssystem angreifbar. Von daher obliegt es den Unternehmen, mittels Richtlinien detailliert festzuschreiben, welche mobilen Endgeräte in der Produktion eingesetzt und wie die vorhandenen Schutzmaßnahmen auf diesen installiert werden, sowie die Einhaltung dieser Regelungen auch sorgfältig zu kontrollieren.

Umfassendes Wissen ist das A und O

Das Konzept zum Einsatz von Apps in der Produktion sollte generell einer Risikobewertung unterzogen werden. Hierbei gilt es, neben dem Nutzen sowohl die Sicherheitsqualität der Apps als auch die Vertrauenswürdigkeit des Herstellers zu überprüfen. Schulungs- und Trainingsmaßnahmen für die Mitarbeiter bezüglich der Gefahrenpotenziale sollten ebenso obligat sein wie eine durchdachte Mobility-Strategie. ■

AUTOR
Wolfgang Straßer
Experte für IT-Sicherheit und IT-Risikomanagement, Geschäftsführer bei der @-yet GmbH, Leichlingen

PROFIL

@-yet GmbH, Leichlingen
Das Beratungshaus mit Fokus auf IT-Risikomanagement, Out & Cloud, Security Awareness verfolgt die aktuellen IT- und Sicherheitstrends sowie Angriffsszenarien und optimiert IT-Prozesse. Mitarbeiter: 28

LINK
www.add-yet.de

Foto: lassedesignen / Fotolia

Unsichere Endgeräte und unsichere Apps ergeben gute Manipulationsmöglichkeiten von Steuerungen.