Zeitschrift: Bulletin Electrosuisse
Herausgeber: Electrosuisse, Verband für Elektro-, Energie- und Informationstechnik
Band: 99 (2008)
Heft: 5

Artikel: Neue Gefahren für Produktionsanlagen
Autor: Ruf, Lukas
DOI: https://doi.org/10.5169/seals-855826

Neue Gefahren für Produktionsanlagen

Einheitliche TCP/IP-Netzwerke bergen auch Risiken

Die Integration von Fertigungs- und Produktionsanlagen in Firmennetzwerke eröffnet dem Supply Chain Management und Enterprise Resource Planning neue Möglichkeiten der Automatisierung und Optimierung. Diese Integration birgt jedoch neuartige Gefahren für die Produktionsabläufe, die eine Risiko- und Sicherheitsbeurteilung der Anlagen und deren Anbindung an das Firmennetzwerk erfordern. Zukünftig müssen in diese Sicherheitsbeurteilung verstärkt Analysen miteinbezogen werden, wie sie für Onlinebanking und generell für Anwendungen, die mit personenbezogenen Daten arbeiten, üblich sind.

Im Bereich der Integration von Industrieanlagen sind zwei Trends feststellbar: Einerseits wird die vertikale Integration von Supply Chain Management (SCM) über Enterprise Resource Planning (ERP) bis hin zu den Produktionsanlagen über ein homogenes Netzwerk mit TCP/IP über Ethernet verstärkt. Andererseits wird horizontal ebenfalls vermehrt auf TCP/IP über Ethernet umgestellt [1]. Zugleich kommen immer häufiger allgemein verwendete Betriebssysteme mit entsprechenden Anpassungen auf allen Stufen zum Einsatz. So finden sich

Lukas Ruf

heute in unterschiedlichsten Komponenten speziell angepasste Varianten von Microsoft Windows oder Unix-Derivaten wie Linux oder BSD-Varianten.

Beide Trends sind mehr als berechtigt, gestatten sie doch eine Vereinfachung der Betriebsabläufe und eine bessere Überwachung der einzelnen Vorgänge vertikal auf allen Stufen. Zudem erlaubt der vereinheitlichte Einsatz von TCP/IP über Ethernet ein effizienteres Wissensmanagement und eine vereinfachte Komponentenverwaltung, da weder spezifische Eigenarten unterschiedlicher Netzwerktechnologien noch grundlegend verschiedene Komponenten verwaltet werden müssen. Interessant wird die horizontale Integration insbesondere dann, wenn beispielsweise Sensoren ihre Informationen in einem einheitlichen System an die Schaltzentralen leiten können.

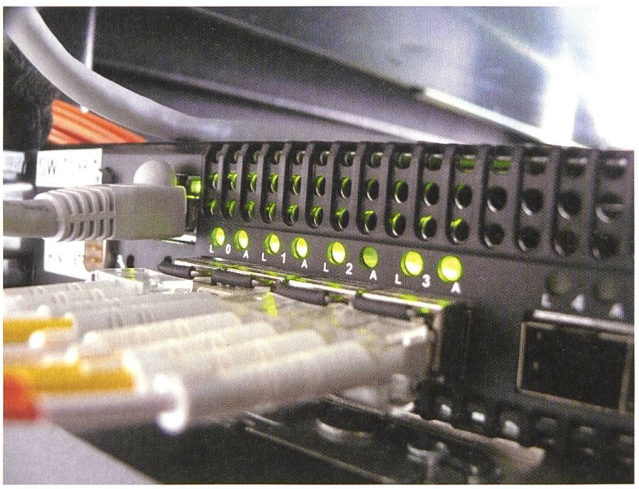
Die verstärkte Homogenisierung hat aber auch zur Folge, dass Produktionsanlagen den gleichen Bedrohungen und Gefahren ausgesetzt werden, wie sie heute beim Onlinebanking oder generell bei personenbezogenen Transaktionen wie bei Spitälern, Krankenkassen, Versicherungen oder staatlichen und Bundesstellen zu bewältigen sind. Diese für Industrieanlagen neuartigen Bedrohungen werden insofern immer relevanter, da eine klare Separierung in Administration und Produktion aus Kostengründen zunehmend verschwindet. Verstärkt wird auf eine logische Segmentierung durch Firewall- oder VLAN-Technologien (IEEE 802.1q) gesetzt, die zwar unter vorgesehenen Umständen das gewünschte Resultat hervorbringt, unter Ausnahmesituationen, die beispielsweise durch menschliche Fehlkonfigurationen hervorgerufen werden können, aber versagen.

Obwohl nicht direkt ein Beispiel für industrielle Produktionsanlagen, sei auf diese Problematik beim neuen Boeing Dreamliner 787 hingewiesen: Man stelle sich vor, die US Federal Aviation Administration (FAA) hätte bei der Zulassung des Boeing Dreamliners 787-8 den Finger nicht auf die ungenügende Trennung des Unterhaltungsnetzwerks vom Steuernetzwerk gelegt, und während eines Fluges hätte der Sitznachbar unglücklicherweise die Höhensteuerung der 787 durch eine unbeabsichtigte Netzwerküberlastsituation lahmgelegt.

Dieses Beispiel verdeutlicht die Relevanz der klaren Unterteilung von Operationsbereichen (Operational Domains). Bei verteilten Steuerungsanlagen in industriellen Anlagen, die gleich wie die 787 unter Kostendruck vermehrt auf eine logische Seg-

Boeing

Bild 1 Erst auf Druck der Behörden trennte Boeing beim Dreamliner 787-8 das Steuernetzwerk für die Piloten vom Unterhaltungsnetzwerk für die Passagiere.



Pixelio.de

Bild 2 Immer mehr Produktionsanlagen kommunizieren über TCP/IP.

mentierung anstelle einer physischen Separation setzen, sind die Herausforderungen für einen sicheren und zuverlässigen Betrieb gleich gelagert. Durch die horizontale Homogenisierung in Netzwerk- und Betriebssystemtechniken wird zudem die Anfälligkeit eines Systems im schlimmsten Fall potenziert, da durch eine unglückliche Verkettung aus einem einzelnen Problem eine erdrückende Lawine werden kann, die zu Systemabstürzen oder Produktionsfehlern führt.

Herausforderungen in vertikal und horizontal integrierten Industrieanlagen können durch ein klares Verständnis der Bedrohungen mit geeigneten Gegenmassnahmen gemeistert werden. Um diese einzuschätzen, ist ein Verständnis der grundlegenden Sicherheitseigenschaften eines verteilten IT-Systems nötig. Diese werden nachfolgend eingeführt und im speziellen Anwendungsfall diskutiert.

Überlegungen zur IT-Sicherheit

Grundlegende Probleme, die für diese Art von eingebetteten, vertikal und horizontal integrierten Systemen auftreten können, manifestieren sich in den klassischen Anforderungen an die IT-Sicherheit: Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Autorisierbarkeit und im Zusammenhang mit einstellungsverändernden Vorgängen (Konfiguration) auch die Nachvollziehbarkeit (Traceability) und Zuordnungsbarkeit (Accountability). Um sie gewährleisten zu können, müssen geeignete Techniken eingesetzt werden.

Während in nicht eingebetteten Systemen, wie sie für Onlinebanking benötigt werden, Speicher (RAM), Rechenleistung und Kommunikationskapazitäten eine untergeordnete Rolle spielen, muss der Einsatz der gewählten Techniken in eingebetteten Systemen genau abgestimmt werden. Aus diesem Grund wird als Teil der Einführung der Sicherheitsanforderungen eine Übersicht über verschiedene Techniken und deren Eigenschaften gegeben.

Vertraulichkeit

Vertraulichkeit bezeichnet die Eigenschaft, dass nur bezeichnete Personen die Information einsehen können, für die sie bestimmt ist. Vertraulichkeit bei kommunizierter Information wird durch Verschlüsselung der übertragenen Daten erreicht. Für die Verschlüsselung kommen unterschiedliche Algorithmen infrage, die entsprechend der jeweils vorhandenen Anforderungen gewählt werden sollten. Primär muss dabei zwischen symmetrischer und asymmetrischer Verschlüsselung unterschieden werden.

Im Fall von symmetrischer Verschlüsselung basiert die Vertraulichkeitsgewährleistung auf dem Vorhandensein eines einzig den involvierten Systemen bekannten Geheimnisses, dem vertraulichen Schlüssel (Secret Key). Heute ist AES (Advanced Encryption Standard) State of the Art. AES basiert auf dem Algorithmus Rijndael, der im Oktober 2000 vom US National Institute of Standards and Technology (NIST) als Nachfolger des DES (Data Encryption Standard, IBM, 1976) in einem über drei Jahre andauernden Selektionsverfahren aus einer engeren Auswahl von fünf Kandidaten (Rijndael, MARS, RC6, Serpent, Twofish) auserkoren wurde. AES zeichnet sich unter anderem dadurch aus, dass er klar und einfach gestaltet ist, ohne Lizenzkosten eingesetzt und einfach in Hardware implementiert werden kann.

Bei asymmetrischer Verschlüsselung wird die Vertraulichkeit durch eine Verschlüsselung gewährleistet, die durch einen öffentlichen und einen privaten Schlüssel gesichert wird. Dabei wird der öffentliche Schlüssel verwendet, um Daten so zu verschlüsseln, dass sie nur mit dem privaten entschlüsselt werden können. Dies bedeutet, dass der öffentliche Schlüssel publiziert werden soll, damit Information möglichst vertraulich übermittelt werden kann, während der private geheim gehalten werden muss. Heute State of the Art ist der RSA-Algorithmus, der als Akronym nach seinen Entwicklern Rivest, Shamir und Adleman benannt wurde. RSA wurde während 25 Jahren patentrechtlich geschützt. Seit September 2000 ist der Algorithmus frei einsetzbar und kann so ohne Lizenzkosten verwendet werden.

Was wird wie verschlüsselt?

Symmetrische Verschlüsselung findet überall dort ihren Einsatz, wo auf vergleichsweise effiziente Art viele Daten verschlüsselt werden sollen. Beispiele sind verschlüsselte Übertragungskanäle, wie sie durch TLS (Transport Layer Security), dem standardisierten Nachfolger von SSL v3 (Secure Socket Layer), realisiert werden. Ein weiteres Beispiel setzt AES ein. AES wird häufig für das Verschlüsseln von Daten in Datenbanken oder verschlüsselten USB-Sticks eingesetzt.

Asymmetrische Verschlüsselung hingegen wird dort eingesetzt, wo eine nahezu unbekannte Gruppe mit einem Empfänger vertraulich kommunizieren soll, indem der öffentliche Schlüssel bedenkenlos verbreitet werden kann. Da asymmetrische Algorithmen aufwendiger in der Verschlüsselung von Daten sind, werden sie üblicherweise nur für die Verschlüsselung eines zufälligen symmetrischen Schlüssels verwendet, der dann für die Verschlüsselung der Daten eingesetzt wird.

Authentizität, Autorisierung, Accountability und Nachvollziehbarkeit

Obwohl häufig in industriellen Anlagen vernachlässigt, ist die Gewährleistung der Vertraulichkeit bei administrativen Vorgängen von essenzieller Bedeutung. Das Ausspionieren von Authentisierungsmerkmalen (Credentials) wie Benutzername und Passwort ermöglicht unberechtigten Drittpersonen Zugriff auf Informationen.

Der Diebstahl von geistigem Eigentum (Intellectual Property Rights, IPR) oder die Veröffentlichung von Informationen hat in industriellen Anlagen während der Produktion sehr wahrscheinlich nur ein geringfügiges Bedrohungsprofil. Doch ist die Gewährleistung der Authentizität, d.h. der korrekten Urheberschaft der Konfigurationsvorgänge kritisch. Frustrierte Mitarbeiter, die als vermeintliche Hacker an die Authentisierungsmerkmale gelangen, können zum Beispiel jegliche Form der Autorisierung von Kon-

figurationseinstellungen umgehen. Insbesondere in grossen, verteilten Anlagen, wo eine zentrale Kontrollstelle sowohl Betrieb als auch Konfiguration und Kontrolle sicherstellt, ist der Schutz der Zugangsmerkmale kritisch, da Bereiche mit einem vom lokalen Bereich abweichenden Vertrauenswürdigkeitsgrad eingesetzt werden können, beispielsweise das Internet. Dadurch wird es für die zentralen Stellen immer schwieriger, sicher zu sein, dass die vertraulichen Daten nicht auch von unberechtigten Drittpersonen mitgelesen werden.

Gerade dort ist es relevant, dass eine klare Zuordnung von Vorgängen (Accountability) bei Konfigurationen und die Nachvollziehbarkeit der einzelnen Vorgänge klar möglich sind. Accountability bedingt, dass Benutzer über mehrere Schritte eindeutig identifiziert werden müssen. Somit ist es möglich, Veränderungen an den Einstellungen der Systeme zu erkennen und die Urheber ausfindig zu machen.

ESP Seattle

Bild 3 Einheitliche TCP/IP-Netzwerke in der Produktion und dem Büro vereinfachen vieles, bergen aber auch Risiken.

Einschränkungen in industriellen Anlagen

Verschlüsselung ist aber ein vergleichsweise ressourcenintensiver Prozess, der nur dort eingesetzt werden soll, wo vertrauliche Daten übermittelt werden. In industriellen Anlagen wird Verschlüsselung per se aus diesem Grund nur, wenn überhaupt, für administrative Konfigurationsvorgänge verwendet. Administrative Aufgaben sollten jedoch unbedingt über verschlüsselte Kanäle erfolgen, wenn sie von einem zentralen Steuerungsrechner ausgehen. Insbesonders ist bei der Planung neuer Anlagen darauf zu achten: Die rasante Weiterentwicklung der horizontalen und vertikalen Integration kann durchaus zur Folge haben, dass heute isoliert administrierte Systeme in naher Zukunft von einem zentralen Rechner eingestellt werden. Zudem: Bei Produktionsabläufen fehlen üblicherweise die Ressourcen, um alle kommunizierten Daten zu verschlüsseln.

Integritätsschutz und Verfügbarkeit

In Produktionsabläufen spielen Integritätsschutz und Verfügbarkeit bei der Kommunikation von Steuerungssignalen eine gewichtigere Rolle, da Produktionsabläufe einerseits unter für die Kommunikation widrigen Umständen erfolgen und andererseits Produktionsmaschinen unter Echtzeitbedingungen reagieren müssen. Man stelle sich vor, was passiert, wenn in einer Zeitungsdruckerei Bitfehler bei einem Rückmeldekontrollsystem (Feedback) auftreten, in dem ein Sensor den Zeitungsstapel misst, um dem Stapler mitzuteilen, ob ein neuer Stapel benötigt wird.

Durch den Einsatz von homogenisierten Netzwerklösungen können kostengünstig Interface-Chips eingesetzt werden, die Bitfehler dieser Art mindestens entdecken oder gar korrigieren können. In ersterem Falle werden empfangene Daten normalerweise einfach verworfen. Heute weitverbreitete Algorithmen, die auf Messagelevel zur Detektion von Datenmanipulationen eingesetzt werden, basieren auf Checksummen. Diese unterscheiden sich prinzipiell in der Art ihrer Berechnungen. Einfache, zyklische Redundanzchecks (Cyclical Redundancy Checks, CRC) sind sehr schnell, haben jedoch den Nachteil, dass Kollisionen auftreten können. Dies bedeutet, dass zwei unterschiedliche Messages die gleiche Checksumme produzieren können und so im ungünstigsten Fall Fehler unentdeckt propagiert werden. Kryptografische Berechnungen von Hash-Werten haben den Vorteil, dass sie praktisch kollisionsfrei sind, leiden jedoch unter dem Nachteil, dass ihre Berechnung zeitaufwendiger ist. Heutzutage weitverbreitete Algorithmen sind HMAC (Hash Message Authentication Code), SHA-1 (Secure Hash Algorithmus, FIPS 180-1) oder MD5 (Message Digest).

Beim Einsatz von Message Authentication Codes (MAC) in Echtzeitsystemen muss eine Abwägung der geforderten Zuverlässigkeit in Relation zum benötigten Aufwand durchgeführt werden, damit das System nicht durch die Berechnung von MACs selbst vollständig ausgelastet wird. Würde diese Abwägung nicht sauber durchgeführt, könnten Überlastsituationen mit daraus resultierendem, stark verzögertem Reaktionsverhalten sehr schnell herangeführt werden: Wenn beispielsweise nur schon eine leicht höhere als normalerweise übliche Daten- resp. Message-Rate empfangen und verarbeitet werden muss, kann ein eng dimensioniertes System an seine Grenzen gebracht werden

Um diese Raten zu kontrollieren, kann dank vereinheitlichter Infrastrukturen auf Switches und Router zurückgegriffen werden, wie sie heute in traditionellen Computernetzwerken wie dem Internet üblich sind. Diese gestatten eine feinstufige Justierung der Daten- und Message-Raten und erlauben die Definition ihres Verhaltens in Ausnahmesituationen. Switches, die für die logische Segmentierung von Netzen eingesetzt werden, verfügen üblicherweise über die Möglichkeit der Ratenbegrenzung.

Die Komplexität nimmt zu

Durch den Einsatz von homogenisierten Plattformen, bei denen allgemein verwendete Betriebssysteme mit spezifischen Anpassungen eingesetzt werden, sinken die Anforderungen beim Wissens- und Komponentenmanagement. Durch die Verwendung von «gewöhnlichen» Betriebssystemen wird es jedoch schwieriger, Systeme und Anlagen vollends kontrollieren zu können. So werden für den Anwendungsfall neuartige Bedrohungen eingeführt, die zuvor nicht existierten.

Dies bedeutet, dass die Komplexität einer vertikal und horizontal integrierten Anlage im industriellen Umfeld mit dem Grad ihrer Integration zunimmt, da nicht mehr nur isolierte, sondern eben auch vernetzte Systeme betrachtet werden müssen, die

sich gegenseitig negativ beeinflussen können.

Da aus Kostengründen zudem vermehrt auf eine physikalische Separation der Anlagen verzichtet und «nur» eine logische Segmentierung umgesetzt wird, steigen die zu meisternden Herausforderungen. Um zu verhindern, dass in Zukunft der Dreamliner als Vertreter eines logisch segmentierten, verteilten Systems von Steuerrechnern und anderweitig eingesetzten Computer einen Schwenker macht, wenn der Nachbar am Spielen ist, müssen vermehrt auch Sicherheitsaspekte in die Architektur, das Design und die Entwicklung der Bordnetzwerke miteinbezogen werden.

So werden durch Integration und Homogenisierung der Plattformen Sicherheitsanalysen und -überprüfungen nötig, die zuvor eine untergeordnete Rolle spielten. Vermehrt spielen auch sicherheitsbezogene System- und Prozessanalysen eine Rolle, damit beispielsweise ein Fernzugriff die Stabilität und somit den Produktionsablauf nicht nachhaltig gefährdet. In der Sicherheit von integrierten Anlagen gibt es keine One-fits-all-Sicherheitslösung. Vielmehr müssen die Anforderungen und möglichen Lösungen individuell und situationsspezifisch betrachtet werden. Die Kenntnis und ein Basisverständnis der grundlegenden Sicherheitseigenschaften sind hingegen generell anwendbar und gestatten ein Erkennen der Problematik und der Herausforderungen, die in Zukunft verstärkt auf uns zukommen werden.

Résumé

De nouveaux dangers pour les installations de production

Les réseaux TCP/IP unifiés présentent eux aussi des risques. L'intégration des installations de fabrication et de production dans les réseaux de sociétés ouvre au Supply Chain Management et à l'Enterprise Resource Planning de nouvelles possibilités d'automatisation et d'optimisation. Cette intégration présente cependant de nouveaux dangers pour les opérations de production nécessitant une évaluation de risque et de sécurité des installations et de leur intégration au réseau de la société. A l'avenir, cette évaluation de sécurité devra comprendre davantage d'analyses telles qu'elles sont déjà courantes dans l'online banking et d'une manière générale dans les applications travaillant avec des données personnelles.

Referenzen

[1] Markus Brändle, Martin Naedele: Automatisierungsanlagen gegen Angriffe sichern, Bulletin SEV/VSE Nr. 7/2007.

Angaben zum Autor

Dr. *Lukas Ruf* ist Geschäftsführer der Consecom AG. In den Bereichen IT-Sicherheits- und -Strategieberatung unterstützt die Consecom AG Kunden bei der Lösung von Sicherheitsanforderungen durch Architektur-, Implementation- und Prozessberatung sowie Reviews und Assessments.
Consecom AG, 8002 Zürich,
lukas.ruf@consecom.com

articles spécialisés