16 17. August – 30. August 2015 / 25. Jahrgang / € 6,– ISSN 1864-0907

IT-BUSINESS

Windows 10 und die Folgen

Windows 10 wird keinen Nachfolger mehr haben. Für Microsoft-Manager Oliver Gürtler hat das weitreichende Konsequenzen für Reseller und Systemhäuser. > 22

Pionier wider Willen

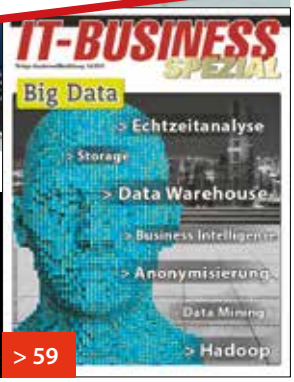
Der spannende Weg eines Systemhauses zum Rechenzentrumsbetreiber und Channel-Dienstleister. > 8

US-Clouds ohne Vertrauen

Amerikanische Cloud-Anbieter haben in Deutschland einen schweren Stand. > 47

IFA mit Sogwirkung

Eine Viertelmillion Besucher und viele IT-Anbieter drängen sich unter dem Berliner Funkturm. > 52



> 59

Vogel Business Media

Der Stand der Vernetzung

Thema: Die vierte industrielle Revolution in der Praxis
Hintergrund: Industrie 4.0 ist gerade erst in den Startlöchern.
[www.bit.ly/ITB_Ind4]

Autor: Dr. Andreas Bergler

email: andreas.bergler@it-business.de
tel: 0821 2177 141

BILD: INDUSTRIEBLICK_FOTOLIA.COM

BILD: BRIDGINGIT

Industrie 4.0: Von der Praxis weit entfernt

Über IP-fähige Maschinen und Systeme soll die reale und virtuelle Welt zusammenwachsen. Martin Jansen von bridgingIT über den aktuellen Entwicklungsstand von Industrie 4.0.

Zur Person

Martin Jansen ist Senior Consultant und Experte für Industrie 4.0 bei bridgingIT. Als unabhängiges IT-Beratungsunternehmen hilft bridgingIT bei der Umsetzung von Unternehmensstrategien und dem Einsatz moderner Technologien und verbindet dabei die Anforderungen der IT mit denen der Fachseite.

> **Intelligente Maschinen, Lagersysteme und Produktionsmittel wirken zusammen, indem sie sich eindeutig identifizieren, untereinander Daten austauschen und sich wechselseitig steuern. Wie realistisch ist das?**
Bis dahin ist noch ein weiter Weg. Fertigungsbetriebe, die schon heute ins Industrie-4.0-Zeitalter starten wollen, müssen mit den Mitteln auskommen, die ihnen der Markt zur Verfügung stellt. Demzufolge defensiv sollten sie ihre Automatisierungsmaschinen, Steuerungssysteme, Sensoren und anderen Fertigungskomponenten und somit ihre vernetzte Fabrik positionieren.

Wo sollten Firmen diese Systeme und Komponenten platzieren?
Auf jeden Fall klassisch und abgeschottet innerhalb der firmeneigenen Cloud. Nur so können sie vor Attacken von außen gut geschützt werden. Im öffentlichen, hoch angriffsgefährdeten Internet haben weder solche Maschinen, Systeme und Komponenten noch fertigungskritische Daten, wozu auch die Auftrags- und Kundendaten gehören, etwas zu suchen.

Ohne Schnittstellen nach außen, wie zu Lieferanten und Logistikunternehmen, wird die vernetzte Fabrik aber nicht funktionieren...
Natürlich sollten an diesen Schnittstellen die Daten stark verschlüsselt übertragen werden. Daneben empfiehlt sich eine Fragmentierung der Datenpakete, um sie am Ziel nach einer vorgegebenen Logik

wieder zusammenzusetzen. Selbst wenn es Angreifern gelingen sollte, die Verschlüsselungsalgorithmen zu dekodieren, haben sie dennoch nur Zugriff auf nichtssagende Paketfragmente. Es versteht sich von selbst, dass die Informationen darüber, wie sich die Datenpakete zusammensetzen, natürlich nicht mit übertragen werden sollten. Zuvor sollte das Fertigungsunternehmen genau hinterfragen, welche Daten der Lieferant beziehungsweise Logistiker zur Ausführung seiner Aufgaben tatsächlich braucht, um die Risiken zusätzlich zu begrenzen. Gleiches gilt für Managementinformationen und Dashboard-Visualisierungen, bei denen externe Medien wie Mobile Solutions, Internet-Applikationen und Social Media zum Einsatz kommen.

Gilt dann das, was für die Anbindung von Lieferanten und Logistikern gilt, auch für eine geografisch verteilte Produktion?
Ja, starke Verschlüsselung und Fragmentierung der Datenpakete sind auch in diesem Fall angemessene Sicherheitsvorkehrungen zum Schutz der Daten, ebenso wie eine gründliche Analyse, welche Daten zur Fertigung der Teile in den Zweigwerken tatsächlich gebraucht werden. Im Zusammenspiel der Werke, erst recht, wenn in Staaten wie China gefertigt wird, sollten für Industrie 4.0 grundsätzliche strategische Überlegungen und Entscheidungen getroffen werden. So sollten für das Gesamtprodukt tragende Teile keinesfalls in Ländern mit hohen Industriespionage-Aktivitäten gefertigt werden. Nur die günstigen Fertigungskosten zu sehen, wäre kurzsichtig. Vorausschauender ist es, den gesunden Menschenverstand walten zu lassen.

Ganz ohne den Austausch kritischer Daten und das Zusammenspiel wichtiger Systeme wird Industrie 4.0 nicht funktionieren. Wie hoch schätzen Sie die Gefahr der Sabotage ein?
Die Risiken, dass kritische Ausführungsketten sabotiert werden könnten, ist nicht von der Hand zu weisen. Zumal die Gefahr wächst, Opfer von Industriespionen zu werden, die auch unter dem Deckmantel von Geheimdiensten attackieren. Deshalb ist es, neben den vorgenannten Überlegungen und Vorkehrungen wichtig, redundante Systeme, Datenbasen und Verbindungen herauszubilden. Zudem sollten Steuerungen so ausgelegt werden, dass auch der Ausfall von Sensoren, die per Funk angesprochen werden, verkraftet werden kann. Dann kann im Fall eines Falles immer ein Ausweichsystem einspringen, um die Ausführungskette aufrechtzuerhalten.

Apropos Industriespionage: Kann angesichts solcher Aktivitäten nicht auch der Einsatz von Systemen, die mehrheitlich aus den USA stammen, Risiken in sich bergen?
Was die installierten IT-Infrastrukturen in den Unternehmen betrifft, könnten die Aktivitäten von Industriespionen und Geheimdiensten dort zu einem Umkehrtrend führen. Nicht mehr Konsolidierung und Homogenisierung auf Basis weniger Herstellersysteme sind angeraten, sondern eine heterogene Auslegung der Systeme mit vielen unterschiedlichen Schnittstellen, um es Angreifern so schwer wie möglich zu machen, tragende Systeme im Back-end zu infiltrieren und zu attackieren. Der Aufbau intelligenter Netze ist hier der entscheidende Punkt, um auch weiterhin Produktionssysteme mit hoher Effizienz zu erreichen. Ein Kunde von uns wird sogar ein eigenes Bus-System für die Verarbeitung der Fertigungsdaten mit Schnittstellen zu Zulieferern und Logistikern und mit integrierten Werkzeugen für Analysen, Simulationen und Trendermittlungen entwickeln. Dadurch schließt er kompromittierte Systeme und Ausspähungen aus. Aber nicht nur technische, sondern auch organisatorische Konzepte werden sich in den Fertigungsunternehmen für Industrie 4.0 ändern müssen.

Das bedeutet?
Wie gesagt, eine klare Trennung von Fertigungsdaten auf der einen und Lieferanten- und Logistikdaten auf der anderen Seite. Ebenso sollten in durch Industriespione und Geheimdienste besonders gefährdeten Ländern keine kritischen Teile gefertigt werden. Bevor Sicherheit in Technik umgesetzt wird, ist Security und die Abwehr von Risiken vor allem eines: eine organisatorische Herausforderung. Sie muss im Kontext neuer Geschäftsmodelle gesehen werden, die sich durch Industrie 4.0 zwangsläufig ändern werden. Last but not least steigt mit jedem Automatisierungsschritt tiefer in die vernetzte Fabrik der Bedarf an einem professionellen Veränderungsmanagement, denn damit gehen soziale Umbrüche einher. Aber das ist noch Zukunftsmusik.
[www.bridging-it.de]

Baustein der Vernetzung: Die vierte industrielle Revolution

> Nach Dampfkraft, Massenfertigung und Automatisierung durch den Einsatz von Elektronik und IT steht nun Industrie 4.0 an. Dahinter steht die Idee, dass Kunden und Geschäftspartner im Internet über Cyber-spezifische Systeme (CPS) an den Geschäfts- und Wertschöpfungsprozessen des Unternehmens aktiv teilhaben, indem sie direkt auf die Gestaltung von Produkten und Dienstleistungen Einfluss nehmen.
Laut Statista wird das weltweit durch die Kommunikation von Maschinen erzeugte Datenvolumen 2018 knapp ein Exabyte monatlich betragen. In den nächsten drei Jahren soll sich das Datenvolumen jährlich verdoppeln.
[www.statista.de]

Sicherheit in der M2M-Kommunikation

BILD:DAVIS_FOTOLIA.COM

Die NSA hat das Vertrauen in amerikanische Hersteller erschüttert.

> Die Unternehmen konzentrieren sich derzeit auf das Sammeln und Bewerten fertigungsrelevanter Daten innerhalb der eigenen Cloud, um sie für Industrie 4.0 nutzbar zu machen, stellt Martin Jansen fest. Die Absicherung von M2M-Transaktionen stehe derzeit weder im Fokus der Unternehmen noch der Lösungsanbieter. Vorerst werden bestenfalls Prototypen gebaut, um Erfahrungen für M2M-Interaktionen zu sammeln. Diese Prototypen seien aber von einer Einsatzreife weit entfernt. Bis der Markt praxistaugliche und hinreichend abgesicherte branchenspezifische Out-of-the-Box-Lösungen bietet, werden noch einige Jahre vergehen – zumal auch hier immer wieder Aufwand und Nutzen hinsichtlich Leistung und Sicherheit abzuwägen sind.

bridging IT

Menschen Methoden Lösungen

BridgingIT GmbH
N7, 5-6
68161 Mannheim
Tel.+49 621 370 902 - 0
www.bridging-it.de

innovation@bridging-it.de