VISIONÄRE GEDANKEN UND REALE MÄRKTE

Als globaler IT-Distributor hat man den großen Vorteil, sowohl die visionären Gedanken und Entwicklungen der IT-Hersteller zu kennen, als auch den realen Markt, seine Marktbeteiligten und seine Gegebenheiten. Daraus ergeben sich stets neue Herausforderungen – aber auch großartige Gelegenheiten für Geschäfte.

Text: **Barbara Eisenberg**

Auch wenn die Individualität von IoT-Projekten nicht größer sein könnte, so haben sie in den gelieferten Mehrwerten für Unternehmen vieles gemeinsam: Zeit- und Ressourceneinsparungen, Beschleunigung von Prozessen, Realisierung neuer Geschäfts- und Profitmodelle, Echtzeitüberwachung von Leistungsindikatoren, Verbesserung der betrieblichen Effizienz durch flexiblere Produktionstechniken und die Nutzung intelligenter vernetzter Systeme sowie Kostensenkung durch Predictive Maintenance, Condition Monitoring oder Track & Trace-Lösungen – um nur ein paar Vorteile zu nennen.

Die Komplexität von IoT-Projekten ist jedoch nicht zu unterschätzen. Sie wird einerseits durch das Zusammenspiel von IT & OT bestimmt, in denen unterschiedliche Standards gelten, andererseits aber auch durch die benötigten hybriden und oft herstellerübergreifenden Umgebungen.

Bei IoT-Projekten ist eine enge Zusammenarbeit der Bereiche Operational Technology und Information Technology unabdingbar.

Tech Data konzentriert sich auf Lösungen für die Branchen Fertigung, Transport & Logistik, Smart Space und Einzelhandel. Für diese Branchen stellen wir Systemintegratoren und Systemhäusern spezialisierte Beratung sowie leistungsfähige, adaptierbare und skalierbare IoT-Lösungen bereit. Das gesamte Spektrum der Entwicklung, Integration und Wartung von IoT-Architekturen wird dabei abgedeckt – von der Sensorebene über die Konnektivität bis hin zu Business Intelligence.

IOT IN DER FERTIGUNGSINDUSTRIE

Durch die Verbindung bestehender industrieller Subsysteme, Sensoren und Maschinen mit Aktoren und Unternehmensanwendungen wird die Grundlage für eine hochintegrierte und intelligente Entscheidungskette geschaffen, und damit für dramatische Verbesserungen der wichtigsten Leistungskennzahlen in der Fertigung. Die Lösungen ermöglichen es Unternehmen, durch effektive Sensorimplementierung/SPS-Integration, Datenerfassung, Analyse-, Maschine Learning- und Visualisierungstools Probleme zu erfassen oder vorherzusagen. Die Produktionsleistung und -qualität wird so maßgeblich verbessert und Maschinenstillstandzeiten im Produktionsbetrieb auf ein Minimum reduziert. Wartungskosten werden nebenbei gesenkt und der Produktionsbetrieb eines Unternehmens erfährt eine Verbesserung der GAE (Gesamt Anlagen Effektivität).

IOT IM LOGISTIK- UND TRANSPORTWESEN

Die Integration von IoT-Lösungen, Analysen und deren Umsetzung – bereits teilweise direkt im LKW – verbessern die Situation sowohl für Fahrer als auch für Unternehmen und Speditionen und können sich u.a. auf Vergünstigungen bei Versicherungsprämien auswirken. Lösungen zur Zustandsüberwachung der Fracht dokumentieren die allgemeine Lieferqualität online. Verbunden mit dem aufgezeichneten Fahrverhalten (dank modernster Kabinenüberwachungssysteme) können neue Trainingsmöglichkeiten identifiziert werden. Fahr- und Arbeitsweisen der Mitarbeiter werden entsprechend optimiert und minimieren zusätzlich die CO2-Emissionen und unnötigen Verschleiß an den Fahrzeugen. Durch die Einführung von Predictive Maintenance-Lösungen bei Fahrzeugen werden Wartungskosten eingespart, ebenso durch die Reduzierung von Ausfällen von LKWs oder Zügen. Aspekte, die einen signifikanten Einfluss auf die Kostenstruktur von Speditionen und Logistikunternehmen haben.

IOT FÜR SMART SPACES

Mit IoT-Lösungen lässt sich einerseits eine deutliche Steigerung der Gebäudeeffizienz durch Reduzierung von Lüftung, Klima oder Heizung in ungenutzten Räumen erzielen, andererseits auch eine optimierte Raumauslastung in modernen Arbeitsplatzumgebungen. Zudem unterstützen sie bei der Zusammenführung bestehender Gebäudesysteme (alte Gebäudetechnik, SCADA, HLK, Beleuchtung mit neueren nachgerüsteten Raumlösungen) und bringen so auch alte Firmentrakte

IOT-RISIKOBEWERTUNG IN VIER SCHRITTEN

1. Bestandsaufnahme der Anlagendaten
2. Identifikation der Angriffsvektoren
3. Berechnung der Risiken (Eintrittswahrscheinlichkeiten und Steuerungskosten)
4. Balancieren der Risiken und Kosten (Prioritäten des Unternehmens)

oder Industriegebäude auf einen aktuellen technologischen Stand. Verbunden mit einer Optimierung der Ressourcennutzung (Strom, Wasser, Gas, Öl etc.) werden Betriebskosten nachhaltig und langfristig reduziert. Die Implementierung der Lösungen kann darüber hinaus Parkplatzmanagement, intelligente Raumbuchungssysteme, Zugangs- und Authentifizierungskonzepte, Alarmierung, Gebäudesicherung und Anomalieerkennung beinhalten.

VERNETZUNG VON IT UND OT

Bei IoT-Projekten ist eine enge Zusammenarbeit der Handelsbereiche Operational Technology (OT) und Information Technology (IT) unabdingbar, da sie sich in ihren jeweiligen Kompetenzen ergänzen und unverzichtbar füreinander sind. So verschieden wie die Technologiestandards in beiden Bereichen sind auch ihre jeweiligen Kontaktpersonen in Unternehmen: Das klassische IT-Systemhaus spricht vorzugsweise mit dem CIO oder IT-Leiter, der OT-Handelspartner mit der Fach- oder Fertigungsabteilung.

Hier gilt es, ein Ökosystem aus den verschiedenen Marktbeteiligten mit ihren jeweiligen Kompetenzen, Zertifizierungen, Branchenerfahrungen und Ressourcen aufzubauen und geschickt zu orchestrieren. Nur so kann das weite Feld eines IoT-Projektes – angefangen von der Sensorik bis hin zum Analytics Dashboard – perfekt bespielt werden und dem Kunden durch moderne Analytics-Lösungen Erkenntnisse und Zusammenhänge liefern, die bisher im Verborgenen blieben.

Die Komplexität wird nicht nur durch das Zusammenspiel von IT & OT geschaffen, sondern auch durch die benötigten hybriden und oft herstellerübergreifenden heterogenen Umgebungen. IoT-Rahmenwerke stellen dabei für alle Marktbeteiligen eine essentielle Grundlage für eine strukturierte Herangehensweise und eine systematische Lösungsentwicklung dar. Die Architekturmodelle (RAMI 4.0, IIRA oder SITAM) vereinen alle eine dreidimensionale Darstellung von Lifecycle & Value Streams, Hirarchieebenen sowie verschiedenen allgemeinen Layern (Assets, Integration, Communication etc.). Komplexe Abläufe werden so in überschaubare Pakete unterteilt, in denen Themen wie Sicherheit und Datenschutz integriert sind.

KEIN IOT OHNE ADVANCED ANALYTICS

Unternehmer brauchen zeitnahe und detaillierte Einblicke, um im nationalen und internationalen Wettbewerb schnelle und korrekte Entscheidungen treffen zu können. Für aussagekräftige IoT-Analysen müssen bereinigte Daten bereitgestellt werden, aus denen – im passenden Kontext mit anderen Geschäftsprozessen – richtige Erkenntnisse, z.B. hinsichtlich des gewünschten Business Mehrwerts, erzielt werden können.

IoT-Daten stellen nicht nur eine riesige Menge an historischen Unternehmensdaten dar, sondern liefern weit mehr Qualität an Kontext und Rückmeldung: Die Daten stammen sowohl von Sensoren als auch von Aktoren, die in der Lage sind, automatisierte regelbasierte Aufgaben zur Ausführung anzuweisen. Das aus den Edge- und Lambda-Cloud-basierten Architekturen gewonnene Wissen wird zur Erkennung, Rückmeldung und Vorhersage genutzt und in granulare Prognosen umgesetzt, womit beispielsweise die Ressourcenplanung und -allokation in jedem industriellen oder kommerziellen Unternehmen deutlich erleichtert wird.

Neu sind dabei die großen Datenmengen der Geräte in Echtzeit. Unternehmen, die auf die einströmende Datenflut sofort reagieren können, verbessern ihre Marktposition immens. Wenn sie es zusätzlich schaffen, ihre Analytics-Daten in Echtzeit mit Predictive Analytics zu kombinieren, um unternehmenskritische Vorhersagen mit größter Zuverlässigkeit und Geschwindigkeit zu treffen, kann großes Potenzial für Wachstum und Differenzierung freigesetzt werden und Warnungen können frühzeitig beachtet werden.

Die zunehmende Anforderung von Unternehmern nach einer Verkürzung der Time-to-Value bedingt vollkommen neue Technologien im Analytics-Segment, um die Latenz weiter zu reduzieren und die Datenübertragungsrate zu maximieren. Load Balancing-Lösungen erzeugen – im Gegensatz zu virtuellen Maschinen oder Follow-the-Sun-Konzepten – elastische Ressourcen, mit denen die Rechen- und Datenkapazität innerhalb von Minuten, nicht Stunden oder Tagen erhöht oder reduziert werden kann. So lassen sich, neben komplexen Projekten und der Zusammenführung einer ganzheitlichen Dateninfrastruktur auch alle weiteren IoT-relevanten Analytics-Themen, wie Stammdatenmanagement, Datenqualität, Data Governance, Discovery und Visualisierung sowie Self-Service-BI bewältigen.

IT-SECURITY – NICHT KÜR, SONDERN PFLICHT

Versteht man eine IoT-Lösung als ein System von Systemen, das auf unterschiedlichsten Standards (IT & OT) aufgebaut ist, wird schnell klar, dass Cybersicherheit von IoT-Lösungen deutlich komplexer als reine IT-Sicherheit ist. Schnell können sie Bedrohungen ausgesetzt sein. Für jede Bedrohung gibt es ein Risiko – und für jedes Risiko einen Preis, um es zu mindern. Ein

ausgeklügeltes Risikomanagement, das vom Systemhaus entwickelt werden sollte, bringt tolerierbares Risiko und Sicherheitskosten in Einklang.

Nach unserem Verständnis für IT-Security ist die aktuell gelebte Strategie vieler Unternehmen, die in IoT-Welten eindringen oder gar die Koppelung von OT und IT forcieren, ein Wagnis mit hohem Risiko.

IT-Security im Einsatz in IoT-Anwendungen ist schon lange keine Kür mehr, sondern Pflichtprogramm für IT-Experten und Unternehmer; nicht nur in der Entwicklungsphase, sondern kontinuierlich und sich stets weiterentwickelnd, um kontinuierlich neue Cyber-Angriffsmethoden abzuwehren.

Cyber-Angriffe finden zwischenzeitlich in allen Branchen statt, die IoT-Lösungen einsetzen – sei es in der Fertigungsindustrie, bei Logistikunternehmen oder im Bereich Smart Building/Smart Spaces. Um beim Beispiel der Fertigungsindustrie zu bleiben: Produktionsmaschinen, die still stehen, sobald sich Angreifer von außen Zugriff zum Firmennetz verschaffen und durch Ransomware-Attacken den Betrieb lahmlegen, sind ein Horrorszenario für jeden Unternehmer. Durch derartige Schadsoftware werden Daten und Zugriffe verschlüsselt oder blockiert und erst nach Zahlung von Lösegeld wieder freigegeben – eine moderne und vor allem einfache Form der Erpressung. Der wirtschaftliche Schaden erstreckt sich vom Lösegeld über die Kosten des Produktionsausfalls, die schwindende Reputation gegenüber Geschäftspartnern bis hin zum Verlust von Produktions-, Produkt- und Kundendaten.

Neben der rein physischen Sicherheit spielt aber auch die Cloud- und Netzwerksicherheit eine immense Rolle. Der Einzigartigkeit der IT-/OT-Schnittstellen ist es geschuldet, hierauf einen besonderen Fokus zu legen, um bei der Übersetzung von proprietären OT-Protokollen in das Internetprotokoll Angreifern keine Türen zu öffnen.

In Zeiten des Internet-of-Everything, der zunehmenden Vernetzung sowie der erhöhten Mobilität von Mitarbeitern kommt ein weiterer „Angreifer" hinzu – nämlich der innerhalb des Firmennetzwerks. Personen-, Identitäts-, Rollen- oder Rechteverwaltung sowie das Management von Mobile Devices sind einige der grundlegenden Bausteine bei der Absicherung von Unternehmenswerten wie Daten, Patenten und Ideen. Verlorene, gestohlene oder gehackte Endgeräte, deren Daten im Darknet verkauft werden, stellen augenscheinlich mikroskopisch kleine Einstiegsstellen dar, der Schaden kann allerdings unabsehbar groß sein.

Elementar wichtig ist es daher, die Kontrolle sowohl über das Firmennetzwerk als auch die Application Services zu haben, um zu wissen, was jedes der Devices gerade macht und mit wem bzw. was es kommuniziert.

Doch was passiert, wenn einfach zu bedienende Devices Unternehmen von außen angreifen? Drohnen und kleine, unauffällige Flugobjekte haben sich zur ernstzunehmenden Gefahr entwickelt. Diese als illegale Waffen eingesetzten Geräte werden zur Lieferung von unerlaubten Waren, zum Ausspähen von Informationen auf dem Gelände, zum Transport und der Ablage von Störsendern oder bedrohlichen Substanzen verwendet.

Unternehmer brauchen zeitnahe und detaillierte Einblicke, um im nationalen und internationalen Wettbewerb korrekte Entscheidungen treffen zu können.

Die IT-Security in Unternehmen steht vor einem Wandel und bedarf höchster Aufmerksamkeit der Führungsspitze, kann aber – und das ist die gute Nachricht – dank einer ganzheitlichen und tagesaktuellen Security Strategie klar als Wettbewerbsvorteil genutzt werden.

FAZIT

Die Next Generation Technologien sowie das Verschmelzen von OT und IT erzeugen eine Welt, die vieles automatisiert und vereinfacht und so den Nutzen für Unternehmen maßgeblich erhöht. Der Mangel an Standardisierung und der kontinuierliche Wandel von Cyber-Bedrohungen sind große technische Herausforderungen, die es im Ökosystem der Partner zu lösen gilt. Richtig und sicher eingesetzt, hat IoT immer einen positiven Einfluss auf das Wachstum, die Wettbewerbsfähigkeit und die Zukunftsfähigkeit von Unternehmen.◀

Hier gelangen Sie zur Autorenseite mit weiteren Empfehlungen von Barbara Eisenberg.

Bild: Tech Data

Barbara Eisenberg

...ist Director der Business Unit IoT & Analytics bei Tech Data, dem weltweit größten IT-Distributor. Die Juristin und B2B-Expertin hat langjährige Erfahrung im IT-Channel und in Next Generation Technologien und begleitet Systemhäuser und den IT-Fachhandel vorwiegend in Projekten der Digitalen Transformation.

MEHR DAZU

...finden Sie unter:
bit.ly/TechDataDE
SAVE THE DATE: **The Future Code** am 6./7. Juni 2019 auf dem Vogel Campus in Würzburg. Weitere Infos unter:
www.TheFutureCode.de