IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

3|2019
Erscheinungstermin:
28. November 2019
www.iot4industry.at

3 x jährlich

Festo

KI ÜBERWACHT UND OPTIMIERT MASCHINEN

Gemeinsam mit Resolto geht Festo den Weg der Künstlichen Intelligenz.

Technik & Medien Verlagsges.m.b.H. • Traviatagasse 21-29/8/2, A-1230 Wien • Österr. Post AG, GZ 17Z041008 M • € 9,- • Maximale Zustelldauer: 5 Werktage

TECHNIK & MEDIEN VERLAGSGMBH

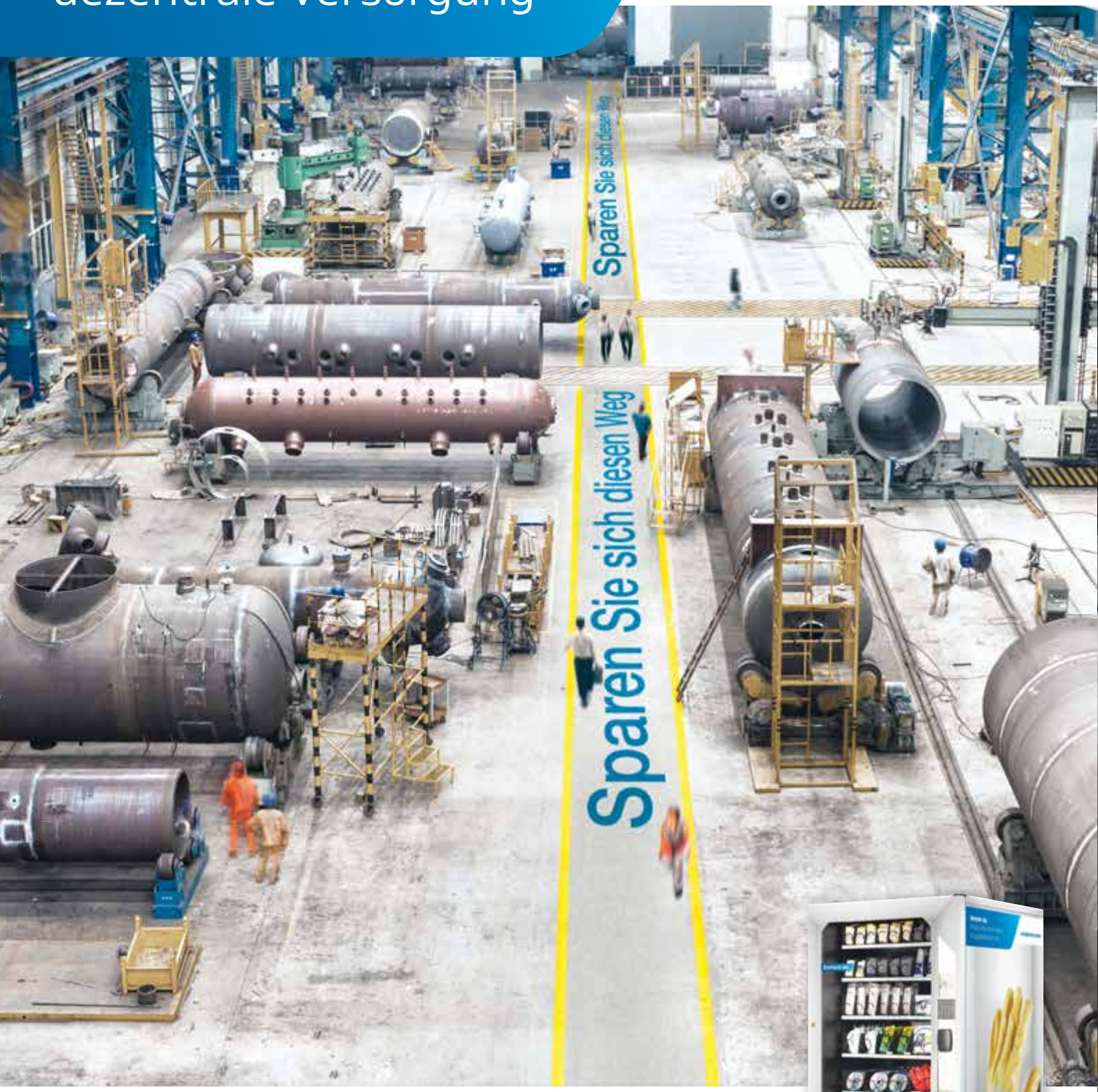
Im Gespräch
MITTEN IN DER CLOUD

Im Fokus
GIBT ES 100 % SICHERHEIT?

Im Gespräch
VERSTEHEN WIR DIGITALISIERUNG?

H-Save Ausgabeautomat
Wege sparen durch dezentrale Versorgung

HABERKORN



Der Ausgabeautomat H-Save von Haberkorn ist die einfache und flexible Lösung für Ihre dezentrale Versorgung. Er ist ideal für Arbeitsschutz, Werkzeuge, Ersatzteile sowie Betriebs- und Hilfsmittel. Gerne beraten wir Sie, wie auch Sie mit H-Save in Ihrem Betrieb Wege einsparen, eine 24-h-Versorgung sicherstellen, Zugriffe kontrollieren und automatisiert nachbestellen.

www.haberkorn.com

SICHERHEIT IST AUCH VERTRAUENSSACHE

Es ist schon klar, dass man nie zu 100 % Sicherheit haben wird, dennoch sollte man davon ausgehen. Wer sein geistiges Eigentum, seine Produkte, sein Kapital schützen möchte, muss wiederum jemand anderem Vertrauen schenken – nämlich dem- oder derjenigen, der/die passende Lösung für mehr Sicherheit anbietet. Ein schwieriges Unterfangen diese Sicherheit.

Vor allem ist es auch so eine Sache mit dem Vertrauen gegenüber den eigenen Mitarbeitern, denn der Mensch gilt in Zeiten der Cyberangriffe gern auch als Risikofaktor. Was kann man also tun, um Herrn/Frau X davor zu bewahren, den USB-Stick ungeachtet der Warnhinweise in den Firmenrechner zu stecken? Wer sagt, dass der neue Mitarbeiter nicht etwas im Schilde führt? In der Medizinbranche geht man bereits den Weg, wichtige „geheime" Dokumente nicht mehr per Boten von A nach B zu transferieren, dies erledigen Roboter. Sie fahren selbstständig, sind vertrauenswürdig und stellen keine Fragen.

Doch auf der anderen Seite wird einem immer wieder nahegelegt, Verantwortung auch abzugeben, dem Kollegen sein Vertrauen zu schenken – „Lassen Sie los!" – heißt es dann. Wenn wir nun aber täglich über die Gefahren der vernetzten Welt lesen, wie soll das dann funktionieren?

In der vorliegenden Ausgabe haben wir das Thema Security etwas genauer betrachtet und Experten zu Wort kommen lassen. Es gibt sie, die Lösungen für die Herausforderungen, die eine unsichere Welt mit sich bringt. Die Initiative Plattform Industrie 4.0 hat eigens einen Leitfaden zu diesem Thema herausgebracht (S. 26), den Sie auch online abrufen können.

Zu guter Letzt muss man auch der Künstlichen Intelligenz ein Stück weit vertrauen, denn sie ist neben intelligent eben auch künstlich. Was bedeutet das nun? Laut Festo (Coverstory) dringt sie vermehrt in die Fertigung der Betriebe vor und übernimmt neue Aufgaben. Was sie kann und ob man auch hier ein Risiko im Haus hat, beantwortet ein anschaulicher Bericht ab Seite 28.

Ich wünsche Ihnen mit der aktuellen Ausgabe spannende Einblicke und verabschiede mich bis zur nächsten Ausgabe im Neuen Jahr 2020!

Stephanie Englert, Chefredakteurin

INHALT
DEZEMBER 2019

IM FOKUS
6 **Schadenfreude**
8 **News Security**
14 **Die Sicherung der IT beginnt am Endgerät**
16 **OT-Security der Elektro-, Automatisierungs- und Prozesstechnik**
18 **Was kostet die Datenpanne?**
20 **Sichere Vernetzung in der Automatisierungstechnik**
22 **Doublecheck** | Andreas Hajek, Rittal
24 **Miteinander statt gegeneinander** | Christian Koch, NTT
26 **Sicher? Sicher!**

IM GESPRÄCH
28 **Coverstory** | KI überwacht und optimiert Maschinen
32 **Eine Sensibilisierung ist entscheidend** | Mike Pichler, ABB
35 **Gastkommentar** | Ein Netzwerkkabel für die komplette Kommunikation
36 **Kein Weg drum herum** | Dr.-Ing. Rolf Sohrmann, Weidmüller
39 **Gastkommentar** | DIY mit Low-Code im IoT: Respekt, wer's selber macht
40 **Verstehen wir Digitalisierung?** | Ing. Robert Erasmus, Eplan
44 **Besser mittendrin, statt nur dabei** | Matthias Fiegl, Magenta Telekom
46 **Mittendrin in der Cloud** | Matthias Straub, NTT
48 **Gute Konjunktur als IoT-Stopper** | Jan Rodig, tresmo
50 **Partnerschaften** | Jürgen Siefert, Schneider Electric
53 **Im digitalen Herz Europas**
54 **Für den Mittelstand geschaffen** | Jutta Jakobi, Deutsche Messe

SECURITY | BIG DATA | CLOUD COMPUTING
56 **zenon macht Werke vergleichbar**
58 **Erpressungsangriffe auf OT- und IIoT-Infrastrukturen**
60 **Klare Regeln für Open Source-Komponenten**
62 **News**

STÄNDIGE RUBRIKEN
65 **Veranstaltungen**
66 **Impressum** | **Vorschau**

Coverstory

Die Künstliche Intelligenz wird immer tiefer in die Fertigung vordringen und neue Aufgaben übernehmen. Festo hat gemeinsam mit Resolto spannende Perspektiven hierzu eröffnet.

www.festo.at

Lesen Sie mehr ab Seite 28!

3 x jährlich

IoT4 INDUSTRY&BUSINESS

22

Klassische IT-Security verlangt heutzutage einiges ab. Doch gibt es überhaupt 100 % Sicherheit? Dieser Frage stellte sich Andreas Hajek, Verkaufsleiter IT bei Rittal Österreich, und erläutert seine Sicht der Entwicklungen in einem Interview.

32

Der Druck auf Unternehmen wächst. Cyberangriffe, kleine Losgrößen und Digitalisierung fordern Flexibilität und Lösungen. Partnerschaften können dabei ein Weg sein, meint Mike Pichler, Account Manager & Cyber Security-Experte im Bereich Energy Industries Öl & Gas von ABB in Österreich.

[ECI215G]

Für die einfache Kommunikation mit der

Cloud ...

... und die Steuerung komplexer

Maschinen

Der Beckhoff IoT-Controller

Mit den kompakten Embedded-PCs der CX-Serie und dem Softwaremodul TwinCAT IoT ermöglicht Beckhoff die Steuerung komplexer Maschinen mit gleichzeitiger Cloud und Big Data Connectivity. Dabei profitieren Anwender gleich doppelt vom Prinzip der offenen Steuerungstechnik: nach unten ins Feld durch variable Feldbusschnittstellen und Anbindung aller gängigen I/O-Signale; nach oben ins Internet of Things durch freie Wahl einer Private oder Public Cloud über die Standardprotokolle AMQP, MQTT und OPC UA.

www.beckhoff.at/IoT-Controller

New Automation Technology BECKHOFF

DATA
SECURITY

IoT
INTERNET OF THINGS

SCHADENFREUDE

Angriffe auf die hauseigenen Systeme sind für viele zwar eine bedrohliche Vorstellung, dennoch schiebt man den Sicherheitsaspekt viel zu oft noch beiseite. Dieser Ansicht sind sich nicht nur die Security-Experten der Plattform Industrie 4.0 bei der Präsentation ihrer Studie kürzlich gewesen.

Ein exzellentes Beispiel, das dieser Tage ins Auge stach, war der im Oktober auf das mittelständische Unternehmen Pilz gerichtete Cyber-Angriff. Die Schwaben waren weitgehend arbeitsunfähig geworden, man versuchte schnellstmöglich alle Systeme wieder zum Laufen zu bringen – doch das dauert. Angriffe auf das persönliche Umfeld sind darüber hinaus meist noch beängstigender und mahnen aber zur absoluten Vorsicht in Zeiten der zunehmenden Digitalisierung. So schilderte Kurt Hofstädter, Vorstandsvorsitzender der Plattform I 4.0, sein persönliches auf ihn gerichtetes Angriffserlebnis im eigenen Fahrzeug via Smartphone. Doch was kann die Lösung sein?

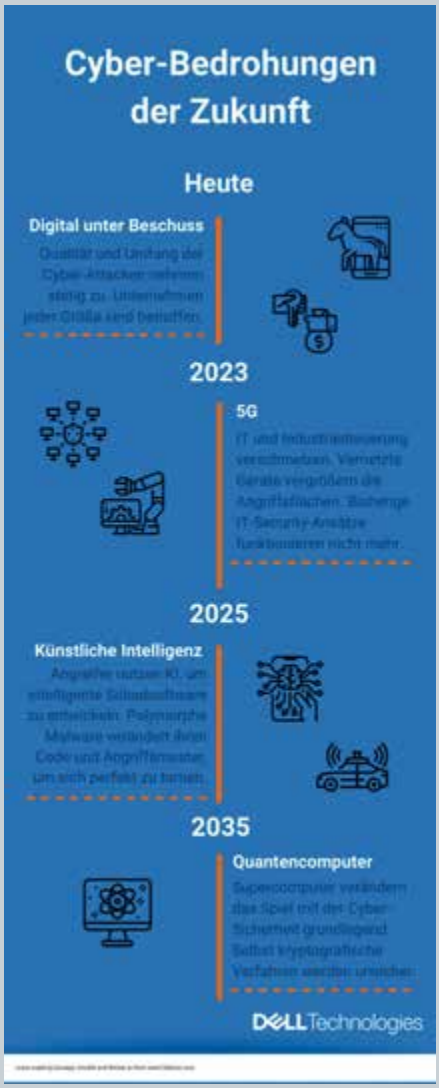
Einerseits erleben wir alle derzeit einen absoluten Boom in Richtung Digitalisierung – sei es auf industrieller Ebene, den Firmen wird dieser Schritt seit Jahren als absolutes Überlebensziel weis gemacht. Andererseits heißt es vermehrt Obacht! Vielleicht sind all zu viele frei zugängliche Daten doch nicht der Weisheit letzter Schluss? Onlinebestellungen nehmen zu, e-Shops wachsen wie Pilze aus dem Boden – Datenklau und das Risiko der Kreditkarte schwingt jedoch immer mit einher. Dafür werden Passwortverschlüsselungen immer komplizierter – verständlicherweise – und der eigene Mitarbeiter ist nicht mehr nur die Basis des Unternehmenserfolges, sondern gleichzeitig auch das hauseigene Risiko.

Es gibt (k)eine Lösung. Bedeutet das, wir schaffen uns selber ab? Ist KI die Zukunft und wir gehen alsbald in Rente, nur der Sicherheit wegen? Diese Fragen sind wahrhaft schwer zu beantworten. Die FH St. Pölten als Beispiel nimmt sich dieser Problematik an und untersucht in einem Forschungszentrum Aspekte der IT-Sicherheit. So ist die Blockchain-Technologie vor allem als Basis von Kryptowährungen allseits bekannt geworden. Doch sie kann weitaus mehr und bietet für die Wirtschaft viele praktische Einsatzmöglichkeiten, etwa zum Verwalten großer Datenmengen oder zum Absichern von Datenbanken und Serversystemen. Auch werden an der FH eigene Studiengänge zum Thema Security angeboten, denn der Bedarf an geschultem Personal ist nachwievor da – auch wenn es sich um Menschen handelt.

Auf der Suche nach einer Idee. Eigens für den Sicherheitsaspekt gestaltete Messen sind wie die it-sa inzwischen ein Muss auf jedem Messekalender. Und die zunehmenden Besucherzahlen bestätigen die Notwendigkeit. Dieses Jahr drehte sich, erstmals vergrößert auf vier Hallen, alles um Mobile- und Cloud-Security, Verschlüsselungen, IT Compliance und Biometrie. So zählte die Veranstaltung 815 Aussteller aus 25 Ländern Europas, Asien und den USA auf der weltweit größten IT-Sicherheitsfachmesse. Das Portfolio an Lösungen ist nicht nur dort umfassend. Die Frage, welche Lösung für mich, gerade auch als KMU, die richtige ist, bleibt auch vielen nach einer Messe immer noch unbeantwortet.

www.it-sa.de
www.plattformindustrie40.at
www.pilz.at
https://www.fhstp.ac.at/de/studium-weiterbildung/informatik-security/it-security

5G UND KI ALS NEUE CYBER-BEDROHUNG



Qualität und Umfang der Cyber-Attacken haben in der Vergangenheit ständig zugenommen und Hacker werden künftig neue Technologien geschickt nutzen, um ihr Handwerk weiter zu perfektionieren. **Dell Technologies** zeigt jetzt drei Cyber-Bedrohungen auf, die in den nächsten Jahren auf die Unternehmen zukommen.

5G wird dafür sorgen, dass deutlich mehr Geräte, Sensoren und kritische Services miteinander vernetzt sind. Dadurch bieten sich Cyber-Kriminellen erheblich mehr Angriffsflächen.

Schon heute nutzen Cyber-Kriminelle in ersten Ansätzen KI-basierte Technologien, um intelligente Malware zu entwickeln. Mit Hilfe von KI erstellen sie polymorphe Schadsoftware, die ihren Code und ihre Angriffsmuster automatisch verändert und sich so bis zur Unkenntlichkeit tarnen kann.

Quantencomputer werden das Spiel mit der Cyber-Sicherheit nochmals grundlegend verändern. Der Einsatz von Quantencomputern wird die Leistungsfähigkeit von Systemen und damit die Ausführung von Berechnungen und Transaktionen auf ein bislang unerreichtes Niveau anheben. Genau das könnte auch Cyber-Kriminellen in die Hände spielen – etwa beim Knacken heute noch sicherer kryptografischer Verfahren.

www.delltechnologies.com

NEUER DATEN-VERSCHLÜSSELUNGS-DIENST

Die Datenverschlüsselungs-App NordLocker für macOS und Windows sichert die auf einem Computer oder in der Cloud gespeicherten Dateien durch eine Ende-zu-Ende-Verschlüsselung. Mit der Veröffentlichung von NordLocker will **NordVPN** erstklassigen Datenschutz für jeden zugänglich machen – unabhängig von den jeweiligen technischen Fähigkeiten. Um dies zu erreichen, hat das Unternehmen die größtmögliche Benutzerfreundlichkeit mit den höchsten Verschlüsselungs-Standards kombiniert. Dazu wurde den derzeit sichersten Verschlüsselungs-Algorithmen – Advanced Encryption Standard (AES-256) und 4096 bit RSA in den eigenen Verschlüsselungsprozess, die Null-Kenntnis Verschlüsselung implementiert.

www.nordvpn.com

VEREINT SAFETY UND SECURITY

Mit PITmode fusion bietet **Pilz** jetzt ein modular aufgebautes Betriebsartenwahl- und Zugangsberechtigungssystem. Das System überzeugt mit mehr Flexibilität und ermöglicht ein effizientes Betriebsartenwahl- und Zugangsberechtigungsmanagement, das Safety- und Security-Vorgaben gleichzeitig abdeckt.

Der neue PITmode fusion besteht aus der Ausleseeinheit Pit-reader mit RFID-Technologie und integriertem Webserver sowie einer sicheren Auswerteeinheit Safe Evaluation Unit (SEU). Durch seinen modularen Aufbau lässt es sich individuell in das Design bestehender Bedienpulte integrieren. Dadurch können vorhandene Taster genutzt werden, was dem Anwender eine bessere Bedienung ermöglicht. PITmode-Geräte werden in Maschinen und Anlagen eingesetzt, in denen zwischen unterschiedlichen Steuerungsabläufen und Betriebsarten umgeschaltet wird.

Die Vorteile: Zutritt erfolgt nur mit Berechtigung bei bis zu fünf sicheren Betriebsarten. Die RFID-Schlüssel können mit einem firmenspezifisch programmierten PITreader codiert werden. Dadurch wird der Verwaltungsaufwand bei der Administration der Zugangsberechtigungen gerade bei internationalen Standorten reduziert. Die Funktionen der Berechtigungsmatrix werden auf dem Schlüssel gebündelt und ersetzen zusätzliche mechanische Schlüssel.

www.pilz.com

PANDA SECURITY ERHIELT ZUSCHLAG

Panda Security stattet die nächsten drei Jahre Telefónica mit Endpoint Detection and Response-Lösungen (EDR) aus. Die IT-Sicherheitslösung „Adaptive Defense 360" des spanischen Unternehmens Panda Security und sein Threat Hunting Service werden in insgesamt 14 Ländern auf 180.000 Computern im globalen IT-Netzwerk von Telefónica eingesetzt. Mit der Unterzeichnung dieses Vertrages Anfang des Jahres vertraut Telefónica Global auf die Dienstleistungen von Panda Security. Neben dem EDR-Schutz und dem Threat Hunting Service hat sich das Unternehmen für weitere IT-Lösungen entschieden, zum Beispiel das Patch Management und den Siem Feeder, welcher die Einbindung in bestehende Siem-Produkte ermöglicht.

www.pandasecurity.com

MEHR VERFÜGBARKEIT UND ZUVERLÄSSIGKEIT

„Accelerate design. Maximize performance" – unter diesem Motto präsentierte **Rohde & Schwarz** sein Portfolio auf der Fachmesse productronica 2019 Mitte November in München. Die Messtechniklösungen des Unternehmens rüsten Ingenieure für Tests in allen Phasen der Entwicklung, Verifizierung und Produktion und schaffen Vertrauen in das Design.

Smart Factories setzen auf drahtlose Kommunikationstechnologien, um die Prozesse zu automatisieren und die Produktivität zu steigern. Daher haben Verfügbarkeit und Zuverlässigkeit der Wireless-Systeme große Bedeutung. Auf der productronica 2019 zeigte Rohde & Schwarz eine Reihe von Lösungen zur Verhinderung von Störungen des Wireless-Systems. Mit Handheld-Spektrumanalysatoren wie dem R&S Spectrum Rider FPH und dem R&S MNT100 HF-Störquellen-Ortungsgerät lassen sich Funkstörungen, die die Produktion beeinträchtigen, schnell detektieren. Um die Abdeckung zu messen und die HF-Performance des Netzwerks zu analysieren, können Hersteller moderne Drive-Test- und Walk-Test-Scanner aus der R&S TSMx-Familie einsetzen. Mit dem Smartphone-basierten Qualipoc Android lässt sich die HF eines Netzwerks innerhalb einer Smart Factory optimieren und dessen Servicequalität bewerten.

www.rohde-schwarz.com

IT-SICHERHEIT FÜR STAAT UND INDUSTRIE

Betreiber von Industrieanlagen müssen heute Infrastrukturelemente über das Internet vernetzen, die ursprünglich nicht dafür konzipiert wurden und teilweise Jahrzehnte alt sind. Mit **secunet**-Lösungen gelingt dies sicher und effizient. Das System secunet edge legt sich wie eine Schutzhülle um eine Maschine und entkoppelt ihren Lebenszyklus von dem der IT-Umgebung. Gleichzeitig ermöglicht secunet edge die sichere und problemlose Anbindung von Maschinen und Anlagen an moderne IoT-Plattformen.
Die Hochsicherheitsarchitektur Sina wird von Behörden und militärischen Organisationen seit vielen Jahren erfolgreich zur Übertragung und Bearbeitung besonders sensibler Daten eingesetzt. Auf der it-sa 2019 stellte secunet neue Client-Varianten und eine innovative Lösung für hochsichere Telefonie vor.
Bei Themen wie Grenzkontrolle und Identitätsfeststellung setzen Sicherheitsbehörden in Deutschland und Europa verstärkt auf Technologie von secunet. Auf der it-sa zeigte das Unternehmen u.a. die mobile App secunet bocoa, mit der mobile Personenkontrollen auch auf gängigen Smartphones durchgeführt werden können.

www.secunet.com

NEUE KRYPTO-MINING-KAMPAGNE

Die **SophosLabs** haben mehrere aktive und organisierte Coin-Miner-Kampagnen entdeckt, die Unternehmensnetzwerke und Lateral-Movement-Techniken nutzen. Die Kampagnen dienen Cyber-Kriminellen zur effizienteren und schnelleren Gewinnung von Kryptowährungen. Unternehmensnetzwerke sind ein beliebtes Angriffsziel, da sie durch den großen Pool an Rechnerleistung auf vielen ähnlich konfigurierten Maschinen ein großes Potenzial bieten, um die Machenschaften effizient durchzuführen.
SophosLabs haben einen genaueren Blick auf die Kampagnen geworfen und die Vorgehensweise der Angreifer analysiert: Wird ein Rechner kompromittiert, durchsucht ein bösartiges Skript das Netzwerk nach geeigneten Zielen und löst eine Reihe von verschiedenen Exploits oder Privilege-Escalation-Funktionen aus, einschließlich Eternal Blue Exploit oder Pass-the-Hash, um sich im Netzwerk zu verbreiten. Dabei hat sich das Coin-Mining weiterentwickelt.

Die Anzahl der kompromittierten Maschinen auf der Weltkarte lässt die Vermutung zu, dass der erste Ausbruch in Südostasien stattfand. Von dort aus haben sich die Coin-Miner-Angriffe weltweit verbreitet, auch in Europa. Die DACH-Region scheint momentan noch wenig betroffen zu sein.

www.sophos.com

AUSGEZEICHNETE FRAUEN

Noch immer sind weibliche Fachkräfte im Bereich Cybersicherheit rar. Mit den Women in Cybersecurity-Awards sollen talentierte Frauen sichtbarer gemacht werden und die verdiente Anerkennung bekommen. Die Awards hat NTT Security in Zusammenarbeit mit Global Digital Women konzipiert, einem internationalen Netzwerk von Gestalterinnen der Digitalbranche. Auf der diesjährigen Information Security World in Wien am 17. September im Studio 44 hat **NTT Security** jetzt die Gewinnerinnen der DACH-Region prämiert. In der Kategorie Professional – also Frauen, die bereits seit mehr als fünf Jahren in diesem Sektor tätig sind – hat Kirsten Davies, Senior Vice President and Chief Information Security Officer bei The Estee Lauder Companies, gewonnen. Siegerin in der Kategorie Newcomer – Frauen, die erst seit zwölf Monaten im Bereich Cybersicherheit arbeiten – wurde Rebecca Vogels, Founder & CEO von All Of The Above. Die Preisvergabe soll dazu beitragen, dass junge Frauen verstärkt eine Karriere im Sektor Cybersicherheit in Betracht ziehen. NTT Security selbst arbeitet kontinuierlich an einer Erhöhung des Frauenanteils im Unternehmen, der europaweit derzeit bei rund 26 Prozent liegt.

www.nttsecurity.com

ÜBER 800 RESELLER BEI SECURITY DAYS

Vom 9. bis 20. September reiste das **Securepoint**-Team mit seiner Roadshow „Securepoint Security Days" durch zehn deutsche Städte. Mit über 800 Teilnehmern war die Roadshow mit Wortmann, Starface und api an Bord für den Veranstalter ein voller Erfolg. „Die vielen Partner und die Teilnahme an den SecDays bestätigen, dass wir mit Unified Security und unseren Angeboten im Bereich Managed Security die richtigen Lösungen für den Channel bieten. Die SecDays sind ein Highlight des Jahres und jedes Jahr aufs Neue spannend für alle Beteiligten. Der große Zuspruch zeigt auch die Bedeutung von IT-Sicherheit aus einer Hand made in Germany", sagt René Hofmann, Senior Manager Strategische Accounts. Securepoint richtete die SecDays bereits zum vierten Mal aus. Dieses Jahr nahmen so viele Partner und Interessenten an der Veranstaltung teil, wie noch nie. Darunter auch viele neue Gesichter.

Bei der Veranstaltung geht es für Securepoint um mehr als einfache Argumente und vermeintlich starke Schlagworte. Mit den SecDays möchte der Hersteller, so Hofmann, Wege zu einer noch erfolgreicheren Partnerschaft zeigen. Dafür hatte das Team Ideen, Unterstützungsangebote und innovative Lösungsansätze im Gepäck, wie z.B. aus den Bereichen produktübergreifende Reportings oder Mobile Security für das sichere Management von Smartphones und Tablets.

www.securepoint.de

PRODUKT- UND FUNKTIONSERWEITERUNGEN

Auf der diesjährigen it-sa zeigte Netzwerkspezialist **Allegro Packets** mit dem Allegro 500 und dem Webshark-Feature die neuesten Entwicklungen im Bereich der Netzwerkanalyse. Je effizienter sich Probleme im Netzwerk erkennen lassen, desto geringer sind Admin-Frust und Ausfallkosten. Das Allegro 500, das zur Messe zum ersten Mal einem großen Publikum präsentiert wurde, versteht sich als portabler Gigabit-Netzwerkanalyzer mit integriertem Management-Port und integrierter SSD.

www.allegro-packets.com

Lückenhafte Security?

Wir schützen Ihr industrielles Netzwerk mit 360° Security

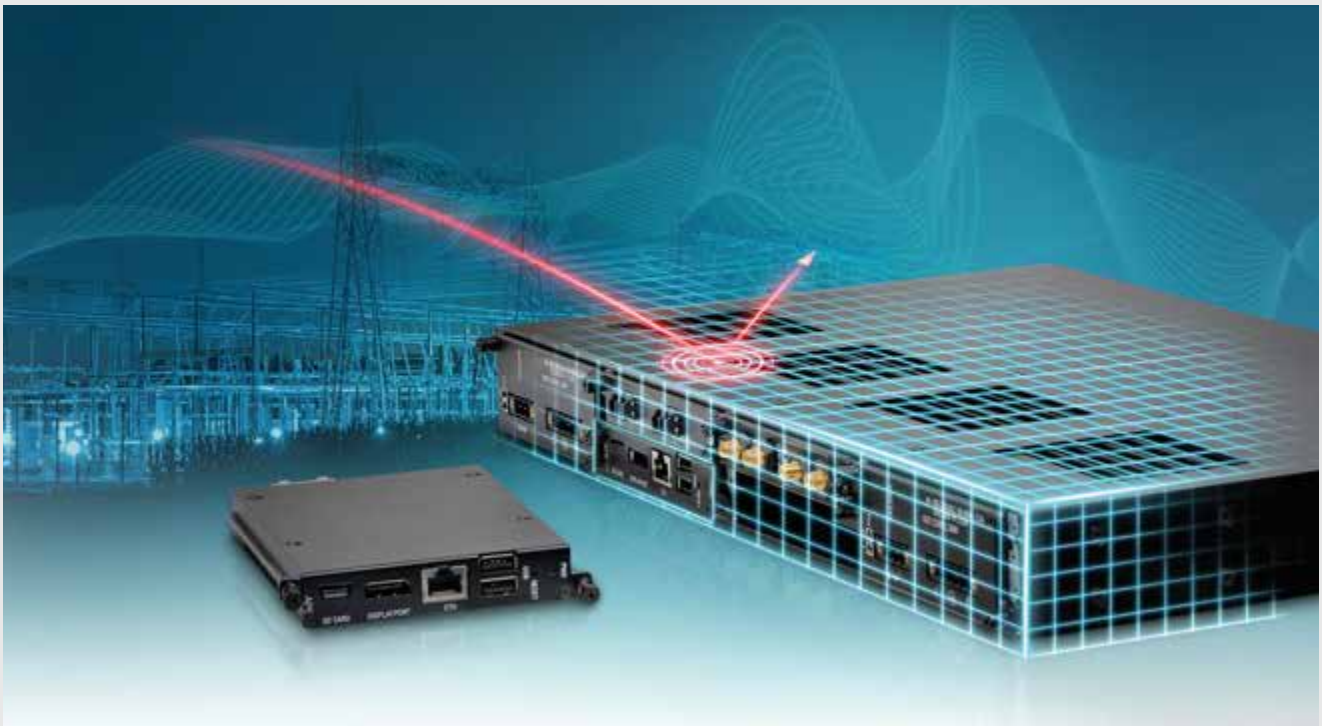
Durch die zunehmende Vernetzung und Anbindung industrieller Steuerungs- und Automatisierungssysteme sind diese zunehmend Cyber-Gefahren ausgesetzt. Phoenix Contact unterstützt Sie mit sicheren Produkten, Dienstleistungen und Industrielösungen zum Schutz Ihrer Systeme und zur Sicherung Ihres Know-Hows. Sprechen Sie uns an, wir beraten Sie gerne!

Mehr Informationen unter Telefon (01) 680 76 oder **phoenixcontact.at**

PHOENIX CONTACT
INSPIRING INNOVATIONS

© PHOENIX CONTACT 2019

INDUSTRIAL APPLICATION HOSTING PLATTFORM FÜR CYBERSECURITY



Siemens hat seine Produktfamilie Ruggedcom Multiservice-Plattform mit robusten Kommunikationsgeräten um eine neue, leistungsstärkere Version der Ruggedcom APE (Application Processing Engine) erweitert. Es handelt sich um eine Industrial Application Hosting-Plattform auf der herstellerunabhängige Softwareapplikationen in rauen und betriebskritischen Umgebungen ausgeführt werden können.

Die Ruggedcom APE1808 gehört zur Produktfamilie Ruggedcom RX15xx mit ihren robusten Layer-2- und Layer-3-Switches und Routern. Diese modulare Plattform mit vor Ort austauschbaren Modulen bietet die Wahl zwischen WAN-, seriellen- und Ethernet-Optionen. Sie eignet sich für Stromerzeugung und -verteilung, sowie für Bahnanwendungen und Verkehrstechnik. Als Modul kann die Ruggedcom APE1808 direkt in jedes Gerät der Ruggedcom RX1500 Multiservice-Plattform eingesteckt werden und so die integrierten Switching- und Routing-Fähigkeiten der Plattform vollständig nutzen. Ruggedcom APE1808 bietet eine Gigabit-Ethernet-Verbindung an der Gerätevorderseite und eine weitere gleichwertige, jedoch vollständig getrennte Verbindung zur Rückwandplatine des RX15xx. Ruggedcom APE steht optional mit einer Schutzbeschichtung (Conformal Coating) zur Verfügung und kann bei Umgebungstemperaturen von -40 bis +75 Grad Celsius betrieben werden. Sie erfüllt alle elektrischen Spezifikationen der Ruggedcom RX15xx Plattform, also die Normen IEC61850-3 und IEEE 1613 für den industrietauglichen Betrieb in rauesten Umgebungen. Aufgrund ihrer Basis, dem Intel Quad Core, der x8664 Architektur mit Support für Linux und Windows 10, bietet die Ruggedcom APE1808 eine normenbasierte Plattform für handelsübliche Software und ermöglicht damit Partnerschaften mit Branchenführern in Sachen Cybersecurity.

Die neue Ruggedcom APE1808 bietet Vorteile bei Anwendungen wie Firewalls, Analysesoftware für Netzwerklast und Logs oder Sensoren für Intrusion Detection-Systeme. Sie kann Daten direkt an der Quelle analysieren - ohne zusätzlichen Aufwand für die Installation eines externen Industrie-PC. Die Ruggedcom APE1808- und die Cybersecurity-Lösungen wurden für Anwendungsbereiche wie Stromerzeugung und -verteilung ebenso entwickelt wie für Verkehrstechnik sowie Öl und Gas, können aber auch in jeder rauen Industrieumgebung eingesetzt werden, um Netzwerke vor einer wachsenden Zahl von Angriffen zu schützen.

Das Ruggedcom-Lösungsportfolio für Cybersicherheit bietet den Zugang zu verschiedenen modernen Cybersecurity-Anwendungen, die im Rahmen einer Partnerschaft mit Fortinet, Nozomi Networks, Secure-NOK und Claroty entwickelt wurden. Die Zusammenarbeit fokussiert die Weiterentwicklung der Sicherheit industrieller Netzwerke vor neu aufkommenden Herausforderungen im Bereich der Cybersecurity. Folgende Lösungen werden auf der Ruggedcom Multiservice Plattform mit gemeinsam zertifizierten Partneranwendungen von Fortinet, Nozomi Networks, Secure-NOK und Claroty zur Verfügung gestellt: Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Deep Packet Inspection (DPI), Next Generation Firewall (NGFW).

Ruggedcom APE1808 ist das Schlüsselprodukt im wachsenden Siemens-Lösungs- und Serviceportfolio für Cybersecurity, zu dem umfassende Netzwerkberatungsdienste ebenso wie Security Assessments, Integration, Bereitstellung, Training und Support vor Ort gehören.

www.siemens.at

CYBERANGRIFFE NEHMEN ZU

Die zunehmende Vernetzung und Digitalisierung in der industriellen Fertigung führt zu wachsenden IT-Abhängigkeiten, dabei nimmt die Zahl der Cyberangriffe zu. „In jüngster Vergangenheit gab es einen deutlichen Anstieg erfolgreicher Angriffe auf die Produktionsanlagen deutscher Maschinen- und Anlagenbauer", sagt Steffen Zimmermann, Leiter Competence Center Industrial Security. „Unsere Umfragen zeigen, dass bereits mehr als ein Drittel der vom **VDMA** befragten Mitglieder von Produktionsausfällen berichten. Kapitalschäden verzeichnen bereits die Hälfte der befragten Unternehmen", sagt der Experte für Cybersecurity. Es bedarf verstärkter Maßnahmen von Firmen und Behörden.

Hackerangriffe mit teilweise nachgelagerter Erpressung machen deutlich, dass die Lage ernst und das Gefahrenpotenzial groß ist. Dabei zeigen die Schadensfälle auf, dass bessere Prävention und professionelle und schnelle Expertenhilfe im Notfall entscheidend sind. Insgesamt ist die Notfall-Hilfe der Behörden im Kontext Cybersecurity gegenüber den mittelständischen Unternehmen ausbaufähig. „Die zentralen Kontaktstellen für Cybercrime können nicht in jedem Bundesland adäquat Unterstützung leisten, das zeigen die Erfahrungen unserer Mitglieder", berichtet Zimmermann.

Cyberresilienz als Präventionsmaßnahme. Zum Schutz vor Security-Vorfällen sowie zur Erkennung und zur Behandlung von erfolgreichen Angriffen bedarf es abgestimmter Maßnahmen. Ein geeigneter Ansatz, dies zu erreichen, ist die Betrachtung der Cyberresilienz. Resilienz beschreibt die Widerstandsfähigkeit gegen Bedrohungen und die Fähigkeit, nach einem erfolgreichen Angriff schnell wieder in einen funktionsfähigen Zustand zurück zu kommen. Resilienz hilft dabei, im Ernstfall bestens gewappnet zu sein. Unternehmen mit einer hohen Cyberresilienz wissen, welche Schritte im Schadensfall zu tun sind. Dazu zählt nicht zuletzt die innere Resilienz der Maschinen und Anlagen im Betrieb. Resiliente Systeme sind robust genug, um Angriffen zu widerstehen und die Hersteller resilienter Maschinen und Anlagen sind fähig, im gesamten Produktlebenszyklus für eine angemessene Security zu sorgen.

Unterstützung seitens des VDMA für Mitglieder. Der VDMA erarbeitet im Arbeitskreis Informationssicherheit eine Notfall-Unterstützung für den Maschinen- und Anlagenbau. Ebenso unterstützt der VDMA aktiv die branchenübergreifende Meldestelle für Schwachstellen „CERT@VDE". Dort können sich Maschinenbauer mit Herstellern von Automatisierungslösungen und Betreibern vernetzen, um frühzeitig Informationen zu Schwachstellen in Produkten zu erhalten.

industrialsecurity.vdma.org

BUXBAUM
Member of the Softing Group
› Netzwerk- und SPS-Diagnose
› Datenintegration
› Kommunikation
› Fernwartung
› Bildverarbeitung
› Identifikation

› +43 2682 70456-0 › office@myAUTOMATION.at › www.myAUTOMATION.at

DIE SICHERUNG DER IT BEGINNT AM ENDGERÄT

Die Erhöhung der IT-Sicherheit hat überall höchste Priorität. Eine entscheidende Rolle nimmt dabei der Schutz von Endgeräten ein, schließlich ist der PC das erste Einfallstor in das Netzwerk.

Eine gängige Praxis von Hackern ist der Versand von Spear-Phishing-E-Mails aus vermeintlich vertrauenswürdiger Quelle an Unternehmensmitarbeiter. Nach dem Öffnen einer E-Mail und eines präparierten Anhangs oder Links wird ein Schadprogramm auf dem Rechner des Mitarbeiters installiert, mit dem Zugangsdaten und Passwörter des lokalen Rechners entwendet werden. Sie werden vom Angreifer für den Zugriff auf verbundene Systeme und eine Seitwärtsbewegung und Ausbreitung im Netz genutzt, bis er schließlich Zugang zu einem Domain Controller oder mehreren privilegierten Accounts hat. Damit besitzt er auch Kontrolle über alle unternehmenskritischen Ressourcen. Das typische Angriffsmuster zeigt, dass für Hacker Endgeräte ein Erfolg versprechendes (Erst-)Ziel darstellen; der PC oder die Workstation dienen ihnen gewissermaßen als Einfallstore und damit als Ausgangspunkte für die weitere Infiltration des Unternehmensnetzes.

Der Ablauf eines Spear-Phishing-Angriffs weist aber auch auf die Schutzmaßnahmen hin, die zwingend ergriffen werden müssen. An erster Stelle steht die Endpunktsicherung zur Unterbindung einer Erstinfektion. Zweitens geht es um die Sicherung und Überwachung von Zugangsdaten zur Vermeidung der Ausbreitung eines Angriffs. Und der dritte Punkt betrifft die Bedrohungserkennung zur rechtzeitigen Einleitung von Gegenmaßnahmen.

Im Hinblick auf die Sicherung der Endgeräte sind mehrere Vorkehrungen zu treffen. Klar ist, dass jedes Unternehmen die eigenen Mitarbeiter für Gefahren sensibilisieren sollte, die von E-Mails mit Anhängen und Links aus unbekannten – aber auch aus vermeintlich bekannten – Quellen ausgehen. Selbstverständliches Prozedere muss zudem das kontinuierliche Patchen von Systemen zur Eliminierung bekannter Sicherheitslücken sein.

Im Fokus: Rechte. Neben diesen beiden elementaren Anforderungen sind aber vor allem zwei weitere Maßnahmen unverzichtbar: Zuerst der Entzug der lokalen Administratorrechte für Standardanwender, um Angreifern im Fall einer Systemkompromittierung nur eingeschränkte Handlungsmöglichkeiten zu eröffnen. Des Weiteren die Überwachung der Applikationen auf den Endpunkten zur Minimierung des Malware-Infektionsrisikos, das

heißt eine Anwendungssteuerung, die die Ausführung schädlicher Programme sowie den Zugriff auf wichtige Dateien und Ressourcen verhindert.
Jeder Rechner in einem Unternehmen enthält standardmäßig integrierte Administratorkonten, die oft aufgrund ihrer Handhabung eine massive Sicherheitsgefahr darstellen. Zum einen werden vielfach Hunderte von Rechnern mit einem identischen Passwort verwaltet, das nie oder zumindest nicht regelmäßig geändert wird. Zum anderen ist das Passwort oft auch dem Endanwender bekannt (und wird damit für die tägliche Arbeit verwendet), damit dieser einen vollständigen Datenzugriff hat. Jeder Nutzer mit lokalen Windows-Administratorrechten kann praktisch uneingeschränkt agieren. Er kann nicht-lizenzierte Software herunterladen, jedes mögliche – auch ausdrücklich untersagte – Programm verwenden, Systemkonfigurationen ändern oder gefährliche Malware installieren – willentlich wie unwillentlich. Die lokalen Admin-Rechte stellen aber nicht nur eine Gefahr hinsichtlich unbeabsichtigter oder böswilliger Aktivitäten der (berechtigten) Anwender dar, sie sind auch von Angreifern nutzbar, wie das Spear-Phishing-Beispiel zeigt. Das Aufspüren lokaler Administratorrechte und der Entzug dieser Rechte ist deshalb ein erster wichtiger Schritt auf dem Weg zu einem starken Endgeräteschutz.
Allerdings sollte keine statische Lösung mit einem endgültigen Entzug von Rechten gewählt werden, denn dies treibt die Betriebskosten durch viele Helpdesk-Anrufe in die Höhe und senkt die Anwenderakzeptanz. Idealerweise bietet eine Lösung für die Endpunktsicherheit auch eine automatisierte Rechteerhöhung an, mit der Anwendern gezielt und in einem limitierten Umfang Zugriffsrechte eingeräumt werden. Damit wird der Benutzerkomfort gewahrt und ein unterbrechungsfreier Betrieb sichergestellt.

Intelligente Anwendungskontrolle. Darüber hinaus ist eine Applikationsüberwachung vor allem im Hinblick auf die nach wie vor grassierenden Ransomware-Attacken erforderlich. Ransomware benötigt im Unterschied zu herkömmlicher Malware nicht immer administrative Zugriffsprivilegien, stattdessen reichen Standardrechte für das Lesen, Schreiben und Editieren von Dateien, die nahezu jeder Mitarbeiter besitzt. Eine intelligente Applikationskontrolle ist eine effiziente Maßnahme, um die Verschlüsselung von Dateien durch Ransomware zu unterbinden.
Eine solche intelligente Anwendungssteuerung umfasst dabei nicht nur eine klassische Software-Blacklist und -Whitelist, sondern vor allem auch eine Greylist-Funktion. Damit kann die Ausführung von bzw. der Zugriff auf Anwendungen begrenzt werden, die nicht explizit vertrauenswürdig oder einfach unbekannt sind. Das heißt, der Anwender kann sie in einem „eingeschränkten Modus“ nutzen, wobei ein Zugriff auf Unternehmensressourcen, vertrauliche Daten oder das Internet unterbunden wird. Auf diese Weise wird zum einen eine Einschränkung des Benutzerkomforts vermieden und zum anderen eine maximale Sicherheit gewährleistet.

www.cyberark.com

Der Autor:
Michael Kleist
... ist Regional Director DACH bei CyberArk in Düsseldorf.

ZUSAMMENARBEIT AUF AUGENHÖHE.

THIS IS SICK
Sensor Intelligence.

Mensch und Roboter rücken enger zusammen. Dabei spielen Sensoren von SICK eine entscheidende Rolle. Egal ob Robot Vision, Safe Robotics, End-of-Arm Tooling oder Position Feedback – SICK-Sensoren befähigen den Roboter zu präziserer Wahrnehmung. Und ermöglichen damit Zusammenarbeit auf Augenhöhe. Wir finden das intelligent. www.sick.at

OPC UA

Security – wo, wann und wie ist man als Verantwortlicher eigentlich gefordert?

OT-SECURITY

DER ELEKTRO-, AUTOMATISIERUNGS- UND PROZESSTECHNIK

Security ist vielfältig und entsprechend muss auch die Fort- und Weiterbildung in diesem Bereich sein. Auf was man als Experte gefasst sein muss und was einen erwartet weiß Security-Experte Erich Kronfuß von Phoenix Contact in Österreich.

Automatisierung begann einst mit festverdrahteten Steuerungen (VPS) über Relais und Kontakte von der Leit- bis zur Zellenebene. Der nächste Level der Automatisierung kam durch die Prozessortechnik mit Bussystemen/Feldbussystemen und speicherprogrammierbaren Steuerungen (SPS). Industrie-Feldbussysteme entstanden in den 1980er Jahren, arbeiten im sogenannten Master-Slave-Betrieb mit eigenen Topologien. In den späteren 1990er Jahren zogen immer mehr vernetzte PC Systeme in der Leittechnik ein. Um klassische IT-Infrastruktur auch bis auf Zellenebene nutzen zu können, forderten Anlagenbetreiber eine Vereinheitlichung. Steuerungshersteller wie Siemens, Phoenix Contact, Rockwell, Beckhoff und weitere entwickelten an Netzwerk-Protokollen für echtzeitfähige Ethernet-basierte Feldbussysteme wie Profinet, Ethernet/IP oder EtherCat.

Die Überschneidungen mit IT-Netzwerken beziehen sich jedoch nur auf den Netzwerkzugang (Layer 1 und 2). Lediglich Ethernet-Kabel, Stecker, MAC-Adresse, EtherType ID sind Verfahren, die ebenfalls genutzt werden. Industrie-Steuerungssysteme für Motion Control, also Bewegungsregelung, benötigen Echtzeit Netzwerkdienste für Feldbussysteme über die das klassische Office TCP/IP-Protokoll (Layer 3 und 4) nicht verfügt.

TSN-fähige (Time-Sensitive Networking) Switches umgehen künftig dieses Manko. OPC UA sowie auch Profinet können durch Hardware-Priorisierung und -Synchronisierung von TCP/IP-Paketen eine Echtzeitfähigkeit nutzen.

Industrie-Netzwerke werden von Elektrotechnikern und Mechatronikern entwickelt und betrieben. Betreiber und Entwickler von Automatisierungs- und Prozesstechnik sind gefordert, diese und weitere Technologieschritte mitzugehen. Denn es ist die Basis um Industrie 4.0 bzw. Digitalisierung umzusetzen, ohne die Kernautomatisierung anzutasten. Pflicht der OT war es immer die Anlagenverfügbarkeit und -sicherheit bei aller Digitalisierung, kompromisslos gewährleisten zu können.

Bislang subsumierte der Begriff OT (Operational Technology) oder auch Betriebstechnik als jener Aufgabenbereich, der die Konfiguration von Hard- und Software zur Steuerung und Regelungen von Maschinen, Anlagen und Prozessen verantwortet. Durch den Einzug Ethernet-basierter Kommunikation ändern sich die Anforderungen an dieses Berufsbild jedoch sehr stark.

Klassische IT-Kenntnisse über Betriebssysteme und Applikationen sind hier nur bedingt nützlich. Auch klassische IT-Security-Methoden greifen hier nicht. Die Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit) sind komplementär zu jenen Netzwerk-Schutzzielen der Industrie, also der OT-Security – hier steht Verfügbarkeit (Echtzeit) an erster Stelle.

OT-Security. OT-verantwortliche Elektrotechniker und Mechatroniker sind nicht nur für technische Lösungen, sondern ebenfalls für die Entwicklung von Prozessen und der Integration bis zum Betrieb gefordert. Bei der Planung und im Betrieb ist durch die OT auch laufend das Security-Niveau zu bestimmen.
Alleine eine Firewall einzuplanen ist nur eine Security-Maßnahme. Wenn Cyber-Security-Maßnahmen gefordert sind, so unterstützen Fachgruppen der Elektrotechnik mit Leitfäden bzw. Standards und Normen für Industrial Security in der Automatisierung. Diese sind:
- IEC (Internationale Elektrotechnische Kommission)
- ÖVE (Österreichischer Verband für Elektrotechnik)
- VDMA (Verband Deutscher Maschinen- und Anlagenbau).

Die internationale Normenreihe der IEC 62443 Industrial Cyber Security für industrielle Systeme der Steuerungs- und Leittechnik“ definiert Rollen für
- Betreiber,
- Integratoren,
- Hersteller.

Phoenix Contact wurde vom TÜV Süd als eines der ersten Unternehmen im deutschsprachigen Raum nach der Normreihe für IT-Sicherheit IEC 62443-4-1 und 2-4 zertifiziert.
Dies bestätigt, dass das Unternehmen:
- die Entwicklung von Secure-by-Design-Produkten entsprechend dem Prozess IEC 62443-4-1 sowie
- das Design von sicheren Automatisierungslösungen entsprechend dem Prozess IEC 62443-2-4 durchführt.

Pilotfabrik Industrie 4.0: Netzwerk- und System-Security nach IEC 62443. Phoenix Contact Österreich hat in der Pilotfabrik 4.0 der TU Wien eine große Investition in Netzwerksicherheit nach IEC 62443 getätigt. So wurde ein realistisches Testumfeld mit echten Produktionsnetzwerken, Echtzeit-Maschinennetzwerken, echten Maschinen, Prozessketten und Produkten (3D-Drucker) geschaffen.

Betreiber und Entwickler von Automatisierungs- und Prozesstechnik sind gefordert, bei den Technologieschritten in puncto Security mitzugehen.

VERANSTALTUNG PRODUCTION DAY

Wie läuft der Echtbetrieb in der Pilotfabrik Industrie 4.0 in Wien wirklich? Dies wird im Jänner durch die dortigen studierenden Mitarbeiter unter Einsatz von Assistenzsystemen, die 3D-Drucker montieren, gezeigt. An diesem Tag steht wissenschaftliches Personal der TU Wien für die einzelnen Fachbereiche bereit und bietet weiters Führungen an. Die Mitarbeiter stehen im Anschluss für fachliche Fragen und Wissensaustausch zur Verfügung.

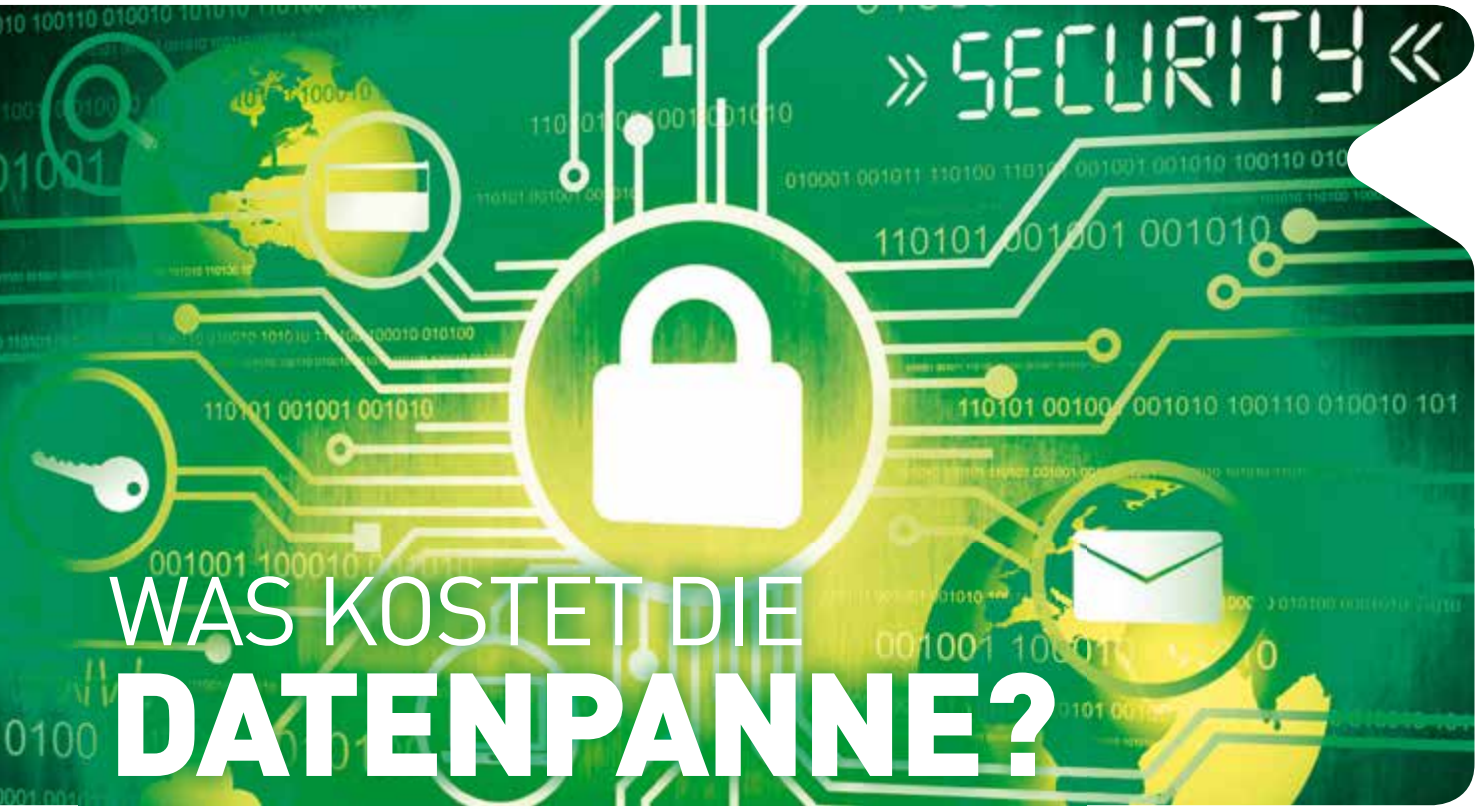
Wann:
16. Jänner 2020 - 14:00 bis 16:00 Uhr
Ort:
Aspern, Seestadtstraße 27/3, 1220 Wien
Kostenfreie Anmeldung:
www.phoenixcontact.at/production-day

Trainings. Weiters gibt es die Möglichkeit von technischen Trainings für Mitarbeiter, so etwa beim TÜV Rheinland. Es handelt sich dabei um ein 4 Tage-Vorbereitungstraining namens „Fundamentals of Cyber Security“ inklusive Prüfung. Die Inhalte orientieren sich an den Empfehlungen des Industriestandard IEC 62443 „Industrial Cyber Security für industrielle Systeme der Steuerungs- und Leittechnik.“
Das Cyber Security-Training vermittelt in deutscher Sprache ausführlich wichtige Grundlagen zur sicheren Vernetzung und Kommunikation in der industriellen Automatisierung. Nach Teilnahme an diesem Training mit erfolgreichem Abschluss erhalten Teilnehmer vom TÜV Rheinland eine formelle Bescheinigung. Das Training bietet Spezialisten aus den Bereichen der Betriebstechnik (OT) und IT sowie Sicherheitstechnik (funktionale Sicherheit) Grundlagen zur Analyse von potenziellen Cyber Security-Schwachstellen wie auch Referenzmodelle zur Umsetzung von sicheren Netzen in der industriellen Automatisierungs- und Steuerungstechnik.

www.phoenixcontact.at/seminare

Industrielles Netzwerkdesign nach IEC 62443

Der Autor:
Erich Kronfuss
... ist Security Experte bei Phoenix Contact in Wien.



WAS KOSTET DIE DATENPANNE?

Der Schutz vor Datenpannen wird für Unternehmen immer komplexer und kostet viel Geld. Laut einer von IBM Security veröffentlichten Studie sind die Kosten für Unternehmen hierbei innerhalb der vergangenen fünf Jahre weltweit um zwölf Prozent gestiegen.

Obwohl Schutzmaßnahmen ein wesentlicher Bestandteil der Cybersicherheit sind, steigt die Wahrscheinlichkeit, Opfer eines Sicherheitsvorfall zu werden, laufend an. Somit steigt auch der Druck auf die Sicherheitsteams einen Plan zu haben, um auf das zu reagieren, was unvermeidlich erscheint: dass ein Sicherheitsvorfall stattfindet. Trotz dieses Trends gibt es auch ermutigenden Ergebnisse der Studie. Ein wirksamer Reaktionsplan im Falle einer Datenpanne kann die Kosten reduzieren.

Welche Faktoren tragen zu den Kosten einer Datenpanne bei? Der Cost of a Data Breach Report untersuchte Hunderte von Faktoren, die die Kosten einer Datenpanne bei mehr als 500 Unternehmen über einen Zeitraum von zwölf Monaten in den Jahren 2018 und 2019 beeinflussten. Das reicht von Erkennungs- und Benachrichtigungskosten über behördliche Geldbußen bis hin zu Gerichtskosten und entgangenem Geschäft. Die Studie ermöglicht es zu verstehen, wie diese verschiedenen Faktoren die Kosten beeinflussen können, im Guten wie im Schlechten.
Einer der größten Kostenblöcke war die Zeit, die gebraucht wird, einen Sicherheitsvorfall zu erkennen und zu beheben. Dieser Zeitraum ist als Lebenszyklus von Datenpannen bekannt. Der durchschnittliche Lebenszyklus von Datenpannen betrug heuer 279 Tage. Unternehmen, die eine Datenpanne in weniger als 200 Tagen erkennen und beheben konnten, hatten Kosten, die im Durchschnitt etwa 1,2 Millionen USD niedriger waren als Unternehmen, die mehr als 200 Tage brauchten, um eine Datenschutzverletzung einzudämmen (3,34 Millionen USD gegenüber 4,56 Millionen USD, eine Differenz von 37 Prozent. Zu den untersuchten Faktoren, die zu diesem Kostenunterschied beigetragen haben, gehörte die Art des Sicherheitsvorfalls. Die teuersten waren diejenigen, die durch böswillige Angreifer verursacht wurden, seien es externe Akteure oder böswillige Insider. Diese Vorfälle dauerten viel länger, bis sie identifiziert und behoben waren (durchschnittlich 314 Tage im Vergleich zum Gesamtdurchschnitt von 279 Tagen).

Incident Response-Teams und Prüfung des Plans. In der Studie wurde untersucht, welche Möglichkeiten es gibt, die Gesamtkosten einer Datenpanne zu senken. Unter den 26 Faktoren war die Bildung eines Incident Response-Teams der wichtigste kostensenkende Faktor, der die durchschnittlichen Gesamtkosten eines Datenverstoßes um 360.000 USD reduzierte (bei bereinigten Durchschnittskosten von 3,56 Millionen USD gegenüber dem Gesamtdurchschnitt von 3,92 Millionen USD). Darüber hinaus reduzierten umfangreiche Tests eines Incident Response-Plans die durchschnittlichen Gesamtkosten um 320.000 USD (bei bereinigten Kosten von 3,6 Millionen USD).

Schritte zur Verbesserung der Reaktion auf Vorfälle. Prävention ist nicht immer möglich, daher sind Vorbereitung und Planung unerlässlich, um die Folgen eines Cyberangriffs zu minimieren. Maßnahmen, um die Reaktionszeit zu verkürzen und die finanziellen und Reputationsschäden einer Datenpanne zu minimieren, können sein:

1. **Stellen Sie Ihr Incident Response-Team und Ihren Plan auf den Prüfstand.** Die Effektivität der Reaktion im Falle einer Datenpanne hängt davon ab, ob man einen Plan erstellen, testen und laufend optimieren kann. Aber ein Plan ist nur so gut wie die Menschen, die ihn ausführen. Teams müssen Führungs-, Kommunikations- und Entscheidungsfähigkeiten trainieren, um mit den schwierigsten Situationen fertig zu werden.
2. **Investieren Sie in Technologien.** Soweit wie möglich sollte man seine Reaktion durch Technologien automatisieren, einschließlich Tools, die bei der Erkennung und Automatisierung der Orchestrierung helfen können. Der Cost of a Data Breach Report ergab, dass die Sicherheitsautomatisierung dazu beiträgt, die Kosten für eine Datenpanne, für die befragten Unternehmen, um bis zu 50 Prozent zu senken.
3. **Nutzen Sie Threat Intelligence.** In der Studie wurden 51 Prozent der Vorfälle bei befragten Unternehmen durch böswillige oder kriminelle Angriffe verursacht. Threat Intelligence kann helfen, Einblicke in die verschiedenen Motive, Fähigkeiten und Absichten von Angreifern zu gewinnen, so dass Sie Ihre Risiken verstehen und effizientere Sicherheitsinvestitionen tätigen können.
4. **Sichern Sie Ihre Systeme und Daten und haben Sie einen Business Continuity-Plan.** Das entgangene Geschäft war der größte von vier Kostenblöcken, die im Bericht über Datenschutzverletzungen 2019 untersucht wurden: teurer als Erkennungs- und Eskalations-, Benachrichtigungs- und Nachbearbeitungskosten sowie Rechtskosten. Niemand möchte, dass die Kosten eines Vorfalls noch zusätzlich durch das Herunterfahren von Systemen oder das Löschen von Daten oder Systemen, die kostspielig wiederherzustellen sind, noch weiter erhöht werden. Unternehmen sollten Backups daher offline speichern.
5. **Wenn alles fehlschlägt, rufen Sie die Experten.** Wenn ein Incident Response-Team unvorbereitet oder überfordert ist, sollten man erwägen, Anbieter von Incident Response-Diensten zur Bewältigung eines komplexen Cyberangriffs zu Hilfe zu holen. Diese können helfen, den Angriff nicht nur einzudämmen, sondern auch zu beheben und die Systeme wieder herzustellen.

www.ibm.at

Der Cost of a Data Breach Report untersuchte Faktoren, die die Kosten einer Datenpanne beeinflussten.

Der Autor:
Stefan Preining
... ist Manager Security Solutions bei IBM Österreich.

Eine Engineering-Lösung für alle Disziplinen

Industrie-4.0-gerechte Anlagenplanung

AUCOTEC
Create Synergy – Connect Processes

Engineering Base

free download: www.aucotec.at

SICHERE VERNETZUNG IN DER AUTOMATISIERUNGSTECHNIK

Die Digitalisierung der modernen Produktionstechnik stellt die Industrie vor neue Herausforderungen. Durch die zunehmende Vernetzung wird die Absicherung der Produktionsanlage gegenüber Angreifern immer schwieriger, da der Angreifer anonym und aus der vollständigen Dunkelheit heraus agieren kann.

Im Angelsächsischen gibt es ein spezialisiertes Wort für die Sicherheit der Anlage gegen Angreifer: Security. Und bei Security handelt es sich um eine Art der Verteidigung und damit um eine Strategie. Eine Strategie ist meist ein Bündel von Maßnahmen, das es dem Angreifer schwer macht, die Werte einer Produktionsanlage, ihre Verfügbarkeit und Informationen, anzugreifen.

Weit verbreitete Schutzmaßnahmen sind heute schon die Abschottung der Netze mittels so genannter Firewalls nach außen. Da diese Mechanismen jedoch nicht unüberwindbar sind, werden Netze innerhalb der Anlage in kleinere Netze getrennt und abgeschottet. Die Authentifizierung jedes Teilnehmers am Netzwerk mittels kryptographischer Schlüssel, die sogenannte Network Access Control, sorgt dafür, dass nur noch bekannte Geräte überhaupt am Netzwerk teilnehmen können. Da man sich unter Vorwänden allerdings auch auf die Liste bekannter Geräte schmuggeln kann, sollten in der nächsten Stufe auch einzelne Nachrichten gegen Manipulation oder Täuschen durch Dritte geschützt werden. Hierzu wird die Nachricht mit einem geheimen Schlüssel, dem Message Authentication Code (MAC), so zu einer Checksumme verrechnet, dass der Empfänger die Authentizität der Nachricht überprüfen kann.

Strategien können vielfältig sein. Strategien können allerdings sehr vielfältig sein. Ob eine Strategie richtig oder falsch ist, lässt sich meist erst nach einem Ereignis sagen. Doch es gibt Orientierungshilfen: Die internationale Norm IEC 62443 „Industrielle Kommunikationsnetzte – IT-Sicherheit für Netze und Systeme“ z.B. gibt einen guten Überblick über wirksame Maßnahmen und den heutigen Stand der Technik. Während generelle Normen den Leser keine konkreten Handlungsanweisungen (Rezepte) geben können, gibt es von professionellen Organisationen für die digitale Kommunikation bereits konkrete Hinweise und Ratgeber.

Die für Profinet verantwortliche Organisation, Profibus International, berät in der umfassenden Broschüre „Profinet Security Guideline“ über mögliche und sinnvolle Maßnahmen zur Abwehr gegen digitale Angreifer. Im Hintergrund wird in der Organisation an weiteren Maßnahmen gearbeitet: Einer Spezifikation zu einer sicheren Kommunikation mit Profinet.

Aber auch Zusammenschlüsse von Akteuren aus Wirtschaft, Forschung und Politik, wie z.B. die Industrial Data Space Association, entwickeln gemeinsam Richtlinien und Möglichkeiten im Umgang mit der Datensicherheit.

Weit verbreitete Schutzmaßnahmen sind heute schon die Abschottung der Netze mittels so genannter Firewalls nach außen.

Sicher und alltagstauglich? Grundlage einer effektiven Sicherheitsstrategie ist immer die genaue Analyse der individuellen Situation. Was soll geschützt werden? Wie groß ist der mögliche Schaden? Wie schnell kann ich mich von einem möglichen Angriff erholen? Die gewählte Lösung muss praktikabel sein und sollte, wenn überhaupt, nur wenige Einschränkungen im Arbeitsalltag bedeuten. Da viele Schutzmaßnahmen mit mechanischen oder digitalen Schlüsseln zu tun haben, ist es von großer Bedeutung, dass die Technologie begreifbar ist und verstanden wird. Ist sich ein Mitarbeiter der möglichen Konsequenzen nicht bewusst, wenn er seinen Werksausweis an sympathische oder autoritär auftretende Dritte weitergibt, spielt die technische Sicherheit dieses Schlüssels kaum noch eine entscheidende Rolle. Daher wird die so genannte „Awareness" von Mitarbeitern im Zusammenhang mit Security gerne betont. Auch Ausnahmesituationen müssen im Security-Konzept berücksichtigt sein. Dazu gehört der Einsatz eines Service-Technikers oder einer Service-Firma bzw. die mögliche Notwendigkeit sich doch einmal Dateien von anderen Systemen zu übertragen. Fehlen diese Möglichkeiten, werden im Ernstfall alle Security-Mechanismen umgangen, um die Verfügbarkeit des Systems wiederherzustellen. Ist dies häufiger notwendig, führt das nicht allzu selten zum regelmäßigen oder gar endgültigen Abschalten der Security-Maßnahmen.

Kryptographie und Identitätsverwaltung. Neben der Praktikabilität im Alltag muss jeder Form von Zugangs- und Zugriffsbeschränkung ein zuverlässiges Verwaltungssystem zugrunde liegen. D.h. der Mensch muss festlegen, wer welchen Zugriff bekommt und die vergebenen Identitäten verwalten. Zugangsbeschränkungen umfassen dabei das physische Unternehmensgelände genauso, wie das digitale Firmennetzwerk sowie jede einzelne Anlage und Nutzungskomponenten. Die Kryptographie kann nicht über Gut oder Böse entscheiden. Es handelt sich bei der Kryptographie um mathematische Methoden, welche mittels eines „Geheimnisses" z.B. die Übertragung von Nachrichten für Dritte unleserlich machen.

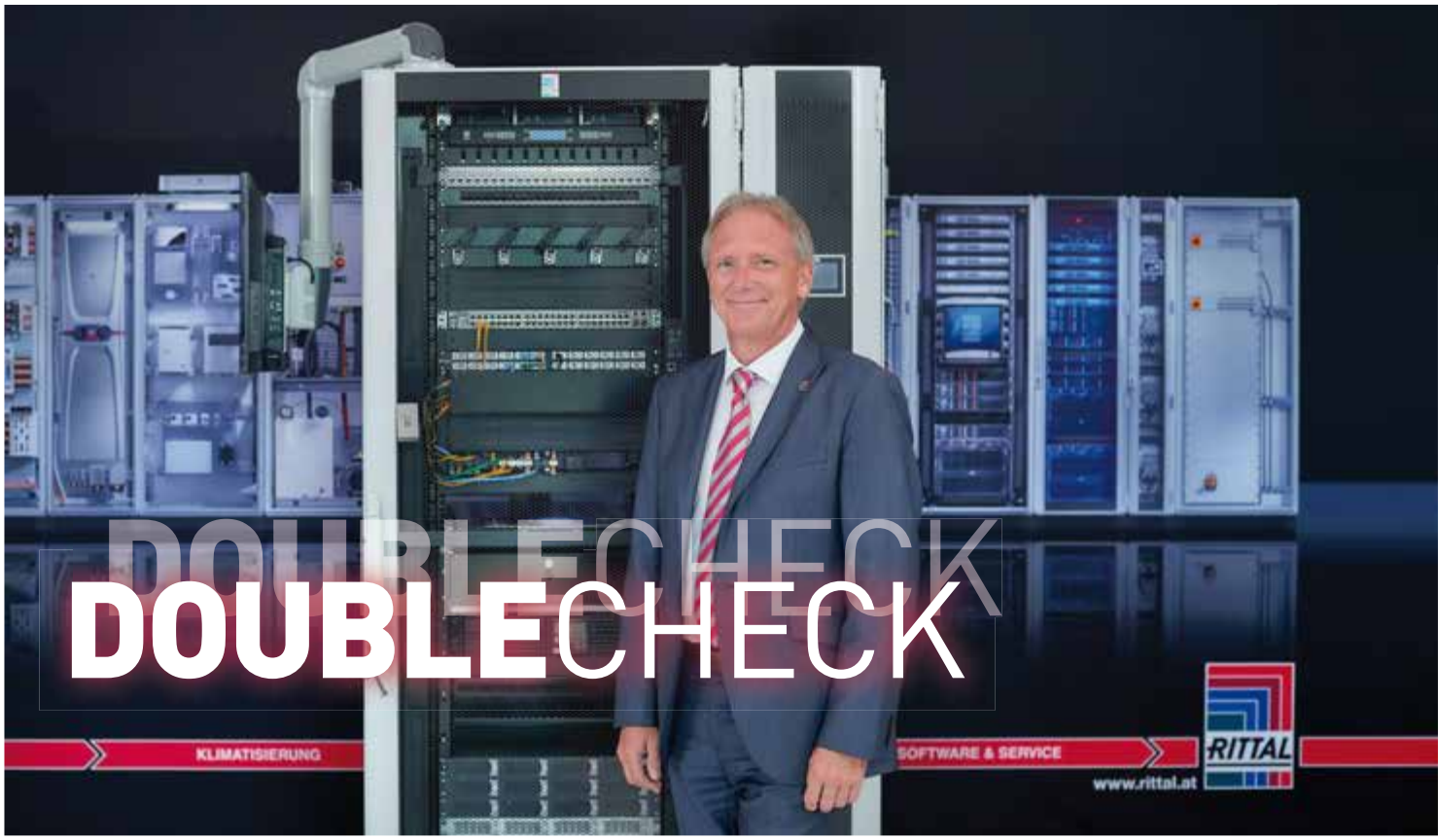
Der Mensch muss die grundsätzliche „Wer darf was"-Entscheidung vorab treffen, und durch Vergabe von Geheimnissen jede einzelne Komponente oder Maschine in den Circle of Trust aufnehmen bzw. für bestimmte Aufgaben legitimieren.

Ein uns allen bekanntes Geheimnis ist das meist mit einem User-Namen gepaarte Passwort. Während wir im privaten Umfeld schon Schwierigkeiten bekommen, die vielen Identitäten im Internet sicher und langfristig zu verwalten, ist die Verwaltung von Identitäten in einer industriellen Anlage mittels persönlicher Passwörter undenkbar (Gruppen-Berechtigungen mit Ein- und Austritt von Mitarbeitern bei über vielen hundert Geräten). Daher wird die Verwaltung von Identitäten von Usern und Geräten künftig von sogenannten Verzeichnisdiensten übernommen. Hier muss man sich zentral authentifizieren und erhält dann den notwendigen Zugriff auf die entsprechenden Ressourcen.

Die Zukunft ist sicher. Selbst wenn eine sichere und effektive Strategie gefunden und implementiert wird, muss auch diese laufend aktualisiert werden. Die Digitalisierung und der allgemeine technische Fortschritt treiben die Entwicklung von digitalen Vernetzungsmöglichkeiten schnell voran.
Im gleichen Tempo wachsen allerdings auch die Bedrohungen. Schnellere Computer machen das Finden von Geheimnissen durch stures Ausprobieren, die sogenannte Brute-Force-Methode immer effektiver und auch auf der Seite der Angreifer wird geforscht. Deshalb müssen Sicherheitsstrategien kontinuierlich weiterentwickelt werden. Die vernetzte Zukunft kommt mit Sicherheit. Wir arbeiten daran, dass sie zur sicheren Realität wird.

www.sick.at

Selbst wenn eine sichere und effektive Strategie gefunden und implementiert wird, muss auch diese laufend aktualisiert werden.



DOUBLECHECK

Klassische IT-Security verlangt heutzutage einiges ab. Doch gibt es überhaupt 100 % Sicherheit? Dieser Frage stellte sich Andreas Hajek, Verkaufsleiter IT bei Rittal Österreich, und erläutert seine Sicht der Entwicklungen.

Von Stephanie Englert

IoT 4 Industry & Business: Security ist DAS Thema vieler Unternehmen. Auf was müssen diese Ihrer Ansicht nach bei all den gebotenen Security-Lösungen besonders achten?

Andreas Hajek: Sicherheit muss mit einem gesamtheitlichen Ansatz betrachtet werden. Oftmals wird sehr viel Augenmerk auf Virenschutz, Firewalls, APT, und ähnliche softwarefokussierte Dinge gelegt. Die physikalische Sicherheit des Gesamtsystems wird dabei oft vernachlässigt.

Vor allem im Bereich der KMU trifft dies besonders zu, da sehr große Unternehmen meist eigene Rechenzentren betreiben die gut abgesichert sind, mittlere Unternehmen aber ihre IT noch oft vor Ort haben und auch nicht immer den Schritt in die Cloud oder ein Colocation-Rechenzentrum wählen.

Letztendlich geht es bei Security um Unternehmenssicherheit – und das umfasst nicht nur IT sondern auch Mitarbeiter, Zugänge, Zulieferer, Logistik, Produktion und vieles mehr. Vor allem die gesteigerten Risiken durch die Vernetzung von Produktionsstraßen und ganzen Fabriken (Industrie 4.0) bringt neue Herausforderungen mit sich.

IoT: Rittal bietet Lösungen an und sagt zugleich: „Neben geringen Latenzzeiten gehören hohe physische Sicherheit und Hochverfügbarkeit der IT heute zu den zentralen Anforderungen der Unternehmen. Wir unterstützen Unternehmen hier bei der Lösung." Inwiefern?

Hajek: Wir haben Dienstleistungspakete entwickelt, die unsere Kunden unterstützen, die relevanten Parameter der physikalischen Sicherheit zu überprüfen und ggfs. Korrekturmaßnahmen durchzuführen. Diese betreffen Bereiche wie Klimatisierung und Stromversorgung, den physikalischen Zugriff auf Systeme, das Monitoring der relevanten Parameter uvm.

Gerade der Schritt der Dezentralisierung, der aktuell durch Edge Computing und Distributed Clouds vollführt wird, erfordert natürlich wieder einen bewussteren Umgang mit Security und die Implementation geeigneter Maßnahmen um die zunehmend vor Ort stehenden Systeme entsprechend vor Zugriffen und Attacken zu schützen. Diese befinden sich ja oft außerhalb des gängigen Firmen-Perimeters und müssen gesondert abgesichert werden, genauso wie die sie verbindenden Netzwerke.

IoT: Was unterscheidet Lösungen von Rittal im Vergleich zu anderen Angeboten?

Hajek: Wir betrachten die Lösungen für unsere Kunden gesamtheitlich und gewährleisten, dass die Lösung systemzertifiziert ist. Das erlaubt eine durchgängige Betrachtung und Funktionsweise sowie eine lückenlose Überwachung der Systeme. Auch integrieren sich unsere Überwachungs- und Monitoring-Tools mit gängigen Anwendungen am Markt, sodass der Kunde von der untersten Schicht bis zur Business-Applikation alles einheitlich und gesamtheitlich überwachen kann. Wir unterscheiden

Andreas Hajek
Verkaufsleiter IT bei Rittal Österreich

„Sobald zu einem System ein physischer Zugang besteht, ist die Sicherheit extrem gefährdet."

uns hierbei durchaus auch dadurch, dass wir viele Leistungen direkt anbieten, die Kompetenzen im Haus haben und unsere Teams von hochkarätigen Experten den Kunden direkt zur Verfügung stehen.

IoT: In Zeiten der zunehmenden Daten und entsprechend auch Angriffe stellt sich die Frage, ob es überhaupt möglich ist, „mein" Unternehmen zu 100 % zu schützen?
Hajek: Hundertprozentiger Schutz ist nahezu unmöglich. Das liegt zum einen daran, dass Angreifer immer einen Schritt voraus sind und die meisten Mechanismen eigentlich nur reaktiv wirken, aber kaum Bedrohungen antizipieren.
Dieser leichte Vorteil wird es immer ermöglichen, dass Attacken erfolgreich ausgeführt werden solange die Security Community diese Bedrohung nicht erkannt, klassifiziert und vermeidbar gemacht hat. Das liegt auch an der steigenden Kreativität der Cyberkriminellen, an der teils mangelnden Qualität von Applikations- und Betriebssoftware und an dem enormen Geschäftspotenzial, welches hinter dem Cybersecurity-Business liegt.
Zum anderen steigen die Kosten enorm an, je höher der Anspruch an Sicherheit wird. Irgendwann muss jedes Unternehmen sich überlegen, wieviel in Security investiert werden soll und wie der Business Case dazu aussieht.

IoT: Abschließend erlauben Sie die „in die Glaskugel" sehende Frage: Wie „sicher" ist Security?
Hajek: Security ist immer nur so sicher wie das schwächste Glied einer Kette. Enorme Investitionen in Software sind umsonst, wenn das Bewusstsein der Mitarbeiter des Unternehmens nicht entsprechend geschult wird und das Thema offen sensibilisiert wird. Das betrifft natürlich auch den Umgang mit der physikalischen Sicherheit. Sobald zu einem System ein physischer Zugang besteht, ist die Sicherheit extrem gefährdet.
Und: Die meisten Gefahren und Schwachstellen sind – so traurig das auch ist – leider immer noch intern zu finden. Man darf nie vergessen, dass Cybercrime ein Multimilliarden-Dollar-Geschäft ist, das heutzutage von absoluten Profis betrieben wird. Aus der Sicht der physikalischen Infrastruktur für IT, Produktionsumgebungen usw. leistet Rittal hier einen signifikanten Beitrag um Unternehmen und ihr geistiges Eigentum zu schützen.

www.rittal.at

- Zuverlässige 3-D-Messungen durch vier Scanebenen
- Sehr gute Winkelauflösung und kleiner Lichtfleck für hohe Präzision
- Zuschaltbarer, sichtbarer Pilotlaser zur exakten Ausrichtung und einfachen Inbetriebnahme

www.pepperl-fuchs.com/pr-R2300

Your automation, our passion.

PEPPERL+FUCHS

Die Vernetzung von Produktionsanlagen stellt die IT- und OT-Abteilungen vor neue Herausforderungen. Neben funktionalen Anforderungen geht es meist auch um das Verständnis für Technik, Organisation und Prozesse, ist Christian Koch, Director GRC & IoT/OT EMEA bei NTT überzeugt.

MITEINANDER STATT GEGENEINANDER

IoT 4 Industry & Business: Wie bringt man Ihrer Meinung nach OT und IT in der Produktion zusammen?

Christian Koch: Will man OT und IT in einem Produktionsunternehmen stärker zusammenführen, müssen beide Bereiche zuerst die gleiche Sprache sprechen – hier ist viel Übersetzungsarbeit erforderlich, weil die Dinge oftmals nicht die gleiche Bedeutung haben. Nehmen wir zum Beispiel den Begriff Sicherheit: Ein IT-Verantwortlicher denkt an Vertraulichkeit, die OT-Fachleute sprechen von Verfügbarkeit. Nicht zu übersehen oder überhören ist aber auch ein grundlegendes Konkurrenzdenken und Fehlerzuweisungen innerhalb beider Parteien, die eine Zusammenarbeit oft erschweren oder unmöglich machen. Es ist wichtig, dass die Mitarbeiter aktiv aufeinander zugehen, wobei die Unternehmensleitung dies natürlich fördern bzw. fordern muss. Ziel ist es, dass die Security-Abteilung schnell über neue Angriffsvektoren und Sicherheitsrisiken informiert und eine Kooperation aus IT- und OT-Team sofort die richtigen Gegenmaßnahmen einleitet und den Angriff abwehrt – dann ist die Zusammenführung gelungen.

IoT: Welche Unterstützung bietet NTT seinen Kunden?

Koch: Wir unterstützen unsere Kunden, die Sicherheits- und Geschäftsrisiken aufzuzeigen und zu bewerten, um auf diese Weise mehr Transparenz zu schaffen – vor allem gegenüber dem Management, das die IT-/OT-Budgets verwaltet. Daneben bieten wir eine Vielzahl technische und organisatorische Lösungen. Oberste Priorität hat in den meisten Unternehmen die Herstellung von Visibilität im OT-Netzwerk. Hier helfen wir unseren Kunden, die Komponenten innerhalb der Produktionsnetze im Detail zu identifizieren, die Wechselwirkungen der Kommunikation innerhalb ihrer gesamten Produktionsstraßen und Produktionszellen zwischen den Komponenten und Systemen aufzuzeigen, zu dokumentieren und die verwendeten Protokolle zu analysieren.

IoT: Welche Verantwortung haben die Hersteller?

Koch: Das Ziel muss sein, dass sich die Hersteller beim Verkauf einer Anlage verpflichten, die IT-Sicherheit über den gesamten Lebenszyklus zu gewährleisten und die Käufer im Fall eines

Cyberangriffs aktiv zu unterstützen und so einen ganzheitlichen Cybersecurity-Prozess zu etablieren. Im Moment fordere ich von den Herstellern den Einsatz von Anlagenbauern und Instandhaltern mit grundlegendem Cybersecurity-Know-how und einer Awareness für Cybersecurity. Oft haben die Techniker und Instandhalter null Verständnis dafür. Das Verbinden von Notebooks mit verschiedenen Kundennetzwerken und die Nutzung von USB-Sticks und unsicherer Remote-Wartung ist leider gang und gebe. Oft werden nur funktionale Anforderungen umgesetzt und keine Sicherheitsfunktionen. Wir wünschen uns Hersteller, die uns hier aktiv unterstützen.

IoT: Macht uns die Freude über die Bequemlichkeiten, die uns die IT ermöglicht, blind für gewisse Angreifbarkeiten?
Koch: Der Komfort, den uns viele IT-Anwendungen auf den ersten Blick bescheren, ist natürlich toll – und es stimmt, vor lauter Begeisterung denken wir nicht an die Risiken, die neue Technologien unausweichlich mit sich bringen. Darum ist ganz wichtig: know your risks! Nur wenn ich das Risiko kenne, kann ich es mit geeigneten Maßnahmen minimieren.
Und für den Fall, dass man einmal angegriffen wird, sollte man unbedingt einen Notfallplan, also einen Incident Response-Plan, zur Hand haben. Viele Unternehmen wissen bei einem Angriff auf ein produktionsnahes Netz nicht, was zu tun ist – das muss sich ändern.

IoT: Kann es sein, dass sich viele Unternehmen für Hacker nicht interessant genug erachten?
Koch: Ja bestimmt. „Wer kennt uns schon, warum soll das uns passieren?" – eine ganz typische Reaktion. Ransomware, also Erpressungssoftware, kann jeden treffen, diese Lösegelderpresser haben nicht einzelne Unternehmen im Visier. Bei einem gezielten Angriff hingegen geht es oft um Intellectual Property (IP), also Geschäftsgeheimnisse oder Spezial-Know-how im Rahmen von Wirtschaftsspionage oder es geht darum, durch Ferneinwirkung auf Produktionsanlagen z.B. die Produktqualität zu beeinflussen. In vielen hart umkämpften Märkten wird das leider auch immer mehr zum Mittelstandsproblem wie insbesondere die letzten Wochen gezeigt haben, längst werden nicht mehr nur namhafte Großkonzerne zur Zielscheibe von Hackern.

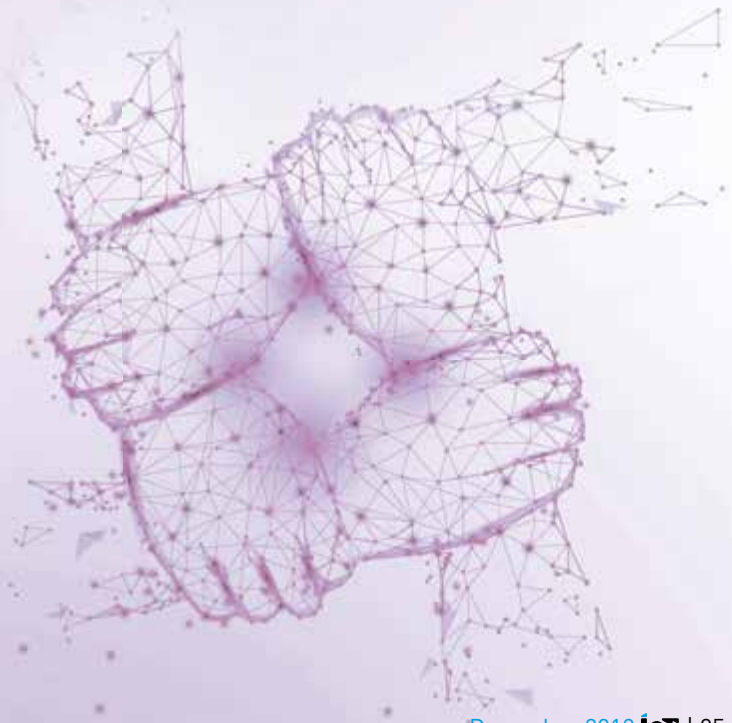
Christian Koch
Senior Manager GRC & IoT/OT bei NTT Security

„Vor lauter Begeisterung denken wir nicht an die Risiken, die neue Technologien unausweichlich mit sich bringen",

IoT: Von einem Aufzug über den Drucker bis zur Überwachungskamera, sehr viele Geräte sind mit außen verbunden. Muss das sein?
Koch: Die Konnektivität mit dem Netzwerk ist gar nicht das Problem – die mangelnden Kenntnisse und fehlendes Risikobewusstsein sind es. Um die Kontrolle darüber, wer wann mit wem kommuniziert, wiederzuerlangen, empfehlen wir alle mit dem Internet verbundenen Geräte, auch ältere Anlagen, technisch und organisatorisch abzusichern. Aber auch und vor allem bei neuen Industrieanlagen muss der Schutz vor Cyberangriffen oberste Priorität haben. Wir beobachten bei unseren Projekten leider sehr oft, dass die Konstrukteure und Installateure der Anlage, aber auch die verantwortlichen Anlagenbetreiber und Instandhalter über kein Security-Know-how, noch nicht mal grundlegende Security Awareness verfügen. Die Hersteller von Industriesteuerungen können noch so viele Security-Funktionen in Steuerungsbausteine wie PLCs einbauen, wenn diese kein Techniker aktiviert, sind sie wertlos.

IoT: Was bedeutet das konkret?
Koch: Bei Industrie 4.0-Anlagen – mittlerweile betrifft das so gut wie jede neu gebaute Anlage – müssen alle relevanten Schnittstellen zum Internet oder Cloud-Diensten, aber auch zu internen Systemen, einzeln betrachtet werden. Die Hersteller der Anlagen zum Beispiel sammeln Informationen verschiedener Anlagen für ihre internen Fehleranalysen, Predictive Maintenance-Maßnahmen oder auch zur Weiterentwicklung ihrer Machine Learning-Modelle. Der Anlagenbesitzer bzw. -betreiber muss darüber natürlich Kenntnis haben – er muss genau wissen, wie auf die Anlage von außen zugegriffen werden kann und zu welchen Daten Externe Zugang haben und muss, falls erforderlich, Daten anonymisieren oder im Worse Case Zugriffe auch sperren können. Der wichtigste Grundsatz ist weiterhin ein risikobewusstes Handeln in OT-Umgebungen. (bs)

https://hello.global.ntt



Die Initiative Plattform Industrie 4.0 bietet anhand eines neuen Security-Leitfadens konkrete Beispiele und Hilfe an.

SICHER? SICHER!

Es gibt sie – Bedrohungen durch Cyberangriffe. Aber betreffen sie wirklich jeden? Dieser Frage stellen sich Unternehmen im Zuge der Digitalisierung und stoßen zunehmend auf mehr Unklarheiten. Ein Leitfaden soll dem nun Abhilfe schaffen.

„Viele KMU glauben, dass sie aufgrund ihrer Größe keine Cyberangriffe befürchten müssen und sind deshalb oft unzureichend geschützt." Dies betonte eingangs eines Gesprächs der Initiative Plattform Industrie 4.0 in Wien Wilfried Enzenhofer, Geschäftsführer der Upper Austrian Research, und sagte weiter: „Gerade das macht sie verwundbar. Die meisten Attacken erfolgen nicht gezielt, sondern automatisiert, d.h. die Angreifer kennen ihr Ziel nicht. Oft genügen schon ein paar einfache Dinge, um sich dagegen zu wappnen – neben technischen Sicherheitsmaßnahmen sind deshalb auch geschulte Mitarbeiter enorm wichtig."

Doch hier sind wir auch gleich beim Problem – dem Nachwuchs. Denn der Fachkräftemangel zieht sich durch alle Branchen und ein Ende ist nicht in Sicht. Dieses Phänomen ist nicht nur den geburtenschwachen Jahrgängen geschuldet, sondern sicher auch der Tatsache, dass es an gezielten Ausbildungen mangelt. Doch auch hier gibt es Bestrebungen, die Ausbildungsanreize zu verbessern und im Rahmen eines Studiums oder auch einer berufsbegleitenden Ausbildung fachliches Wissen zu erlernen.

Doch wo auf der einen Seite das Problem des menschlichen Nachwuchses im Raum steht, gibt es auf der anderen Seite die Herausforderung, dass der Mensch für viele Unternehmen auch in gewisser Hinsicht ein Problem darstellt, in dem er oder sie die Schadstoffsoftware entweder versehentlich aktiviert, mit in den Betrieb bringt oder eben Türen für potenzielle Angriffe öffnet. „Oft fehlt es einfach am Bewusstsein für die Gefahr, die ein USB-Stick mit sich bringt oder eine vermeintlich ungefährliche Auskunft am Telefon mit sich ziehen kann", so die Experten im Gespräch übereinstimmend. In der Studie heißt es hierzu: Angriffe auf Industrieunternehmen durch Infektionen mit einer Schadstoffsoftware sind laut BSI-Analyse die zweithäufigste Angriffsform hinter Social Engineering-Angriffen wie Phishing Mails.

Voller Angriff auf Österreich. Enzenhofer betont, dass im Zuge der Studie herauskam, dass Österreich zu den beliebtesten Angriffszielen für Cyberangriffe zähle (Platz 5). Dies sei auch der Excellence der heimischen Firmen und ihren Produkten geschuldet, die entsprechend im Interesse der Angriffe stünden. Die Angriffe kämen selber (laut IP-Adressen) hauptsächlich aus Russland und den USA. Die Studie zeige weiters, dass 87 % der Befragten bereits „Opfer" eines Störfalles geworden sind. Ein nicht unwichtiger Prozentsatz gab auch an nicht zu wissen, ob man bereits Ziel eines Angriffes war. Was ein vermeintlicher Produktionsstillstand bedeute, stehe laut Enzenhofer sowieso außer Frage.
Doch was bedeutet das alles nun? Der Cyber Security-Leitfaden der Plattform Industrie 4.0 stellt in wenigen Kapiteln die wichtigsten Arten von Sicherheitsrisiken vor und gibt praktische Tipps mit konkreten Schutz- und Gegenmaßnahmen. Zu den Hauptrisiken zählen Mitarbeiter, Infektionen mit Schadsoftware über Internet und Intranet im Produktionsbereich sowie auch DoS- und DDos-Angriffe.
Hierzu erklärte Helmut Leopold, Head of Center for Digital Safety & Security AIT: „Die Anzahl und Dauer der DoS-Angriffe steigt ständig, auch deren Komplexität nimmt zu. Unternehmen sollten deshalb Schutz- und Gegenmaßnahmen implementieren, um weder einen wirtschaftlichen noch einen Imageschaden davonzutragen." Um KMU nun Unterstützung zu bieten, hat die WKO die Cyber Security-Hotline 0800 888 133 eingerichtet – rund um die Uhr werden WKO-Mitglieder zu Cyberattacken wie Schadsoftware beraten. Schadsoftware ist dabei eines der häufigsten IT-Sicherheitsprobleme. Allein im Frühjahr 2019 waren 900 Mio. verschiedene Schadprogramme im Umlauf, darunter BlackEnergy, Mirai, Stuxnet, WannaCry, Emotet oder Regin.

V.l.: Wilfried Enzenhofer (GF Upper Austrian Research), Roland Sommer (GF Plattform Industrie 4.0 Österreich), Helmut Leopold (Head of Center for Digital Safety & Security am Austrian Institute Of Technology – AIT) und Kurt Hofstädter (Vorstandsvorsitzender der Plattform Industrie 4.0 Österreich & Leiter Siemens Digital Strategy CEE).

Copyrights: Brandenstein Communications / Plattform Industrie 4.0 Österreich

Mehr kritische Faktoren. „Cyber Security wird immer mehr zu einem kritischen Faktor für Unternehmen. Als Plattform ist es uns deshalb wichtig, für produzierende KMU, die oft nicht die Zeit haben, sich eingehend mit der Sicherheitsthematik zu beschäftigen, einen praxisorientierten Leitfaden zur Verfügung zu stellen", so auch Kurt Hofstädter, Vorstandsvorsitzender der Plattform Industrie 4.0 Österreich & Leiter Siemens Digital Strategy CEE, während der Diskussionsrunde.
Doch es gibt auch Wege zu einer sicheren Umgebung. In der Studie heißt es hierzu: Mitunter führen schon einfache Maßnahmen zu einer erhöhten Sicherheit. Regeln zur Gestaltung von Passwörtern und deren Nutzung in unterschiedlichen Anwendungen sind dabei ein erster Schritt. Eine Grundregel lautet, nie die gleiche Kombination von Mailadresse und Passwort in verschiedenen Anwendungen zu nutzen. Hierzu gibt es zudem einen interessanten Hinweis: Auf der Webseite https://haveibeenpwned.com ist zu finden, welche Zugangsdaten wie Mailadressen oder Passwörter bereits gehackt wurden und eventuell auch im Darknet gehandelt werden.

Cloud oder lieber nicht? Wie heutzutage üblich, können Industrieunternehmen Teile ihrer für die Verwaltung oder für die Produktion benötigten IT-Komponenten auf Cloud-Plattformen von IT-Dienstleistern auslagern. Der IT-Dienstleister betreibt in diesem Fall die Systeme mehrerer Kunden gemeinsam auf derselben technologischen virtualisierten Cloud-Plattform. Dazu in der Studie: Bei nicht-ordnungsgemäßer Trennung der Kunden (Mandanten) innerhalb dieser Cloud-Plattform durch den IT-Dienstleister sind unter Umständen Übergriffe zwischen den Netzen, Daten und Systemen verschiedener Mandanten möglich. Die Ursache dieser Übergriffsmöglichkeit kann entweder eine Fehlplanung oder -konfiguration des IT-Dienstleisters sein, oder auch eine kritische Schwachstelle in der Virtualisierungstechnologie des Cloud-Anbieters.
Solche Systemschwächen können einerseits zur Spionage genutzt werden, z.B. von konkurrierenden Industrieunternehmen, die denselben IT-Dienstleister nutzen. Andererseits besteht die Möglichkeit, dass ein gezielter externer Angreifer zunächst einen anderen Kunden des IT-Dienstleisters (z.B. über den Onlineshop des Kunden) ins Visier nimmt, und nach erfolgreicher Kompromittierung des ersten Kunden über die Übergriffsmöglichkeit auf sein Hauptziel, das Industrieunternehmen, zugreift. (se)

www.plattformindustrie40.at
www.wko.at/cyber-security-hotline

Zum Security-Leitfaden
https://plattformindustrie40.at/wp-content/uploads/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf

KI ÜBERWACHT UND OPTIMIERT MASCHINEN

Die Künstliche Intelligenz wird immer tiefer in die Fertigung vordringen und neue Aufgaben übernehmen. Der Automatisierungsspezialist Festo hat daher im vergangenen Jahr Resolto – ein führendes Unternehmen im Bereich Künstliche Intelligenz für Industrieanwendungen – an Bord geholt und in die Festo-Gruppe aufgenommen. Das eröffnet, wie die Praxis zeigt, spannende Perspektiven.

Coverstory

KI werden immer besser. Auch wenn sie in vielen Bereichen noch nicht die Leistungsfähigkeit von Menschen haben – etwa wenn es um Kreativität oder das oft so wichtige „Bauchgefühl“ geht. Es gibt jedoch Anwendungen, da punkten sie mit ihren Vorzügen schon heute. Festo und Resolto treiben diese Entwicklung in der Industrie aktiv voran. Etwa mit einer KI-Lösung, die die Steuerung CPX-E-CEC und den Motorcontroller CMMT von Festo überwacht. Diese können jetzt mit Machine Learning-Algorithmen von Resolto erweitert werden und bieten intelligentes Prozess-Monitoring, beispielsweise zur Detektion fehlerhafter Batterien. Das ist aber nur ein Beispiel für die neue Generation industrieller KI, die direkt an der Maschine Daten interpretiert und künftig Betreibern und Herstellern deutlich mehr Transparenz bringen wird.

KI beim Handling von Batterien. Ein anschauliches Praxisbeispiel zeigt, in welche Richtung Festo und Resolto gemeinsam arbeiten. Während ein Handling-Portal von Festo Batterien anhebt, überwacht die KI von Resolto die Motorströme und Positionswerte der Achse auf der Steuerung CPX-E-CEC. Treten dabei Anomalien auf – zum Beispiel wenn das Handling eine zu schwere Batterie aufnimmt oder ins Leere greift – wird eine Meldung erstellt und über das IoT-Gateway von Festo an die zentrale Überwachung geschickt. MyDashboards heißen diese bei Festo. Bei anderen Herstellern kann es auch das eigene Portal oder eine individuelle SCADA-Oberfläche sein, die über eine REST-Schnittstelle (Representational State Transfer) auf die interpretierten Daten der KI zugreift. Das ist aber nur ein Anwendungsbeispiel – viele weitere Anwendungsfälle sind bereits in Umsetzung und Planung.

Selbständig lernen. Die Entwicklung der Algorithmen geht immer weiter. Sie werden künftig selbständig Aktionen auslösen, wie Maschinen stoppen, fehlerhafte Teile ausspeisen oder deren Einstellungswerte optimieren. Der große Unterschied zu den schon lange bewährten, regelbasierten CMS-Systemen ist die Fähigkeit der KI, selbständig zu lernen. Die Software braucht keinen Programmierer, der aufwändige Regeln und Schwellwerte definiert. Sie erlernt zum Beispiel den normalen Produktionsfall mit seinen „gesunden“ Datenströmen und erkennt dann Abweichungen, also Anomalien, die gar keine Schwellwerte verletzen müssen.

Neue Möglichkeiten durch KI. Mittels ausgeklügelter KI werden Komplexitäten abbildbar, die bisher programmiertechnisch kaum zu bewältigen gewesen wären – beispielsweise bei heterogenen Fertigungsanlagen. Tanja Maaß, Geschäftsführerin Resolto Informatik: „Regelbasierte Fehlererkennung findet immer nur solche Fehler, die schon bekannt sind, aber keine unbekannten Anomalien. Zudem kann das Programmieren solcher Regeln sehr aufwändig werden und so zu zusätzlichen Fehlern – also False Positives bzw. False Negatives – führen. Eine Lücke, die die selbstlernende KI schließt.“ Resolto und Festo arbeiten daran.

Mensch und Maschine ergänzen sich. Maschinen im Betrieb sind hoch individuell – sogar der Betriebsort kann eine wesentliche Rolle bei Problemen spielen. Darum muss das technische Wissen über die jeweilige Maschine in die KI einfließen. Dabei sind menschliches Know-how und Erfahrung gefragt. >>

Dipl.-Ing. (FH) Rainer Ostermann
Geschäftsführer Festo Österreich

„KI werden ein wichtiger Baustein von Industrie 4.0 – schon heute erkennt man, wohin die Reise geht.“

Die Steuerung CPX-E-CEC liefert der KI Informationen zum Betrieb der Aktoren.

Auch vom Motorcontroller CMMT können wichtige Zustandsdaten kommen, an Hand deren die KI eine Anomalie feststellt.

Tanja Maaß: „Jede Anomalie hat ihren typischen Fingerabdruck. Die Algorithmen können immer weiter lernen und fragen ihr Wissen auch von den Technikern und Bedienern ab. Wir nennen das Human-In-The-Loop – ein entscheidender Faktor, damit sich das tiefe, unentbehrliche Fachwissen der Experten mit der Leistungsstärke der Algorithmen ergänzt."
Der Mensch sagt der Software ob es sich bei der gefundenen Anomalie tatsächlich um einen Fehler handelt, wie er heißt und was die folgende Handlungsempfehlung oder Aktion sein muss. Danach erkennt die Software selbst ob eine ähnliche Anomalie auftritt und handelt entsprechend.

KI als Teil der Maschine. Transparenz, Effizienz und weniger Ausfallzeiten, das sind nur einige der Ziele, die mit KI-Lösungen in der Industrie verfolgt werden. Dafür gilt es jedoch, noch einige Hürden zu nehmen. So konnte KI-Technologie bisher im operativen Feld nur bedingt überzeugen: Zu groß sind meist die Datenmengen, die über ohnehin überlastete Leitungen den Weg in die Cloud finden müssen. Zu lang sind die Latenzen, um schnelle Informationen von den Algorithmen zu erhalten.
Dipl.-Ing. (FH) Rainer Ostermann, Geschäftsführer Festo Österreich: „KI werden ein wichtiger Baustein von Industrie 4.0 – schon heute erkennt man, wohin die Reise geht. Es gibt aber auch noch einige Herausforderungen. Mit Resolto arbeiten wir gemeinsam an deren Lösung."
Es ist zum Beispiel entscheidend, die KI direkt an die Maschine zu bringen und die Interpretation an der Quelle aller Daten in Echtzeit durchführen zu lassen. Mit der Resolto-Technologie funktioniert dieser Ansatz auch ohne Lock-In bei großen Cloud-Anbietern und steht allen Betreibern und Herstellern von Produktionsanlagen zur Verfügung.

Edge-Komponente, die mit jeder Cloud kann. Es gibt heute große Bemühungen namhafter Cloud-Betreiber Edge-Technologie für die Industrie anzubieten. Teilweise wird die entsprechende Hard- oder Software sogar verschenkt. Der Haken ist aber, dass sich diese maschinennahen Komponenten immer nur mit den Cloud-Services des jeweiligen Anbieters verbinden lassen. So soll eine Kundenbindung entstehen, die sich aber später in steigenden Betriebskosten niederschlagen könnte. Resolto geht da andere Wege. Tanja Maaß: „Unsere Edge-Komponente kann sich mit jeder Cloud als IaaS (Infrastructure as a Service) verbinden und darum auf Wunsch sogar vollständig ‚onPremise' laufen. Da ist man voll flexibel."

Unabhängige Architektur der KI. Die Software von Resolto besteht aus zwei Komponenten, die eine nennt sich „Field", die andere „Brain". Field läuft immer maschinennah, zum Beispiel auf einer kleinen Steuerung. Es kommt ein vortrainiertes Modell zur Anwendung, das nur minimale Anforderungen an eine Hardware stellt und auch ohne jede Datenverbindung zur zentralen Komponente (Brain) zuverlässig Datenströme interpretiert. Hierfür können diverse Datenquellen mit Field verbunden werden, nicht nur aus der Steuerung oder Sensorik, sondern auch aus externen Quellen, wie ERP, Wetterdienst oder Raumklima-Messdaten. So lange die eingehenden Daten dem gelernten Normalmodell entsprechen, entsteht keinerlei Netzwerk-Traffic.

Field an Brain: Bitte kommen. Erkennt das Field eine Abweichung vom Normalzustand, die signifikant genug ist, meldet es diese Anomalie an Brain, das auf einem zentralen Server oder in der Cloud installiert ist. Brain kann nun mit einer entsprechenden Meldung einen menschlichen Experten hinzuziehen oder einer bekannten Handlungsempfehlung folgen, wie etwa dem Senden einer Ersatzteilbestellung an das ERP oder dem Planen eines Wartungsfensters. Eine schlanke Struktur, die für Tempo sorgt und den Netzwerk-Traffic in einem ausgesprochen überschaubaren Rahmen hält. Damit setzen Resolto und Festo spannende Impulse für industrielle KI-Lösungen von morgen.

Die Interessen der europäischen Industrie. Durch die Übernahme von Resolto in die Festo-Gruppe ist beiden Unternehmen ein wichtiger strategischer Schritt zur gemeinsamen Verbreitung von Künstlicher Intelligenz im produzierenden Mittelstand gelungen und auch zur Absicherung der Interessen der europäischen Industrie. Denn der Einsatz solcher Algorithmen wird für viele Maschinenhersteller und -betreiber künftig zwingend sein – unabhängige KI-Module und der Aufbau eigener Kompetenzen bieten dabei eine Alternative zu amerikanischen Cloud-Anbietern.

Sicherer Weg in die Cloud und exklusiver Zugang zur individuellen Digitalisierung: das IoT-Gateway CPX-IoT von Festo.

Maschinenbauer und Informatiker müssen für diese Technologien eng verzahnt arbeiten – es wäre daher möglicherweise bedenklich, die eigenen Rohdaten dauerhaft mit Cloud-Algorithmen der US-Anbieter zu „verheiraten". Darum werden bewusst Kooperationen mit Herstellern und Betreibern gesucht, um gemeinsame Geschäftsmodelle aufzusetzen.

KI als Zulieferteil. „Letztlich ist eine gute KI auch nur ein Zulieferteil für ein größeres Wertschöpfungsmodell", unterstreicht Tanja Maaß. Deshalb betrachtet man bei Resolto die Kunden als Partner und OEM, denen man hilft, neue Service-Modelle zu ermöglichen. Dazu kommt zum Beispiel die Steigerung der Qualität in der Produktion, also weniger Ausschuss, schnellere Zyklen, mehr Effizienz – Themen, mit denen sich Festo und Resolto intensiv beschäftigen. Hier wurden inzwischen hunderte Use Cases umgesetzt. Insbesondere für Mittelständler ist es attraktiv, fertige Lösungen bestehend aus schlanker Hardware, passend trainierten Algorithmen und Beratungskompetenz extern einzukaufen, anstatt komplette Fachabteilungen selbst aufzubauen. Resolto unterstützt die Anwender jedoch auch dabei, eigene Kompetenz zu entwickeln und sogar eigene Algorithmen in die Software zu integrieren.

IoT-Gateways als „Field"-Hardware. Festo und Resolto arbeiten gemeinsam daran, möglichst viele fertige Anwendungsmodelle für die KI zu erstellen. So können Kunden künftig zum Beispiel mit dem CPX-IoT-Gateway von Festo als „Field"-Hardware ihre Maschinen und Anlagen ohne Datenübertragung überwachen lassen und dabei aus zahlreichen Zielsetzungen wählen. Die IoT-Gateways verbinden sich bei Bedarf mit MyDashboards, in die ein Brain mit Zugriff auf viele vorkonfigurierte Modelle eingebettet ist. Dipl.-Ing. (FH) Rainer Ostermann: „Industrielle Automatisierungstechnik in Verbindung mit Künstlicher Intelligenz – das eröffnet eine unvorstellbare Anwendungsvielfalt. Maschinen zu überwachen und zu optimieren ist gegenwärtig Stand der Technik. Resolto arbeitet aber bereits intensiv an noch leistungsstärkeren Algorithmen, die sich auf der Feldebene selbst trainieren. Das ist beispielsweise für die kollaborative Robotik oder andere kreative Handling-Lösungen ausgesprochen interessant – ein großer Schritt in Richtung digitale Zukunft."

www.festo.at
www.resolto.com

Tanja Maaß
Geschäftsführerin Resolto Informatik

„Letztlich ist eine gute KI auch nur ein Zulieferteil für ein größeres Wertschöpfungsmodell".

EINE SENSIBILISIERUNG IST ENTSCHEIDEND

Der Druck auf Unternehmen wächst. Cyberangriffe, kleine Losgrößen und Digitalisierung fordern Flexibilität und Lösungen. Partnerschaften können dabei ein Weg sein, meint Mike Pichler, Account Manager & Cyber Security-Experte im Bereich Energy Industries Öl & Gas von ABB in Österreich.

Von Stephanie Englert

IoT 4 Industry & Business: ABB und Dassault Systèmes haben Anfang des Jahres bekannt gegeben, eine globale Software-Partnerschaft für digitale Industrien zu gründen. Was ist der Hintergrund?

Mike Pichler: ABB und Dassault Systèmes haben Anfang 2019 eine weitreichende globale Partnerschaft bekannt gegeben, um Kunden aus der digitalen Industrie ein einzigartiges Software-Lösungsportfolio anzubieten. Das Angebot reicht vom Produktlebenszyklus-Management bis hin zu Investitionssicherheit.
Die beiden Unternehmen werden ihren Kunden ein umfassendes Angebot an fortschrittlichen, offenen digitalen Lösungen offerieren: Diese verbessern die Wettbewerbsfähigkeit von Industrieunternehmen und erhöhen die Flexibilität, Geschwindigkeit und Produktivität der Produktlebenszyklen, der Fertigung und des Betriebs ihrer Produkte.

IoT: Inwiefern ist diese Zusammenarbeit für ABB und Unternehmen allgemein ein Schritt in Richtung Digitalisierung?

Pichler: In der hoch automatisierten Industrie von heute helfen digitale Fabrikationsmodellierung und flexible, robotergestützte Fertigungssysteme den Unternehmen dabei, mehr Design-Iterationen schneller und mit solideren Designs zu erstellen. Dies wiederum trägt dazu bei, die Verlagerung von der Massenproduktion hin zur individualisierten Fertigung in großer Stückzahl zu beschleunigen, bei der Waren in einer größeren Vielfalt und in kleineren Chargen sowie in kürzeren Produktlebenszyklen hergestellt werden.
Für viele Hersteller sind die Kosten für Ausfallzeiten in den letzten Jahren dramatisch gestiegen, da die Just-in-Time-Lieferung zur Norm geworden ist. Eine Stunde Ausfallzeit an einem modernen Produktionsstandort kann mehr als eine Million US-Dol-

lar kosten. Die Partnerschaft von ABB und Dassault Systèmes fokussiert sich im ersten Schritt auf folgende Themen:

• Fabrikautomatisierung und Robotik

Die Erfahrungen von ABB und Dassault Systèmes im Bereich digitaler Zwillinge zur durchgängigen Optimierung von Prozessen und Systemen in Kombination mit der Flexibilität der Roboterautomatisierung werden Unternehmen die Agilität geben, sich an immer dynamischere Märkte anzupassen.

• Intelligente Gebäude

Die digitale Partnerschaft zwischen Dassault Systèmes und ABB rund um digitale Zwillingssysteme wird einen nahtlosen Arbeitsablauf bei der Planung, dem Engineering und dem Betrieb von Gebäuden sowie vernetzte nachhaltige Transportlösungen ermöglichen.

• Prozessindustrie: Beispiel Bergbau

Ein digitales Modell der Untertageumgebung in Verbindung mit Minenplanungs- und -steuerungssystemen würde den Energieverbrauch und die Minenautomatisierung optimieren sowie Minenbetreibern ermöglichen, die Produktion in Echtzeit zu überwachen und zu optimieren, während sie virtuelle Simulationen zukünftiger Szenarien durchführen können.

IoT: Und mit welchen Vorteilen punktet ABB im Rahmen der Dassault-Partnerschaft gegenüber dem Mitbewerb?

Pichler: Diese wegweisende Partnerschaft ermöglicht unseren Kunden Innovations- und Wachstumssprünge. Mit unserem Angebot können sie ihre gesamte Wertschöpfungskette grundlegend verändern, um die großen Chancen der industriellen Digitalisierung zu nutzen. Zusammen bieten wir ein offenes, durchgängig digitales Portfolio – vom digitalen Zwilling bis hin zu Investitionssicherheit. Mit Dassault Systèmes erweitert ABB ihr starkes Partnernetzwerk für die industrielle Digitalisierung, dem unter anderem Microsoft, HPE und IBM angehören.

IoT: Inwiefern?

Pichler: Bisher nutzt ABB die ‚3DExperience'-Plattform von Dassault Systèmes für die Modellierung und Simulation ihrer Lösungen, bevor diese ausgeliefert werden. Mit der Partnerschaft sollen nun digitale Zwillinge entwickelt und Anwendern zur Verfügung gestellt werden. Damit können unsere Kunden ihre Arbeitsprozesse mit verbesserter Effizienz, Flexibilität und Nachhaltigkeit betreiben.

Die Unternehmen werden sich in einem stufenweisen Ansatz auf Lösungen für die Fabrikautomatisierung und Robotik, Prozessindustrieautomatisierung sowie Elektrifizierung für intelligente Gebäude konzentrieren.

IoT: Welche Digitalisierungsstrategie hat ABB im Allgemeinen?

Pichler: ABB verfügt mit ABB Ability bereits über ein führendes digitales Lösungsangebot für die Industrie. Es wurde 2017 auf den Markt gebracht und bietet mehr als 210 digitale Lösungen für die Planung, den Aufbau und den Betrieb von Industrieprozessen mit höherer Produktivität und Sicherheit zu niedrigeren Kosten.

ABB Ability vereint unser branchenübergreifendes digitales Know-how und erstreckt sich vom einzelnen Gerät über den Netzwerkrand bis hin zur Cloud. Die Geräte, Systeme, Lösungen, Services und ABB Ability-Plattform versetzen unsere Kunden in die Lage, schneller, besser und weiter zu gehen – gemeinsam mit uns.

IoT: Das Thema Security ist derzeit wieder verstärkt in den Fokus gerückt. Angriffe auf „vernetzte" Unternehmen nehmen zu. Wie begegnet ABB mit seinen Produkten am Markt diesem heiklen Thema bzw. was wird für die Sicherheit geboten?

Pichler: Die Cyber-Gefahren für industrielle Prozesse sind in den vergangenen Jahren immer mehr in den Fokus geraten. Dennoch schätzen viele Verantwortliche die allgemeine Gefahr höher als die für ihre eigene Organisation ein. In dieser Situation ist es wichtig, für geeignete Cyber-Security-Maßnahmen zu sensibilisieren und diese auszubauen. ABB hat eine schrittweise Vorgehensweise definiert, durch die die Kunden über mehrere Entwicklungsstufen zu bestmöglicher Sicherheit begleitet werden.

Wir schaffen Aufmerksamkeit für die Problematik, wir setzen Basismaßnahmen um, beispielsweise gehärtete Systeme, und wir leiten aus Cyber-Security-Assessments bedarfsgerechte Spezialmaßnahmen aus unserem detaillierten Serviceportfolio ab. Ergänzt werden diese Maßnahmen durch unsere Remote und Online Security Services aus dem Collaborative Operation Center. »

IoT: Spielen beim Thema Security Partnerschaften ebenfalls eine Rolle für ABB?
Pichler: Die umfassende Kompetenz von ABB als Partner in Sachen Informationssicherheit zeigt sich auch in einem jüngst erreichten Zertifizierungserfolg: In nur vier Monaten hat der Geschäftsbereich Grid Automation von ABB Deutschland das Zertifikat für die Einführung und Aufrechterhaltung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO 27001 erworben; Cyber Security ist einer der Aspekte der Zertifizierung.
Um das Zertifikat zu erreichen, musste dieser Geschäftsbereich einen dreistufigen Prozess mit Definition des Anwendungsbereichs, Schutzbedarfsanalyse und Risikobewertung durchlaufen. Damit ist der Bereich Grid Automation in der Lage, den Kunden zu belegen, dass seitens ABB die gleichen Vorgaben erfüllt werden, die sie als Betreiber einer kritischen Infrastruktur nach gesetzlichen Vorgaben selbst zwingend einhalten müssen. Damit macht es ABB für den Kunden bei dessen eigener Zertifizierung viel einfacher, nachzuweisen, dass sein ISMS der Norm entspricht – denn die normkonformen Schnittstellen zu den Lieferanten sind Teil des ISMS.
Des Weiteren engagieren sich ABB und Microsoft in einer engen strategischen Partnerschaft für die digitale Transformation in Kundensegmenten wie Robotik, Marine und Häfen, Elektrofahrzeuge und erneuerbare Energien. Mit der Wahl von Microsoft Azure als Cloud-Lösung für die integrierte Konnektivitätsplattform erhalten Kunden Zugang zu einer Cloud-Infrastruktur der Enterprise-Klasse, die mit milliardenschweren fortlaufenden Investitionen ständig weiterentwickelt wird.
Gemeinsam werden ABB und Microsoft die Entwicklung neuer digitaler Lösungen beschleunigen, die die Produktivität der Kunden durch erhöhte Verfügbarkeit, Geschwindigkeit und Ertragskraft verbessern werden.

IoT: Ein Beispiel: Im Bereich der Prozessindustrie ist das Thema Fernwartung eine Komponente, die einen Angriff auf die Systeme begünstigt. Sehen Sie diesen Schritt der Digitalisierung gleichzeitig auch als Risiko für Cyberangriffe?
Pichler: Wir empfehlen Security-Maßnahmen nach dem Defense-in-Depth-Konzept. Das bedeutet, dass bestimmte Bereiche durch koordinierte Sicherheitsmaßnahmen sowohl technisch als auch prozessbezogen ineinandergreifen und im Zusammenspiel eine starke Abwehr sicherstellen. Und weil Menschen Fehler machen, sind das Vier-Augen- Prinzip mit definierten Freigabeprozessen sowie Monitoring auf Protokollebene ein guter Schutz gegen Fehler aus dem Inneren.
Somit stellt das Biological Interface, also der Mensch vor dem System, immer mehr im Fokus. Social Engineering identifiziert in einer immer stärker vernetzten Welt die Schwachstellen eines Menschen und nutzt diese aus. Grundsätzlich sollten Hersteller, Betreiber und Integratoren im Dialog stehen. Die Kommunikationswelten von OT und IT müssten sich noch stärker verbinden, um Gefahren in der Zukunft noch stärken entgegen wirken zu können. Und – last not least – sollte Cyber Security bei Investitionen in digitale Infrastruktur einen angemessenen Anteil von 5 bis 10 % der Gesamtinvestition erhalten.

IoT: Wie kann man dem in Zukunft bestens begegnen?
Pichler: ABB als Partner, eröffnet unseren Kunden mit ABB Ability den Zugang zu attraktiven Möglichkeiten des industriellen Internets der Dinge und lässt dank unserer Dienstleistungen und Expertise mit ABB Ability auf Daten Taten folgen. So schließt sich der Kreis und es entsteht in der physischen Welt echter Mehrwert für den Kunden.
Während andere erst vor Kurzem den Wert der Digitaltechnologie entdeckt haben, sind wir seit Langem Experten für die Integration von digitalen Komponenten in die Steuerungssysteme unserer Kunden. Dazu zählen Sensoren, Software, digitale Netzwerke und neuerdings die Möglichkeiten des IIoT. Mit ABB Ability machen wir nun die geballte Macht unseres kollektiven Wissens sichtbar und zeigen auf, wie dieses Know-how für unsere Kunden integriert und angewendet werden kann. So arbeiten zum Beispiel unsere Wissenschaftler im ABB-Konzernforschungszentrum in Dättwil an weiteren Lösungen im Bereich Cyber Security, um dieser Thematik auch in Zukunft zielgerichtet begegnen zu können.

www.abb.at

Mike Pichler
Account Manager & Cyber Security-Experte, Energy Industries Öl & Gas von ABB in Österreich

„Während andere erst vor Kurzem den Wert der Digitaltechnologie entdeckt haben, sind wir seit Langem Experten für die Integration von digitalen Komponenten in die Steuerungssysteme unserer Kunden."

EIN NETZWERKKABEL FÜR DIE KOMPLETTE KOMMUNIKATION

Maschinenbauer und produzierende Industrie stehen vor einer gemeinsamen Herausforderung: Die steigende Komplexität der Produktion macht ihnen immer mehr zu schaffen. Um mit den einhergehenden Herausforderungen zurecht zu kommen, bedarf es einer neuen Generation an Automatisierungslösungen.

Die industrielle Produktion wandelt sich. Von reinen Massenprodukten geht der Trend hin zu individualisierten Produkten. Die heutigen Produktionslinien, die oft nur auf ein einziges Produkt ausgelegt sind, können diesen Anforderungen nur schwer nachkommen. Um kleine Losgrößen wirtschaftlich zu produzieren, braucht es kleinere und modulare Fertigungseinheiten, die jederzeit neu konfiguriert werden können – schnell und ohne großen Aufwand.

Innovationssprung ermöglichen. Die Basis um diese Herausforderungen zu bewältigen und eine flexible Produktion real werden zu lassen, ist ein herstellerübergreifender Netzwerkstandard. Nur mit einem einheitlichen echtzeitfähigen Netzwerk, das interoperabel ist und die Standards der IT mit den Standards der Industrie vereinheitlicht, ist der Sprung hin zu Innovationen für die Produktion von kleinen Losgrößen für Maschinenbauer erreichbar.

Nur eine Schnittstelle. Mit einem offenen Standard wird aus der Vielzahl an Protokollen ein einziges mit nur einer Schnittstelle. Diese Schnittstelle tauscht standardisierte Daten mit den Netzwerkteilnehmern aus. Führende Hersteller von Automatisierungs- und Informationstechnik setzen hierbei auf die herstellerunabhängige Kommunikationslösung OPC UA over TSN. Bisher musste der Maschinenbauer eine Vielzahl an Schnittstellen aufwändig definieren und alle Systeminformationen einarbeiten. Mit OPC UA over TSN entfällt dieser Aufwand. Die Kommunikationslösung überträgt im Gegensatz zu anderen Protokollen nicht nur einzelne Daten, sondern Informationen. Diese werden ohne weitere Erklärung von jedem Teilnehmer im Netzwerk verstanden. Die Fehleranfälligkeit sinkt und flexible Maschinenkonzepte lassen sich viel einfacher umsetzen.
Mit OPC UA over TSN wird für jedes Gerät ein eigenes Informationsmodell erstellt, indem alle relevanten Informationen gespeichert sind. Dadurch kann zum Beispiel jeder beliebige Antrieb – egal von welchem Hersteller und ohne großen Zeitaufwand – in jede beliebige Maschine eingebunden werden. So reduziert sich unter anderem der Aufwand beim Tausch eines defekten Geräts maßgeblich.

Schnell und Sub-Mikrosekunden genau. Eine Schnittstelle und eine einheitliche Sprache für unterschiedliche Geräte ist jedoch nur ein Teil der Gesamtlösung: Zykluszeiten und Bandbreiten spielen eine genauso wichtige Rolle. Zeitkritische Anwendungen, wie die Synchronisierung eines Roboters mit einem intelligenten Track-System, erfordern Zykluszeiten bis in den Mikrosekundenbereich. OPC UA over TSN hat 18x mehr Performance im Vergleich zu anderen Protokollen. Schnelle zentrale Antriebskonzepte lassen sich mit OPC UA over TSN genauso lösen wie intelligente dezentrale Architekturen. Der Durchsatz einer Maschine steigt und die Produktqualität wird verbessert.
Nur wenn OPC UA over TSN vollständig in Hard- und Software integriert ist, wird für den Maschinenbauer eine herstellerübergreifende Netzwerkinteroperabilität möglich. Dadurch wird er flexibler denn je. Zudem öffnet sich der produzierenden Industrie die Tür zu neuen modularen Maschinen für die Produktion bis hin zu Losgröße 1. Was vor Jahren noch als Zukunftsvision galt, ist heute mit OPC UA over TSN Realität – lediglich ein Netzwerkkabel reicht für die komplette Kommunikation im ganzen Netzwerk.

www.br-automation.com

Der Autor:

Konstantin Klein

... ist Product Manager Industrial IoT Network Solutions bei B&R.

KEIN WEG DRUM HERUM

Dr.-Ing. Rolf Sohrmann, BDM Industrial Analytics & IoT bei Weidmüller, sieht keinen Weg an Machine Learning und den sich daraus ergebenen Mehrwerten vorbei. Er empfiehlt aber die passenden Use Cases auszuwählen und Digitalisierung nicht zum Selbstzweck werden zu lassen.

Von Barbara Sawka

IoT 4 Industry & Business: Auf der Internetseite von Weidmüller steht: Digitalisierung ist kein Selbstzweck. Was meinen Sie damit?

Dr.-Ing. Rolf Sohrmann: Für uns steht immer der Mehrwert in der Anwendung im Vordergrund. Wir haben technisch heute deutlich mehr Möglichkeiten, als man wirtschaftlich sinnvoll umsetzen kann. Im Gespräch mit unseren Kunden fallen uns in zwei, drei Stunden sicher 25 Use Cases ein. Im Bereich Machine Learning können wir technisch 80 bis 90 Prozent realisieren. Aber ob das nachher wirtschaftlich Sinn macht, das ist eine ganz andere Frage. Das ist die Kernidee hinter dem Thema „Digitalisierung ist kein Selbstzweck".

Rittal – Das System.

Schneller – besser – überall.

zum Video

SCHALTSCHRÄNKE STROMVERTEILUNG KLIMATISIERUNG

FRIEDHELM LOH GROUP

IoT: Überall wird über Digitalisierung gesprochen. Möchte jetzt jeder digitalisieren – oder doch nicht?
Sohrmann: Bei uns ist es in der Tat so, dass die Kunden eher zu uns kommen, weil sie konkrete Aufgabenstellungen mit Machine Learning angehen wollen und nicht einfach nur wegen dem übergreifenden Thema Digitalisierung. Unsere Kunden sind schon so weit, dass sie den Begriff Digitalisierung für sich heruntergebrochen haben.
Nur bei Themen wie Condition Monitoring und Machine Learning muss manchmal noch auseinanderdividiert werden. Hier denken Anwender oftmals, dass man auf die Zustandsüberwachung der Maschine, wie wir sie heute in der Steuerung und Regelungstechnik haben, irgendwie einfach Machine Learning drüber packen kann. Dafür ist aber eine ganz andere Herangehensweise notwendig. Keine regelbasierte Grenzwertbetrachtung, sondern eine modellbasierte Herangehensweise, die man oft nicht mehr mit den vertrauten Regeln erfassen kann.

IoT: Smarte Fabrik, Industrie 4.0, IoT – jeder versteht etwas anderes darunter, die Begriffe werden vermischt, ohne die Unterscheidungskriterien zu kennen.
Sohrmann: Ja, das ist etwas, das auch wir in unseren Gesprächen feststellen. Wenn wir zehn Leute fragen, werden wir zehn verschiedene Antworten bekommen. Aus Weidmüller-Sicht geht es um die Operationalisierung von Industrie 4.0 und IoT. Konkret braucht es dafür Use Cases, um die Mehrwerte in der Fabrik umzusetzen. Und da können sie sowohl mit Hard- als auch Softwarelösungen ansetzen. Um wieder auf das Thema Machine Learning zu kommen. Für unsere Kunden ist es wichtig, einen Partner zu haben, der auf drei Beinen steht. Zum einen haben wir ein ganzes Hardware-Portfolio, um Daten zu akquirieren und sie vom Feld bis in die Cloud zu bringen. Zum anderen haben wir ein Team aus Experten, die das Thema Industrial Analytics operativ umsetzen können. Und dann sind wir ja auch selber Maschinenbetreiber mit einer großen eigenen Fertigung und der entsprechenden praktischen Erfahrung.

Dr.-Ing. Rolf Sohrmann
BDM Industrial Analytics & IoT bei Weidmüller

„Die Möglichkeiten, die wir heute beim Machine Learning oft erst noch auf dem Papier vor Augen haben, die werden kommen. Ja oder ja. Es gibt aus meiner Sicht keinen Weg drum herum."

IoT: Was muss eine smarte Fabrik können?
Sohrmann: Das ist ein breites Feld. Wenn wir von unserer Produktseite kommen, ist es sicherlich so, dass die Komponenten kommunikationsfähig sein müssen. Also dass Maschinen und Komponenten miteinander verbunden sind. Dass sich Standards in der Industrie entwickeln ist auch sehr wichtig. Vor allem, dass sie akzeptiert werden, dass Schnittstellen von den Herstellern zur Verfügung gestellt werden und man so alles miteinander vernetzen kann. Das ist ein wesentlicher Punkt von „smart". Wobei klar ist, dass man nicht nur aus Selbstzweck die Dinge miteinander vernetzt.

»

Oncite: Die All in One Edge Lösung für die digitale Fabrik

Rittal, German Edge Cloud, IoTOS und Bosch Connected Industry bieten mit Oncite gemeinsam die erste Komplettlösung zur Integration, Harmonisierung und Analyse industrieller Produktionsdaten an. Oncite ist das fabrikinterne Edge-Rechenzentrum für die Digitalisierung der Produktion.

- Sicherer Supply-Chain-übergreifender Datenaustausch
- Bietet volle Flexibilität bei voller Datensouveränität
- Kurze Latenzzeiten für KI-Anwendungen
- Daten werden zeit- und ortsnah erfasst, gespeichert, verarbeitet und ausgewertet

IT-INFRASTRUKTUR SOFTWARE & SERVICE

RITTAL

www.rittal.at/oncite

Industrial Analytics steht für applikationsgerechte KI/ML-Anwendungen, mit denen man Anomalien erkennen und klassifizieren und so Stillstandzeiten effektiv reduzieren kann.

IoT: Sie haben schon Industrial Analytics angesprochen. Was versteht Weidmüller darunter?
Sohrmann: Es geht darum den Zustand der Maschine zu analysieren und mit den Möglichkeiten des Machine Learnings Anomalien zu erkennen sowie Klassifizierungen, Predictive Maintenance, Predictive Quality-Themen oder die Realisierung neuer Geschäftsmodelle anzubieten. Weil die optimale Nutzung und Auswertung von Maschinen- und Prozessdaten der Schlüssel zu mehr Effizienz und Kostenkontrolle über den gesamten Lebenszyklus ist. Und das ist es, was wir von A bis Z mit unseren Kunden machen.
Vor zirka fünf Jahren sind wir mit Analytics-Projekten in der eigenen Fertigung gestartet. Vor drei Jahren haben wir eine eigene Business Unit für das Thema gegründet und gesehen, dass es eine Dienstleistung ist, die wir erfolgreich am Markt anbieten können.

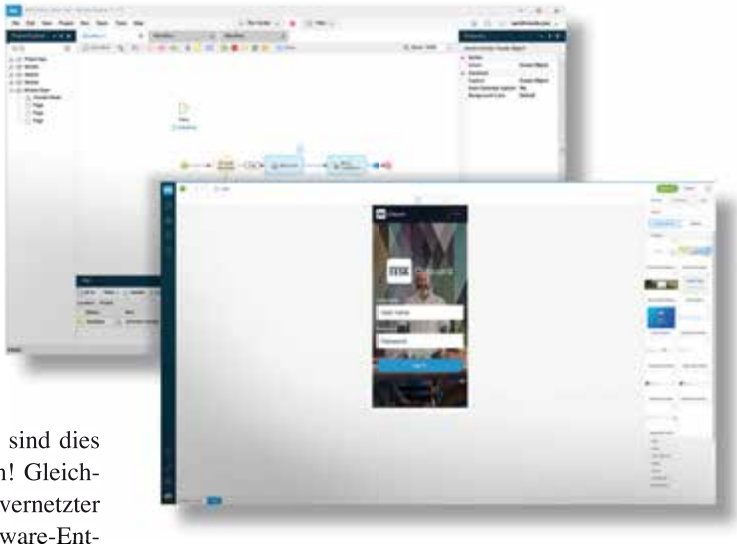
IoT: Gehen die Kunden in Sachen Digitalisierung mit, weil sie sich ökonomische Vorteile versprechen oder weil es einfach ein natürliches Fortschreiten der Arbeitswelt ist?
Sohrmann: Was ich bei den Maschinenbauern wahrnehme, ist die Steigerung von Output, das Erzielen von mehr Umsatz aufgrund von neuen Produktfeatures und weniger auf dem Einsparen von Ressourcen.
Das Denken geht hier ganz klar in Richtung Mehrwert zum Markt. Bei den Maschinenbetreibern geht es dagegen überwiegend um Effizienzsteigerung und Kostensenkung. Die Möglichkeiten, die wir heute beim Machine Learning oft erst noch auf dem Papier vor Augen haben, die werden kommen. Es gibt aus meiner Sicht keinen Weg drum herum. Und ich würde sagen, wer in den nächsten Jahren diese Features und Mehrwerte nicht mit anbietet, wird nicht mehr über Wachstum sprechen. Der wird einfach Marktanteile verlieren. Ich glaube, dass ist vielen Firmen schon klar.

IoT: Glauben Sie, dass Entwickler und Hersteller wie Weidmüller den Kunden Zeit geben sich in den nächsten Jahren mit dem Status quo zurechtzufinden. Oder werden immer neue Angebote geschaffen, ohne die Chance zu haben mit den vorhandenen zurechtzukommen?
Sohrmann: Es stimmt. Wir sind Getriebene und wir müssen treiben. Was wir aus dem Consumer-Bereich kennen, das ist in der Industrie bisher nur sehr partiell angekommen. Aber diese Durchdringung wird uns das nächste Jahrzehnt intensiv beschäftigen. Vielleicht nicht mit dieser ganzen Aggressivität des Consumer-Bereichs, aber annähernd vergleichbar. Es ist für die Industrie heute noch verhältnismäßig schwer herauszufinden, auf welchen Zug man aufspringen soll. In der Industrie gibt es hier ganz andere Zeitspannen als im Consumer-Bereich – Maschinen und Anlagen müssen über zehn bis 15 Jahre oder gar länger in den Fabriken funktionieren.
Mein Lieferant soll also auch in fünf Jahren noch da sein und diese Lösungen mit mir weiterentwickeln. Also wer ist da der richtige Partner. Das umzusetzen, glaube ich, ist zukünftig sehr schwer. Viele Startups kommen mit ganz tollen Ideen. Aber welche Bedeutung hat das in der Industrie? Können wir das integrieren? Ist das nachhaltig? Und da ist es dann wichtig, sich an offenen Standards zu orientieren. Also zu hinterfragen, auf welcher Umgebung arbeiten die Anbieter, mit welchem Selbstverständnis arbeiten sie, und mit welcher Wahrscheinlichkeit haben wir sie auch in drei Jahren noch zur Hand. Das ist natürlich schwer zu beurteilen, aber man sollte es zu mindestens hinterfragen. Das wäre ein Punkt, den ich einfach nur empfehlen kann.

www.weidmueller.at

DIY MIT LOW-CODE IM IoT: RESPEKT, WER'S SELBER MACHT.

Zwischen 20 und 50 Milliarden Geräte werden bis 2020 im IoT vernetzt sein. Diese Zahl schwankt zwar – abhängig vom jeweiligen Analystenhaus – sehr stark, zeigt aber eindrücklich, wie rapide dieser Markt wächst.



Umgerechnet auf die Gesamtweltbevölkerung sind dies zwischen 2,6 und 6,5 IoT-Geräte pro Person! Gleichzeitig stellt die schnell wachsende Anzahl vernetzter Devices enorme Anforderungen an die Software-Entwicklung, sodass der Bedarf mit klassischen Methoden kaum noch gedeckt werden kann. Low-Code kann hier für Entlastung sorgen.

Das Analystenhaus Gartner hat es in seinen jüngsten „Magic Quadrant für Low-Code-Anwendungsplattformen" klar gezeigt: Low-Code ist die Zukunft der App-Entwicklung. So werden bis 2024 über 60 Prozent der Anwendungen in Unternehmen auf Basis von Low-Code entwickelt. Dabei dreht es sich jedoch längst nicht nur um klassische Unternehmensanwendungen oder Mobil-Apps. Gerade für das Internet der Dinge bietet sich diese Art der Software-Entwicklung an.

Denn die Erstellung vernetzter, smarter IoT-Anwendungen ist für viele Firmen nach wie vor ein Buch mit sieben Siegeln. So zeichnen sich entsprechende Apps dadurch aus, dass sie nicht nur Daten verarbeiten müssen. Sie müssen darüber hinaus auch Endpunkte, Plattformen und Backend-Systeme integrieren und verwalten können. Dies stellt enorme Anforderungen an die Entwickler entsprechender Lösungen. Doch durch den immer stärker zunehmenden Fachkräftemangel gibt es in Unternehmen viel zu wenige Experten, die diese tatsächlich erfüllen können.

Der Autor:

Georg Maureder

... ist Manager Solution Architects bei Mendix.

Die richtige Plattform für den Start ins IoT-Universum. Daher gilt es für die Verantwortlichen auf Firmenseite, jetzt umzudenken. Software-Entwicklung für das Internet der Dinge ist nicht mehr länger ein Experten-, sondern vielmehr ein Plattform-Thema. So haben beispielsweise bereits heute die verschiedenen Cloud-Anbieter wie Amazon Web Services, Microsoft Azure oder IBM Bluemix, um nur ein paar zu nennen, zahlreiche IoT-Services in ihren Portfolios. Und wird es mal noch technischer, gibt es Unternehmen wie GE (Predix), PTC (Thingworx) oder Siemens (Mindsphere), die sich auf das Industrial Internet of Things (IIoT) spezialisiert haben.

Dabei profitiert gerade Mindsphere von den Vorteilen von Low-Code. Denn seit Siemens vor etwas über einem Jahr den Low-Code-Marktführer Mendix übernommen hat, wurde die Plattform zunehmend in das Siemens Software-Portfolio integriert und zur Basis zukünftiger Software-Entwicklung. So können die innerhalb der Mendix Low-Code-Plattform geschaffenen Apps direkt auf die Daten aus der IIoT-Plattform MindSphere zugreifen, diese sammeln und auswerten, sie darstellen und sogar mit Daten aus anderen Quellen verknüpfen. Selbst der Zugriff auf externe Datenbanken, beispielsweise in SAP, ist möglich. Dies erlaubt es Unternehmen auch, mit relativ geringem Aufwand Anwendungen zu erstellen, die die Integration von eigentlich veralteten Legacy-Programmen in den Siemens Digital Industries Software-Kosmos ermöglichen.

Nachdem die App-Entwicklung mittels Low-Code nicht nur deutlich einfacher, sondern auch deutlich schneller ist, bietet sie sich also besonders für den rapide wachsenden IoT-Markt an. Denn wenn innerhalb kurzer Zeit Unmengen an Anwendungen für die unterschiedlichsten Geräte geschaffen werden müssen, kommt es nicht auf möglichst elaborierten Code an – sondern auf schnellen Turnaround und eine hohe Fehlersicherheit. Und das kann Low-Code beides problemlos erfüllen.

www.mendix.com

Die Frage nach dem „Was ist Digitalisierung?“ steht der Frage „Kann ich sie mir leisten?“ gegenüber.

VERSTEHEN WIR DIGITALISIERUNG?

Mit der Studie Engineering 4.0 eröffnete Eplan spannende Einsichten in die Effizienz- und Handlungsfelder des Engineerings. Was Engineering 4.0 schließlich in der Praxis ausmacht und wo es derzeit eher Herausforderungen als Erfolge gibt, diskutierte Ing. Robert Erasmus, Leiter Professional Services AT/SEMEA, am neuen Eplan Österreich-Standort in Stift Ardagger mit Stephanie Englert.

IoT 4 Industry & Business: Im Juni stellte Eplan die Studie Engineering 4.0 vor. Weshalb wurde diese in Auftrag gegeben?

Ing. Robert Erasmus: Zu viele Unternehmer stellen sich immer noch die Frage, weshalb der Weg in die Digitalisierung für sie der richtige sei. Die Vorteile, die mit ihr und den Produkten am Markt, wie eben dem Eplan-Angebot, einhergehen – vor allem in Zeiten des ausgeprägten Facharbeitermangels – sind leider noch nicht überall vorgedrungen.

Das bedeute für uns ganz klar eines: Nämlich, dass die strategische Digitalisierung der Konstruktion und steuerungstechnischen Auslegung von Maschinen und Anlagen im Rahmen der Studie durch das European 4.0 Transformation Center am RWTH Aachen Campus in Deutschland untersucht wurde. Das Ergebnis ist der 38-seitige Forschungsbericht Engineering 4.0. Dieser fußt auf einer achtmonatigen Felduntersuchung bei deutschen Maschinenbauern im Serien- und Sondermaschinenbau, bei Ingenieurbüros bzw. Hardwareplanern sowie Geräteherstellern. Ich zitiere: „Die entwickelte Methodik zur Quantifizierung von Potenzialen und Maßnahmen im Engineering ermöglicht somit erstmals eine fundierte Reflexion gegenwärtiger Engineering-Workflows im Serien- und Sondermaschinenbau.“ Die zentrale Erkenntnis, die wir als Eplan daraus geschlossen haben, lautet: Wer sein Engineering teilautomatisiert, erzielt das betriebswirtschaftlich optimale Verhältnis von Aufwand und Nutzen.

IoT: Was wurde bei der Erhebung hinterfragt?

Erasmus: Es wurde mit einer so genannten Bewertungsmatrix mit fünf Effizienzstufen gearbeitet. Der Efficiency Level (eLevel)-Matrix mit weitreichenden Aussagen zum Methodik-Workflow ist einer Use Level-Matrix beigestellt. Sie beschreibt und bewertet die Nutzung von CAE-Software als Grundvoraussetzung für Engineering 4.0.

Ing. Robert Erasmus
Leiter Professional Services AT/SEMEA, Eplan Österreich

„Wer sein Engineering teilautomatisiert, erzielt das betriebswirtschaftlich optimale Verhältnis von Aufwand und Nutzen."

Die Studie lässt gleich zu Beginn auf den Forschungsgegenstand schließen. Untersucht wurden insgesamt zehn Prozessschritte, die das Engineering im Maschinenbau (Serien-/Sondermaschinenbau) prägen. Das erstellte Engineering-Workflow-Modell umfasst die typischen Arbeitsschritte eines Auftragsdurchlaufs.

IoT: Mit welchem Ergebnis?
Erasmus: Aus den erhobenen Daten leiteten die Wissenschafter ab, dass Unternehmen von eLevel zu eLevel um die 20 % effizienter werden könnten. Ein Beispiel: 10 % Aufwand für eine Standardisierung ermöglicht eine um 50 % schnellere Stromlaufplanerstellung. 25 % Zeitersparnis bei der Stromlaufplanerstellung bringt die geräteorientierte Arbeitsweise. Die Hälfte der Zeit bei der Stromlaufplanerstellung sparen Nutzer mit einer Schaltungsbibliothek für Produktfunktionen. 75 % geringerer Aufwand in der Prüfung der Schaltpläne wird erreicht durch Nutzung einer umfassenden Schaltungsbibliothek und 100 % Zeitersparnis bei der Erstellung aller Reports sind durch eine Standardisierung erreichbar.

IoT: Was bedeutet das in der Praxis? Sind „alle" Unternehmen zu Eplan-Lösungen gewechselt?
Erasmus: Das wäre sicherlich wünschenswert, aber so ist es noch lange nicht. Aufklärungsarbeit, das klassische Consulting, das auch in meinen Aufgabenbereich fällt, ist noch vielfach in der Praxis anzuwenden. Die Unternehmen wollen mit ihren offenen Fragen abgeholt werden. Somit spielt der so genannte Presales, die Beratung und Unterstützung vor dem Vertrieb, eine nicht zu unterschätzende Rolle. Dann erst folgt der klassische Vertrieb und im dritten Schritt die Implementierung.

IoT: Und mit dieser dann auch der Support.
Erasmus: Das ist richtig. Unsere Hotline und unser Support sind Teil der Professional Services bei Eplan. Da wir insgesamt in 56 Ländern weltweit vertreten sind sowie unsere Produkte in insgesamt 19 Sprachen (Tendenz steigend) zu erwerben sind, ist auch unsere Hotline internationalisiert und 24/7 erreichbar.

IoT: Sie sagen, Eplan ist weltweit vertreten. Industrie 4.0, Digitalisierung, IoT etc. sind ebenfalls globale Themen. Sind demnach auch alle Länder/Kontinente gleichauf mit den jeweiligen digitalen Entwicklungen?
Erasmus: Nein. Man merkt hierbei ganz deutlich, dass die Entwicklung in den unterschiedlichen Ländern auch unterschiedlich ausgeprägt ist. In manchen wird stärker versucht, die eher technologischen Entwicklungen voranzutreiben als »

in die Unternehmen die Digitalisierung zu bringen. Ein sehr wichtiges Thema in Zentraleuropa ist aktuell die durchgängige Wertschöpfungskette bei unseren Kunden. Die Industrie ist überall anders und das macht es aber auch wieder sehr spannend.

IoT: Sie sind nun seit sieben Jahren bei Eplan Österreich. Wie hat sich in dieser Zeit Ihr Aufgabengebiet in Zuge der parallellaufenden digitalen Entwicklungen am Markt selber entwickelt?
Erasmus: Bei Eplan Österreich sind wir derzeit 35 Mitarbeiter. Davon sind 1/3 zuständig für den klassischen Vertrieb und das Business Development. Ein weiteres Drittel bilden das klassische Marketing, die Auftragsabwicklung und Administration etc. und das letzte Drittel sind wir – mein Team und ich mit den Kompetenzfeldern Beratung, Training und Hotline. Und dieser ganze Bereich des Professional Services wird nicht nur meiner Ansicht nach sondern auch belegbar immer wichtiger.

IoT: Weshalb?
Erasmus: Als ich im November 2012 anfing, waren in meinem Team insgesamt zwei Berater. Seitdem sind wir kontinuierlich gewachsen. Inzwischen zähle ich sechs Mitarbeiter. Darüber hinaus haben wir zwei hauptberufliche Trainer hier im Haus in Stift Ardagger. Mit dem neuen Standort haben wir jetzt auch mehr Schulungsräume – und zwar drei. Zusätzlich zählen wir weitere Trainingsmöglichkeiten für Graz, Salzburg, Innsbruck und Wien.

IoT: Und mit welchem Produkt ist Eplan am erfolgreichsten?
Erasmus:: Einen wichtigen Anteil unseres Geschäftes machen wir mit Eplan Electric P8, unserem „Werkzeug für den Elektriker". Hier können Stromlaufpläne, Maschinenverkabelungen etc. durchgeführt werden. Weiters haben sich im Laufe der Zeit parallel zu unseren Kernprodukten weitere Entwicklungen ergeben. So bieten wir etwa Eplan Fluid für Drucklufttechniker, Hydrauliker etc. an. Auch Eplan Pro Panel für den Schaltschrank in 3D-Ansicht ist auf dem Markt erfolgreich angekommen. Weiters bieten wir Eplan Harness proD für das Kabelengineering in der gesamten Industrie an.
Der digitale Zwilling spielt auch immer stärker eine Rolle beim Arbeiten. Er dient der Vereinfachung der täglichen Arbeit und wird meiner Ansicht nach DAS pulsierende Herzstück der industriellen Produktion im 21. Jahrhundert werden. Es hat sich in den letzten Jahren auch immer mehr herauskristallisiert, dass es bei dieser Entwicklung am Markt um die so genannte Datendurchgängigkeit im Zuge der Digitalisierung geht. Die Frage: Wie kann ich digitalisieren? ist eine Frage, der man sich eben stellen muss.
Ein weiterer ganz wichtiger Bereich, den wir immer wieder ansprechen, ist das Thema des Methodenwechsels in der Art und Weise wie Engineering betrieben wird. Unsere Kunden sind gefordert nicht bei jedem Projekt wieder mit Copy&Paste aus bestehenden Projekten neue Anforderungen umzusetzen (das nennen wir engineer to order), sondern vielmehr aus Bibliotheken mit vorgedachten Teillösungen oder Baukästen über Konfigurationen neue Projekte zusammenzustellen (das nennen wir configure to order). Mittels Standardisierung werden hier Fehler vermieden und für Anwender werden die immer wiederkehrenden, langweiligen Arbeiten stark reduziert.

IoT: Ist Digitalisierung somit bei den Betrieben angekommen? Das ist doch die Frage, die immer wieder aufkommt.
Erasmus: Und die Antwort lautet „ja", aber nur im Verständnis und nicht in der Umsetzung. Hier stehen viele unserer Kunden noch ziemlich am Anfang und das ist das große Problem. Wenn ich eine Digitalisierungsstrategie durchführe kommt einher, dass ich mich um meine Stammdaten kümmern muss. Mir liegen dann zwei Möglichkeiten vor. Vereinfacht gesprochen kann ich ein Team ein halbes Jahr lang damit im stillen Kämmerlein beschäftigen, alle Stammdaten einmal zu digitalisieren. Ich kann auf der anderen Seite natürlich auch schleichend, je nach Projekt, den jeweiligen Leiter sich damit befassen lassen und die Stammdatenbearbeitung nach und nach abarbeiten.

Ing. Robert Erasmus
Leiter Professional Services AT/SEMEA, Eplan Österreich

„Digitalisierung ist bei Kunden inzwischen zwar angekommen, aber nur im Verständnis und nicht in der Umsetzung. Hier stehen viele noch ziemlich am Anfang und das ist das große Problem."

Dann liegt aber plötzlich der Fall vor, dass der Zeitrahmen eines Projektes zu Beginn um Tage länger dauern kann. Dann stellt sich selbstredend die Frage, weshalb man digitalisieren muss und trotzdem der Prozess im Endeffekt nun länger dauert als die Digitalisierung es prophezeit?

IoT: Vielen Unternehmen dauert auch der ROI zu lange.
Erasmus: Das stimmt. Es ist also auch eine Frage der Unternehmensgröße. Denn oft ist es der Fall, dass man sich fragt, wie man die Digitalisierung angeht, nicht ob ich sie vollziehe. Bei vielen fehlen schlichtweg auch die Ressourcen. Ein anderer entscheidender Faktor ist aus meiner Sicht, dass es eine klare Entscheidung des Managements geben muss, die Digitalisierung zu 100 % mitzutragen.

IoT: Die Unternehmenslandschaft in Österreich besteht hauptsächlich aus KMU. Haben wir also ein Digitalisierungsproblem?
Erasmus: Nein, dieses Problem sehe ich nicht. Denn unsere Kunden geben eigentlich schon eine Antwort. Wir verzeichnen den wirklichen 1-Mann/Frau-Betrieb genauso wie die großen Anlagen- und Maschinenbauer. Es geht einfach darum, sich frühzeitig um die erwähnte Stammdatenaufbereitung zu kümmern. Und wir als Unternehmen innerhalb der gesamten Loh-Gruppe bieten hier optimale Ansätze. Viele Projekte bei KMU zeigen schon, dass man sich im harten Wettbewerb durch Standardisierung und Optimierung Vorteile verschaffen kann.

IoT: Das bedeutet: „Wir" sind am Weg der Digitalisierung?
Erasmus: Ja und gleichzeitig wirken wir mit unseren Lösungen auch dem Fachkräftemangel dieser Zeit entgegen. Durch den Einsatz unserer Produkte und anhand des digitalen Zwillings wird der Arbeiter bereits im Vorfeld darüber informiert, was in der Praxis geht bzw. eben nicht geht.

IoT: Das bedeutet der digitale Zwilling eliminiert die Fachkräfte in manchen Bereichen?
Erasmus: Nein, denn die Situation ist ja eine andere. Das Problem bei den Fachkräften ist doch, dass wir zu wenig in das reine Engineering hineinbekommen. Einen wirklich guten Techniker, der/die weiß was er/sie kann und macht, der/die eine solide Ausbildung genossen hat und bereits über Praxiserfahrung verfügt, diese Gruppe bekommt man nur noch sehr wenig am Arbeitsmarkt, leider. Und diese wollen dann oft auch nicht ins Engineering, genauso wenig wie auf der anderen Seite die Akademiker das möchten.

IoT: Die goldene Mitte fehlt.
Erasmus: Das ist Tatsache. Daher ist die österreichische HTL-Ausbildung grundsätzlich ja eine gute Ausbildung, aber es fehlen einfach die Menschen, die diese Ausbildung absolvieren. Eplan hat aber auch hier ein Konzept, um bereits in der Ausbildung aktiv zu werden. Wir unterstützen die Ausbildung mit unserer Eplan Education-Software, die bereits einen Großteil der HTL in Österreich einsetzt.
Diese geht mittlerweile soweit, dass die Schüler eine Zertifizierung zum Eplan Certified Student in Kooperation mit der „Technischen Akademie in Esslingen" abschließen können. Darüber hinaus wird die Education-Software auch in Lehrwerkstätten zur Ausbildung von Facharbeitern sowie in manchen Werkmeisterkursen eingesetzt.

IoT: Das bedeutet?
Erasmus: Den Fachkräftemangel möchten wir schließen, indem wir versuchen die Fachkräfte, die ja noch da sind, auf eine andere Ebene hin zu bewegen. Man muss auch ganz klar festhalten, dass der Engineeringmitarbeiter im Büro heutzutage vielleicht beliebter ist als der Produktionsmitarbeiter bei der Maschine.

IoT: Kommen wir noch einmal zum Eplan-Produktangebot zurück. Hier steht ja auch seit einiger Zeit das Thema Cloud im Fokus. Gleichzeitig stellt sich dann auch wieder die Frage nach der Datensicherheit. Wie begegnen Sie dieser Herausforderung?
Erasmus: Wir entwickeln innerhalb der Friedhelm Loh-Gruppe unsere Cloud-Angebote und haben dabei die Bedürfnisse unserer Kunden stets im Blick. Das Eplan-Data-Portal ist dabei etwa weltweit etabliert als Hersteller-Bibliothek zum Download von Gerätedaten. Seit einiger Zeit haben wir Eplan eView, um das Spektrum der Lösungen, mit dem ECAD-Projekte gesichtet, geprüft und per Redlining-Workflow kommentiert werden können, erweitert. Unter dem Dach von Eplan ePulse wird der begonnene Kurs der agilen Cloud-Entwicklung nun im Diskurs mit Kunden und Partnern konsequent fortgesetzt. Insgesamt ist das Angebot der Loh-Gruppe sehr umfangreich und strategisch in eine Richtung klar ausgelegt: Digitalisierung.

IoT: Das bedeutet, Security ist auch ein wichtiges Thema bei Eplan?
Erasmus: Security ist ganz klar Thema, denn alle Produkte von uns werden am Server oder Notebook installiert. Somit spielen diese Bereiche eine wesentliche Rolle. Die Diskussionen beginnen meist dann, wenn Maschinenhersteller ihr Know-how nicht in die Cloud geben wollen, obwohl diese ja auch ausgedruckt vorliegen und somit der 100prozentige Sicherheitsaspekt ebenso in Frage gestellt werden kann. Ängste spielen hier eine große Rolle. Die muss man den Kunden dann nehmen.

www.eplan.at

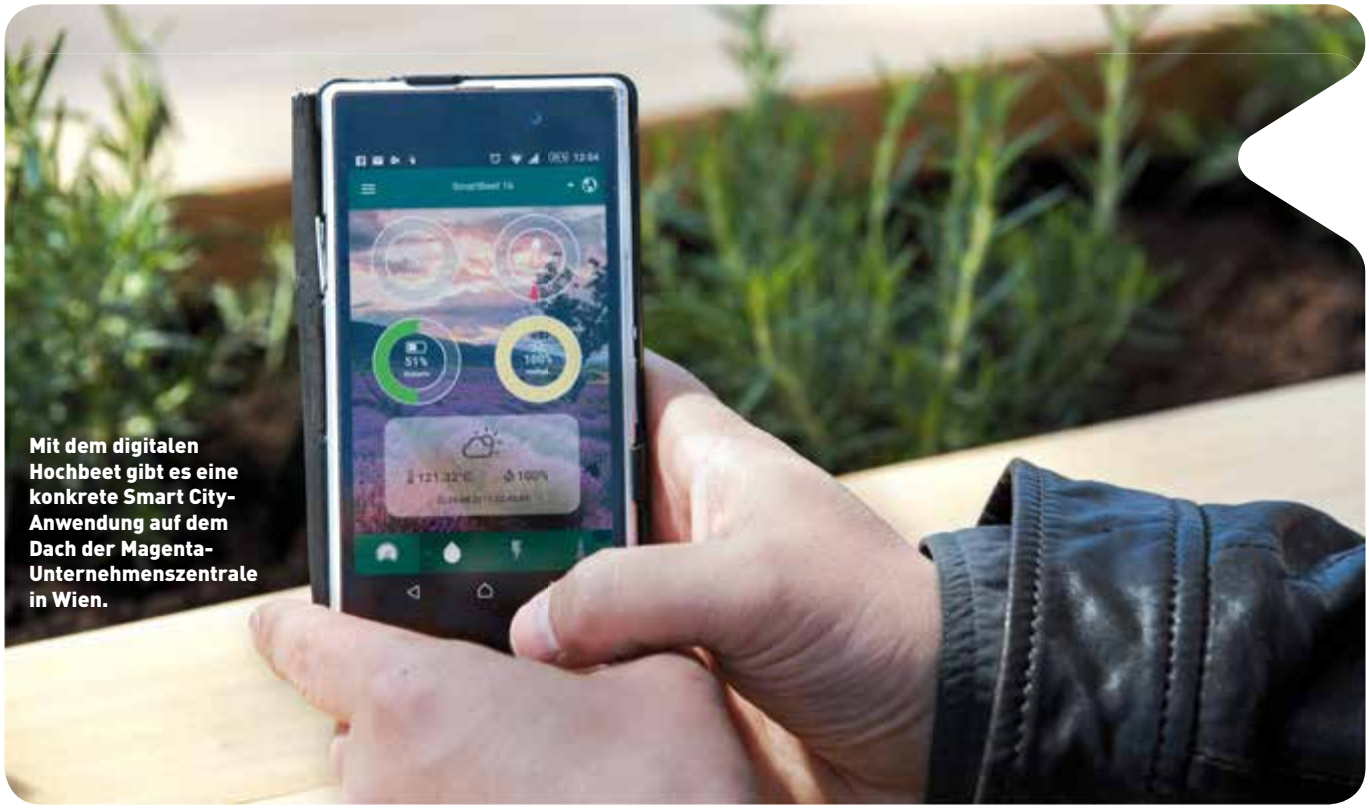
BESSER MITTENDRIN, STATT NUR DABEI

Digitale Hochbeete und smarte Mülltrennung sind nur einige der aktuellen IoT-Projekte von Magenta Telekom. Was es damit auf sich hat, erklärt Matthias Fiegl, Abteilungsleiter IoT & Big Data im Gespräch mit Barbara Sawka.

IoT 4 Industry & Business: Sehr viele Leute haben Angst vor der Digitalisierung und vielleicht auch Angst vor dem Thema Smart City. Sie sicherlich nicht?
Matthias Fiegl: Ich bin jemand, der nach vorne schaut. Wir alle sollten keine Angst davor haben, sondern eher mitgestalten, damit es auch richtig gemacht wird. Ich bin der Meinung, man sollte es im Sinne der Menschen gestalten und nicht im Sinne irgendwelcher Konzerne.

IoT: Da zählen wahrscheinlich auch die digitalen Hochbeete am Dach der Magenta-Zentrale in Wien dazu. Können Sie uns das Projekt erklären?
Fiegl: Im Rahmen des Projektes „Industry meets Makers" ging es 2017 darum, Startups für unterschiedliche Projekte zu gewinnen und gemeinsam mit dem Unternehmen daran zu arbeiten. Wir als Magenta haben eine IoT-Box entwickelt und dafür Anwendungsfälle gesucht. Das Ergebnis waren die digitalen Hochbeete mit Photovoltaikanlage, Wassertank, Motor und Steuerung über unsere IoT-Box. Das Ganze wurde noch mit Sensorik versehen, die Temperatur, Luftgüte, Feuchtigkeit in der Erde misst und selbstständig gießt.
Zusätzlich kann man alles mit einer App steuern. Dann ist jemand bei uns auf die Idee gekommen, unsere Dachterrasse, die nie genutzt wird, mit den smarten Hochbeeten auszustatten und eine „Gartlgruppe" unter den Mitarbeitern zu gründen. Innerhalb von fünf Minuten waren die 20 Hochbeete vergeben. Jedes Jahr wird die Betreuung neu ausgeschrieben und es melden sich immer wieder 200 Leute, die sie betreuen.

IoT: Diese IoT-Box ist ja ursprünglich nicht entwickelt worden, um Beete zu gießen.
Fiegl: Die Box war für uns ein Instrument, Unternehmen für die Digitalisierung zu begeistern. Man muss schon sagen, dass vor drei Jahren Digitalisierung in Österreich nicht sehr groß geschrieben wurde. Wir wollten das mit der IoT-Box mehr antreiben und Unternehmen dazu bringen, sich mit dem Thema



Mit dem digitalen Hochbeet gibt es eine konkrete Smart City-Anwendung auf dem Dach der Magenta-Unternehmenszentrale in Wien.

Digitalisierung auseinanderzusetzen und die ersten Gehversuche zu unternehmen. Deshalb haben wir die Box günstig angeboten, teilweise sogar verschenkt. Und wir haben Workshops mit dem Namen „IoT angreifbar machen" veranstaltet. Das ist sehr positiv angekommen und die Teilnehmer hatten danach einfach ein besseres Verständnis für Digitalisierung. Wir bieten diese Workshops übrigens immer noch an.

IoT: Haben Sie eine Veränderung im Bewusstsein der Menschen in den letzten drei Jahren bemerkt?
Fiegl: Ja absolut. Das Thema betrifft uns mittlerweile alle. Digitalisierung ist am Vormarsch. Egal in welcher Industrie ist jetzt mehr Interesse da. Die Leute sind auch gebildeter, da auch in den Medien sehr viel passiert ist. Man kann stundenlang in der Presse über IoT, 5G und Digitalisierung lesen.

IoT: Meist sind das nur Schlagworte. Man spricht von Digitalisierung und es ist vielen nicht klar, was tatsächlich der Stand der Dinge und Realität ist.
Fiegl: Stimmt. Vieles entspricht noch nicht der Realität. Aber wie gesagt, in letzter Zeit hat sich sehr viel getan. Also auch wenn mit diesen Begriffen um sich geworfen wird und nicht alle wissen, wovon die Rede ist, ist der gemeinsame Nenner für alle: Wer das beherrscht, hat einen Vorteil. Auch wenn man nicht genau weiß warum. Auch die Städte fangen vermehrt an ihre Anlagen zu vernetzen. Der nächste Schritt werden die digitalen Services für die Bürger sein. Die großen Städte Österreichs beginnen mit den ersten Pilotprojekten.

Matthias Fiegl
Abteilungsleiter IoT & Big Data bei Magenta Telekom.

„Wir sollten keine Angst vor der Digitalisierung haben, sondern eher mitgestalten."

IoT: Passend dazu haben Sie mit der Firma Saubermacher in Niederösterreich ein Projekt umgesetzt.
Fiegl: Das ist auch eine ganz interessante Sache. Wir standen 2017 ganz kurz vor dem Rollout unseres ersten IoT-Netzes. Das hat Saubermacher gehört und ist – noch bevor wir die ersten Masten online geschaltet haben – mit der Idee eines digitalen Mistkübels auf uns zugekommen und hat gesagt: es geht los. Dabei ging es um die Füllstandsmessung der Mülltonnen und die optimale Routenplanung für deren Abholung. Das war der erste Schritt. Dann kam im Bezirk Horn das Projekt mit den Glascontainern dazu. Die Städte haben keine Kontrolle darüber, wann die Glascontainer voll sind. Sie werden einfach zu fixen Zeiten angefahren und entleert. Im Bezirk Horn sind mittlerweile alle 600 Glascontainer vernetzt. Damit weiß Saubermacher ganz genau, wann ein Glascontainer voll ist und optimiert so auch die Routen. Anfang Oktober diesen Jahres haben wir ein neues Projekt vorgestellt. Dabei geht es um die richtige Mülltrennung. Es wurde ein Restmüllscanner entwickelt, der den Müll genau identifizieren kann und erkennt, welche Wertstoffe sich im Restmüll befinden.

IoT: Das wird dem Einzelnen aber nicht besonders wichtig sein, oder?
Fiegl: Doch. 85 % der Österreicher sehen in der Mülltrennung ihren wichtigsten Beitrag zum Umweltschutz. Deshalb gibt Saubermacher den Haushalten Feedback in Form von von Smileys direkt über die Magenta-Mobilfunknetz-App und sagen den Menschen: Du hast heute gut oder schlecht getrennt.

IoT: Sie haben vorhin ihr IoT-Netz angesprochen, mit dem das Saubermacher-Projekt ermöglicht wurde. Wie funktioniert das?
Fiegl: Wir haben 2017 die standardisierte Narrowband-IoT-Technologie, kurz NB-IoT, kommerziell ausgerollt. Den ersten Masten haben wir in Sankt Pölten aufgestellt, im September 2018 war das Netz österreichweit fertig. IoT-Anwendungsfälle müssen meistens nur ein paar Kilobyte übertragen und dafür ist das NB-IoT geeignet, weil es Daten energieeffizient und kostengünstig übertragen kann.

IoT: Neben technischen Bedenken neuen Technologien gegenüber, gibt es auch immer wieder gesundheitliche Ängste.
Fiegl: Sobald die Mobilfunker einen Technologiewechsel bewerben, wird von der Bevölkerung das Thema Gesundheit ins Treffen geführt. Dann gibt es immer den Versuch zu beweisen, dass Mobilfunk schlecht für die Gesundheit ist. Bis dato gibt es aber noch keine Studie, die das bewiesen hat. Es gibt sehr viele Studien, die beweisen, dass es keine Auswirkungen gibt, zum Beispiel auch von der WHO. Jeder will sein Smartphone nutzen. Wie soll das ohne Mobilfunk funktionieren?
Die Bevölkerung hat sehr oft Angst vor neuen Technologien. Und wie ich schon eingangs erwähnt habe, glaube ich, dass es klüger ist mitzugestalten als abzuwehren. Dann kann man es so verändern, dass es für einen selbst Sinn macht.

www.magenta.at

Schnelle Verfügbarkeit, Skalierbarkeit und die Kosten sprechen für viele Unternehmen für den Weg in eine Cloud.

MITTEN DRIN IN DER CLOUD

Laut Matthias Straub, Senior Director Consulting bei NTT Ltd. in Deutschland, überwiegen die positiven Aspekte für Unternehmen, ihre Daten der Cloud anzuvertrauen. Allerdings rät er ihnen, sich eine Strategie zurecht zu legen und sich die Anbieter genau anzuschauen. Hier gilt: Je transparenter, desto besser.

IoT 4 Industry & Business: Der Begriff Cloud war vor einigen Jahren in aller Munde, dann ist es ein bisschen ruhiger geworden. Wo stehen wir jetzt?

Matthias Straub: In der Tat bin ich gespannt, ob wir in 50 Jahren auch noch von der Cloud sprechen. Aktuell ist es so, dass Cloud Computing weitestgehend etabliert ist – ein Großteil der Unternehmen setzt mittlerweile auf die Cloud. Und auch die Sicherheitsrisiken hat man mittlerweile im Griff – die Bedenken mit Blick auf die Gesetzeskonformität oder den Schutz geschäftskritischer Informationen und die damit verbundene Zurückhaltung in den Unternehmen schwinden. Ich würde sagen, die Cloud ist „erwachsen geworden".

IoT: Was hat diesen Wandel hervorgerufen?

Straub: Cloud Computing ist der Treiber der Digitalen Transformation, ob es um komfortable Dateninfrastruktur- oder Storage-Lösungen, Data Warehouse-Anwendungen oder Machine Learning Tools geht. Für Unternehmen sind Amazon, Google und allen voran Microsoft mit Office 365 und Azure die wichtigsten Anbieter und sie waren es auch, die mit ihren umfangreichen Service-Portfolios und günstigen Preisen einen großen Beitrag dazu geleistet haben, dass heute fast jedes Unternehmen und jede Behörde in der Cloud ist.

IoT: Welche Vorteile sehen sie bei Cloud-Lösungen für die Unternehmen?

Straub: Ein elementarer Vorteil sind sicherlich die Kosten. Ausgaben für Hardware sowie die Verwaltung, Wartung oder Updates fallen bei Cloud-Services weg und bei den meisten Cloud-Modellen zahlt man auch nur die IT-Ressourcen und Software, die das Unternehmen benötigt bzw. tatsächlich nutzt. Aber auch die schnelle Verfügbarkeit ist ein Argument, denn Cloud-Anwendungen sind im Vergleich zu lokalen Anwendungen sofort einsatzbereit. Hinzu kommt die einfache Skalierbarkeit. IT-Leistungen aus der Cloud sind dynamisch und innerhalb kurzer Zeit an neue Unternehmensanforderungen anpassbar.

IoT: Durch die Digitalisierung in der Produktion werden Daten häufig vor Ort benötigt, Stichwort Edge Computing. Hier macht die Cloud ja gar keinen Sinn, oder?

Straub: Es stimmt, in der Produktion müssen manche Daten binnen kürzester Zeit lokal verarbeitet werden – eine Übertragung zu zentralen Cloud-Servern kostet zu viel Zeit und stellt ein regelrechtes Sicherheitsrisiko dar. Alle anderen Daten aber, die nicht in Echtzeit prozessiert werden müssen, können natürlich in die Cloud.

IoT: Bislang sprechen wir nur von den Vorteilen, gibt es auch reale Bedenken?
Straub: Es sind vor allem Sicherheitsbedenken, die Unternehmen davon abhalten, in die Cloud zu gehen. Das ist natürlich auch völlig richtig – als IT-Security-Anbieter empfehlen wir jedem Unternehmen einen solchen risikoorientierten Ansatz zu verfolgen, um so das Risiko eines unberechtigten Zugriffs auf besonders sensible und geschäftskritische Daten, eines Datenverlusts oder einer Datenschutzverletzung im Fall einer Auslagerung zu kennen und bei der Wahl des richtigen Cloud-Anbieters zu berücksichtigen. Tendenziell ist es aber so, dass Cloud-Provider sehr gute Sicherheitsprozesse und -technologien im Einsatz haben und damit oft einen besseren Schutz der Daten garantieren, als dies das Unternehmen selbst kann.

IoT: Als Privatmensch nützen wir oft sehr unreflektiert Cloud-Dienste. Überträgt sich dieses private Verhalten auch auf das Verhalten im Unternehmen?
Straub: Das tut es bestimmt. Ich glaube aber, dass wir dank der starken Sensibilisierung für das Thema Datensicherheit und Datenschutz durch die Medien sowie der Security-Awareness-Trainings in den Firmen heute verantwortungsvoller mit unseren persönlichen Daten umgehen, was sich wiederum auch positiv auf das Verhalten im Unternehmen auswirkt.
Die Kritik richtet sich vielmehr an die Unternehmen, die oft keine richtige Strategie für den Umgang mit den Daten in der Cloud haben. Es gilt zu entscheiden, welche Daten in die Cloud dürfen, wie man damit umgeht und wie man sie schützt und es müssen die (IT)-Governance-Prozesse überarbeitet und an die neue Cloud-Strategie angepasst werden.

IoT: Welche Kriterien sprechen für eine gute Cloud?
Straub: Cloud-Dienste werden nach verschiedenen Qualitätskriterien bewertet, unter anderem Funktionalitäten wie Sicherheit, Verfügbarkeit oder Skalierbarkeit, die Gesetzeskonformität, die vertraglichen Gestaltung, der geografische Standort oder der Integrationsaufwand. Grundsätzlich würde ich sagen, je transparenter über Sicherheit, Datenschutz, Datenzugriff, Cloud-Architektur und Service Level Agreements informiert wird, desto besser. Am Ende ist die Zusammenarbeit aber eine Frage von Vertrauen – wie bei jeder Partnerschaft.

IoT: Hackerangriffe stehen mittlerweile auf der Tagesordnung. Sind die großen Cloud-Anbieter nicht besonders gefährdet? Es lagern hier besonders viele Daten sehr vieler verschiedener Unternehmen.
Straub: Vor einigen Wochen haben die Medien berichtet, dass eine amerikanische Bank Kundendaten bei einem Cloud-Anbieter verloren hat. Das Risiko ist also nicht von der Hand zu weisen, bei den großen Marktführern aber als gering einzustufen, da diese schon allein aufgrund des Business-Modells über eine hohe Security-Expertise verfügen müssen. Und auch die Statistiken belegen, dass die Daten bei den großen Cloud-Anbietern am besten vor Cyberangriffen geschützt sind.

IoT: Sie haben eingangs erwähnt, dass Sie nicht sicher sind, ob wir in 50 Jahren noch über die Cloud sprechen werden.
Straub: Die Cloud selbst wird sicher nicht verschwinden. Sie wird eher so alltäglich und so stark in den normalen Geschäftsbetrieb integriert sein, dass wir über die Technologie selbst nicht mehr reden werden, sondern nur noch über die Dienste und Lösungen.

IoT: Generell hört man, dass Unternehmen gewillt sind, sich mit Digitalisierung zu beschäftigen. In der Tat tun es immer noch nicht so viele. Ist das auch Ihre Wahrnehmung?
Straub: Das würde ich so nicht sagen. Der Großteil der Unternehmen ist im Zeitalter der Digitalisierung angekommen. Viele Entwicklungen passieren aber im Hintergrund und sind für Außenstehende nicht immer sichtbar. Im internationalen Vergleich hinken wir vielleicht etwas hinterher, aber wir sind auf dem richtigen Weg von der Digitalisierung hin zu einer Society 5.0 – einer vollständig vernetzten Gesellschaft. (bs)

https://hello.global.ntt

Matthias Straub
Senior Director Consulting bei NTT Ltd. in Deutschland

„Unternehmen haben oft keine richtige Strategie für den Umgang mit den Daten in der Cloud."

Ein großer IoT-Hemmschuh ist in Deutschland der Fokus auf die wirtschaftliche Berechenbarkeit der IoT-Projekte.

GUTE KONJUNKTUR ALS IoT-STOPPER

Welchen Nutzen IoT bringen kann, ist noch nicht für jedes Unternehmen ersichtlich. Dass es im deutschsprachigen Raum daher Aufholbedarf gibt, weiß auch Jan Rodig, Berater für Digitale Transformation, Innovationen & IoT.

IoT 4 Industry & Business: Was befeuert Unternehmen sich mit dem Thema IoT zu beschäftigen?
Jan Rodig: Ich sehe hier vier Muster. Zum Ersten beschäftigen sich Unternehmen mit IoT, weil ihre Kunden sie darauf ansprechen, etwa wenn es um Predicitve Maintenance geht. Das zweite Muster ist: Der Komponentenhersteller geht direkt zum Kunden des Maschinenbauers und bietet z.B. After-Sales-Services an – das macht dann den Maschinenbauern Angst und sie beginnen sich selbst damit zu beschäftigen.
Beim dritten Muster tritt ein komplett neuer Anbieter mit neuen Technologien auf. Das wollen die Maschinenbauer natürlich nicht. Und das vierte Muster ist der allgemeine Wettbewerbsdruck.

IoT: Viele Anlagenbauer oder Komponentenhersteller bieten oft Insellösungen an – also z.B. ein Sensor, der vernetzt ist. Selten wird IoT in seiner Gesamtheit angeboten. Richtig?
Rodig: In der Tat gibt sehr viele Angebote, die unter IoT laufen und die man im engeren Sinne wahrscheinlich nicht unter IoT oder nicht unter einem holistischen Service verstehen könnte. Das liegt sicherlich auch daran, dass erst einmal viel experimentiert wird und häufig noch keine gesamtheitliche Strategie da ist. Die kostet aber natürlich auch Geld und dauert auch ein bisschen länger. Deswegen wird bei den meisten Unternehmen erst mal mit kleinen Lösungen gestartet und experimentiert.
Meines Erachtens ist es am erfolgversprechendsten, wenn man neben diesem Experimentieren auch eine ambitionierte Vision verfolgt und die Organisation und Strategie konsequent darauf-hin ausrichtet.

IoT: Wie sehen die großen Hemmschuhe aus?
Rodig: Beim Launch neuer Produkte und Geschäftsmodelle bremst ganz klar die Tatsache, dass sich das nicht so einfach rechnen lässt. Gerade im deutschsprachigen Raum sind ja alle sehr stark auf Business-Cases und Wirtschaftlichkeitsberechnungen aus. Und fast alles was sich nicht in zwei, drei Jahren rechnet, wird nicht gemacht.
Es ist einfach unglaublich schwer, die Unternehmen dazu zu bekommen, an solchen unsicheren Themen zu arbeiten, wenn die Konjunktur ihnen sowieso die Auftragsbücher füllt. Projekte, denen man sich experimentell nähern muss, kann man nicht

Neben seiner Tätigkeit als Berater für Digitale Transformation, Innovation und IoT engagiert sich Jan Rodig in der AG „Digitale Geschäftsmodelle" der Plattform Industrie 4.0.

starten, wenn man am Anfang schon wissen will, ob sich das Ding nach zwei Jahren amortisiert. Das ist tatsächlich die größte Bremse. Besser ist es, einen bewussten Raum zum systematischen Testen von Hypothesen zu schaffen, in dem auch mal etwas gesponnen und experimentiert werden darf.

IoT: Wie werden sich die Geschäftsmodelle durch IoT verändern?
Rodig: Die drei großen Trends die man sieht, sind zum einen die Plattform-Ansätze. Das können Technologie-Plattformen sein oder Geschäftsmodelle, bei denen es darum geht verschiedene Parteien zu verknüpfen, was sich dann beispielsweise über App-Stores monetarisieren lässt. Das zweite Modell ist das As-a-Service-Modell, das gerade in Branchen, wo die Kapitalkosten sehr hoch sind, zur Anwendung kommt. Das dritte Modell toppt das As-a-Service-Modell noch einmal mit reinen performance-orientierten Betriebslösungen, bei denen etwa im Anlagenbau bestimmte Verfügbarkeiten vom Hersteller garantiert werden – fällt der Wert dann darunter, entfällt die Vergütung. Das steckt aber noch in den Kinderschuhen. Über alles andere wird sehr viel geredet, aber passiert ist noch nicht so viel.

IoT: Sie haben den IoT-Dienstleisters tresmo als CEO von der Gründung bis auf 40 Mitarbeiter aufgebaut. Wie sah dort die klassische Aufgabenstellung der Kunden aus?
Rodig: Da lassen sich drei Fallgruppen unterscheiden, die sich chronologisch an einem typischen Projektablauf orientieren: In Phase eins geht es darum, strategisch die richtige Richtung zu finden, die Chancen und Risiken zu verstehen, eine erste Vision zu formulieren und Budgets und Mitarbeiter für IoT-Projekte bereitzustellen. Das ist klassische Strategieberatung. Phase zwei ist dann schon konkreter – es geht um spezifische Use Cases und die sich daraus ableitenden digitalen Services und smarten Produkte sowie die damit möglichen Geschäftsmodelle. Hier unterstützt man vor allem methodisch mit modernen Innovations- und Validierungsansätzen und berät auf Basis der Erfahrung aus vielen anderen Projekten. Anschließend kommt die dritte Phase, dann geht es um die technische Umsetzung, bei der auch Fragen nach der richtigen IoT-Plattform und IT-Architektur beantwortet werden müssen. Leider passiert es häufig, dass die Phasen eins und zwei übersprungen oder nicht gründlich genug angegangen werden. Da kommen dann Ideen raus, die für viel Geld technisch umgesetzt werden und dann stellt man fest, dass die Kunden das gar nicht brauchen und nicht bereit sind dafür zu zahlen.

IoT: Wenn man jetzt in eine Glaskugel schauen würde, wie weit wird uns IoT „überrollen" bzw. „helfen"?
Rodig: Ich glaube, dass Überrollen leider tatsächlich das richtige Wort ist. Am Beispiel der Automobilindustrie ahnt man schon, was große Technologieumbrüche in sehr wettbewerbsintensiven und volkswirtschaftlich bedeutenden Branchen anrichten können. Und was auch ausländische Wettbewerber mit ganz neuen Ideen und Ansätzen bewirken können. Ich befürchte einfach momentan, so wie ich mir die Geschwindigkeit gerade im deutschsprachigen Raum in Bezug auf die IoT-Umsetzung im Maschinen- und Anlagenbau oder der Elektrotechnik anschaue, dass wir da sehr langsam unterwegs sind.
Ehrlich gesagt ist insbesondere China eine sehr ernstzunehmende Gefahr. Dort trifft Produktionskompetenz mit starken Investitionen in die Produktvernetzung und eine konsequente Förderung von Künstlicher Intelligenz zusammen. Aus meiner Sicht müsste in Deutschland auf allen Ebenen viel mehr passieren und man bräuchte deutlich mehr Mut um neue Dinge auszuprobieren. (bs)

www.tresmo.de

Schneider Electric ist von Partnerschaften überzeugt und ermöglicht mit der Plattform Exchange den offenen Austausch untereinander.

PARTNERSCHAFTEN

Starke Partnernetzwerke sind für Jürgen Siefert, VP Industrial Automation DACH bei Schneider Electric, ebenso nötig um erfolgreich zu sein, wie Antworten auf die Frage: Wie mache ich aus „Big Data" „Smart Data". Im Gespräch erzählt er auch, wie lange sich Schneider schon mit Industrie 4.0 beschäftigt.

IoT 4 Industry & Business: Digitalisierung ist das Schlagwort des Jahres schlechthin. Dahinter verbirgt sich dennoch ein langer Prozess. Wie geht es Schneider Electric damit?
Jürgen Siefert: Digitalisierung ist bei uns keine Revolution, sondern eine Evolution. Wir haben schon 1997 als einer der ersten Player am Markt Internet- und Webtechnologie zur Verkettung von Maschinen und Datenanalysen realisiert und damit den Trend zum IIoT mit „losgetreten". Da hat noch keiner von Industrie 4.0 gesprochen. Vor zehn Jahren haben wir mit EcoStruxure als Plattform begonnen und sie sukzessive durch eigene Entwicklungen und strategische Zukäufe mit Leben gefüllt. Ich denke, mit dem Begriff Industrie 4.0 haben viele Kinder den gleichen Namen bekommen. Was sich speziell in den letzten zwei Jahren entwickelt hat, ist die Dynamik. Was lange nur ein Hype war, kommt jetzt langsam in der Realität an. Die Endkunden fragen vermehrt nach Lösungen.

IoT: Es gibt viele Insellösungen. Jedes Gerät ist mittlerweile kommunikationsfähig. Wie weit ist die Digitalisierung wirklich angekommen?
Siefert: Das ist sehr stark herstellergetrieben. Wenn ich Sensoren produziere, dann will ich auch, dass sie bei diesem neuen Trend mitmachen.
Unser Ansatz ist ein anderer. Wir sind zutiefst überzeugt, dass OEMs und die Endkunden selbst immer weniger Kapazitäten haben, um diese Dinge selbst zu selektieren und einzusetzen. Das ist eine riesige Herausforderung. Deshalb versuchen wir zwei Dinge konsequent zu machen: Unseren EcoStruxure-Baukasten so gut wie möglich zu füllen, aber auch gleichzeitig mit standardisierten Schnittstellen Sicherheit zu bieten, um alle möglichen Fremdprodukte anbinden zu können. Wir bieten Easy-to-use-Lösungen für Industrie 4.0. Das ist ein starkes Differenzierungsmerkmal.

IoT: Schneider Electric legt sehr viel Wert auf die Partnerschaften. Dazu haben Sie sogar die offene Plattform Exchange ins Leben gerufen. Was hat es damit auf sich?
Siefert: Ich bin zutiefst davon überzeugt, dass in Zukunft nur die Unternehmen erfolgreich sein werden, die das gesamte Netzwerk nutzen. Nehmen Sie zum Beispiel einen OEM, der in viele Länder exportiert. Die Empfehlung, für die Implementierung einen Schneider-Mitarbeiter hinzuzuziehen, wäre nicht zielführend. Lokale Partnernetzwerke mit regionaler Nähe zu dem Werk sind aus meiner Sicht unersetzbar. Wenn man diesen Weg geht, kann man das durch ein starkes Partnernetzwerk viel besser, als wenn man versucht, alles selber zu machen.

IoT: Im Mittelpunkt des Innovation Summit hier in Barcelona steht EcoStruxure. Für alle, die es noch nicht kennen: Was ist das?
Siefert: Die offene, skalierbare, IoT-fähige Lösungsarchitektur besteht aus den drei Kernbereichen: vernetzte Produkte, Edge Control sowie Apps, Analysen und Services. Die ganzheitliche Architektur ermöglicht so die durchgängige Konnektivität auf allen Ebenen moderner Fertigungsbetriebe. Die unterste Ebene sind die vernetzten Komponenten, also intelligente Sensoren, Geräte an der Mensch-Maschine-Schnittstelle. Die nächste Ebene darüber ist die Edge Control. Die deckt die ganze Steuerungstechnologie ab. Der Zukauf von Invensys und die umgekehrte Übernahme von Aveva haben uns in der dritten Ebene bei den Apps und Analysen gestärkt.

Jürgen Siefert
VP Industrial Automation DACH

„Wenn Sie am Ende des Tages die Daten nicht vorverarbeiten, dann reicht irgendwann kein Server der Welt mehr, um die Daten zu speichern. Und es macht auch keinen Sinn."

IoT: Und was ist die Green Box?
Siefert: Die setzt genau dort an, wo man Maschinen und Anlagen Industrie-4.0-fähig macht. Wir haben vor zwei Jahren begonnen erste Lösungen umzusetzen. Im Grunde ist die Green Box Connect einfach ein VPN Tunnel, um einen sicheren Zugang von außen zu haben. Das ist ein immens wichtiges Thema. Die zweite Stufe ist die Green Box Eco. Hier hat der Anwender zum einen die Möglichkeit, die Verbindung in die Cloud zu schaffen, um einen Machine Advisor für den OEM oder den Endkunden bereitzustellen, ihn aber auch on premise zu haben. Die dritte Stufe ist die Green Box Pro. Hiermit können Werksleiter ihre Produktion komplett visualisieren. Unsere Lösung ist absolut skalierbar. Man kann dort einsteigen, wo der Bedarf liegt und sich Schritt für Schritt weiterarbeiten.

IoT: Ein Produktionsbetrieb sammelt sehr viele Daten. Manchmal vielleicht auch zu viele. Was muss man tatsächlich wissen?
Siefert: Wir haben hier in den letzten Jahren viel gelernt. Wir haben gemeinsam mit den Endkunden und den Maschinenbauern Lösungen entwickelt und realisiert. Mit unseren Analytics-Angeboten können wir die Daten aus den Maschinen holen und sie vorverarbeiten. Das ist das Stichwort: Wie mache ich aus „Big Data" „Smart Data". Wenn sie am Ende des Tages die Daten nicht vorverarbeiten, dann reicht irgendwann kein Server der Welt mehr, um die Daten zu speichern. Und es macht auch keinen Sinn. Wenn man die Anomalien mit einem Datensatz pro Stunde erkannt hat, kann man in der nächsten Stunde tiefer hineinblicken. Im ersten Schritt ist es aber wichtig, die Datenmenge auf ein Minimum zu reduzieren.

IoT: EcoStruxure hat im Moment drei Ebenen. Wird es vielleicht einmal eine vierte Ebene geben?
Siefert: Interessanter ist die Frage: Wie passen EcoStruxure und Exchange zusammen. Letztendlich steht der Plattformgedanke im Fokus. Mit unserem neuen Businessportal Exchange gehen wir den Schritt, dass wir die Toolbox EcoStruxure und das Anwender-Netzwerk zusammenbringen. Mit dem Kollaborationsportal, welches auf die Kraft interdisziplinärer Zusammenarbeit setzt, wird die Welt transparenter und man kommt schneller zu richtigen Lösungen. Die Partner können ihre Lösungen auf der Plattform teilen. Wenn man schon die fertige Lösung in der Schublade hat, dann sollte man sie auch teilen. Das ist die Idee dahinter.

www.se.com

Jean-Pascal Tricoire, CEO und Chairman von Schneider Electric verspricht bis 2025 CO_2-neutral zu werden, denn „der Klimawandel ist die größte Einzelgefahr für die Gesundheit und das Wohlergehen."

SCHNEIDER ELECTRIC WILL BIS 2025 CO_2-NEUTRAL WERDEN

Zwei Tage lang tauschten sich Experten und Spezialisten beim Innovation Summit von Schneider Electric in Barcelona über EcoStruxure sowie die Businessplattform Exchange aus. Mittendrin die Ankündigung von Jean-Pascal Tricoire Chairman & CEO von Schneider Electric, das Unternehmen bis 2025 CO_2-neutral zu machen.

Ganz in grün präsentierte sich das Barcelona International Convention Center am 2. und 3. Oktober für den Innovation Summit von Schneider Electric. 3.500 Besucher nützten die Gelegenheit in mehr als 40 Veranstaltungen, Workshops und Business Talks mit rund 100 Referenten mehr über Schneider Electric zu erfahren.

Grün versucht sich Schneider Electric auch in Sachen Klimawandel zu präsentieren. Dazu kündigte Jean-Pascal Tricoire, Chairman & CEO von Schneider Electric im Rahmen seiner Keynote an, bis 2025 CO_2-Neutralität im erweiterten Ecosystem erreichen zu wollen. „Der Klimawandel ist die größte Einzelgefahr für die Gesundheit und das Wohlergehen – und damit in letzter Konsequenz für den Fortbestand unserer Gesellschaft. Wir müssen zusammenarbeiten, um unsere CO_2-Emissionen zu reduzieren und den Temperaturanstieg zu stoppen", sagt Tricoire. Dazu hat er auf der Klimawoche NYC 2019 vom 24. bis 30. September ein dreiteiliges Maßnahmenpaket angekündigt. Dazu gehört auch die Zusammenarbeit mit Lieferanten in Richtung einer Netto-Null-Lieferkette bis 2050.

Gedankenaustausch heißt Exchange. Im Rahmen der Presseveranstaltung zog Christophe de Maistre, CEO & Zone President DACH seine Bilanz nach seinen ersten 100 Tagen im Amt. Dabei betonte er seine klare Zielsetzung für die kommenden Jahre. Dazu zählt die Marktposition von Schneider weiter zu stärken, den Bekanntheitsgrad zu steigern und weiterhin den Fokus auf Partnerschaften zu setzen. Dazu gehört auch die im April dieses Jahres neu installierte Businessplattform „Exchange". Sie soll die vielfältige Community bei der Entwicklung und Skalierung von Geschäftslösungen sowie der Erschließung neuer Marktpotenziale unterstützen. Bislang haben sich 45.000 Teilnehmer registriert und damit Zugang zu einem riesigen Pool von technischen Tools und Ressourcen erhalten. Nutzer haben Zugriff auf APIs, Analysen und Datensätzen. Im Austausch mit anderen Nutzern sollen dadurch neue Lösungen entstehen.

Drei Ebenen. Im Mittelpunkt des Innovation Summit in Barcelona stand vor allem EcoStruxure, eine IoT-fähige, offene und interoperable Plug & Play-Architektur. Die Lösung verbindet die drei Technologiekernbereiche: vernetzte Produkte, Edge Control sowie Apps, Analysen und Services in einer ganzheitlichen Architektur und ermöglicht so die durchgängige Konnektivität auf allen Ebenen moderner Fertigungsbetriebe.

Produkte mit integrierten intelligenten Messgeräten und Sensoren ermöglichen die Erfassung dedizierter Maschinen- und Anlagedaten, die dann auf Edge Control-Ebene mittels leistungsstarker Steuerungsplattformen lokal oder in der Cloud gesammelt werden. Moderne Digitalisierungslösungen wie die „EcoStruxure Asset Advisor"-Software stellen anschließend ein zielgenaues Monitoring sowie eine umfassende Datenanalyse und -auswertung sicher. So können Prozess- und Energiedaten beispielsweise standortunabhängig und zu jeder Zeit abgerufen werden, um Fehlerpotenziale bereits frühzeitig zu erkennen. Kunden erhalten einen Echtzeit-Einblick in den gesamten Lebenszyklus des Betriebes, können zielgerichtete Optimierungen vornehmen und alle Mehrwerte der Digitalisierung effektiv für sich nutzen.

www.se.com

IM DIGITALEN HERZ EUROPAS

Im Rahmen der Barcelona Industry Week von 29. bis 31.Oktober präsentierte sich die Stadt als Plattform für smarte, vernetzte und autonome Produktion. Blockchain, Artificial Intelligence und IoT schwebten nicht nur als Buzzwords über dem Kongress, sondern in Form echter Use Cases.

Insgesamt sieben Veranstaltungen fanden gleichzeitig im Rahmen der Barcelona Industry Week statt. Der IoT Solutions World Congress war Teil davon sowie u.a. die Blockchain Solutions World und das AI & Cognitive Systems Forum. Entwickler, IT-Entscheider und internationales Technologiepublikum tauschten sich in der Gran Via Messehalle in Barcelona über Technologien der Gegenwart und Zukunft aus. 350 Aussteller erfüllten den größten Ausstellungsbereich. Österreich war mit einem Länderpavillon vertreten.

Der Solutions World Congress gliederte sich in verschiedene Ausstellungsbereiche, die aber eines gemein hatten: Technologie nicht nur erklärt, sondern auch zum Angreifen und Verstehen. Es wurden industrielle Internetanwendungen live vorgeführt, die sich durch Innovation und Effizienz bei der Prozessverbesserung auszeichnen und zwar in den unterschiedlichsten Bereichen – von Landwirtschaft über Versicherungen bis in die Forschung und Überwachung von seltenen Tierarten.

Anwendungen aus dem Testbed-Bereich:

- Drohnen, Sensoren und Blockchain, die die Wasserqualität der Wolga überwachen,
- eine Plattform, die IoT, KI und 5G kombiniert, um eine vorausschauende medizinische Versorgung zu gewährleisten und Notfälle bei älteren und chronisch kranken Menschen zu bewältigen,
- ein System zur Inspektion und Reparatur von Windkraftanlagen mit Drohnen und
- ein Montagehilfesystem, das die Mitarbeiter einer Fabrik genau durch die verschiedenen durchzuführenden Schritte führt.

Am IoT Solutions World Congress nutzten auch 23 österreichische Unternehmen die Gelegenheit am Stand „Advantage Austria“ der IoT-Community zu demonstrieren, welche Innovationskraft sie zu bieten haben. Lösungen und Produkte für IoT-Anwendungen präsentierte mit Compax ein Familienunternehmen, das aus der klassischen Softwarewelt kommt. Mit seinem Partner Digital Republic tat man den Schritt in die IoT-Welt. Gemeinsam setzen sie mit Kunden wie Volvo, Georg Fischer oder Tesla (ein Projekt gemeinsam mit der Swisscom) neue Geschäftsmodelle um. Das burgenländische und mittlerweile weltweit tätige Softwareunternehmen Mavoco öffnet Produzenten und Telekomanbietern ebenfalls Tür und Tor zu neuen Geschäftsfeldern. Die angebotene IoT-Plattform unterstützt so gut wie alle Lizenzmodelle für branchenübergreifende Einsatzgebiete des IoT.

Der steirische Komplettlösungsanbieter Microtronics präsentierte sich ebenfalls und überzeugte mit seinen Referenzprojekten für IoT und M2M. Mit einer neuen und innovativen Technologie für IIoT und Industrie 4.0-Anwendungen sind die Vertreter von SLOC vor Ort. Das steirische Unternehmen hat ein intelligentes Device entwickelt, das mit einzigartigen Algorithmen Informationen vom Sensor direkt ins IT-System des Kunden übermittelt. Die 6. Ausgabe des IoT Solutions World Congress findet dann vom 27. bis 29. Oktober 2020 statt. (gl)

Luka Mustafa, CEO und Gründer des slowenischen Startups irnas, macht nach eigenen Worten „Projekte, die niemand macht. Die verrückt und außergewöhnlich sind.“

Integra aus Sevilla präsentierte mit Smart Eye eine Smart Farming IoT-Lösung.

Der rot-weiß-rote Technologie-Blickfang des IoT SWC: der Gemeinschaftsstand „Advantage Austria“.

FÜR DEN MITTELSTAND GESCHAFFEN

Auf dem Pressegespräch wurde bereits betont: Die Twenty2X versteht sich als Digital Enabler für den Mittelstand und wendet sich in erster Linie an KMU aus der DACH-Region.

Mit der Twenty2X möchte die Deutsche Messe 2020 durchstarten und den Platz der ehemaligen CEBIT ein wenig füllen. Gelingt dies, können sich die Veranstalter glücklich schätzen. Das Angebot an Events, gerade im Digitalisierungsumfeld, ist nämlich inzwischen enorm groß.

Im Interview mit Jutta Jakobi, Global Director Digital Business bei der Deutschen Messe AG und verantwortlich für die Twenty2X, zeigt sich, dass Ideen vorhanden sind. Nun gilt es diese umzusetzen.

IoT 4 Industry & Business: Die neue Messe Twenty2X findet nach dem Aus der bekannten CEBIT auch wieder in Hannover statt. Welche Erwartungen haben Sie an die neue Veranstaltung und inwiefern ist sie mit dem Format der CEBIT identisch?
Jutta Jakobi: Mit der Twenty2X beginnt eine neue Ära. Auch wenn das Thema Digitalisierung an die „alte" CEBIT erinnert, so haben wir mit der Twenty2X ein neues Format entwickelt. Wir konzentrieren uns auf die Kernbereiche der geschäftlichen IT-Anwendungen und setzen den Fokus auf Besucher aus kleinen und mittelständischen Unternehmen aus der DACH-Region. Mit zwei belegten Hallen, drei Messetagen und sechs Themenschwerpunkten ist die Twenty2X kompakt und klar strukturiert. Hier finden Entscheider, was sie brauchen. Nur die Essenz, keinen Schnickschnack.

IoT: Ist Hannover der geeignete Standort für eine Digitalmesse Ihrer Ansicht nach?
Jakobi: Hannover ist der perfekte Standort für Messen rund um die Digitalisierung. Wir bieten den besten Service und ein hervorragendes Messegelände mit einer technisch herausragenden Infrastruktur, das ab Mitte nächsten Jahres mit einem weiteren Pluspunkt aufwarten kann: Als eines der ersten Messegelände in Europa wird das Areal mit einem 5G-Campus-Netz ausgestattet und so zu einem Smart Venue. Wir werden das Netz übrigens nicht nur für Veranstaltungen nutzen, sondern es auch als 5G-Testlabor der Industrie zur Verfügung stellen.

IoT: Welche Erwartungen knüpfen Sie an die erste Veranstaltung im kommenden Jahr?
Jakobi: Wir erwarten eine sehr „geschäftige", businessorientierte Veranstaltung, die Unternehmen aus dem Mittelstand dabei unterstützt, ihre Prozesse und Abläufe mit digitalen Technologien zu verbessern, um sie fit zu machen für das aktuelle Geschäft und die Anforderungen der Zukunft. Geschäftsführer, CIOs und alle

TWENTY2X
NEW TECH. NEW BUSINESS

Was? Twenty2X – Neue Messe für IT-Lösungen
Wann? 17.-19.3.2020, täglich 9:30-18 Uhr
Wo? Hannover
Preis? 45 Euro Tagesticket

weiteren Personen, die im Unternehmen über digitale Projekte entscheiden, treffen auf der Twenty2X auf Aussteller, die ihr Angebot gezielt auf die Anforderungen kleiner und mittlerer Unternehmen ausrichten sowie auf ein Konferenzprogramm, das speziell für diese Zielgruppe entwickelt wurde. Darüber hinaus stellen wir neue Formate zur Verfügung, die einen offenen und kreativen Austausch fördern, der IT-Anbieter mit IT-Anwendern und Startups zusammenbringt und neue Impulse entstehen lässt – und das in einer angenehmen Atmosphäre auf Augenhöhe.

IoT: Und weshalb lässt man die neue Veranstaltung auch wieder im März stattfinden? Schließlich wurde bei der CEBIT noch versucht durch eine Verlegung in die Sommermonate das Konzept am Leben zu erhalten bzw. ihr einen neuen Schwung zu verpassen.
Jakobi: Wir haben die Planungsphasen aller Beteiligten berücksichtigt und die Twenty2X bewusst in den März gelegt. Der Frühjahrstermin korrespondiert mit dem Vertriebszyklus der Aussteller und ist früh genug für den Planungszyklus der Besucher.

IoT: Wen möchten Sie mit der neuen Veranstaltung gezielt erreichen? Und wie weit ziehen Sie den Kreis für Aussteller und Besucher rein ländertechnisch gesehen?
Jakobi: Wir setzen bei der Twenty2X gezielt auf die Besuchergruppe des kleinen und „gehobenen" Mittelstands – und hier in erster Linie auf Anwender aus Deutschland, Österreich und der Schweiz. Was die Aussteller betrifft, lässt sich der Kreis natürlich erweitern: Jedes Unternehmen, das IT-Angebote für die Zielgruppe Mittelstand aus der DACH-Region anbietet, ist auf der Twenty2X willkommen.

IoT: Durch die Digitalisierung sind auch eine Reihe von neuen Messe-Formaten bzw. -Ergänzungen und weiteren digitalen Events im Laufe der Zeit entstanden. Meinen Sie nicht, dass die Sättigung am Markt diesbezüglich bereits erreicht ist?
Jakobi: Was einzelne Fachthemen betrifft, mag das zutreffen. Eine branchenübergreifende Messe, die IT-Lösungen für Geschäftsprozesse fokussiert und sich speziell an die Zielgruppe Mittelstand wendet, gibt es derzeit nicht. Gerade diese Zielgruppe verfügt aber häufig nicht über die Kapazitäten, unzählige Events an verschiedenen Orten zu besuchen. Mit der Twenty2X bieten wir die Chance, sich in kurzer Zeit an einem Ort einen Überblick über die IT-Lösungen zu verschaffen, die aktuell und zukünftig Unternehmensprozesse verbessern und beschleunigen – und darüber hinaus speziell für mittelständische Unternehmen entwickelt wurden.

IoT: Wer sind die Aussteller der Twenty2X?
Jakobi: Die Aussteller sind zum überwiegenden Teil selbst mittelständische Unternehmen, die schon allein deshalb die Anforderungen des Mittelstands kennen und zielgenaue Lösungen anbieten werden.

IoT: Da es in den vergangenen Jahren oft der Fall war, dass man sich als Unternehmen oder auch als Messe immer wieder neu erfinden muss um am „Leben zu bleiben" – gerade in Zeiten der Digitalisierung – wie viel Zeit geben Sie der Twenty2X oder gehen Sie davon aus, dass sie im geplanten Format sehr lange Bestand haben wird?
Jakobi: Wir haben die Twenty2X als jährliche Veranstaltung geplant, und das auf Jahre hinaus. (se)

www.twenty2x.de

Jutta Jakobi
Global Director Digital Business bei der Deutschen Messe AG und verantwortlich für die Twenty2X

„Wir setzen bei der Twenty2X gezielt auf die Besuchergruppe des kleinen und „gehobenen" Mittelstands – und hier in erster Linie auf Anwender aus DACH."

ZENON MACHT WERKE VERGLEICHBAR

Daten haben einen sehr hohen Stellenwert, denn es wird immer wichtiger, aus ihnen aussagekräftige Reports zu erstellen. Bei einem Kunden sammelt zenon Live-Daten aus weltweit verteilten Werken in einer zentralen Datensenke und bereitet sie zur Analyse auf. Mit dieser Lösung sind alle Beteiligten auf dem letzten Stand.

Ein Hidden Champion aus Deutschland ist durch die Gründung und den Zukauf von Werken in nahezu allen Erdteilen zu einem global agierenden Konzern geworden. Durch die Akquisition von früheren Wettbewerbern kamen Fabriken mit unterschiedlicher Anlagentechnik in das Unternehmen. Eine Vergleichbarkeit der Auslastung und des Leistungsvermögens der weltweit verteilten Werke war unter diesen Gegebenheiten äußerst zeitaufwändig. Das Konzernmanagement initiierte deshalb ein Projekt, das Daten aus der Produktion an den verschiedenen Standorten ermitteln und zur Auswertung an ein zentrales Datencenter übertragen sollte. Die Softwareplattform zenon wurde zum wichtigen Bestandteil des Projektes.

Eine der größten Herausforderungen war das heterogene Automatisierungsumfeld. Jedes Werk besaß eine andere installierte Basis an SPSen. Eine weitere Schwierigkeit war die limitierte Bandbreite der Datenverbindung. Die einzige Konstante war: Alle Werke sind über VPN-Verbindungen an das zentrale Firmennetzwerk angeschlossen. Eine schlanke Datenkommunikation war erforderlich. Der Kunde entschied sich daher für das moderne Kommunikationsprotokoll MQTT (Message Queue Telemetry Transport).

MQTT hat einige Vorteile:

- Der Sender kommuniziert nicht direkt mit dem Empfänger. Die beiden müssen sich also nicht direkt „sehen“. Zwischen Sender und Empfänger steht immer ein Vermittler, der sogenannte Broker.
- Die Verbindung kann durch Zertifikate verschlüsselt erfolgen.
- Es gibt drei unterschiedliche Übertragungsarten, die von „shoot-and-forget“ bis hin zu 100 Prozent garantierter Übertragung inklusive Datenpufferung bei Kommunikationsausfall reichen.

Nur ein Merkmal von MQTT kann man als Nachteil interpretieren:

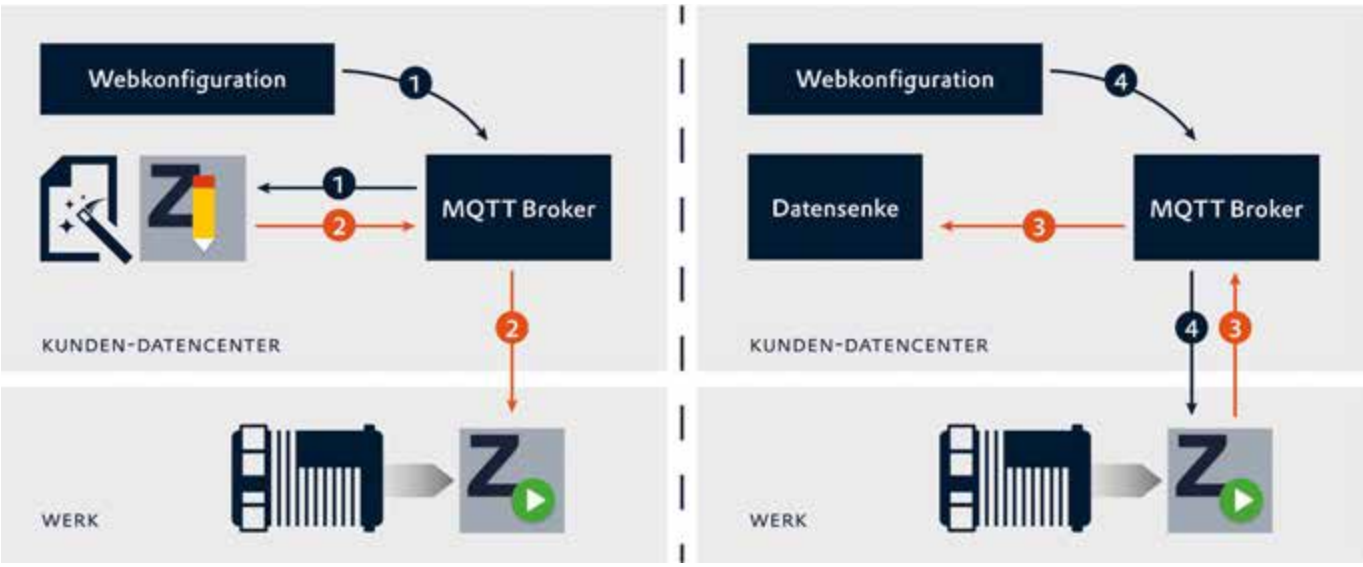
- Das Protokoll ist völlig offen, was Daten betrifft, die transportiert werden sollen. Es gibt keinen Standard, der die sogenannte Payload festlegt. Sender und Empfänger müssen deshalb dieselbe Payload implementieren, damit die Kommunikation funktioniert. Besonders wenn Sender und Empfänger von unterschiedlichen Firmen entwickelt werden, bedingt das eine sorgfältige Abstimmung.

Zuerst wurde ein gemeinsames Konzept ausgearbeitet. Der Kunde wollte eine zentrale, webbasierte Oberfläche haben, um die einzelnen Werke zu konfigurieren. Diese Weboberfläche wurde von einer Drittfirma umgesetzt. In dieser Applikation kann der Anwender einiges bestimmen: Das Produktionswerk, den Treiber, welche Variablen in welcher Zykluszeit übertragen werden sollen, welche Berechnungen durchzuführen sind und vieles mehr.
Von der Weboberfläche wird ein Anforderungstelegramm an den zenon Editor geschickt. Der Editor erzeugt daraus mithilfe eines Vorlagenprojekts vollautomatisch das zenon-Projekt. Dank der strikten Trennung von zenon Editor und Runtime ist das realisierbar. Die Runtime-Dateien des Editors werden dann per MQTT über den Broker zum entsprechenden Werk geschickt. Jedes Werk hat eine eindeutige Plant ID. Die Plant ID als Schlüssel im MQTT-Header stellt sicher, dass das richtige Projekt zum richtigen Werk kommt.
Im Werk selbst kommuniziert ein Standard-Windows-PC im Schaltschrank über eine Firewall mit dem MQTT-Broker und mit den SPSen im Produktionsnetzwerk. Auf dem PC läuft ein MQTT-Client, der das Paket vom Editor empfängt und die zenon Runtime als Dienst startet. Das System kann auch hier vollautomatisch als Gateway arbeiten und benötigt keinerlei Benutzerinteraktion. Die zenon Runtime nimmt die Arbeit auf und fragt die Werte von den angeschlossenen SPSen zyklisch ab. Um die Daten zum Empfänger (Datensenke) zu senden, wurden drei unterschiedliche Datenarten implementiert:

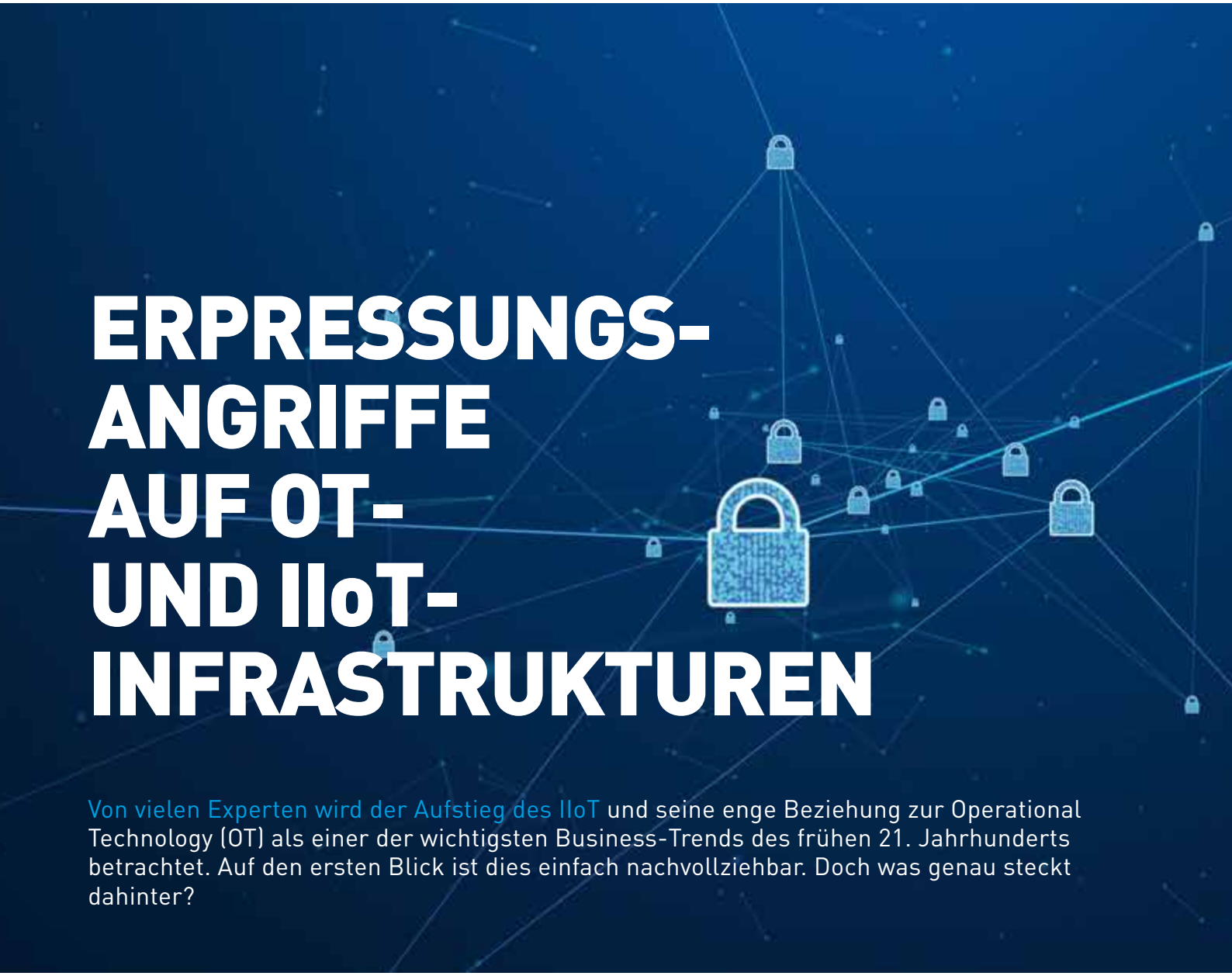
1. **Realtime-Daten:** Daten werden sofort beim Auftreten versendet. Der Treiber wurde auf eine Abtastzeit von einer Sekunde eingestellt, somit wird maximal ein Wert pro Sekunde gesendet. Da zenon nur bei einer Wertänderung notifiziert, werden auch nur bei einer Wertänderung Daten übertragen. Bei einer limitierten Bandbreite ist das besonders wichtig.
2. **Getriggerte Daten:** Über die Weboberfläche kann der Kunde bestimmen, in welchem Zyklus Daten übertragen werden sollen. Je nach Anwendung lässt sich hier einstellen, ob jede Minute, alle fünf Minuten oder gar nur einmal pro Stunde Messwerte übertragen werden sollen. Der Kunde kann die Zykluszeit jederzeit mit der Weboberfläche ändern.
3. **Berechnete Werte:** Es wurden verschiedene Berechnungen gefordert, wie Min/Max, Mittelwertberechnung usw. logische Operationen wurden auch umgesetzt, beispielsweise eine Erkennung, ob ein Förderband leerläuft oder mit Material bestückt ist. zenon Logic führt alle Berechnungen durch und überträgt die Ergebnisse im eingestellten Zyklus per MQTT. Selbstverständlich wird auch das zenon Logic-Projekt zu 100 Prozent automatisiert vom zenon Editor erstellt.

Für alle drei Datenarten wurde ein gemeinsames MQTT-Protokoll für die Übertragung von Messwert, Zeitstempel und Qualität entwickelt. Ebenso wurde entschieden, dass die Werte eines Zyklus immer geblockt verschickt werden. So werden z.B. bestimmte Messwerte alle fünf Minuten in einem einzigen Telegramm verschickt. Auch diese Maßnahme führt zu einer sehr schlanken Kommunikation.
Die Offenheit der Softwareplattform zenon in Kombination mit der Fähigkeit, Projekte komplett automatisiert zu erstellen, hat zu erheblichen Kosteneinsparungen bei der Implementierung und Ausrollung der Lösung geführt. Aussagekräftige Reports generieren Mehrwert auf allen Ebenen und ermöglichen transparentes Benchmarking über geografische Grenzen hinweg.

www.copadata.com



1. Initiale Konfiguration: Webkonfiguration schickt Konfigurationsdatei zum zenon Editor.
2. zenon Editor erzeugt Projekt und überträgt RT-Dateien zur zenon Runtime.
3. Datenfluss: zenon Runtime überträgt die Daten zyklisch zur Datensenke.
4. Rekonfiguration der Zykluszeit: Geänderte Übertragungsrate wird direkt zur Runtime geschickt.



ERPRESSUNGS-ANGRIFFE AUF OT- UND IIoT-INFRASTRUKTUREN

Von vielen Experten wird der Aufstieg des IIoT und seine enge Beziehung zur Operational Technology (OT) als einer der wichtigsten Business-Trends des frühen 21. Jahrhunderts betrachtet. Auf den ersten Blick ist dies einfach nachvollziehbar. Doch was genau steckt dahinter?

Eine Vielzahl von Geräten, Sensoren und Equipment mit dem Internet verbinden und das in Kombination mit M2M-Kommunikation und -Automatisierung klingt nach der nächsten großen Industrieumwälzung. Und die Aussicht auf integrierte Lieferketten, Echtzeit-Rückmeldungen über Prozesse, auftretende Probleme und vorhandene Bestände, bei denen selbst die kleinsten Elemente eines industriellen Prozesses miteinander verbunden wären, ist dabei äußerst erfolgsversprechend. Ein pessimistischerer Blick – man könnte ihn auch realistischer nennen – sieht die flächendeckende Verbreitung von IIoT und OT aber auch als ein neues Feld digitaler Sicherheitsrisiken. Diese könnten in ähnlicher Weise unterschätzt werden, wie die Risiken des konsumentenorientierten IoT in den ersten Jahren. Nicht nur für Sicherheitsskeptiker dürfte dabei klar sein – je mehr Geräte, Equipment, Sensoren und Anwendungen miteinander verbunden werden, desto größer ist die gegenseitige Abhängigkeit und Empfindlichkeit gegenüber Störfällen.

Gefahren kommen und gehen. Da sich Industrie 4.0 und IIoT aber noch im Aufbau befinden und viele Technologien und Standards noch nicht final implementiert sind, sind auch potenzielle Schwachstellen für Cyberangriffe nicht immer offensichtlich. Ein Beispiel dafür sind smarte Logistikanwendungen, die es ermöglichen, einzelne Werkzeuge oder bestimmte Vorgänge im Werk zu lokalisieren. Solche Anwendungen sind in der Regel auch ans Intranet angebunden und können so durch Cyberangriffe gezielt kompromittiert werden. Noch besorgniserregender ist, dass ICS-Fertigungsmaschinen zunehmend direkt im Internet eingebunden sind, um Status-Updates zur vorausschauenden Instandhaltung zu senden – damit steigen auch die Cyberrisiken. Jüngste Cyberangriffe auf Fertigungsanlagen zeigen definitiv, dass Anlass zur Sorge besteht. Laut dem letzten Data Breach Investigations Report (DBIR) von Verizon, der die Zahlen von 2017 analysierte, zählte das verarbeitende Gewerbe 42 bekannte Verstöße und 389 Cybervorfälle verschiedener Art. Damit liegt es direkt hinter Sektoren

Der Autor:
Jörg Schuler
... ist OT-Security-Portfolio-Manager bei Airbus CyberSecurity.

wie Gesundheitswesen, Finanzen und Einzelhandel. Etwa 90 Prozent davon gehen eher von externem Hacking aus als von einer internen Kompromittierung oder einer Fehlkonfiguration. Verizon weist zudem darauf hin, dass 86 Prozent gezielte Angriffe waren, die speziell für die Penetration bestimmter Unternehmen entwickelt wurden.
„Die überwiegende Mehrheit der Angriffe unterstreicht, dass Kriminelle bestimmte Produktionsstätten mit einem ganz bestimmten Zweck verfolgen", heißt es im Bericht. Diese Zahlen sagen noch keine Details darüber aus, wie anfällig IIoT und OT für Cyberangriffe sein könnten, aber sie unterstreichen, dass sie bereits flächendeckend ins Visier genommen werden mit einer Reihe von Absichten, darunter geopolitische Vorteile und finanzielle Gewinne.

Wie könnten sich Angriffe entwickeln? Cyberangriffe basieren auf einer Kombination aus technischen Mitteln – der Schwachstelle, die ausgenutzt wird, um in ein Zielnetzwerk einzudringen – und der kriminellen Absicht, dies ohne Rücksicht auf Risiken und Kosten zu tun. Jüngste Vorfälle zeigen, dass dabei das häufigste Vorgehen für Angriffe wahrscheinlich die gezielte Cyber-Extortion (=Erpressung) ist.
Ein warnendes Beispiel, wie gefährlich dies werden kann, gab der Vorfall im März 2018 in der Stadt Atlanta. Unter Verwendung einer Hacking-to-Ransomware-Plattform namens SamSam drangen Angreifer in das Netzwerk der Stadt ein, um eine Reihe von Anwendungen zu verschlüsseln. Die Lösegeldforderung von 51.000 USD wurde zwar anscheinend nicht erfüllt, trotzdem kostete der Angriff schließlich 2,6 Millionen USD, um ihn zu bereinigen. SamSam wurde zudem für weitere Angriffe 2018 verantwortlich gemacht, darunter auf die Häfen von Barcelona und San Diego.
Zusätzliche Gefahr geht davon aus, dass IiIoT-Systeme immer noch oft über keine effizienten Sicherheitsstrategien oder ausgereifte Sicherheitsmodelle verfügen. Fehler bereits beim Sicherheitsdesign sorgten in der Vergangenheit zu oft für vielfältige Penetrationsmöglichkeiten. Dazu kommt, dass industrielle Netzwerke, die IIoT unterstützen, in der Regel nicht von Grund auf neu aufgebaut werden, sondern von der etablierten Netzwerksicherheit und den Protokollen einer Organisation abhängen. Ein grundlegendes Problem dabei ist, dass IIoT und OT naturgemäß die Anzahl der Geräte erhöhen, die über Internetprotokolle kommunizieren und so die Angriffsfläche vergrößern. Angreifer müssen dann nur einen Schwachpunkt oder ein Protokoll finden – Remote Desktop Protocol (RDP) war SamSams bevorzugte Einstiegsmethode – von dem aus sie einen tieferen Einbruch in das Zielnetzwerk aufbauen können. Wenn eine betroffene Institution merkt, dass sich ein Angreifer im Netzwerk befindet, ist es in der Regel schon zu spät.

Wie kann man Sicherheitslücken verhindern? Wie können Unternehmen das erforderliche Sicherheitsniveau ermitteln und wie können sie dieses erreichen und Risiken minimieren? Da die Bedrohung zumeist technologischer Natur ist, ist die Versuchung groß, nur nach einer technologischen Antwort zu suchen. Gleichzeitig können IT-Sicherheitsansätze aber nicht einfach auf OT- und IIoT-Architekturen übertragen werden.
Verantwortliche, typischerweise Projektleiter oder CISOs, müssen also eine gute Balance finden, zwischen einem umfassenden und ganzheitlich risikobasierten Ansatz – was natürlich Zeit braucht, aber ein kritischer, wiederkehrender Prozess ist und einer Implementierung von kurzfristigen Best Practices. Eine wichtige Grundlage ist zunächst das Verständnis der bestehenden Sicherheitsbestimmungen (z.B. der NIS-Richtlinien) und der bestehenden Normen und Richtlinien (ISO 27001, IEC 62443), die für ein bestimmtes Industriesegment gelten.
Ein weiteres wichtiges Tool ist der Maturity Check, der sich auf die Faktoren Mensch, Prozess und Technologie konzentriert. Mit diesem Ansatz erschließt sich ein umfassenderes Bild des gesamten Sicherheitsstatus. Für den Faktor Mensch ist eine einfache, aber wichtige erste Maßnahme, das Sicherheitsbewusstsein mit geeigneten Trainings zu erhöhen. Eine weitere wichtige Maßnahme auf technischer Ebene ist die Segmentierung des Netzwerks, zudem müssen ICS-Systemanbieter von Fernzugriffslösungen für deren Sicherheit sorgen.

www.airbus-cyber-security.com/de

KLARE REGELN FÜR **OPEN SOURCE-KOMPONENTEN**

Open Source ist längst ein fester Bestandteil verschiedenster Software. Aus Zeit- und Kostengründen kommen Entwickler auch bei sicherheitsrelevanten Anwendungen nicht mehr darum herum. Die Nutzung von Open Source-Bibliotheken (OSB) kann für Unternehmen allerdings zum Problem werden, wenn sie unentdeckte Schwachstellen enthalten, die Hacker ausnutzen können.

Für Entwickler bedeuten OSB Zeitersparnis, indem sie für Standardanforderungen vorgefertigte Bausteine verwenden können, anstatt alles komplett selbst zu schreiben. Das senkt nicht zuletzt die Kosten der Unternehmen. Daher verwundert es auch nicht, dass die Anzahl der Open Source-Bibliotheken weltweit steigt. Bis 2030 könnte es 500 Millionen davon geben.

Entdecken Hacker in Open-Source-Komponenten Schwachstellen, haben sie im schlimmsten Fall Zugriff auf etliche Anwendungen verschiedener Unternehmen, die alle diese Komponente nutzen. Ein weiteres Problem ist, dass die Open Source-Komponenten meist nicht so eingehend geprüft werden wie Eigenentwicklungen. Eine Anwendung kann noch so gut programmiert sein, wird sie nachdem sie aus einer OSB gezogen wurde nicht auf Schwachstellen untersucht, setzt sich ein Unternehmen damit dem Risiko aus angegriffen zu werden. So zeigen Studienergebnisse von Veracode auf, dass 44 Prozent aller Anwendungen mit Open Source-Komponenten erhebliche Schwachstellen aufweisen.

Aktuell basiert das Wissen vieler Unternehmen über anfällige Komponenten immer noch auf öffentlichen Common Vulnerabilities and Exposures (CVEs). Dieses System stammt noch aus einer Zeit vor DevOps und dem massenhaften Einsatz von OSBs. Heute sind die Release-Zyklen so schnell, dass Anwendungen oft schon veröffentlicht sind, bevor Schwachstellen von OS-Komponenten auf öffentlichen Listen bekanntgegeben werden.

Anwendungssicherheit stets im Blick behalten. Unternehmen können es sich heute nicht mehr leisten, auf OSBs zu verzichten. Die zusätzliche Entwicklungszeit wäre ein zu großer Wettbewerbsnachteil. Der Schnelligkeit sollte man aber keinesfalls die Sicherheit opfern, daher sind klare Policies für den OS-Einsatz in Unternehmen Pflicht. Es müssen Vorkehrungen getroffen werden, um den Schadenseintritt durch eventuell vorhandene Sicherheitslücken aufzuhalten. Schwachstellen in OSBs bedeuten noch nicht automatisch, dass ein Unternehmen angreifbar wird. Es kommt darauf an, welche Open Source-Komponenten genutzt werden und ob diese von der Anwendung aufgerufen werden. Anwendungen müssen über ihren gesamten Lebenszyklus hinweg getestet werden.

Entwickler und Sicherheitsexperten müssen sich kontinuierlich austauschen und zusammenarbeiten, um Schwachstellen in ihren Codes schnell zu identifizieren. Zu einer umfassenden Sicherheitsstrategie gehört es auch, zu definieren, welche Bibliotheken für Entwickler erlaubt sind und das eindeutig festzuhalten. Das fördert und beschleunigt auch ein zentrales Patch-Management. Ebenso sollte es klare Vorgaben geben, in welchem Zeitraum Probleme behoben werden müssen. Sicherheitstest sollten in vorgegeben Intervallen und nach definierten Prozessen durchgeführt werden. Dafür werden Tools für statische Code-Analysen und Werkzeuge für Software Composition Analysis (SCA) immer wichtiger.

www.veracode.com

Der Autor:
Julian Totzek-Hallhuber
... ist Solution Architect beim Spezialisten für Anwendungssicherheit Veracode und bringt mehr als 15 Jahre Erfahrung im IT-Sicherheitsumfeld mit.

FÜNF TREIBER FÜR DIE **FABRIK DER ZUKUNFT**

Die Gestaltung der Fabrik der Zukunft erfordert Investitionen und technologische Neuerungen auf allen Ebenen eines Fertigungsunternehmens. Zentrale Fragestellungen richten sich daher nicht nur darauf, welche Investitionen erforderlich sind, sondern, in welcher Reihenfolge sie getätigt werden sollten, um beschleunigt Vorteile zu erzielen.

Der Autor:
Dirk Löhmann
... ist Regional Vice President Continental Europe, Epicor Software.

Digitale Transformation bedeutet oft, mit zahlreichen Innovationsprojekten gleichzeitig konfrontiert zu sein, was die IT-Abteilung an die Grenzen ihrer Belastbarkeit bringen kann. Hier ist die Gefahr groß, dass viele Tests mit neuen Technologien zwar erfolgreich verlaufen, aber im Pilotstatus steckenbleiben, wie es auch das World Economic-Forum in einer Studie vom Jänner 2019 beschreibt.
Ein Blick auf die Treiber einer Fabrik der Zukunft kann helfen, im Rahmen eines Frameworks für die Digitale Transformation die individuell richtigen Prioritäten zu setzen:

1. Digital Twinning und Predictive Analytics für die Zusammenarbeit in Eco-Systemen

Je komplexer die Vernetzung eines Fertigungsunternehmens mit Zulieferern, Dienstleistern und Kunden gestaltet ist, umso eher wird es damit konfrontiert, über Unternehmensgrenzen hinaus eine automatisierte Zusammenarbeit zu gewährleisten. Das reicht von der Abstimmung von Produktionskapazitäten und Lieferkonditionen bis hin zur gemeinsam koordinierten Produktentwicklung. Letzteres kann erheblich von Digital Twinning profitieren, wie es etwa Gartner beschreibt.

2. Intelligente Vernetzung von Produktion mit Management

IIoT hat sich bereits in zahlreichen Pilotprojekten bewiesen, vor allem europäische Unternehmen investieren hier kräftig, so eine Studie von Bain. Vor allem sind Anwendungen in der Qualitätskontrolle im Remote-Monitoring von Anlagen sowie für das Tracking von Ausrüstungen an Produktionsstätten von wachsendem Interesse. Allerdings: Um die Vorteile von IIoT auch umfassend ausschöpfen zu können, ist eine mit dem ERP-System vernetzte Produktionssteuerung über MES-Lösungen eine Schlüsselanforderung, wie auch PwC in seiner Studie Digital Factories 2020 unterstreicht.

3. Blockchain für sicherheitskritische Produkte

Bei Produkten, die Compliance-Richtlinien unterliegen oder sicherheitskritisch sind, werden beschleunigt Technologien eingesetzt, die die Rückverfolgbarkeit von Produkten, deren Herstellung und Ausgangmaterialien sowie Lieferwege vereinfachen. Neben IIoT wird zukünftig auch die Blockchain-Technologie hier eine wichtige Rolle zur lückenlosen Überwachung der Lieferkette spielen.

4. Advanced Robotics mit Intelligenz für mehr Effizienz und Flexibilität in der Produktion

Wer in der Fertigung verstärkt auf Advanced Robotic für Produktivitätssteigerungen setzt und damit auch auf den Wettbewerbsvorteil einer stärkeren Individualisierung von Produkten abzielt, profitiert insbesondere von intelligenten Systemen – von ML bis hin zu KI. Diese Technologien helfen, Roboticsinvestitionen beschleunigt zu amortisieren. Eine Analyse von Boston Consulting Group ergab, dass der Einsatz von Advanced Robotics die Verarbeitungskosten um bis zu 15 Prozent senken kann.

5. Intuitive Mensch-Maschine-Interaktion

Innovative Mensch-Maschine-Schnittstellen erweitern die Möglichkeiten, die Produktivität von Mitarbeitern in den Bereichen Fertigung, Wartung und Engineering sowie die Sicherheit in den Anlagen zu erhöhen. Insbesondere Voice-Controlled-Systems, Cobots sowie Wearables wie Smart Glasses mit AR stehen hier im Vordergrund. Die Zahl der Unternehmen, die Technologien wie diese implementieren, wird sich laut PwC in den nächsten fünf Jahren verdoppeln.

www.epicor.com

Hier lesen Sie den ausführlichen Bericht.

NEUER STUDIENGANG

© Martin Lifka Photography

Das Bundesministerium für Bildung, Wissenschaft und Forschung (BMBWF) stellt im Rahmen des Fachhochschulentwicklungs- und Finanzierungsplans zusätzliche Studienplätze für den FH-Sektor bereit. Die **FH St. Pölten** erhält für den Master Studiengang „Cyber Security und Resilience" 30 neue Studienplätze. Ziel des Studiengangs ist es, die Studierenden bestmöglich auf eine herausfordernde Tätigkeit im Bereich Cyber Security vorzubereiten. Die Absolventen verfügen nach Abschluss über das notwendige Know-how für eine Absicherung digitaler Services in Unternehmen und Institutionen. Der praxisnahe Studiengang ist als duales und berufsfreundliches Studium organisiert. Die enge Zusammenarbeit mit Kooperationspartnern aus Wirtschaft und Forschung will den Studierenden eine praxisnahe Ausbildung ermöglichen. Synergien mit fachlich verwandten Studiengängen an der FH St. Pölten werden genutzt und ermöglichen eine interdisziplinäre Ausbildung. Das Studium wir in englischer Sprache abgehalten. Der neue Studiengang wird nun im Detail ausgearbeitet, geplanter Start – vorbehaltlich der Genehmigung durch die AQ Austria – ist im Herbst 2020.

www.fhstp.ac.at

IVALUA ERWEITERT FÜHRUNGSTEAM

Ivalua erweitert mit Pascal Bensoussan als Chief Product Officer (CPO) sein Führungsteam. In dieser neu geschaffenen Funktion wird Bensoussan die strategische Ausrichtung, die Roadmap sowie die Go-to-Market-Planungen für die Cloud-basierte Plattform von Ivalua verantworten. Die neue CPO-Rolle soll die umfangreichen Investitionen von Ivalua in noch schnellere Innovationen und in den Erfolg der Kunden verstärken. Bensoussan setzt sich intensiv für die Transformation von Unternehmen mit Hilfe von Technologien ein. Er ist häufiger Keynote Speaker und Board-Mitglied einiger Startups. „Bei allem, was wir tun, muss der Kunde im Zentrum stehen", betont Pascal Bensoussan. „Ich freue mich darauf, vertrauensvoll und partnerschaftlich mit den Kunden von Ivalua zusammen zu arbeiten, um ihre digitale Transformation zu beschleunigen. Wir wollen das volle Potenzial ihrer Beschaffung und ihrer Lieferketten erschließen."

Pascal Bensoussan, Chief Product Officer (CPO) von Ivalua

www.ivalua.com

WANDEL ERFORDERT NEUES MINDSET

©Dietmar Wajand

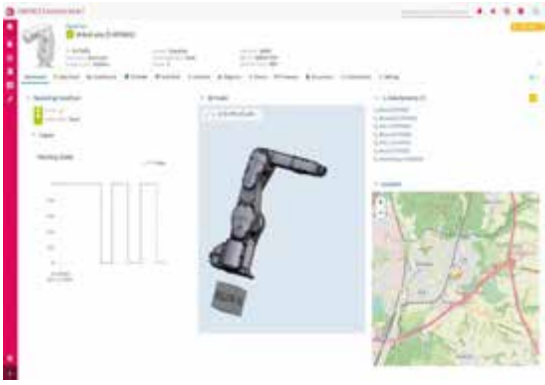
V.l.n.r.: Dieter Jandl (addIT), Martina Klementin (Moderation), Matthias Strolz (Keynote), Johann Martin Schachner (Atos Österreich)

Am 3. Oktober fand zum 12. Mal die addSUCCESS, Kärntens größte IT-Fachveranstaltung, unter dem Motto „Change your mind" in Klagenfurt statt. Gastgeber **addIT**, ein Atos-Tochterunternehmen, ging gemeinsam mit über 200 Event-Teilnehmern der Frage nach, welche Konsequenzen wirtschaftlich, technisch aber auch in Bezug auf Sicherheitsfragen für Unternehmen notwendig sein werden, um künftig im globalen Wettbewerb bestehen zu können. Die vielen Vorträge und Fachgespräche der IT-Experten beleuchteten die vielschichtigen Herausforderungen und lieferten Angebote, Antworten und Lösungsansätze der Technologiebranche. Bei der Podiumsdiskussion diskutierten die Teilnehmer auch über den Einfluss von globalen Entwicklungen auf ihre Branche und deren Unternehmen.

www.addit.at

CONTACT SOFTWARE UND MITSUBISHI ELECTRIC WERDEN IoT-PARTNER

Contact Software ist neues Mitglied der e-F@ctory Alliance von Mitsubishi Electric. Dieses Partnernetzwerk unterstützt den Mitsubishi Electric-Geschäftsbereich Factory Automation dabei, seinen Kunden passgenaue Komplettlösungen für die intelligent vernetzte Fertigung bereitzustellen. „Mit Elements for IoT können unsere Kunden Komplettlösungen für die digitale Fabrik realisieren, die individuell auf ihre Anforderungen zugeschnitten sind und gegebene Infrastrukturen berücksichtigen", sagt Thomas Lantermann, Senior Business Development Manager e-F@ctory Solution bei Mitsubishi Electric Europe, Factory Automation EMEA. „Durch Contact Software wird die e-F@ctory Alliance um einen starken Akteur ergänzt." Contact Elements for IoT generiert digitale Zwillinge von Mitsubishi Electric-Industrierobotern, um die Betriebsdaten des integrierten Condition Monitorings zu visualisieren und weiter zu verarbeiten. Dabei können Teilprozessanlagen eines übergreifenden Prozesskontextes ergänzt werden, etwa um vordefinierte Aktionen automatisch anzustoßen – z. B., wenn Produktionsprozesse zu optimieren sind oder Wartungsaufgaben anstehen.



www.contact-software.com

NEUER LEITER AZURE CLOUD BEI MICROSOFT ÖSTERREICH

Alexander Thiede (47) übernimmt ab sofort die Position des Business Group Lead für Cloud und Enterprise bei **Microsoft Österreich**. Ausgerüstet mit 20 Jahren IT-Branchenerfahrung und fundierter Führungskompetenz von Cloud-Transformationsprojekten, ist der gebürtige Wiener in dieser Rolle für die Geschäftsbereichsentwicklung der Microsoft Azure Cloud in Österreich verantwortlich. Thiede konnte zuvor bereits umfangreiche Erfahrungen bei Microsoft sammeln. Er war in den Bereichen Cloud Transformation von Business Intelligence & CRM bei Microsoft International tätig und für die Entwicklung von digitalen Strategien für Sales & Marketing und internationalen Change Management-Projekten zuständig. Zuletzt war er als Cloud Solution Architect bei den größten österreichischen Microsoft Azure-Kunden im Bereich Cloud Enablement, Data & AI aktiv. Nach abgeschlossenem Studium an der TU Wien startete Alexander Thiede seine Karriere als selbständiger IT Berater. 2002 folgte der Wechsel zu Microsoft Österreich, wo er als IT & Cloud-Experte in verschiedenen Abteilungen in Österreich, Western Europe und international tätig war.

Alexander Thiede
Business Group Lead für Cloud und Enterprise
Microsoft Österreich

www.microsoft.com

IoT ZWISCHEN UTOPIE UND DYSTOPIE

Um die gemeinsame Sprache und Standards für die Verständigung in der Welt des IoT ging es beim 3. IoT Fachkongress von Austrian Standards am 23. Oktober in Wien. Mit dabei war auch eine Delegation russischer Geschäftsleute und Wissenschafter. Eine vernetzte Welt wirft aber auch viele ethnische Fragen auf. Christopher Frauenberger, Forscher an der TU Wien, sprach von einer Verschiebung der Machtverhältnisse im Sinne von Produktivität und Effektivität. „Technologie wirft nicht nur Fragen auf, sondern schafft auch Möglichkeiten", hieß es. Und 5G ist eine der Technologien, die gerade im IoT-Bereiche viele Türen öffnet. Für den Lead-Partner der Veranstaltung (Drei) sprach Elisabeth Rettl, Senior Head of Drei Business, darüber, dass das mehr an Bandbreite, nicht nur eine größere Menge an vernetzten Geräte ermöglicht, sondern aufgrund der besseren Latenzzeiten auch in sicherheitskritische Anwendungen Anwendung findet. Im Themenblock Smart Mobility standen autonome Fahrzeuge, im Zentrum des Interesses. Der nächste Termin steht ebenfalls fest: 4. November 2020.

www.austrian-standards.at

STANDARDISIERTE CLOUD

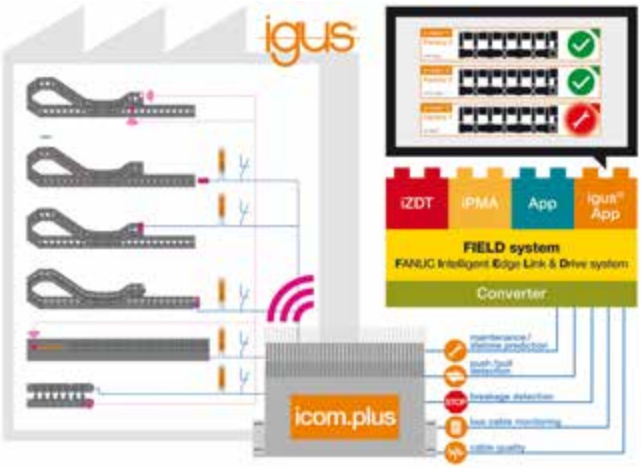
Cloud Computing hat sich in den letzten Jahren flächendeckend durchgesetzt mit einer steigenden Vielfalt an Lösungen verschiedener Anbieter. Das Problem: Unterschiedliche Vorgaben und inkompatible Schnittstellen erhöhen den Aufwand und machen die Verbindung über Cloudgrenzen hinweg sehr komplex. **Harting** beteiligt sich deshalb an einer Initiative für einen einheitlichen Standard zur Cloud-übergreifenden Kommunikation. Diese Standardisierungsinitiative DIN SPEC 92222 besteht aktuell aus 31 Unternehmen, Verbänden und Forschungsinstituten. Betrachtet wird hierbei die Kommunikation von Maschinen (bzw. sogenannter Edge-Geräte) in die Cloud eines fertigenden Unternehmens sowie unternehmensübergreifend zu weiteren Cloud-Systemen.

Die DIN SPEC 92222 realisiert ein Referenzmodell für die industrielle „Cloud Federation". Das Ziel: Eine durchgängige und standardisierte Kommunikation vom Feldgerät bis zur Multi-Cloud-Applikation auf Basis von OPC UA. Beteiligt sind Unternehmen wie Bosch, IBM, Fujitsu, Kuka, Microsoft, die Verbände VDMA und Bitkom sowie Forschungsinstitute von Fraunhofer. Für das Ziel einer durchgängigen und standardisierten Kommunikation soll die Zahl der einzusetzenden Technologien, Normen und Standards minimiert werden. Als Voraussetzung für eine Multicloud-Infrastruktur werden für das Routing zwischen Clouds einheitliche Schnittstellen definiert.

www.harting.com

SMART FACTORY MIT IoT

Um Daten von Maschinen und Anlagen zentral auswerten zu können, stellte Fanuc seine neue offene industrielle IoT-Plattform Fanuc Intelligent Edge Link & Drive System (kurz: Field) auf der EMO vor. Mit dem Field System können sich Produktionsmaschinen miteinander vernetzen. Dazu kann es sowohl on premise oder zukünftig mit Cloud-Anbindung arbeiten. Das System sammelt und analysiert die Maschinendaten vor Ort. So können die Betriebsdaten sowie auch Sensordaten der Maschinen über nur einen Server zentral gesammelt und abgerufen werden. Die Effizienz lässt sich einfach überwachen, Produktionsabläufe beschleunigen sowie Wartungseinsätze planen. Durch die Offenheit der Plattform sind alle Maschinen ans System anschließbar. Apps für das System werden von Fanuc sowie von Drittanbietern angeboten. So hat auch der motion plastics Spezialist **igus** jetzt eine App für seine Smart Plastics entwickelt und der Field-Plattform zu Verfügung gestellt. Mit der Einbindung der igus Smart Plastics App können Anwender den Zustand ihrer Energieketten und Leitungen jederzeit überwachen und die Wartung vorausschauend planen. Zukünftig wird auch der Zustand von Rundtisch-, Linear- und Gleitlagern mit der App überwachbar sein.



Unter dem Namen isense führt igus Sensoren unterschiedlichster Art, die den Zustand der igus-Komponenten erfassen. Sie messen unter anderem im laufenden Betrieb den Verschleiß und geben Alarm, sobald eine Reparatur oder ein Austausch erforderlich ist. Das Kommunikationsmodul icom.plus stellt die igus-Daten über einen integrierten OPC UA-Server bereit. Diese werden über den Fanuc-Converter in die Plattform übernommen.

www.igus.at

VERANSTALTUNGSKALENDER

DEZEMBER 2019

StrategieTage Information Technology
3.-4.12.2019 | Zürich

StrategieTage IT Security
3.-4.12.2019 | Zürich

WorldCIS – World Congress on Internet Security
9.-11.12.2019 | London

IT-Tage 2019
9.-12.12.2019 | Frankfurt/Main

JÄNNER 2020

CES
7.-10.1.2020 | Las Vegas

Software Quality Days
14.-17.1.2020 | Wien

Japan IT Week
29.-31.1.2020 | Osaka

The Things Conference
30.-31.1.2020 | Amsterdam

FEBRUAR 2020

ScaleUp 360° Automotive AI
4.-5.2.2020 | Digitalveranstaltung

CPX 360 – Cyber Security Summit and Expo
4.-6.2.2020 | Wien

Smart Building Conference ISE
10.2.2020 | Amsterdam

ScaleUp 360° Smartes Variantenmanagement
11.-12.2.2020 | Digitalveranstaltung

The Smart City Event
11.-14.2.2020 | Fort Lauderdale

Industrial IoT Conference
11.-14.2.2020 | Fort Lauderdale

IoT Evolution Expo
11.-14.2.2020 | Fort Lauderdale

Intelligent Edge Expo
11.-14.2.2020 | Fort Lauderdale

SCSD - Swiss Cyber Security Days
12.-13.2.2020 | Freiburg

Smart Factory Expo
12.-14.2.2020 | Tokio

EuroCIS
16.-20.2.2020 | Düsseldorf

Bosch Connected World
19.-20.2.2020 | Berlin

embedded world
25.-27.2.2020 | Nürnberg

DMS – Design Engineering & Manufacturing Solutions Expo
26.-28.2.2020 | Tokio

MÄRZ 2020

TECH.AD Europe
2.-3.3.2020 | Berlin

Command Control – Cybersecurity
3.-4.3.2020 | München

Cyber Security Fairevent
4.-5.3.2020 | Dortmund

ScaleUp 360° Cognitive Business Automation
4.-5.3.2020 | Digitalveranstaltung

StrategieTage Information Technology
10.-11.3.2020 | Köln

ScaleUp 360° Big Data
11.-12.3.2020 | Digitalveranstaltung

Smart IoT
11.-12.3.2020 | London

Cloud Expo Europe
11.-12.3.2020 | London

Data Centre World
11.-12.3.2020 | London

Cloud & Cyber Security Expo
11.-12.3.2020 | London

Big Data & AI World
11.-12.3.2020 | London

Blockchain Tech World
11.-12.3.2020 | London

Industry of Things World USA
12.-13.3.2020 | San Diego

IoT Tech Expo
17.-18.3.2020 | London

Cyber Security & Cloud Expo
17.-18.3.2020 | London

Blockchain Expo
17.-18.3.2020 | London

AI & Big Data Expo
17.-18.3.2020 | London

5G Expo
17.-18.3.2020 | London

Twenty2X – Neue Messe für IT-Lösungen
17.-19.3.2020 | Hannover

VORSCHAU

IoT4 NR. 1 | MÄRZ 2020

Erscheinungstermin: 3. März 2020 | Anzeigenschluss: 17. Februar 2020

TWENTY2X: WER HAT DIE BESTE LÖSUNG?

„Wir haben diese neuen Formate gemeinsam mit unseren Ausstellern und potenziellen Besuchern entwickelt", erklärt Jutta Jakobi, Global Director Digital Business bei der Deutschen Messe AG und verantwortlich für die Twenty2X. Wann geht's los? Im kommenden März 2020 (17.-19.). Den Besuchern sollen zahlreiche Möglichkeiten über die Chancen der Digitalisierung geboten werden mit dem Fokus KMU. „Für die meisten IT-Herausforderungen gibt es nicht nur eine Lösung", hieß es weiter. In der kommenden Ausgabe geben wir einen Einblick in das neue Veranstaltungsformat und informieren im Vorfeld ausführlich über die Twenty2X und dann live vor Ort.

SMART CITIES 2020

Wiens sozialer Wohnbau ist weltweites Vorbild, wie jetzt die UNESCO anerkennt. Anlässlich des Internationalen Tages der Städte (World Day of Cities am 31. Oktober 2019) haben die UNESCO und Netexplo, ein Unternehmen im Feld der Zukunfts- und Innovationsforschung, zehn Weltstädte für ihre Spitzenleistungen in bestimmten Gesellschaftsfeldern prämiert. Wien erhielt den Preis für seine „innovative, intelligente, vernetzte und ausdrücklich nachhaltige" Wohnbaupolitik. Was Städte 2020 alles leisten müssen und wie smart sie wirklich schon sind zeigen wir in der kommenden Ausgabe.

Impressum

Medieninhaber und Verleger:
Technik & Medien Verlags Ges.m.b.H.
Traviatagasse 21-29/8/2, 1230 Wien
Tel.: +43/(0)1/ 876 83 79-0
Fax: +43/(0)1/ 876 83 79-15

Chefredaktion:
Stephanie Englert
+43/(0)676/848 205 11
s.englert@technik-medien.at

Freie Mitarbeiterin:
Mag. Barbara Sawka

Anzeigenverkauf:
Thomas Lunacek, DW 13
+43/(0)676/848 205 13
t.lunacek@technik-medien.at

Mag. (FH) Gudrun Lunacek
+43/(0)676/848 205 12
g.lunacek@technik-medien.at

Administration, Redaktionsassistenz, Abo-Service:
Gilda Csokor, DW 14
+43/(0)676/848 205 14
g.csokor@technik-medien.at

Anzeigenverkauf Schweiz:
Arack-Media
Tel.: +41 62 87 19 162
info@arack.ch

Art Direction:
Tom Sebesta

Druck:
Ferdinand Berger & Söhne GmbH
Wiener Straße 80, 3580 Horn

Der Verlag nimmt Manuskripte zur kostenlosen Veröffentlichung an. Honorare ausschließlich nach Vereinbarung. Für unverlangt eingesandte Manuskripte wird keine Verantwortung übernommen. Nachdruck oder Kopien von Beiträgen bzw. Teilen davon nur mit Genehmigung. Der Verlag behält sich vor, Beiträge auch in anderen verlagseigenen Zeitschriften zu publizieren bzw. für Sonderdrucke zu verwenden. Das Copyright der Bilder liegt, wenn nicht anders angegeben, bei den jeweiligen Firmen bzw. beim Verlag.

3. Jahrgang
©2019 by Technik&Medien Verlag GmbH,
Auflage: 13.000 Exemplare

Der Kunde haftet gegenüber Technik & Medien Verlagsges.m.b.H. dafür, dass die von ihm überlassenen Lichtbilder und Beiträge sein uneingeschränktes Eigentum darstellen, er hinsichtlich derselben über die uneingeschränkten Urheberrechte bzw. Weitergaberechte verfügt und insofern berechtigt ist, diese der Technik & Medien Verlagsges.m.b.H. zur geschäftlichen Verwertung, Veröffentlichung und Verbreitung zu übergeben und verpflichtet sich, die Technik & Medien Verlagsges.m.b.H. hinsichtlich sämtlicher Schäden, Aufwendungen und Nachteile schad- und klaglos zu halten, welche aus der Verwendung derselben ihr erwachsen. Weiters haftet der Kunde dafür, dass durch die überlassenen Lichtbilder und Beiträge sowie deren Inhalte in keinerlei Rechte (insbesondere Urheberrechte, Markenrechte, Musterreche, Persönlichkeitsrechte etc.) Dritter eingegriffen wird und auch keinerlei Persönlichkeitsrechte abgebildeter Personen verletzt werden. Auch diesbezüglich übernimmt der Kunde die Verpflichtung zur Schad- und Klagloshaltung.
Aus Gründen der besseren Lesbarkeit verzichten wir auf die parallele Nennung männlicher und weiblicher Sprachformen. Sämtliche Personenbezeichnungen gelten selbstverständlich für beide Geschlechter.

MM
MASCHINENMARKT

DAS FACHMAGAZIN FÜR ÖSTERREICHS INDUSTRIE

MM SONDERAUSGABE PUMPEN MIT ANBIETERVERZEICHNIS! MM 1/2020

ANZEIGEN- & REDAKTIONSSCHLUSS: **7. JÄNNER 2020**
ERSCHEINUNGSTERMIN: **28. JÄNNER 2020**

SONDERTHEMEN 2020 IM MM

MM 2: **KI IN DER FABRIK VON MORGEN** | Was kann ein moderner Betrieb alles leisten?
MM 3: **HANNOVER MESSE + PARTNERLAND INDONESIEN**
MM 4a: **SMART WIEN** | Sonderausgabe
MM 4b: **INTERTOOL** | Sonderausgabe
MM 5: **LEBENSMITTELINDUSTRIE** | Sonderausgabe
MM 6-7: **WIRTSCHAFTSMARKT JAPAN**
MM 8: **ENERGIE** | Effiziente Gewinnung und Verteilung
MM 9: **ELEKTROMOBILITÄT** | Alternative Antriebe im Fokus
MM 10: **LEBENSMITTELINDUSTRIE** | Prozesstechnik, Kennzeichnung, Verpackung
MM 11: **ADDITIVE FERTIGUNG** | 3D-Druck im Visier – Methoden und Möglichkeiten
MM 12: **MEDIZINTECHNIK** | Smarte Produktionstechnologien für den Patienten

Alle Termine auf **www.maschinenmarkt.at** unter „Mediadaten“

SO LIEST MAN HEUTE TECHNIK.

TECHNIK & MEDIEN VERLAGSGMBH

www.maschinenmarkt.at

ORANGE BOX –
Sprechen Ihre Maschinen IoT?

www.br-automation.com/Orange-Box

IoT-Upgrade für Bestandsanlagen

- Gebrauchsfertige Lösung
- Unabhängig vom Steuerungshersteller
- Skalierbar von der kleinen Maschine bis zur großen Anlage
- Höhere Produktqualität
- KPIs für Transparenz im Produktions-prozess

PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP