IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

1 | 2021
Erscheinungstermin:
8. März 2021
www.iot4industry.at

3 x jährlich

Interview mit Reinhard Mayr, Head of Information Security & Research Operations Copa-Data

DAS ZENON SERVICE GRID VERVOLLSTÄNDIGT DIE SOFTWAREPLATTFORM

Im Fokus
EIN LUKRATIVES GESCHÄFT

Im Fokus
MYTHEN DER IoT-SICHERHEIT

Im Gespräch
AUFMACHEN – UMDENKEN!

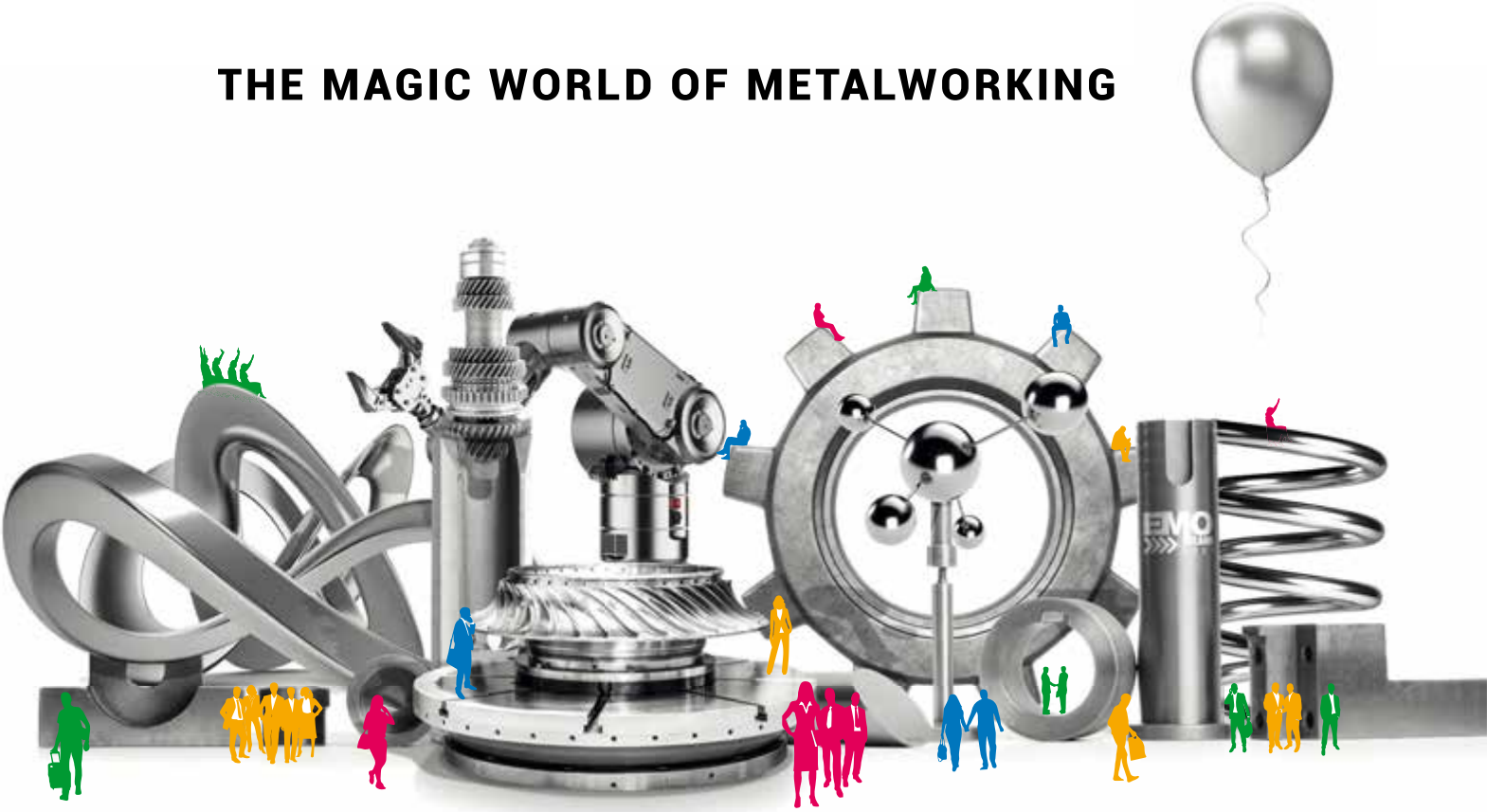
TECHNIK & MEDIEN VERLAGSGMBH

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

EMO MILANO 2021

fieramilano 4-9 October

THE MAGIC WORLD OF METALWORKING



emo-milan.com

FONDAZIONE UCIMU

ITA ITALIAN TRADE AGENCY

EFIM

FIERA MILANO

Find here all the information to plan your participation at EMO MILANO 2021

AUS SCHADEN WIRD MAN KLUG – ODER?

Man unterscheidet in der Biologie zwischen dem obligatorischen und dem fakultativen Lernen. Ersteres ist das so genannte „notwenige“ Verhalten des Menschen, um zu überleben, Letzteres ist ein Verhalten, das zwar Vorteile erschafft, aber für das Überleben nicht unbedingt notwendig ist. Der derzeitige Hype um die neue App Clubhouse wäre so ein fakultatives Lernen. Ich gebe zu, auch ich darf den „neuesten Trend“ gerade aktiv mitverfolgen und gehöre zu den iPhone-Usern. In einer sehr kleinen, im eigenen Umfeld getätigten Umfrage kam heraus, die meisten haben kein Apple iPhone oder finden Clubhouse „nicht überlebenswichtig“. Ich bin ehrlich gesagt noch unschlüssig.

Wie so oft ist es bei einer App nicht nur die Frage, welchen Nutzen sie für mich ganz persönlich als Anwender hat, sondern auch: Was gebe ich preis? Bodo Ramelow, Ministerpräsident in Deutschland, war sich dessen zu Beginn eher weniger bewusst. Sein „naives“ Verhalten spiegelt jedoch auch wider, wie oft sich User im Internet „fehlverhalten“. Im Clubhouse-Fall Ramelow ging es letztendlich um den eigenen Ruf und das Vertrauen der Bürger in die Politik. Doch wenn Internetnutzer durch ihr Fehlverhalten dem Unternehmen schaden, in dem sie etwa Viren in das Firmengeflecht einschleppen, dann ist das zwar auch ein unerwünschtes Fehlverhalten, aber kann man in diesem Fall dem Mitarbeiter zur Gänze die Schuld auflasten?

Phishing-E-Mails, Deep Fakes, USB-Sticks ... all das haben wir bereits gehört oder gelesen, dass es das gibt und dass es gefährlich werden kann. Doch in einem Moment, in dem im Homeoffice mehr Ablenkung herrscht als nötig, der PC oder Laptop auf die Schnelle auch für Firmenarbeiten genutzt werden muss, passiert es öfter als gedacht, dass der Feind bereits im Firmengeflecht eingedrungen ist. Wer haftet für den Schaden? Wer ist verantwortlich? Diese Fragen beschäftigen derzeit viele, genauso wie die Frage: Wie lange gibt es das Homeoffice noch „nach“ der Pandemie? Oder ist es zu gefährlich?
Können sich Vorgesetzte auf Mitarbeiter in der Ferne wirklich zu 100 % verlassen? Funktionieren Anweisungen per Zoom? Was kann ich den Kollegen zutrauen? Ich denke die Antwort ist eindeutig: Nur wer seinem Team gegenüber Vertrauen ausspricht und selber ein Vorbild ist, der kann auf einen guten Rückhalt und ein gutes Ergebnis hoffen. Das wird auch der Grund sein, weshalb zwar einige Journalisten sich über das Fehlverhalten Bodo Ramelows zu genüge äußerten, er sich aber nachwievor im Amt befindet. Vertrauen hin oder her, jeder macht Fehler. Das ist ja auch ein biologisches Verhalten, man lernt aus Fehlern dazu.

Ich hoffe, dass wir Ihnen mit unserem erneuten Schwerpunkt zum Thema Security in der Ihnen vorliegenden Ausgabe auch einen Mehrwert bieten und Sie Neues erfahren. Und wer jetzt auch neugierig auf Clubhouse geworden ist, auch hier entsteht der Mehrwert durch die Anwendung. Seien Sie neugierig, vielleicht treffen wir uns bald in einem „Raum“, etwa zum Thema „Security“.

Bleiben Sie gesund!

Stephanie Englert, Chefredakteurin

INHALT
MÄRZ 2021

22
Kryptowährungen erfahren derzeit einen wahren Hype. Der Bitcoin steigt im Wert und sogar Elon Musk von Tesla heizt das Feuer mit an. Zu Recht? Michael Mertens, CEO der CryptoTec GmbH und Experte auf diesem Gebiet gab Antworten und das, obwohl er derzeit ziemlich gut beschäftigt ist.

Coverstory

Das zenon Service Grid vervollständigt die Softwareplattform. Hierzu Reinhard Mayr, Copa-Data, im Interview.

www.copadata.com

Lesen Sie mehr ab Seite 12!

IM FOKUS

6 Catch me if you can
8 News Security
12 Coverstory | Zukunft willkommen
14 Interview Coverstory: Ein sicherer Zugriff | Reinhard Mayr, Copa-Data
16 Coverstory | Alles im Blick
18 Ein lukratives Geschäft | Stefan Dydak, HP
21 Gastkommentar | Klimawandel in der IT-Sicherheit
22 „Die Bitcoin-Blockchain ist vermutlich das sicherste IT-System“ | Michael Mertens, CryptoTec
24 Die Mythen der IoT-Sicherheit
27 Gastkommentar | Rundum abgesichert

IM GESPRÄCH

28 „Wir wollen mit gutem Beispiel vorangehen“ | Stefan Lau, ABB
31 Gastkommentar | Vorsicht Falle!
32 Aufwachen – Umdenken! | Roman Oberauer, NTT Ltd.
34 Das weltweit größte Software-Ökosystem
36 Interview: Mehr Gestaltungsmöglichkeiten | Stefan Bina, B&R

SECURITY | BIG DATA | CLOUD COMPUTING

37 Ihre Verbindung wird gehalten
40 Herausforderung digitales Engineering
42 Es bewegt sich was
45 Gastkommentar | Fertigungsoptimierung dank Blockchain
46 Let me be your friend
50 Spatial Computing kann die Industrie transformieren
52 Entscheiden Sie!
54 Die Macht des Wollens
56 Im digitalen Flow

STÄNDIGE RUBRIKEN

65 Veranstaltungen
66 Impressum | **Vorschau**

3 x jährlich

IoT4 INDUSTRY&BUSINESS

32

Kürzlich ist die Studie „Future Disrupted: 2021" mit den wichtigsten Prognosen zu aktuellen Technologietrends erschienen. Im Interview stellt Roman Oberauer, Vice President go to Market & Technical Services, NTT Ltd. in Österreich eindeutig klar, dass Österreich zwar auf dem richtigen Weg sei, bei der digitalen Transformation. Dennoch sei auch noch viel Luft nach oben vorhanden.

46

KI – Feind oder Freund? So einfach lässt sich das nicht beantworten oder ist es gar eine falsch formulierte Frage? Was genau ist KI und was eher nicht? In Gesprächen mit Experten kristallisiert sich ein eindeutiges Bild heraus: der freundschaftliche Weg ist der produktivere.

[AT12-19G]

XPlanar®: Schwebend, kontaktlos, intelligent!

Freie 2D-Produktbewegung mit bis zu 6 Freiheitsgraden

www.beckhoff.com/xplanar

XPlanar eröffnet neue Freiheitsgrade im Produkthandling:
Frei schwebende Planarmover bewegen sich über individuell angeordneten Planarkacheln auf beliebig programmierbaren Fahrwegen.

- Individueller 2D-Transport mit bis zu 2 m/s
- Bearbeitung mit bis zu 6 Freiheitsgraden
- Transport und Bearbeitung in einem System
- Verschleißfrei, hygienisch und leicht zu reinigen
- Beliebiger Systemaufbau durch freie Anordnung der Planarkacheln
- Multi-Mover-Control für paralleles und individuelles Produkthandling
- Voll integriert in das leistungsfähige PC-basierte Beckhoff-Steuerungssystem (TwinCAT, PLC IEC 61131, Motion, Measurement, Machine Learning, Vision, Communication, HMI)
- Branchenübergreifend einsetzbar: Montage, Lebensmittel, Pharma, Labor, Entertainment, …

New Automation Technology BECKHOFF

48%
System HACKED

HOME OFFICE

CATCH ME IF YOU CAN

Cyberbedrohungen nehmen rasant zu und sind zu einem alltäglichen Thema geworden. Die Unübersichtlichkeit wird aber auch durch das steigende Angebot im Internet gefördert. Sichere Passwörter und moderne Endgeräte sowie geschulte Mitarbeiter bedarf es künftig gezielter zu fördern. Von Stephanie Englert

Anfang Februar fand zum ersten Mal in seiner Geschichte der BSI, Deutsche IT-Sicherheitskongress virtuell statt und zwar mit insgesamt mehr als 8.000 Teilnehmern. Und die deutsche Bundeskanzlerin Dr. Angela Merkel gab in ihrem Grußwort zu verstehen, dass auch bei der Vergabe künftiger Fördergelder – etwa im medizinischen Bereich – verstärkt darauf geachtet werde, dass hier mindestens 15 % der Gelder in die IT-Sicherheit zu investieren seien. Der Sicherheitsbedarf wächst, gerade auch im Gesundheitsbereich.
Durch die Pandemie ist bei vielen Unternehmen, aber auch Institutionen die eigene Vulnerabilität mehr als verdeutlicht worden. Zu wenig wurde in Homeoffice-Arbeitsplätze in der Vergangenheit aus fehlendem Vertrauen in die eigenen Mitarbeiter investiert, von Schulungen in puncto eigenem Internet-Verhalten etwa bei Phishing-E-Mails ganz zu schweigen. Viele wissen gar nicht, wie „gefährlich" eine simple E-Mail für das komplette Unternehmen sein kann. Dennoch zeigt sich jetzt: Wer seinen eigenen Mitarbeitern nicht vertraut, wem sollen dann eigentlich die Kunden vertrauen?

Alte Strukturen rächen sich. Derzeit hört man auch immer wieder von einer steigenden Chip-Nachfrage, da nun adhoc in Laptops und Tablets etc. investiert wird. Doch die Zeit zwischen dem nun vermeintlich „sichereren Mitarbeiter" und dem, was derzeit noch viel zu oft stattfindet, nämlich am eigenen privaten Endgerät sensible Firmendaten bearbeiten, ist mehr als gefährlich. Die Angriffsfläche für Hacker ist groß geworden. Und viele Prognosen, was allein 2021 beim Thema Security passieren wird, sagen voraus, dass „der Diebstahl von Daten dramatisch wachsen wird." Es ist ein Spiel mit der Zeit und die haben wir bekanntlich zu wenig. Ein Vergleich mit der momentanen Beschaffung von Covid-19-Impfstoffen kann hergestellt werden: Wer hat richtig gehandelt und wer vorausschauend? Es ist doch so: Fast jeder schaut beim Überqueren einer vielbefahrenen Straße zunächst, ob die Fahrbahn frei, ergo gefahrenfrei ist. Man rennt nicht einfach los. Abgelenkt etwa durch Kopfhörer oder ein Gespräch nimmt die Gefahr für das eigene Leben zu. Doch weshalb agieren wir im Internet und E-Mail-Verkehr oft so sorglos?
Wahrscheinlich, weil die Schmerzgrenze so weit entfernt ist. Wen schmerzt der Angriff in Folge zuerst – dem Unternehmen oder mir selber? Und hierbei stellt sich dann wiederum die Frage, wie stark sich jeder einzelne mit dem Arbeitgeber eigentlich heutzutage noch identifiziert? Ein Zusammenhang wäre möglich.
Festzuhalten ist, dass das Thema Security in all seinen Facetten uns alle, als Arbeitnehmer und -geber, noch sehr lange begleiten wird. Zu den Gewinnern zählen hierbei nicht nur die Unternehmen und Einrichtungen sowie Länder, die bereits fortschrittlich und zukunftsdenkend gehandelt haben, sondern auch der Nachwuchs, der sich jetzt für eine Ausbildung in Richtung IT entscheidet – und zwar nach der Schule, denn auch hier wird gerade in aller Deutlichkeit preisgegeben, wie wenig ernst auch Bildungseinrichtungen Digitalisierung immer noch nehmen.

www.bsi.de

NEUE ARBEITSMETHODEN

Die Covid-19-Pandemie hat die Geschäftswelt quasi auf den Kopf gestellt. Zu den gravierenden Veränderungen gehören etwa die rasche Umstellung auf Remote-Arbeit, die verstärkte Cloud-Nutzung oder die Beschleunigung der digitalen Transformation. Der Wandel in der Arbeitswelt hat neue Sicherheitsanforderungen mit sich gebracht, die Projekte in 2021 dominieren werden. **CyberArk** sieht vier zentrale Herausforderungen für die IT-Sicherheit.

1. Remote-Arbeit: Immer mehr Unternehmen werden mittel- und langfristig auf Remote-Arbeit setzen, dadurch werden verteilte IT-Umgebungen zunehmend zum Status quo. Die Firmen-Firewall auf Netzwerkebene ist für die Sicherheit zu Hause de facto wertlos geworden. Umso wichtiger ist es, den Schutz auf der Endgeräte-Ebene vor Malware zu erhöhen und damit einen wichtigen ersten Eintrittspunkt in das Firmennetzwerk abzusichern. Ein Virenschutz ist an dieser Stelle allerdings nicht ausreichend, unverzichtbar ist vielmehr ein Least-Privilege-Ansatz inklusive starker Authentifizierung für den Nutzer.

2. Social Engineering: Auch Social-Engineering- und Phishing-Angriffe werden weiter zunehmen. Zur Unterstützung solcher Attacken werden künftig wahrscheinlich auch verstärkt Deepfakes eingesetzt. Der erste Schritt zur Unterbindung erfolgreicher Social-Engineering-Angriffe ist der Awareness-Aufbau bei den Mitarbeitern.

3. Automatisierung: Die zunehmende Automatisierung in Unternehmen erhöht ebenfalls die Sicherheitsgefahren, etwa durch Robotic Process Automation im Business-Umfeld oder Automationswerkzeuge wie Ansible im Bereich der IT. Folglich müssen auch Applikationen beziehungsweise ihre Programme und Automatismen eine passende Rechtestruktur besitzen und die Zugänge müssen genauso gesichert und kontrolliert werden wie diejenigen von Personen.

4. Cloud-Nutzung: Auch die stärkere Nutzung von Cloud-Lösungen und -Services ist mit Sicherheitsgefahren verbunden. Eine zentrale Herausforderung besteht darin, dass die hohe Zahl an Cloud-Rechten, die ein User erhalten kann, kaum mehr manuell zu verwalten ist. Erschwerend kommt hinzu, dass die Rechte bei jedem Hyperscaler unterschiedlich benannt werden und unterschiedlich umfangreich sind. Im Hinblick auf die Cloud-Gefahren ist in erster Linie eine unternehmensweite Verankerung von Zugriffsrichtlinien erforderlich, das heißt, ein konsistentes Management von privilegierten Accounts und Zugangsdaten. Zudem sollte ein Unternehmen Tools nutzen, mit denen Tausende von verschiedenen Cloud-Rechten

zentral zusammengeführt und versteckte, falsch konfigurierte oder ungenutzte Berechtigungen ermittelt werden können.

Was kann erwartet werden? „Auch 2021 wird die IT-Sicherheit zu den zentralen Herausforderungen aller Unternehmen gehören. Und dabei ist nicht von einer abgeschwächten, sondern von einer verschärften Gefahrenlage auszugehen. So hat die Covid-19-Pandemie zwar die digitale Transformation beschleunigt, dabei sind aber gleichzeitig vielfach Sicherheitsaspekte zu kurz gekommen", erläutert Michael Kleist, Regional Director DACH bei CyberArk. „Die Erhöhung der IT-Sicherheit werden Unternehmen also im kommenden Jahr verstärkt in Angriff nehmen müssen, und zwar nicht mit Inselösungen, sondern mit einer durchgängigen Sicherheitsstrategie, die unterschiedliche Bereiche und Anforderungen vom Homeoffice bis zur Cloud abdeckt."

www.cyberark.com

RENOMMIERT

Die **Schweizer Spitch AG**, Spezialist für Sprachverarbeitungssysteme von der Stimmerkennung bis zur Künstlichen Intelligenz, ist unter die Top 100 CyberTech Companies des Jahres

2020 nach eigenen Angaben gewählt worden. Die von der Analysten-Denkfabrik **FinTech Global** veröffentlichte Aufstellung der 100 innovativsten Hightech-Unternehmen für die internationale Finanzbranche gilt als eine Krönung in der Branche. „Diese Unternehmen sollte jede Finanzinstitution kennen, wenn es um die strategische Entwicklung ihrer Informationssicherheit und Verbrechensbekämpfung geht", urteilt FinTech Global.

Die Analysten schreiben dazu: „Die 2020er-Liste benennt die Lösungsanbieter der nächsten Generation, die die Zukunft der Informationssicherheit und CyberTech-Branche bestimmen werden. Die Aufstellung unterstützt Führungskräfte und Cybersecurity-Fachleute bei der Evaluierung, welche Technologielösungen Marktpotenzial besitzen und wahrscheinlich mit Erfolg den nachhaltigsten Einfluss auf die Branche haben werden." Im „Gartner's Market Guide for Speech-to-Text Solutions" (STT-Lösungen) vom Frühjahr 2020 nannte bereits die renommierte Gartner Group den Sprachspezialisten Spitch in einem Atemzug mit Marktführern wie Google, IBM, Microsoft und anderen.

www.spitch.ch

INFIZIERUNGEN STEIGEN

Die Botnet-Gruppierung KashmirBlack hat in den zurückliegenden Monaten mindestens 230.000 Websites infiziert. Die Hacker nutzen dabei eine seit zehn Jahren bekannte Schwachstelle (die PHPUnit RCE Sicherheitslücke) aus und zielen vor allem auf CMS-Systeme wie Wordpress, Joomla oder Drupal ab. Sie profitieren damit von der Corona-Pandemie, die viele Unternehmen zwang, ihre Prozesse schnell zu digitalisieren und auf einfache Web-Frameworks, wie eben Wordpress, setzen mussten. Das Botnet ist derzeit in über 30 Ländern aktiv und installiert automatisierte Schadprogramme auf den gekaperten Rechnern. Das ist das Ergebnis einer sechsmonatigen Untersuchung von Imperva, einem führenden Anbieter von Cybersicherheits-Lösungen.

Die Experten von **Imperva** schätzen das Bot-Netzwerk als überdurchschnittlich ausgereift ein. Die gut durchdachte Infrastruktur kann ohne großen Aufwand um neue Exploits und Payloads erweitert werden; zudem kann das Botnet sich sehr gut tarnen und bleibt so lange Zeit unentdeckt. Der Bot weicht zur Zwischenablage auch auf populäre Command&Controll-Kontrolldomänen wie Pastebin, Github aber auch Dropbox-Server aus. Die Schäden durch die Angriffe sind mannigfaltig und reichen von gestörter Web-Performance bis hin zu Denial-of-Service-Serverausfällen.

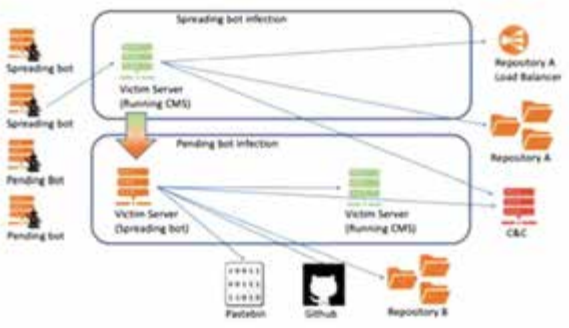


Figure 1: KashmirBlack botnet flow diagram

Sobald ein Server von der Schadsoftware befallen ist, besteht die Gefahr, dass der Bot weitere Server infiltriert – ein Teufelskreis, der zu erheblichen Schäden in Form von zuerst Daten- und dann Einnahmeverlusten bis zur Rufschädigung bei den betroffenen Unternehmen führt.

www.imperva.com

SCHÜTZEN SIE IHR UNTERNEHMEN DURCH ETHICAL HACKING

Der von der Pandemie ausgelöste Digitalisierungsschub bietet Cyberkriminellen neue Angriffsziele. Einzelne Mitarbeiter rücken dabei stärker in den Fokus. Ingram Micro Security bietet vielfältige Services, um gemeinsam effektive, integrierte und skalierbare Sicherheitslösungen zu entwickeln. Das Angebot reicht von Schulungen und Beratungen in den Bereichen Schwachstellenmanagement und Pen Testing bis hin zu Assessment Services.

Um sich im Falle eines Cyberangriffes bestmöglich schützen zu können, muss bereits vor Eintreten des tatsächlichen Vorfalls ein solider Plan zur Aufrechterhaltung des Geschäftsbetriebes erstellt werden. Eine Möglichkeit hierfür bietet das Vulnerability Assessment: Im Zuge der Evaluierung identifizieren und klassifizieren Experten (Sicherheits-) Schwachstellen in der Computer-, Netzwerk- oder Kommunikationsinfrastruktur des Unternehmens. Hierdurch können Angriffspunkte aufgezeigt und akribisch dokumentiert werden. Beim Ethical Hacking, das beispielsweise im Rahmen des Basic Penetration Testing zum Einsatz kommt, führen Spezialisten einen realistischen Hackerangriff durch, um so zu einer konkreten Einschätzung zu gelangen, wie es um die Sicherheit der IT-Systeme und -Infrastruktur bestellt ist.

One-Stop-Shop für Security-Lösungen

Mit zertifizierten Mitarbeitern und einem hausinternen Data Center in München schafft Ingram Micro Security vielfältige Services für Kunden und Partner. Im Fokus stehen dabei vor allem Lösungen, die von einer klassischen Endpoint-Sicherung zur Cloud oder einer hybriden Absicherung führen. Denn bereits bei der Implementierung sollte auf eine zukunftsorientierte IT-Infrastruktur geachtet werden, um auch künftig angemessen Schutz bieten zu können.

Alle Details zum One-Stop-Shop finden Sie unter **at.ingrammicro.com**

Advertorial

SICHERER UMSTIEG

SailPoint Technologies Holdings, Inc. (NYSE: Sail), Spezialist für den Schutz von Identitäten, veröffentlichte eine internationale Studie, die die Sicherheitsrisiken der Fernarbeit aufzeigt. Mitarbeiter stellen demnach stets ein gewisses Sicherheitsrisiko dar, auch im Lockdown. „Als die Pandemie ausbrach, mussten die Unternehmen quasi über Nacht einen Schalter umlegen, um Fernarbeit möglich zu machen. Angesichts dieser Eile konzentrierten sich viele Unternehmen auf die Bereitstellung der Zugriffe und vernachlässigten dabei deren Absicherung. Dies führte zu einer enormen Zunahme ungeschützter Zugriffe auf Technologien im gesamten Unternehmen", so Juliette Rizkallah, CMO, SailPoint (Bild).

Studienergebnisse. Für die SailPoint-Studie wurde eine repräsentative Stichprobe von Verbrauchern im Alter von 18+ Jahren in den USA, Großbritannien, Frankreich, Deutschland, Australien und Neuseeland befragt. Dabei wurde scheinbar harmlosen Vorfällen nachgegangen, die auftreten können, wenn ein Mitarbeiter plötzlich von zu Hause aus arbeitet. Knapp zwei Drittel (66,3 %) der von zuhause aus arbeitenden Befragten in Deutschland gaben an, in den ersten sechs Monaten im Homeoffice gezielte Phishing-Mails, -Anrufe oder -Textnachrichten erhalten zu haben, sei es in privatem oder beruflichem Zusammenhang. Gut jeder fünfte (22,89 %) aus dieser Gruppe sah sich sogar wöchentlich mit solchen Angriffen konfrontiert. Auch mehr als die Hälfte der Befragten im gesamten EMEA- sowie im ANZ-Raum (51 %) haben seit Beginn der Pandemie bereits eine Phishing-Attacke erlebt.

Juliette Rizkallah CMO, SailPoint

Wie die Umfrage von SailPoint weiters ergab, verwendet die Hälfte der Mitarbeiter in der EMEA-Region, Australien und Neuseeland für die Arbeit von zu Hause aus ihre eigenen Computer und Smartphones. In den USA ist dies bei einem von drei Mitarbeitern der Fall. Zugleich zeigen die Erkenntnisse von SailPoint, dass es während der Pandemie immer üblicher geworden ist, zuhause Passwörter weiterzugeben. „Wenn Passwörter für berufliche und private Konten an andere weitergegeben werden, kann das dazu führen, dass zahlreiche Systeme kompromittiert werden", warnt Rizkallah. „Sobald ein Hacker im Besitz dieser Zugangsdaten ist, kann er direkt in das Unternehmensnetzwerk eindringen. Ganz gleich, wie sich die Belegschaft entwickelt: Zugriffe dürfen nicht einfach gewährt werden, sondern müssen kontinuierlich geschützt sein.

Zu einem modernen digitalen Unternehmen gehören zahlreiche neue Tools, Plattformen, Datenbanken, Cloud-Infrastrukturen und mehr. Deshalb benötigt heute jedes Unternehmen eine skalierbare und dynamische Identity-Lösung, um jeden Mitarbeiter und jeden Zugangspunkt zu sensiblen Assets zu schützen, gleich, welches Gerät verwendet oder wo gearbeitet wird – im Büro oder zu Hause."

www.sailpoint.com

REKORDANSTIEG BEI NETZWERKANGRIFFEN

Der vor einiger Zeit veröffentlichte Internet Security Report von **WatchGuard Technologies** für das dritte Quartal 2020 wartet im Hinblick auf die Bedrohungssituation mit einer überraschenden Erkenntnis auf: Denn obwohl im Zuge von Corona die Arbeit aus dem Homeoffice bei vielen Unternehmen weltweit nach wie vor gang und gäbe ist, führte dies auf Seiten der Cyberkriminellen in den Monaten Juli bis September nicht automatisch zu einer Verlagerung der Konzentration auf Endpunkte. Stattdessen standen die klassischen Unternehmensnetzwerke sogar noch stärker als in der Vergangenheit unter Beschuss.

Insgesamt verzeichnen die Experten des WatchGuard Threat Lab für das dritte Quartal 2020 über 3,3 Mio. Netzwerkangriffe, was einer 90-prozentigen Steigerung gegenüber dem Vorquartal entspricht und den höchsten Stand seit zwei Jahren darstellt. Gleiches gilt auch hinsichtlich des Aufkommens ganz neuartiger (Zero-Day)-Bedrohungen. Der Aufwärtstrend bei Angriffsversuchen mit bisher nicht bekannter Signatur ist weiterhin ungebrochen. Daher sollten Unternehmen dem Schutz von Netzwerken und den darin befindlichen Anwendungen sowie Daten nach wie vor hohe Priorität einräumen und dabei gleichzeitig den spezifischen Anforderungen einer zunehmend mobilen bzw. dezentral arbeitenden Belegschaft Rechnung tragen. „Unternehmen kommen künftig einfach nicht mehr umhin, sowohl Netzwerke als auch Endpunkte konsequent abzusichern", so Corey Nachreiner (Bild), Chief Technology Officer bei WatchGuard. „Wichtig ist in dem Zusammenhang ein ganzheitlicher Ansatz, bei dem unterschiedlichste Sicherheitsfunktionalitäten passgenau zusammenspielen. Nur so lässt sich den mannigfaltigen, fortschrittlichen Bedrohungen, die immer häufiger verschlüsselt daherkommen und sich gezielt zu tarnen wissen, Einhalt gebieten." Der vollständige Bericht mit vielen weiteren Details steht online zum Download bereit:

Corey Nachreiner Chief Technology Officer bei WatchGuard

https://www.watchguard.com/wgrd-resource-center/security-report-q3-2020

Der Report beinhaltet dabei auch eine detaillierte Analyse des Twitter-Hacks vom Juli 2020, bei dem 130 Konten prominenter Personen im Zuge eines Bitcoin-Betrugs kompromittiert wurden.

www.watchguard.de

CYBERSICHERHEIT MUSS ÜBER MINDESTSTANDARDS HINAUSGEHEN

„Cybersicherheitsversagen steht im **Global Risk Report 2021** des Weltwirtschaftsforums an vierter Stelle als „eindeutige und aktuelle Gefahr". Dies sollte nicht überraschen, da wir 2020 besonders viel Vertrauen in alles, was mit Technologie zu tun hat, setzen. Rechenleistung war maßgeblich an der Erforschung und Entwicklung von Impfstoffen beteiligt. Betriebstechnologie (OT) innerhalb kritischer Infrastrukturen unterstützt nun die Kühlkette und die Logistik und erleichtert die sichere Lieferung und Lagerung von Impfstoffampullen. Während die Leistungsfähigkeit der Technologie im Jahr 2020 voll zur Geltung kam, kamen auch die potenziellen Fallstricke zum Vorschein. Das Problem bei dieser Art von Vertrauen ist: Wenn wir weiter voranschreiten, ohne zuerst die Sicherheit dieser Technologie zu gewährleisten, werden die Bedrohungen unsere digitale Wirtschaft und Lebensweise immens beeinträchtigen.

Im Jahr 2020 haben wir gesehen, dass Bedrohungsakteure nicht davor zurückschrecken, Schwachstellen innerhalb der Sicherheitsmaßnahmen für finanzielle und sogar politische Zwecke auszunutzen. Während Regulierung und global akzeptierte Rahmenbedingungen effektiv sein können, um die Bedeutung von Cybersicherheitsbemühungen zu erhöhen, ist beides allein nicht ausreichend. Jede Cybersicherheitsinitiative muss über die Erfüllung von Mindeststandardanforderungen hinausgehen und sich mit den tatsächlichen Risiken, denen Unternehmen ausgesetzt sind, befassen. Sie muss die Rolle der Cybersicherheit – als strategische Geschäftsfunktion und kritisches Unternehmensrisiko – aufwerten", kommentierte für **Tenable** Bob Huber (Bild), Chief Security Officer.

Bob Huber
Chief Security Officer

www.tenable.com

INVESTITIONEN GEFORDERT

Securepoint fordert mehr Investitionen für Absicherung von Medizin-IT. Zwei aktuelle Studienergebnisse des BSI (Bundesamt für Sicherheit und Informationstechnik) machen das schlechte IT-Sicherheitsniveau in der Medizin nämlich sehr deutlich. Die dort aufgeführten Sicherheitslücken zeigen, dass Arztpraxen und Krankenhäuser der IT-Sicherheit noch lange keinen ausreichenden Stellenwert beimessen. Der deutsche Hersteller Securepoint hat sich gemeinsam mit seinem spezialisierten Tochterunternehmen „Medical IT Services" vorgenommen, das mit seinen zertifizierten Lösungen der Unified Security zu ändern. Mit diesen lassen sich Medizinumgebungen, wie im Digitale-Versorgung-Gesetz beschrieben, umfassend absichern und geschützt betreiben.

www.securepoint.de

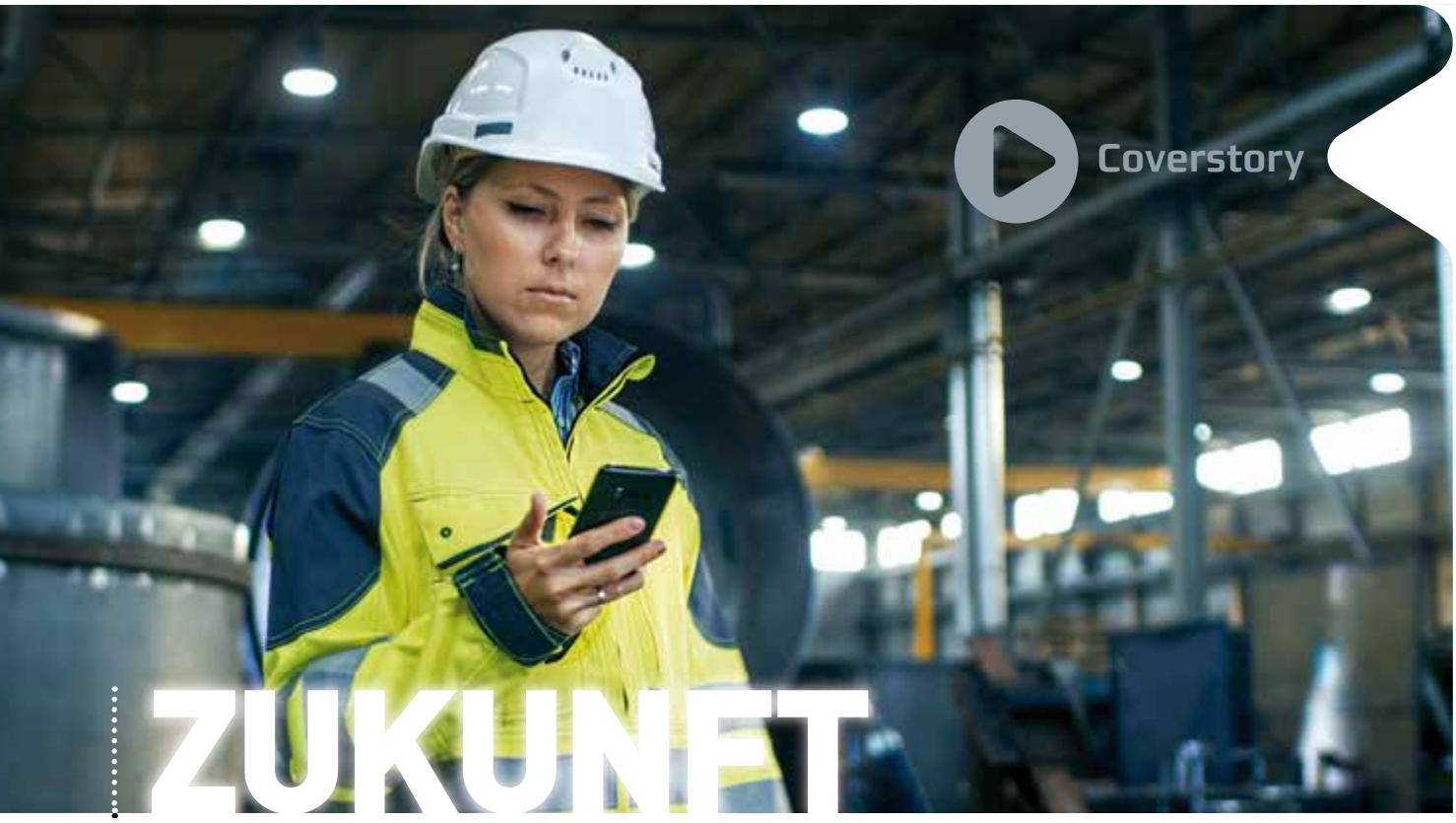
IoT4 INDUSTRY&BUSINESS

SCHLECHTER TREND

Trend Micro veröffentlichte kürzlich neue Studienergebnisse, wonach 23 Prozent der Unternehmen weltweit in den vergangenen zwölf Monaten sieben oder mehr Cyberangriffe erlebten, die ihre Netzwerke oder Systeme infiltrieren.

Die überwiegende Mehrheit (83 Prozent) der befragten Unternehmen erwartet, dass solche Angriffe in den nächsten zwölf Monaten „etwas" bis „sehr" wahrscheinlich erneut vorkommen werden. Die Erkenntnisse stammen aus der neuesten Version des Cyber Risk Index (CRI) von Trend Micro. Dieser Index wird vom unabhängigen Ponemon Institute berechnet und beschreibt die Differenz zwischen dem aktuellen Sicherheitsniveau von Unternehmen und der Wahrscheinlichkeit eines Angriffs.

Das Ponemon Institute befragte im Oktober 2020 weltweit 2.795 IT- und IT-Security-Fachkräfte, davon 824 in Europa. Die vollständige Methodik der Studie ist unter **www.trendmicro.com/cyberrisk** zu finden.



ZUKUNFT WILLKOMMEN

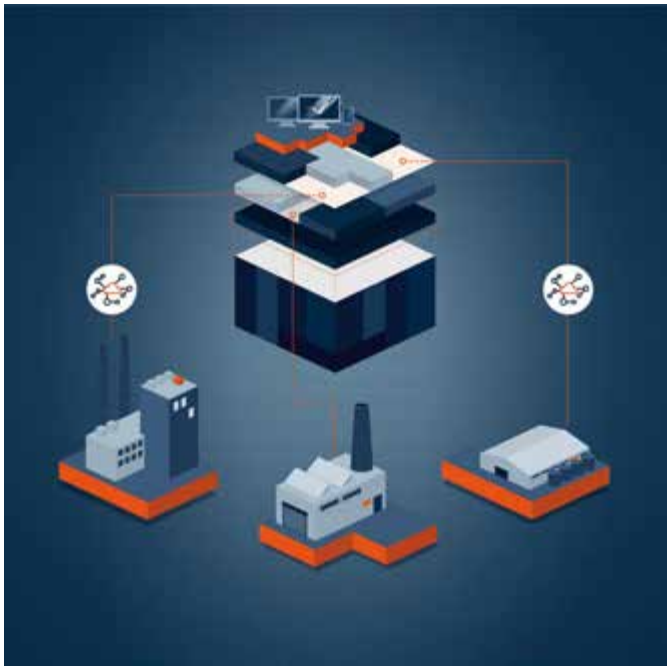
Mit den Werkzeugen der Vergangenheit kann man die Lösungen der Zukunft schlecht umsetzen. Davon ist auch Copa-Data überzeugt. Die technologische Erweiterung der Softwareplattform zenon durch das Service Grid ist ein Schritt in die Zukunft.

Die Softwareplattform zenon von Copa-Data wird zum Werkzeug für die Anwendungen der Zukunft. So lautet das Credo der Salzburger. Denn auch künftig werden Anwendungen im industriellen Umfeld und in der Energiewirtschaft extremen Anforderungen standhalten müssen, etwa robust und stabil zu laufen – oft im permanenten Betrieb, rund um die Uhr. Speziell in der Datenakquise, -verarbeitung und -speicherung, Alarmierung und Anlagensteuerung müssen sich Kunden hundertprozentig auf zenon verlassen können – so der Tenor des Unternehmens. Das war bisher so und wird sich auch in einer vernetzten modernen Welt nicht ändern.

Modularität und Flexibilität. Vorausgesetzt ist immer eine Umgebung, die modular erweiterbar und flexibel anpassbar ist, um Anwendungen auf den initialen Use Case maßzuschneidern und dann trotzdem laufend weiterentwickeln zu können. Bisher unterstützen der modulare Aufbau von zenon und Features wie die Mehrprojektverwaltung diese Anforderungen. Künftig wird die Modularität und Flexibilität von zenon neue Dimensionen annehmen, wenn einzelne Aufgaben auch modular in einer flexiblen Systemarchitektur erledigt werden können. So kann beispielsweise die Anbindung von Drittsystemen über das API-Gateway in der Cloud laufen, während die Datenakquise und -verarbeitung On-Premise an der Maschine erledigt wird.
Dass der Umfang an Datenmengen extrem steigt, dieser Umstand begleitet alle kontinuierlich und seit vielen Jahren. In Folge investierte Copa-Data sehr viel in die Verbesserung der Performance, um die stetig steigende Zahl an Datenpunkten und Datenvolumina meistern zu können. Der Trend geht in die Richtung, nicht mehr nur auf einem physischen Rechner oder einer virtuellen Maschine zu skalieren, sondern Workloads flexibel auf unterschiedliche Ressourcen zu verteilen. Das schafft weitere Möglichkeiten im Handling großer Datenmengen und hilft kritische Bereiche zu entlasten.

Agilität und Wartbarkeit. Einerseits besteht die Anforderung, Softwareanwendungen schnell zu erstellen und anzupassen – andererseits ist es wichtig, diese Anwendungen auch nach vielen

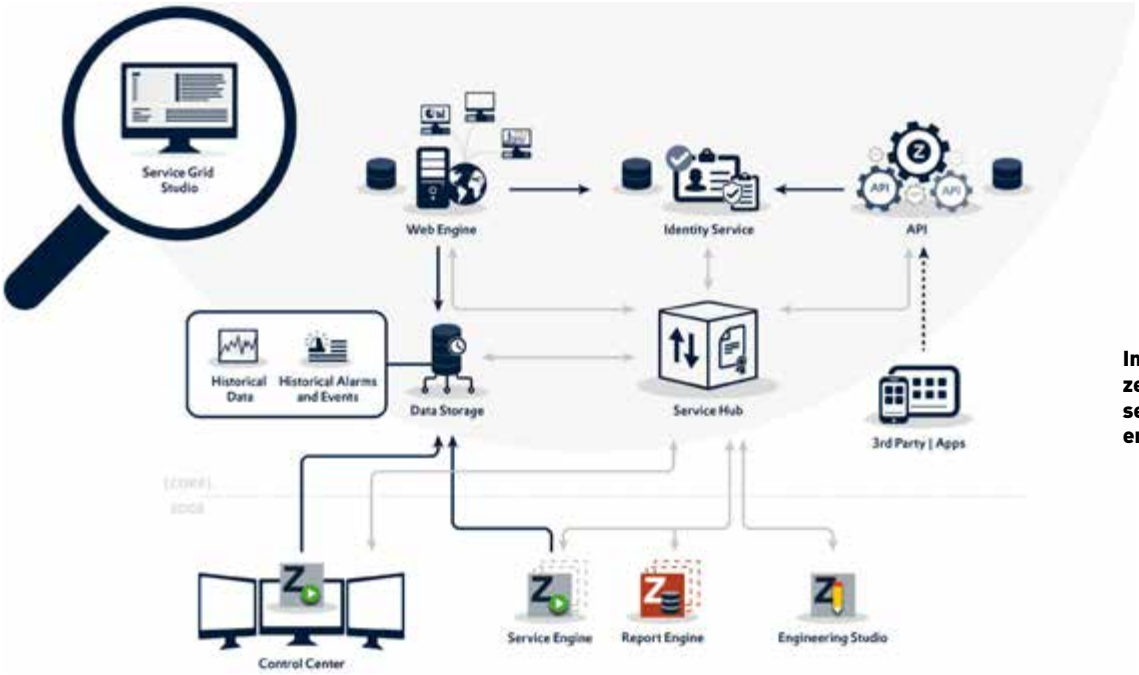
Jahren und über den ganzen Lebenszyklus hinweg übersichtlich und wartbar zu halten. Sie müssen auch wartbar bleiben, wenn sich über die Jahre deren Komplexität deutlich gesteigert hat oder wenn die Mitarbeiter, die eine Anwendung ursprünglich konfiguriert haben, nicht mehr im Unternehmen sind.
Bisher wurde mit konfigurierbaren Anwendungen, einer Projektierung ohne Programmierung, einem zentralen Ansatz in der Projektierung und kontinuierlicher Kompatibilität über Versionen hinweg sichergestellt, dass zenon-Projekte langfristig wartbar und erweiterbar bleiben. Das bleibt auch so in einer Welt, in der zenon serviceorientiert vom Sensor bis zur globalen Vernetzung eine durchgängige Softwareplattform bietet.
Das Zusammenwachsen der Disziplinen der Automatisierung und Unternehmens-IT wird oft als Konvergenz von IT und OT (Operational Technology) bezeichnet. Jahrzehntelang waren wir es gewohnt, dass beide Bereiche autarke Welten waren – nicht nur technologisch, sondern auch organisatorisch und von der Einstellung her. Bisher bedeutete vertikale Integration mit zenon unter anderem die Verbindung der Produktionsebene mit dem ERP- oder MES-System. Das war vorrangig ein Schnittstellen- und Kommunikationsthema. In Zukunft kann sich zenon selbst flexibel vertikal erstrecken. So können einzelne Komponenten der Plattform weiterhin direkt in der Maschine laufen und andere Komponenten im unternehmensweiten Rechenzentrum. Dabei sind alle Komponenten trotzdem Teil eines eingespielten Ganzen.



Mit der ständigen Weiterentwicklung von zenon, wie mit dem Service Grid, versichert Copa-Data seinen Kunden, auf eine langfristig verlässliche und zukunftssichere Softwareplattform zu setzen.

Horizontale Integration. Am komfortabelsten ist es für den Anwender, möglichst viele Disziplinen gleich innerhalb der Softwareplattform zenon abzubilden. Trotzdem gibt es immer wieder Anwendungsfälle, in denen zenon als Teamplayer in einem großen Ökosystem unterschiedlicher Systeme und Technologien agiert. „Bisher haben wir mit offenen Schnittstellen und der Unterstützung von Industriestandards dafür gesorgt, dass zenon perfekt mit dritten Komponenten integrierbar und erweiterbar ist“, erklärt Reinhard Mayr, Head of Information Security & Research bei Copa-Data in Salzburg. „Diese Offenheit führen wir konsequent weiter: Künftig wird zenon nicht mehr nur in der Automatisierung zu Hause sein, sondern auch in der klassischen Unternehmens-IT. Gleichzeitig hilft die Plattform, technologische Brücken zwischen beiden Bereichen zu überwinden.“
Mit der ständigen Weiterentwicklung von zenon, wie beispielsweise mit dem Service Grid, versichert Copa-Data seinen Kunden, auf eine langfristig verlässliche und zukunftssichere Softwareplattform zu setzen.

www.copadata.com



In Zukunft kann sich zenon von Copa-Data selbst flexibel vertikal erstrecken.

>>

Interview

Datenmengen werden seit Jahren kontinuierlich mehr, diese gilt es zu bewältigen.

EIN SICHERER ZUGRIFF

Die Fabrik von morgen ist ein viel gedachtes Phänomen. Doch was macht sie letztendlich aus? Und welche Rolle spielt das zenon Service Grid dabei? Reinhard Mayr, Head of Information Security & Research bei Copa-Data in Salzburg, gibt Antworten. Von Stephanie Englert

IoT 4 Industry & Business: zenon wird bei Copa-Data intern auch als „Werkzeug für die Anwendungen der Zukunft" bezeichnet. Was genau ist damit gemeint und welchen Vorteil gibt es für den Anwender und seine Produktion?

Reinhard Mayr: Schon heute zeigt sich, dass sich die klassischen Architekturen in der Produktion ändern. Verteilte Systeme sind im Kommen. Das bedeutet, dass vor allem Daten, die in der Produktion entstehen, (global) verteilt bzw. integriert werden müssen – und das über die klassische Produktions-Domäne hinaus. Zu den klassischen HMI/Scada/MES-Komponenten kommen neue hinzu, um die Daten in verteilten Strukturen zu sammeln und zu verarbeiten. Dabei geht es um weit mehr als einfache Gateways und Storage-Systeme.

IoT: Können Sie ins Detail gehen?

Mayr: Zum Beispiel an der Edge (dem Übergabepunkt) bedarf es einer gewissen Intelligenz um Daten aufzubereiten (z.B. Semantik oder Vorverdichtung), bevor diese von beispielsweise in der Cloud betriebenen Komponenten durch etwa KI (Künstliche Intelligenz) weiterverarbeitet werden können. Die zenon-Plattform kann schon heute aus einer Hand diese notwendigen Komponenten zur Verfügung stellen und wird sich die nächsten Jahre noch stark in diese Richtung weiterentwickeln. Der Kunde kann frei aus den zenon-Plattform-Komponenten wählen, um für sich daraus die ideale Umsetzungs-Strategie für die Digitalisierung seiner Produktion zu entwickeln. Use Cases, die sich einfach damit umsetzen lassen, wären:

- Security Gateway
- zentrales Steuern und Überwachen von verteilten Infrastrukturen (Standorten)
- sicherer HTML5 Webclient-Zugriff
- REST-Schnittstellen basierter Datenzugriff für Dritt-Systeme

IoT: Durch die zenon-Weiterentwicklung „Service Grid" soll eine langfristige und zukunftsorientierte Serviceplattform geboten werden. Weshalb?

Mayr: Mit dem zenon Service Grid gehen wir erstmals den Weg einer neuen Software und damit neuer Lösungs-Architekturen. Service Grid folgt einer sogenannten Microservice-Architektur und ist daher unter anderem komplett plattformunabhängig bzw. auch in Container und Virtualisierungs-Lösungen enthalten (z.B. auf Basis von Cloud-Plattformen betreibbar). Hinzu kommt, dass Service Grid in naher Zukunft skalierbar sein wird. Sprich: Das System passt sich an die Leistungs-Anforderungen an, es kann automatisch skalieren.

All diese technologischen Faktoren sind die Grundvoraussetzung dafür, neue serviceorientierte Business-Modelle zu entwickeln und auch zu betreiben: Systeme mit hoher Verfügbarkeit, hoher Daten-Durchsatzrate, aber auch andere Verrechnungsmodelle (z.B.: pay per use) werden dadurch erst möglich.

IoT: Was genau bietet das Service Grid nun im Detail?

Mayr: Aktuell handelt es sich vor allem um eine zentrale Daten-Drehscheibe innerhalb der zenon-Plattform. Anders formuliert könnte man auch sagen: Bei Service Grid handelt es sich um die IIoT-Komponenten in der zenon-Plattform.

Das zenon Service Grid ist in der Lage, auf Daten aus dem zenon-Engineering, der zenon-Runtime, aber auch dem zenon-Analyzer zuzugreifen. Diese Daten können dann z.B. über eine standardisierte REST-Schnittstelle an anderen Applikationen zur Verfügung gestellt werden. Das Neue daran ist – neben der Schnittstelle – dass die Daten sicher (verschlüsselt und nur gegen Authentifizierung) und ohne Rückkopplungen auf die zenon-Runtime zur Verfügung gestellt werden können.

Aber auch plattformintern nutzen wir Service Grid bereits, um

Daten zwischen den einzelnen Komponenten auszutauschen oder einen Zugriff über Web-Browser (HTML5) zu ermöglichen. In der aktuellen Version kommt weiters noch ein integriertes Identity Management dazu. Integriert kann dies auch in zentrale Services, wie dem Azure Active Directory betrieben werden.

IoT: Aus welchen Komponenten bzw. Eigenschaften besteht das Service Grid?
Mayr: Im Wesentlichen handelt es sich um einen Satz von Software-Services, die einzelne Aufgaben übernehmen.
Die Wichtigsten sind:

- **Data Hub** – ein zentraler Service, der den Datenaustausch zwischen den einzelnen Services koordiniert.
- **Data Storage:** Als zentraler Datenspeicher im Service Grid für mehrere zenon-Projekte.
- **Identity Services** verwalten die Zugriffsrechte, Benutzer und notwendigen Zertifikate.
- Eine **REST-Schnittstelle** für den Zugriff auf die Daten der zenon-Plattform (oder mehrerer zenon-Plattformen).

IoT: Ist es für Anwender einfach zu installieren?
Mayr: Für den Anwender bieten wir zwei einfache Herangehensweisen an. Wie in zenon gewohnt, gibt es ein Setup für die Windows-basierte On-Premise-Konfiguration; mit wenigen Mausklicks installiert man die neue Komponente. In meinen Augen aber noch komfortabler ist der von uns zur Verfügung gestellte vorkonfigurierte Docker Container mit Service Grid; dieser ist nach dem Deployment direkt verwendbar.

IoT: Wie steht es nun um den Aspekt der Sicherheit? Ist das Service Grid den Herausforderungen dieser Zeit, sprich den zunehmenden Cyberangriffen gegenüber gut gewappnet?
Mayr: zenon Service Grid wurde bereits von Beginn an unter dem Security-Gedanken designed und entwickelt (Security by Design). Wir wollten von Anfang an eine Komponente entwickeln, die einen sicheren Zugriff auf die Daten der zenon-Plattform erlaubt. Wir empfehlen auch den Einsatz des zenon Service Grid, wann immer ein Zugriff bzw. eine Integration von externen Komponenten in der Produktion umgesetzt werden soll.
Service Grid inkludiert dazu alle gängigen Mechanismen zur Verschlüsselung und Authentifizierung, wie zum Beispiel TLS-Verschlüsselung (zertifikatsbasiert) oder auch die Integration externer Identity Services, wie etwa Azure Active Directory.
Ein besonderes Augenmerk lag in der Entwicklung aber auch auf der Rückkopplungsfreiheit zu den anderen Komponenten der zenon-Plattform. Das bedeutet, dass selbst wenn Service Grid einem möglichen Cyberangriff ausgesetzt wird, hat dies keine negative Auswirkung auf die dahinterliegenden Systeme, wie der zenon-Runtime. So kann ein störungsfreier Betrieb der Produktion gewährleistet werden.

IoT: Was muss bei Produktweiterentwicklungen alles beachtet werden?
Mayr: Bei der Entwicklung war es vor allem wichtig, das passende Softwaredesign bzw. die passende Architektur zu finden. Unter anderem mussten wir unsere Coding Guidelines erweitern, aber auch unsere QA-Strategien um beispielsweise das gezielte Vulnerability Monitoring der eingesetzten Komponenten oder Stresstest der Schnittstellen zu berücksichtigen. Geholfen hat uns dabei auch die Zertifizierung unseres SDL (Secure Development Lifecycle) nach IEC 62443-4-1 durch den TÜV Süd. Zukünftig gilt es vor allem am „Ball zu bleiben" und rechtzeitig die passenden Technologien in die Plattform zu integrieren. Durch den modularen und serviceorientierten Aufbau von Service Grid können wir hier aber flexibel auf neue Herausforderungen reagieren.

IoT: Aktuell betrachtet durch die Zunahme von Fernwartung, Homeoffice etc., merken Sie eine erhöhte Nachfrage Ihrer Lösung?
Mayr: Ich würde mal so sagen: Wir konnten zumindest feststellen, dass für uns Ansprechpartner heute zur Verfügung stehen, die sich vor der Krise vermutlich weniger intensiv mit dem Thema Digitalisierung der Produktion und den damit verbundenen Sicherheitsrisiken auseinandergesetzt haben. Das Bewusstsein zu den Möglichkeiten hat sich da doch bei vielen Entscheidungsträgern verändert.
Ich denke, wir konnten die Krise sehr gut nutzen, um uns und unsere Lösungen bei einigen Big Brands zu platzieren und das stimmt uns sehr optimistisch für die kommende Periode und bestätigt uns gleichzeitig in dem, was wir in den letzten Jahren an Arbeit und Know-how investiert haben.

IoT: Abschließend würde ich bitte gerne eine Einschätzung für das laufende Jahr von Ihnen haben. Wird für Copa-Data 2021 die größere Challenge als 2020 werden?
Mayr: Neben den vielen technologischen Herausforderungen und unserem Neubau des zweiten Firmengebäudes wird es sicherlich wirtschaftlich, aber auch organisatorisch ein spannendes Jahr. Zum einen müssen wir die internationalen Entwicklungen in unseren Schlüsselmärkten beobachten und unsere Ziele realistisch gestalten. Aber zum anderen auch – und vor allem in der Organisation – wieder in einen „Regelbetrieb kommen". Dies wird noch eine spannende Challenge. Vor allem bezogen darauf, inwiefern sich die neuen Arten der Zusammenarbeit, der Vertriebsorganisation etc. etablieren werden. Ich denke, hier werden viele neue spannende hybride Arbeitsmodelle entstehen.

IoT: Vielen Dank!

Reinhard Mayr
Head of Information Security & Research bei Copa-Data in Salzburg

„Wir wollten eine Komponente entwickeln, die einen sicheren Zugriff auf die Daten der zenon-Plattform erlaubt."

>>

ALLES IM BLICK

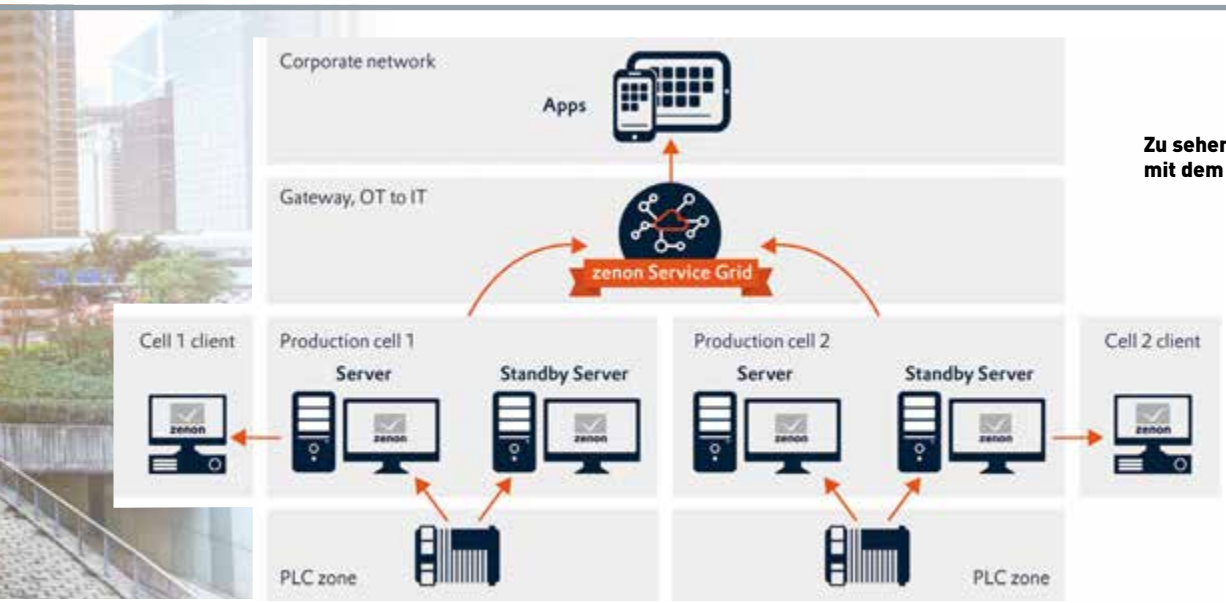
zenon ist bei Anwendern sehr beliebt. Ein Grund ist die einfache Anwendung. Ein anderer Grund ist die Möglichkeit der Erweiterung. Das zenon Service Grid vervollständigt die Softwareplattform vor allem für verteilte Anwendungen.

IoT- und IIoT-Anwendungen kommunizieren über das Internet oder mobile Funkverbindungen, ohne teure, wartungsaufwändige und fehleranfällige VPN-Hardware zu nutzen. Dazu werden IoT-Protokolle wie MQTT oder AMQP für die verschlüsselte, internet- bzw. WAN-fähige Kommunikation verwendet. Diese Protokolle sind so auslegt, dass sie auch über unterbrechungsbehaftete 4G- oder dann 5G-Mobilfunknetze mit niedriger Bandbreite korrekt arbeiten. Neben Protokollen müssen auch die Softwarekomponenten so ausgelegt sein, dass sie bei Netzwerkunterbrechungen Daten puffern und nach erneuter Verbindungsherstellung mit dem übergeordneten System abgleichen. Zudem erfordert der Einsatz im öffentlichen Netz von allen Softwarekomponenten ein schnelles Schließen von Sicherheitslücken. Das zenon Service Grid bietet innerhalb der Softwareplattform zenon all diese Features standardmäßig.
Es besteht aus einem System von modularen Softwarekomponenten, den sogenannten Microservices. Diese kommunizieren untereinander, wodurch sich ein Kommunikationsnetz bildet. Daher kommt der Name Service Grid – ein Netz aus Diensten, in dem jeder einzelne Dienst eine bestimmte Aufgabe übernimmt und das ideal für geografisch verteilte Anwendungen geeignet ist.

Die Komponenten. Der wichtigste Dienst hierbei ist der Service Hub, der aus zwei Komponenten besteht: zum einen dem Data Hub, der als Drehscheibe für die Daten dient, zum anderen dem Hub Controller, der die Nodes verwaltet, also alle angebundenen lokalen Anlagen oder Services. Erst wenn ein Node im Hub Controller autorisiert wurde, kann dieser über eine sichere Verbindung mit dem Data Hub kommunizieren. Der Data Hub überträgt bidirektional Daten zwischen den Diensten des Service Grid oder lokalen Anlagen. So können lokale Anlagen auch gesteuert werden. Sollte einmal ein Endgerät in die falschen Hände geraten, kann ein Administrator den Zugang des Geräts mit wenigen Klicks und mit sofortiger Wirkung sperren.

Neben der sicheren Kommunikation oder der Autorisierung von Geräten ist die Benutzerverwaltung ein wichtiger Baustein von IoT-Plattformen, um Benutzer oder Applikationen zu authentifizieren und zu autorisieren. Authentifizierung bedeutet, die Identität eines Benutzers gegenüber einem System nachzuweisen und zu verifizieren. Das wird im Service Grid durch den Identity Service erledigt. Er verwendet hierfür das Standardprotokoll OAuth 2.0, mit dem Web-Applikationen, Desktop-Applikationen, mobile Geräte und IoT-Geräte authentifiziert werden. Sie können den Identity Service auch als Federation Gateway nutzen, um weitere Verzeichnisdienste wie Microsoft Azure Active Directory, Active Directory Domain Services oder Lightweight Directory Access Protocol (LDAP) anzubinden. Single Sign-on (SSO) erlaubt das einmalige Einloggen im System und die Nutzung verschiedener Komponenten ohne erneute Anmeldung.
Unter Autorisierung versteht man das Zuweisen und die wiederholte Überprüfung von Zugriffsrechten auf Dienste und Ressourcen, beispielsweise auf historische Daten über das Service Grid API. Hierfür wird im Service Grid der Policy Service verwendet.

Die sichere Schnittstelle. Das Service Grid API ist eine webbasierte Programmierschnittstelle, die Zugriff auf Echtzeit- und historische Daten wie Variablenwerte, Alarme und Ereignisse erlaubt. Um Daten von der API abzufragen oder zu ändern, muss sich die Client-Applikation zuvor am Identity Service anmelden, falls noch nicht geschehen. Nach der erfolgreichen Anmeldung erhält die Client-Applikation einen sogenannten Access-Token. Damit können Daten von der API abgefragt oder geändert werden, solange der eingeloggte Benutzer die notwendigen Rechte dazu besitzt.
Das Service Grid API wurde nach der für Programmierer üblichen Methode Representational State Transfer (REST) entwickelt. Diese Web-Service-Schnittstelle kommuniziert über das HTTPS-Protokoll. So kann Drittanbietersoftware,



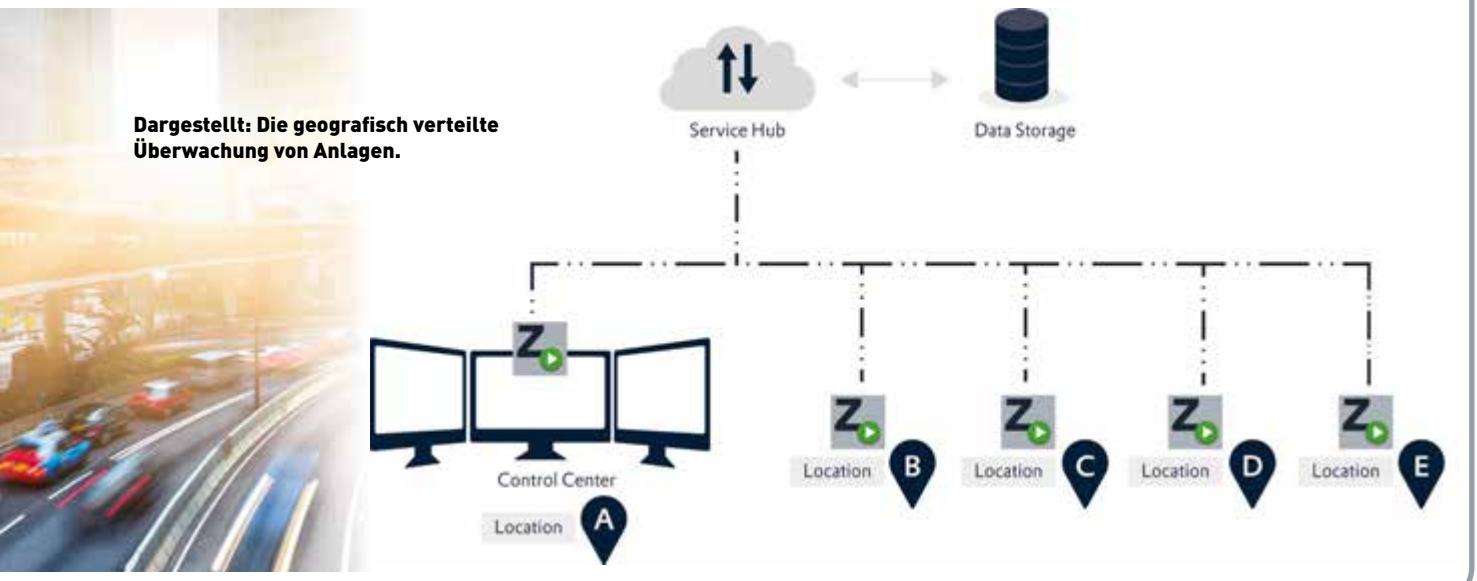
Zu sehen: Security Gateway mit dem zenon Service Grid.

etwa Grafana, im zenon Service Grid angebunden werden. Einfacher ist die Verwendung der integrierten Lösung mit der HTML5 Web Engine. Diese erlaubt die webbasierte Visualisierung von Prozessbildern und Dashboards. Beispielsweise können Alarme, Ereignisse und Trends auf dem Desktop oder mobilen Endgeräten angezeigt werden. Der Data Storage speichert historische Daten, etwa Zeitreihendaten. Diese werden beispielsweise für die Darstellung von Trends in der HTML5 Web Engine oder beim Abruf von historischen Daten über das Service Grid API aus dem Data Storage geladen.

Kommunikation in beide Richtungen. Die zenon Runtime besitzt ab der Version 8.10 die Möglichkeit, sowohl Echtzeit- als auch historische Daten in Form von Variablenwerten, Alarmen und Ereignissen an den Service Hub zu liefern. Während in zenon 8.10 die Kommunikation durch ein Add-in im Projekt erledigt wurde, dient dazu ab der Version 8.20 eine integrierte Funktionalität, der Service Grid Ingress Connector. Mit zenon Supervisor Services des zenon Service Grid. 8.20 und zenon Service Grid 2.0 werden Archivdaten in den Data Storage publiziert. Mit dem Egress Connector können Daten wiederum vom Service Grid eingelesen werden, um beispielsweise eine Leitwartenanwendung zu realisieren.

Bei der Installation werden alle gängigen Betriebssysteme wie Linux und Windows sowie Cloud-Systeme unterstützt. Die Bereitstellung des Service Grid durch die IT-Abteilung ist dank der Verwendung von Docker einfach möglich. Dabei lassen sich Services als Container, die alle nötigen Pakete enthalten, leicht als Dateien transportieren und installieren. Das Update der Software erfolgt durch den Austausch des Containers – Produktionsdaten gehen dabei natürlich nicht verloren.

Die Technologie des zenon Service Grid ist vor allem für geografisch verteilte Anwendungen über das öffentliche Netz ausgelegt und bietet viele Möglichkeiten. Natürlich können Sie daneben auch lokale Anwendungen erstellen.



Dargestellt: Die geografisch verteilte Überwachung von Anlagen.

Bilder: © HP Inc.

EIN LUKRATIVES GESCHÄFT

Bedrohungsszenarien im virtuellen Raum werden die Geschäftswelt auch 2021 auf Trab halten. Das prognostizieren die Security-Experten von HP Inc. in ihrer kürzlich vorgestellten Cybersecurity-Prognose für das Jahr 2021. Stefan Dydak ist Security-Experte bei HP und kennt die Tricks der Angreifer. Von Stephanie Englert

IoT 4 Industry & Business: Zu den von Ihnen angekündigten maßgeblichen Bedrohungen 2021 in puncto Cybersecurity zählt HP von Menschen initiierte Ransomware, Thread Hijacking, unbeabsichtigte Insider-Bedrohungen, kompromittierte geschäftliche E-Mails und Whaling-Angriffe. Was bedeuten diese Bedrohungen in der Praxis?

Stefan Dydak: Einfach gesagt geht es um unterschiedliche und hochentwickelte Formen von Cyberkriminalität. Die genannten Bereiche stellen heute in der Tat eine ernsthafte und realistische Bedrohung für Unternehmen beziehungsweise deren IT-Netzwerke dar. Hinter diesen Technologien stecken hoch innovative Prozesse und Hacker, die Profis auf ihrem Gebiet sind und daraus ein lukratives Geschäft entwickelt haben.

Von Cyberkriminellen initiierte Ransomware-Angriffe sind etwa zu einer akuten Bedrohung und zum bevorzugten Werkzeug geworden. Von Ransomware mit „double extortion" ist vor allem der öffentliche Sektor betroffen: Netzwerke werden infiltriert und sensible Daten abgezogen. Die Täter bauen in Folge großen Druck auf und drohen damit, die gestohlenen Daten zu veröffentlichen, sollte bis zu einem vorgegebenen Zeitpunkt nicht ein gewisser Geldbetrag – meist in Form von Kryptowährungen – überwiesen worden sein. In den USA wurden zuletzt mehrere Städte in dieser Form angegriffen.

Innovationen beim Phishing hingegen führen zu so genanntem Thread-Hijacking und zu Whaling-Angriffen. Beim E-Mail-Thread-Hijacking wird das System kompromittiert, indem Mails über autorisierte User im Unternehmen verschickt werden. Der Empfänger ahnt nichts Böses, da das Phishing-Mail von einem ihm bekannten Sender kommt. Hat das Thread-Hijacking ausgewählte Personen zum Ziel, so ist es eine Form von Spear

Phishing. Auch hier haben es die Täter darauf abgesehen, sensible Daten abzugreifen und Geld zu erpressen.

IoT: Wo liegen die Herausforderungen, wenn Mitarbeiter plötzlich im Homeoffice arbeiten?
Dydak: Wenn ein Großteil der Unternehmens-Hardware außerhalb der Unternehmensmauern genutzt wird, stellt dies Security- und IT-Teams vor völlig neue Aufgaben. Auch heute noch berücksichtigen viele Firmen beispielsweise Endgeräte nicht ausreichend in ihren Sicherheitskonzepten.
Durch die aktuelle Entwicklung sind die Aufgaben der IT-Verantwortlichen dramatisch gestiegen. Zudem hat die Komplexität deutlich zugenommen. Wichtig ist eine detaillierte Analyse des Unternehmens: Welche Prozesse sind kritisch und welche Teile der Infrastruktur müssen unbedingt verfügbar sein?

IoT: Haben denn seit März 2020 Ihrer Erfahrung nach Unternehmen entsprechend schnell auch auf diese (möglichen) Cyberattacken reagiert und die Ausstattung des Homeoffice angepasst?
Dydak: Unternehmen standen vergangenen März vor der Herausforderung, ihre Mitarbeiter von heute auf morgen ins Homeoffice schicken zu müssen. Oftmals ohne, dass die technischen Voraussetzungen dafür gegeben waren. Es wurde improvisiert. Die IT-Security sicherzustellen stand erstmal nicht im Vordergrund. Durch diese abrupte Dezentralisierung der IT-Infrastruktur hat die Angriffsoberfläche aber drastisch zugenommen – beispielsweise waren plötzlich heimische Router und Drucker im Einsatz. Heimdrucker sind nur in den seltensten Fällen sicher konfiguriert, oder mit Sicherheitstechnologie ausgerüstet. Somit sind sie ein gutes Angriffsziel.
Ist ein solches Gerät kompromittiert, versuchen Cyberkriminelle sich Zugriff zum Rechner und dem Unternehmensnetzwerk zu verschaffen. Ein weiteres kritisches Thema sind sensible Unternehmensdaten in der heimischen Umgebung. Viele Firmen haben aber bereits begonnen, ihre derzeitige Lage zu analysieren und konkrete Pläne für zukünftige Arbeitsmodelle auszuarbeiten.

IoT: Sie sagen weiters, dass Mitarbeiter „das schwächste Glied der Security-Kette sind, da die Grenzen zwischen geschäftlichem und privatem Equipment verschwimmen." Dennoch haben viele meist zwei PC, zwei Handys etc. – trennen also private von geschäftlichen Aktionen. Wird demzufolge nicht viel zu leicht den eigenen Mitarbeitern die „Schuld" für einen Cyberangriff auf das Unternehmen in die Schuhe geschoben?
Dydak: Ich stimme Ihnen zu: Für die IT-Security ist das Unternehmen zuständig und muss dafür die technischen Rahmenbedingungen schaffen. Die Aussage ist auch nicht als Schuldzuweisung zu verstehen, sondern als Aufruf zur Sensibilisierung.
Es ist wichtig, dass Mitarbeiter aktuelle Angriffsszenarios kennen und sich möglicher Fallstricke bewusst sind. Phishing-E-Mails, bei denen auf einen Link zu einer mit Malware gespickten Website geklickt wird, sind eine beliebte Attacke von Cyberkriminellen. Dabei ist die Qualität der Angriffe deutlich gestiegen >>

Stefan Dydak
HP Security-Experte
„Es ist wichtig, dass Mitarbeiter aktuelle Angriffsszenarios kennen und sich möglicher Fallstricke bewusst sind."

CREATING SAFE PRODUCTIVITY.

THIS IS SICK
Sensor Intelligence.

Mehr Produktivität, ohne an Sicherheit einzubüßen: Mit uns als Partner profitieren Sie davon, dass Prozesse reibungslos laufen, Mensch und Maschine zum Team werden und wir gemeinsam die Grenzen des Machbaren verschieben. Schlüsselfertige Komplettlösungen, sichere Roboter und mobile Plattformen sowie Outdoor Safety werden dadurch zu einem großen Ganzen. Mit Sicherheit. Wir finden das intelligent. www.sick.at

– Rechtschreibfehler oder schlechtes Deutsch als Erkennungsmerkmal werden immer seltener.
Oft ist schon der Hausverstand ein guter Ratgeber – Stichwort: Wenn es zu schön ist, um wahr zu sein, dann ist es das vermutlich auch. Bei anderen Themen braucht es gezielte Schulungsmaßnahmen, um auch raffiniertere Angriffe erkennen zu können.

IoT: „Innovationen beim Phishing führen zu Thread-Hijacking und Whaling-Angriffen: 2021 wird es eine höhere Zahl innovativer Phishing-Angriffe geben", heißt es von Ihrer Seite. Wie kann es sein, dass Angreifer innovativer sind als die „andere" Seite, nämlich die der möglichen Angegriffenen? Was läuft hier „falsch"?
Dydak: Der Angreifer hat immer einen Vorteil: Er muss nur ein Schlupfloch finden, das Unternehmen hingegen muss alle Schlupflöcher kennen und schließen und selbst dann gibt es keine 100-%ige Sicherheit. Stichwort „Social Engineering". Hier machen sich Angreifer weniger die Technik zu Nutze, sondern vielmehr die menschliche Psychologie.
Beim bereits erwähnten Thread-Hijacking geben sich Angreifer etwa als gestresste Kollegen aus, die unter Druck stehen und dringend Unterstützung benötigen. Besonders in großen Firmen ist die Wahrscheinlichkeit hoch, dass sich nicht alle Mitarbeitenden untereinander kennen und in Bezug auf Firmenzugehörigkeit und Kompetenzen leicht getäuscht werden können. Sensible Daten werden dann zu schnell preisgegeben. Bei Tricks dieser Art handelt es sich um Bedrohungsszenarien, die tatsächlich ein hohes Maß an Sensibilität und Awareness auf Seiten der Angegriffenen fordern.

Stefan Dydak
HP Security-Experte
„Der Angreifer hat immer einen Vorteil: Er muss nur ein Schlupfloch finden."

IoT: IT- und Security-Teams seien oftmals unterbesetzt, hört man immer wieder. Fehlt es an Know-how möglicher neuer Mitarbeiter oder ist das Ausbildungswesen nicht den Gegebenheiten angepasst um auf Trends zu setzen?
Dydak: Dass in der IT-Branche Fachkräfte auch unter normalen Umständen händeringend gesucht werden ist kein Geheimnis. Das vergangene Jahr hat den Bedarf an IT- und Security-Experten aber nochmals erhöht – die Nachfrage ist regelrecht explodiert. Dass diese nicht ausreichend bedient werden kann, hat mehrere Faktoren.
Am Ausbildungsangebot kann es nur teilweise liegen. Auf den Universitäten, aber auch insbesondere an den Fachhochschulen, gibt es ein breit gefächertes Angebot an Informatik-Studiengängen sowie Studien mit IT-Security-Schwerpunkt. Meine Einschätzung ist: Die Schüler und Studierenden von heute leben zwar vollends in der digitalen Welt, dass sie sich in

Für die IT-Security ist das Unternehmen zuständig und muss dafür die technischen Rahmenbedingungen für seine Mitarbeiter schaffen.

dieser aber sicher bewegen können, wird als selbstverständlich hingenommen.
Welch große Bedeutung IT-Security für unser digitales Leben und Arbeiten hat, wie gefragt Fachexperten in diesem Bereich sind und die guten Arbeitsbedingungen und Verdienstmöglichkeiten, die sich dadurch ergeben, ist vielen nicht bekannt. Viele Unternehmen decken den Bereich nicht mehr selbst ab, sondern lagern diese Aufgaben an IT- Beratungs- und Dienstleistungsunternehmen aus. Auch die Channel-Partner nehmen hier eine Schlüsselfunktion ein.

IoT: Und wie informieren Sie Ihre Zielgruppe zu möglichen Lösungen bzw. was bieten Sie aus dem Hause HP an?
Dydak: HP verfolgt bei all seinen Security-Konzepten einen holistischen Zugang. Dazu gehört das, was Security-Experten als „gestaffelte Sicherheit" bezeichnen: Jede Hardware-Entscheidung ist eine Sicherheits-Entscheidung. Systeme zu schützen fängt daher bei der Hardware an, hört dort aber noch lange nicht auf. Relevante Softwarelösungen und die Sensibilität für aktuelle Security-Bedrohungen auf Anwender-Seite sind ein genauso relevanter Aspekt eines jeden Security-Konzeptes. Unsere Kunden profitieren von konkreten Lösungen, wie etwa HP Sure Click Pro – ein Programm, das vor Malware, Ransomware und Viren schützt. HP Sure Click Pro basiert auf dem Prinzip der Virtualisierung. Klickt ein Mitarbeiter beispielsweise auf einen Link oder wird ein Attachment geöffnet, wird die Webseite oder das Dokument in einem vom System isolierten Fenster geöffnet. Mögliche Schadsoftware kann nicht auf das System zugreifen.
Abseits technischer Lösungen stehen unsere Experten Unternehmen auch beratend zur Seite, bieten Risikoanalysen, Event Analytics oder generisches Security Consulting an. Im vergangenen Jahr waren auch Strategieempfehlungen stark gefragt, wie Unternehmen mit den neuen Risiken in „Work From Home"-Situationen umgehen können. Unser Arbeitsleben wird dynamischer und die Bedrohungsszenarien diverser. Ein ganzheitlicher Zugang ist daher kriegsentscheidend.

www.hp.com

Die Corona-Krise beschleunigt die Digitalisierung. Daher findet derzeit ein Umdenken statt und die IT-Sicherheit rückt in den Fokus. Welche Trends wichtig werden, erläutert Dr. Matthias Rosche, Managing Director von Orange Cyberdefense Germany.

KLIMAWANDEL IN DER IT-SICHERHEIT

Die Bedrohungslandschaft in der IT wandelt sich so rasch, aber beständig, wie das Wetter. Es gibt verschiedene Faktoren, die den Wandel beeinflussen; zum einen die Kreativität der Hacker und zum anderen neue Technologien. Am Ende steht eine Erkenntnis: Die eine Bedrohung gibt es nicht, sondern unterschiedliche Gefährdungen entwickeln sich gegen verschiedene Schwachstellen. Der Security Navigator-Report 2020 von Orange Cyberdefense zeigte in einer Analyse von insgesamt 263.109 Events aus elf CyberSOCs und 16 SOCs auf, dass ein Anstieg von 34 Prozent bei verifizierten Security-Incidents verzeichnet werden konnte.
Im Rahmen der Orange Cyberdefense World 2020 diskutierten zahlreiche Sicherheitsexperten aus der EMEA-Region die Cyberrisiken, die sie für das Jahr 2021 am häufigsten erwarten. Darunter fallen vermehrte Angriffe gegen Produktionsanlagen und Fertigungsstraßen. ICS/Scada-Anlagen und die gesamte OT sind bereits ins Visier der Cyberkriminellen geraten. Außerdem sind Angestellte mit ihren Homeoffice-Geräten stark gefährdet. Abgesehen davon, lassen sich fünf übergeordnete Trends feststellen, die 2021 die Lage der IT-Sicherheit bedingen werden:

Trend 1: Zweite Welle der Covid-19-bezogenen Hacks gegen Tele-Arbeiter bestehend aus Ransomware. Die verlangten Lösegeldsummen haben sich bereits deutlich von vier- bis fünfstelligen Beträgen auf sechs- bis siebenstellige erhöht.

Trend 2: Zunehmende Auslagerung der IT-Sicherheit an professionelle Dienstleister. Diese Entwicklung nahm schon im letzten Jahr Fahrt auf, gewinnt aber Geschwindigkeit durch die Corona-Krise. Faktoren sind vor allem die geringeren Kosten, dass Fachkräfte fehlen, so dass sogar Dienstleister Schwierigkeiten bei der Rekrutierung haben. Darüber hinaus auch die Möglichkeit der Dienstleister eine Rund-um-die-Uhr-Betreuung an sieben Tagen die Woche 24 Stunden täglich anzubieten.

Trend 3: Detection und Response anstatt Protection. Der althergebrachte Ansatz, das gesamte Budget in die Prävention zu stecken, wird aufgegeben. Es ist schlicht nicht möglich, jeden Angriff abzuwehren.

Trend 4: Cloud-Transformation erfordert neue Art der IT-Sicherheit. Zwei Wege sind möglich: Entweder als Sicherheit für die Cloud, was bedeutet, dass neue Sicherheitslösungen speziell für Cloud-Umgebungen – oder sogar serverlose Konzepte im Rahmen von Docker-Containern – entwickelt werden. Diese müssen mit neuen Tools, wie CASB, CWPP oder CSPM, kompatibel sein. Oder als Sicherheit aus der Cloud, was wiederum auf zwei Weisen realisiert werden kann. Zum einen durch Secure Access Service Edge, um von Lan-Strukturen wegzugehen und direkt den Weg über das Internet zur Cloud zu suchen. Zum anderen Zero Trust Network Access, das das klassische Virtual Private Network ersetzt und sichere Verbindungen zwischen Firmennetzwerken, Cloud-Umgebungen und tragbaren Geräten von Mitarbeitern im Homeoffice ermöglicht.

Trend 5: Das Security Operations Center 2.0 besteht aus maschinellem Lernen, Automatisierung und Threat Intelligence. Die Menge und Geschwindigkeit von modernen Bedrohungen wird durch bisher erprobte Forensik nicht mehr gestemmt, weswegen Data Science als Prinzip nötig wird. Dieses wird durch die Automatisierung und Threat Intelligence ermöglicht, die eine Bedrohung im Kontext analysiert, ihr Verhalten prüft und zu anderen Gefahren in den Vergleich setzt, um so zu lernen und schneller zu reagieren.

https://orangecyberdefense.com

Der Autor
Dr. Matthias Rosche
... ist Managing Director von Orange Cyberdefense in Deutschland, einem weltweit führenden Telekommunikationsanbieter.

„DIE BITCOIN-BLOCKCHAIN IST VERMUTLICH DAS SICHERSTE IT-SYSTEM“

Kryptowährungen erfahren derzeit einen wahren Hype. Der Bitcoin steigt im Wert und sogar Elon Musk von Tesla heizt das Feuer mit an. Zu Recht? Michael Mertens, CEO der CryptoTec GmbH und Experte auf diesem Gebiet gab Antworten und das, obwohl er derzeit ziemlich gut beschäftigt ist. Von Stephanie Englert

Wer von Kryptowährungen bis 2020 noch nichts gehört hatte, konnte sich seit dem Beginn der Pandemie zumindest davon nicht mehr freisprechen. Kein anderes Thema bestimmt die Medien seit einigen Monaten so intensiv wie der Bitcoin. Mitte Februar stieg sein Wert auf fast 60.000 US-Dollar, fiel einen Tag später wieder auf 46.000 US-Dollar. Diesen Höhenflug hatte auch Tesla-Gründer Elon Musk zuletzt mit verursacht und verkündete ihn als künftiges Zahlungsmittel in seinem Unternehmen.

Doch man muss gar nicht so weit schauen, um zu merken, Kryptowährungen gewinnen an Alltagsgewohnheit. Auch Ärzte, etwa in Wien, befürworten in ihren Praxen bereits ein alternatives Zahlungsmittel und geben dies auf ihrer Praxiswebsite an. Und selbst Gastwirte, kleinere Läden etc. verstehen Kryptowährungen als normales Zahlungsmittel.

Doch es gibt auch Skeptiker und vor allem Kritiker, so etwa EZB-Chefin Christine Lagarde, die in einem Interview davor warnte, dass Bitcoin für Geldwäschezwecke verwendet werde. Doch es gibt Möglichkeiten auch hier zu regulieren. Und Michael Mertens? Er hat einen klaren Blick auf das, was uns noch bevorsteht.

IoT 4 Industry & Business: Die Kryptowährung Bitcoin erlebt derzeit einen wahren Hype. Ähnlich geht es auch anderen Kryptowährungen. Was ist der Grund für diese Entwicklung und was hat die Covid-19-Pandemie damit zu tun?

Michael Mertens: Es stimmt, die Nachfrage nach Bitcoin und anderen Kryptowährungen wird immer größer. Das liegt insbesondere an dem zunehmenden Interesse von institutionellen Investoren. So hat allein Tesla im Gegenwert von 1,5 Milliarden US-Dollar Bitcoin gekauft. Im Vorfeld hatte bereits das Unternehmen MicroStrategy 425 Millionen US-Dollar in Bitcoin investiert, um unabhängiger von dem US-Dollar zu werden.

Aufgrund der – wegen Covid-19 erhöhten Geldmenge – ergibt sich eine Inflationsgefahr des US-Dollars, die zu dem gesteigerten Interesse an Bitcoin führt. Denn die Menge der Bitcoin ist bei der Kryptowährung fest auf 21 Millionen begrenzt.

IoT: Und wie lange wird Ihrer Einschätzung nach dieser rasante Anstieg, vor allem bei Bitcoins, noch anhalten? Sind Kryptowährungen denn wirklich so krisensicher(er)?

Mertens: Der Preis von Bitcoin wird durch Angebot und Nach-

Michael Mertens
CEO CryptoTec GmbH

„China steht an der Spitze der Länder, die virtuelle Währungen einführen."

Wird der Bitcoin wirklich ein gängiges künftiges Zahlungsmittel werden bzw. ist er es bereits?

frage bestimmt. Inwieweit der Anstieg anhält, kann niemand voraussagen. Derzeit sieht es so aus, dass das Interesse an Bitcoin weiter steigt. Nach Einschätzung des größten, weltweiten Vermögensverwalters BlackRock kann Bitcoin ein neuer Wertspeicher werden. Laut der US-Bank JP Morgan kann Bitcoin als Wertanlage so beliebt werden wie Gold.

IoT: Viel wird derzeit auch über die neue chinesische digitale Währung, den digitalen Yuan, gesprochen. Europa und auch die USA scheinen hier zögerlicher zu agieren. Weshalb und welche Chancen bietet der digitale Yuan Ihrer Meinung nach?
Mertens: Der digitale Yuan wird von der chinesischen Zentralbank, der People's Bank of China (PBoC) herausgegeben. Wie auch bei anderen digitalen Zentralbankwährungen entspricht der Wert des digitalen Yuan dadurch dem des herkömmlichen Yuan. Daher gibt es keine Kursschwankungen.
Der digitale Yuan kann schnell und weltweit übertragen werden. Dies ermöglicht die schnellere Abwicklung von Zahlungen. Digitale Währungen können zudem an Smart Contracts gekoppelt werden. Das sind Verträge, die beim Eintreten vorher festgelegter Bedingungen automatisch ausgeführt werden. Dies ermöglicht eine starke Automatisierung und vollkommen neue Geschäftsmodelle. Jeder der weiß, wie schwer es ist Verträge vor Gericht einzuklagen weiß, welche Vorteile Smart Contracts bieten. Dass Europa so zögerlich ist, halte ich für einen Fehler.

IoT: Und wird der digitale Yuan über kurz oder lang den Handel bzw. die Industrie global beeinflussen?
Mertens: Ja, denn China steht an der Spitze der Länder, die virtuelle Währungen einführen. Die chinesische Zentralbank möchte durch den digitalen Yuan die eigene Währung beliebter machen und so das globale Monopol des US-Dollars brechen. Für China bietet sich angesichts der schlechten Beziehungen zu den USA, die Chance sich im von den USA dominierten Finanzsystem zu schützen. Es ist sogar denkbar, dass chinesische Unternehmen in der Zukunft nur noch Zahlungen in Form des digitalen Yuan akzeptieren werden. Dies wird deutliche Auswirkungen auf den internationalen Handel und die Industrie haben.

IoT: Schließlich stellt sich bei Kryptowährungen dann auch die Frage der Sicherheit. Wie sicher sind Kryptowährungen denn eigentlich?
Mertens: Die verwendeten Verfahren von Kryptowährungen wie Bitcoin gelten seit langem als sicher. Es gibt keine bekannten Angriffe, die in naher Zeit durchführbar wären. Falls es Angriffe auf die zugrundeliegenden kryptographischen Algorithmen in Zukunft geben sollte, ist dazu zu sagen, dass die vorhandenen Onlinebanksysteme damit ebenfalls angreifbar wären.

IoT: Aber ist eine Blockchain wirklich zu 100 Prozent sicher?
Mertens: Die Bitcoin-Blockchain ist vermutlich das sicherste IT-System, dass die Menschheit bisher gebaut hat. Andere IT-Systeme können eine Menge von Bitcoin lernen.

IoT: Abschließend würde ich gerne von Ihnen wissen, ob Sie der Ansicht sind, dass uns Hacker-Angriffe künftig eher überhäufen werden? Wie ist Ihre Einschätzung?
Mertens: Ich denke schon. Angriffe werden uns sehr wohl überhäufen, denn Großteile unserer aktuellen industriellen IT-Systeme halten Hacker-Angriffen nicht lange stand. Durch die zunehmende Vernetzung sind Angriffe nun aus der ganzen Welt möglich. Und in vielen Unternehmen ist die Sicherheit der eigenen IT-Systeme nicht ausreichend bekannt. Wenn Sie dies bei sich testen möchten, können Sie Ihren IT-Sicherheitsverantwortlichen die einfache Frage stellen, gegen welche Angriffe das eigene Unternehmen derzeit geschützt ist.

IoT: Vielen Dank!

www.cryptotec.com

Die Sicherheit auf dem Gerät wird sehr viel weniger wichtig, wenn Daten- und Netzwerkkontrollen eingerichtet sind.

DIE MYTHEN DER IoT-SICHERHEIT

Konventionelle Ansätze der Cybersicherheit konzentrieren sich auf ein grundlegendes Konzept: jedes in Sichtweite befindliche Gerät schützen, um Hacker, Angreifer und Diebe fernzuhalten.

Was bedeutet das jedoch für Unternehmen? Wenn sie im traditionellen Sicherheitsansatz feststecken, ist es an der Zeit, ihre Sicherheitsinitiative neu zu starten, um eine grenzenlose Computing-Umgebung widerzuspiegeln. Das IoT unterscheidet sich sehr von der IT. Es ist wichtig, sich auf das Netzwerk und die gesamte Datenumgebung zu konzentrieren, anstatt auf das spezifische Gerät.
Palo Alto Networks nennt hierzu die fünf wesentlichen Mythen der vernetzten Sicherheit und Tipps, wie Unternehmen sie überwinden können.

Mythos Nr. 1:
Das IoT ist einfach die nächste Phase der IT-Sicherheit. Nichts könnte weiter von der Wahrheit entfernt sein.
Vernetzte Geräte und Systeme stellen einen stärker dezentralisierten Ansatz für die Computing- und Cybersicherheit dar. Für IT-Teams erfordert die Umstellung auf das IoT einen gewaltigen konzeptionellen Sprung, da sie nicht mehr der Käufer oder Gerätebesitzer sind.
Das Problem ist, dass die IT-Teams versuchen, dieselben Tools und Ansätze zu verwenden, die schon bei der Gründung von Fort Knox verwendet wurden. Sie gehen ein Geschäftsproblem als IT-Problem an. Beim IoT geht es nicht um Laptops und Smartphones. Es geht nicht um den Schutz von Benutzernetzwerken. Unternehmensleiter, die das IoT wirklich verstehen, erkennen, dass sie die Cybersicherheit vereinfachen können, wenn sie einen eher ganzheitlichen, datenzentrierten Ansatz verfolgen, anstatt alles noch komplexer zu machen.

Mythos Nr. 2:
Die IT sollte die Sicherheit des IoT überwachen.
Wenn die IT-Abteilung für die Sicherheit des IoT verantwortlich ist, greift sie in der Regel auf konventionelle Werkzeuge, Technologien und Ansätze für diese Aufgabe zurück. Dieser „One-size-fits-all"-Ansatz führt häufig zu enttäuschenden Ergebnissen. Das IoT geht über die Grenzen konventioneller Computersysteme hinaus. Daten befinden sich auf verschiedenen Geräten innerhalb und außerhalb eines Unternehmens und fließen über viele weitere Berührungspunkte. Es gibt aber noch ein anderes, manchmal größeres Problem. Da sich das IoT über Teams, Abteilungen und Unternehmen erstreckt, ist es leicht, sich mit einem isolierten Ansatz zur Cybersicherheit abzufinden. In einigen Fällen können verschiedene Gruppen, die sich mit Sicherheitsfragen befassen, Doppelarbeit leisten oder sogar versehentlich Methoden anwenden, die miteinander in Konflikt stehen – und letztlich ein Unternehmen ungeschützt lassen.
Die Abstimmung zwischen IT- und Cybersicherheits-Teams ist im Zeitalter des IoT sogar noch wichtiger. Dies erfordert eine enge Zusammenarbeit zwischen CIOs, CSOs und CISOs. Man muss wirklich eine Analyse durchführen, all seine Ressourcen identifizieren und verstehen, wie, warum und wo Daten verwendet werden. Nur dann kann man einen Rahmen entwerfen, der für das IoT optimiert ist. Dies kann die Einstellung oder Umschulung von Mitarbeitern mit den richtigen Fähigkeiten und Fachkenntnissen erfordern. >>

Mythos Nr. 3:

Herkömmliche Sicherheitstools und -strategien werden uns schützen.

Der Burg-und-Graben-Ansatz in der Cybersicherheit kann die IoT-Sicherheit tatsächlich „untergraben". Malware-Schutz und andere herkömmliche Tools sind zwar immer noch wertvoll, wurden aber nicht für die Verwaltung von Datenströmen über Sensoren, Edge-Umgebungen und moderne Mehrzweckgeräte konzipiert.

Das bedeutet nicht, dass ein Unternehmen diese Schutzmechanismen beseitigen sollte, es muss sie nur anders einsetzen und neue Funktionen hinzufügen, sobald sie verfügbar sind. Dies können zum Beispiel Datenverschlüsselung während der Übertragung oder Tools zur Netzwerküberwachung sein, die erkennen, wann Daten besonders gefährdet sind. Es könnte auch die Einrichtung separater Netzwerke für verschiedene Arten von Daten sein. Selbst wenn jemand ein Gerät oder ein System hackt, kann es dann passieren, dass er nichts Wertvolles erhält.

Palo Alto Networks meint, dass ein Unternehmen, sobald es vollständig versteht, wie Daten auf einer IoT-Plattform verwendet werden, die richtigen Schutzvorkehrungen zuweisen kann, einschließlich Governance-Modell, Praktiken, Prozessen und Tools. Dies kann von der Endpunkt- und Netzwerküberwachung über Verschlüsselung in Bewegung bis hin zu noch fortschrittlicheren Methoden des maschinellen Lernens und der Künstlichen Intelligenz reichen.

KI kann IoT-Geräte in einem Netzwerk finden, einschließlich zuvor verborgener Geräte, sicherstellen, dass sie kritische Updates und Sicherheits-Patches erhalten haben, und andere potenzielle Probleme identifizieren. Durch maschinelles Lernen können IoT-Geräte auf der Grundlage von Sicherheitsrisiken in Gruppen eingeteilt werden, ohne dass zusätzliche Sicherheitssoftware und manuelle Prozesse erforderlich sind. Dieser Ansatz ermöglicht Risikobewertungen, wann Geräte „normal" oder „verdächtig" funktionieren, und hilft bei der Durchsetzung von IoT-Richtlinien.

Mythos Nr. 4:

Es dreht sich alles um den Schutz des Geräts.

Die Anwendung des konventionellen IT-Sicherheitsdenkens auf das IoT öffnet eine weitere Falle. IoT-Sicherheit erfordert einen breiteren Ansatz, der Netzwerkauthentifizierung, Konnektivität, Clouds und mehr umfasst. „Es ist an der Zeit, nicht mehr an IoT-Geräte als kleine PC zu denken. Die meisten dieser Geräte sind einfach und dumm", heißt es.

Tausende oder Zehntausende von IoT-Sensoren und -Geräten machen es unmöglich, jedes einzelne in einem intelligenten Unternehmen, einer Lieferkette oder einer Stadt zu schützen. Es ist zwar wichtig, ein medizinisches Gerät oder ein Auto vor Hackerangriffen zu schützen, aber viele angeschlossene Sensoren und Geräte haben schreibgeschützte Komponenten, die nicht kompromittiert werden können. Folglich müssen sich die IoT-Schutzmaßnahmen in Unternehmen um komplexere Beziehungen zwischen Systemen und Daten drehen.

„Man muss wirklich mit den Grundlagen beginnen", betont Jamison Utter, Business Development Manager IoT, Palo Alto Networks. „Das bedeutet, dass man ein Zero-Trust-Framework schaffen muss." In dieser neuen Ordnung des IoT ist das Netzwerk das Ding – und alle Sensoren, Geräte, Systeme und Daten müssen ganzheitlich betrachtet werden. „Durch die Klassifizierung von Daten, die Einrichtung von Zonen und die Erstellung von Whitelist-Anwendungen und -Prozessen ist es möglich, die richtigen Schutzvorrichtungen und Werkzeuge für die richtige Aufgabe zu identifizieren."

Das bedeutet zum Beispiel, dass man sich von einem traditionellen Modell, bei dem alle Sensoren und Geräte in dasselbe Netzwerk eingebunden werden, entfernen muss. Stattdessen kann ein Unternehmen davon profitieren, wenn es seine Anlagen nach Geschäftsaufgaben, Datensicherheits- und Vertrauensebene organisiert.

Mythos Nr. 5:

Die Sicherheitsvorkehrungen der Hersteller sind entscheidend.

Die vorherrschende Mentalität ist, dass Anbieter starke Schutzvorrichtungen in ihre Produkte einbauen müssen. Und wenn es einen Patch gibt, muss der Benutzer ihn nach der Installation in aller Eile installieren. Leider ist dies ein fehlerhaftes Konzept im Zeitalter der vernetzten Geräte. Das soll nicht heißen, dass Sicherheit nicht in die Produkte eingebaut werden sollte. Es soll nur nicht heißen, dass ein Unternehmen die Sicherheit der Anbieter von IoT-Geräten nicht als primäre Form des Schutzes betrachten sollte.

Da viele Sensoren lediglich „dumme Endpunkte" sind, die ersetzt und nicht gepatcht werden. Selbst wenn es sich um komplexere Geräte handelt, „setzen die meisten Unternehmen IoT-Komponenten ein und aktualisieren oder patchen diese nie". Teil des Problems ist, dass Firmware-Patches und -Upgrades bei Tausenden von vernetzten Geräten zu einem Albtraum werden.

Das Fazit? Die Sicherheit auf dem Gerät wird sehr viel weniger wichtig, wenn Daten- und Netzwerkkontrollen eingerichtet sind. Das IoT erfordert eine umfassendere übergreifende Strategie, die sich über alle Gerätehersteller erstreckt. Letztendlich muss sich der Schutz des IoT nicht als mühsam erweisen. Er erfordert jedoch das richtige Fachwissen – und ein Verständnis dafür, dass der konventionelle Ansatz zur Cybersicherheit angepasst werden muss. Wenn Führungskräfte diese Realität verstehen, so Palo Alto Networks, können sie Entscheidungen und Budgets entsprechend anpassen.

www.paloaltonetworks.com

RUNDUM ABGESICHERT

Mit der steigenden Digitalisierung und Vernetzung von Produktionsanlagen wachsen auch die Gefahren durch Cyberangriffe. Diese Angriffe können sowohl von außerhalb des Produktionsnetzes erfolgen (Internet, Funkschnittstellen) als auch von innen. „Deshalb ist eine ganzheitliche Cybersecurity-Strategie unabdingbar. Die Herausforderungen an sichere Datenübertragung und den Schutz von Systemen vor Manipulation durch Angreifer steigen insbesondere durch die wachsende Vernetzung im Umfeld von Industrie 4.0.“, so Alexander Magerling, Team Leader Market Application Engineers & Cybersecurity Specialist bei Sick Österreich.

Cybersecurity bildet die Basis für das Vertrauen des Nutzers in digitale Produkte. Mit Cybersecurity nicht zu verwechseln ist der Begriff Safety, womit der Schutz des Menschen vor Maschinen gemeint ist.

Der Schutz. Für Lösungen von Sick gelten höchste Qualitätsanforderungen. Die Cybersecurity-Strategie beginnt bereits vor der Entwicklung von neuen Produkten, die Cybersecurity-Architektur umfasst die gesamte Infrastruktur vom Sensor über sichere Industrie-Gateways und Produktionsnetze bis in die Cloud. Das Cybersecurity-Managementsystem von Sick orientiert sich an der internationalen Normenreihe IEC 62443 „Industrial communication networks – Network and system security“. Systematisch verankert sie die Cybersecurity-Strategie im gesamten Unternehmen. Die Normenreihe dient außerdem als Grundlage für die Entwicklung von Produkten, für die Cybersecurity relevant ist.
„Neue Entwicklungen werden für unterschiedliche Anwendungen und Einsatzbereiche spezifiziert – entsprechend den Anforderungen an die Cybersecurity. Sie wird hinsichtlich der Umsetzung und Wirksamkeit der definierten Sicherheitsmaßnahmen geprüft und in Labors getestet. So behält der Lösungsanbieter die Cybersecurity aller Produkte von Anfang an und über deren gesamten Lebenszyklus hinweg im Blick.“, ergänzt Magerling.

Cybersecurity sicherstellen. Bei der Definition geeigneter Sicherheitsmaßnahmen zur Sicherstellung von Cybersecurity ist es wichtig, dass zu erstellende Zielsystem ganzheitlich und – je nach Kritikalität – individuell zu betrachten. Sick verfolgt die sogenannte Defense-in-Depth-Strategie: Sick-Produkte sind durch mehrere Schichten von Cybersecurity-Maßnahmen geschützt und Sensordaten von nicht vertrauenswürdigen Netzwerksegmenten werden separiert. Bei der Wahl der eingesetzten Cybersecurity-Mechanismen setzt man auf etablierte Standards aus dem Bereich Verschlüsselung (z.B. SSH, TLS, VPN) sowie weitere Industriestandards. So wird sichergestellt, dass robuste und bewährte Verfahren im Einsatz sind.
Sick betrachtet die Cybersecurity von Produkten über ihren gesamten Lebenszyklus hinweg. Das Sick PSIRT steuert die Untersuchung, interne Koordination und Offenlegung von Sicherheitsschwachstellen. „Das Aufdecken von Schwachstellen wird als ein gemeinsames Bestreben verschiedenster Parteien bei uns verstanden, mit dem Ziel unseren Kunden durchgängig ein hohes Sicherheitsniveau zu bieten.“, betont Magerling. Auf www.sick.com/psirt veröffentlicht das Sick PSIRT sogenannte Security Advisories zu bestätigten Sicherheitsschwachstellen. Diese bieten Informationen und konkrete Handlungsempfehlungen zu einer Schwachstelle. Um auch für zukünftig auftretende Bedrohungen gewappnet zu sein, überwacht es die Sicherheitslage kontinuierlich.

Beispiel: Remote Service. Der Sick Remote Service bietet durch seine Sicherheitsarchitektur schon heute eine sichere und leistungsstarke Fernwartungsverbindung. So sind auch während des Betriebs sichere Ferndiagnosen durch Experten möglich.

www.sick.at

Der Autor:
Alexander Magerling
... ist Team Leader Market Application Engineers & Cybersecurity Specialist bei Sick Österreich

„WIR WOLLEN MIT GUTEM BEISPIEL VORANGEHEN!“

Eine effiziente Projektabwicklung haben viele im Sinn. Doch laut Stefan Lau, Vertriebsleiter der Energy Industries Division von ABB in Deutschland, sei dies mittels ABB Adaptive Execution nun auch möglich. In einem Interview mit IoT4 Industry & Business erklärt er weshalb. Von Stephanie Englert

IoT4 Industry & Business: Im Herbst vergangenen Jahres stellte ABB das ABB Adaptive Execution vor. Ziel sei es den Angaben nach die Projektabwicklung für große Investitionsprojekte effizienter zu gestalten. Waren oder sind die derzeitigen Arbeitsweisen wirklich so ineffizient?

Stefan Lau: Kunden aus energieintensiven Industrien sehen sich häufig mit langen Projektlaufzeiten konfrontiert, die komplex und ständigen Veränderungen unterworfen sind. Sie benötigen eine Methode, die eine termingerechte und budgetkonforme Projektabwicklung gewährleistet und die Ergebnisse über alle Phasen des Projektlebenszyklus hinweg sicherstellt. Investitionsprojekte sind komplexer geworden, mit einer größeren Abhängigkeit von Zusammenarbeit, agilen Prozessen und innovativen Technologien. Der Erfolg erfordert einen transformativen Ansatz, der über die gesamte Projektlaufzeit hinweg messbare Verbesserungen bringt. ABB Adaptive Execution kombiniert Technologie und Fachwissen, um die Projektabwicklung zu verbessern und messbare betriebswirtschaftliche Vorteile zu erzielen. Dank seines skalierbaren Ansatzes ist ABB Adaptive Execution unsere Antwort sowohl auf Investitions- als auch auf Modernisierungs- und Expansionsprojekte.

IoT: Wo liegt der genaue Mehrwert für den Anwender?

Lau: ABB Adaptive Execution versetzt unsere Kunden in die Lage, während der gesamten Projektlaufzeit auf Veränderungen flexibel zu reagieren. Wir helfen ihnen, komplexe Hindernisse durch eine einzigartige Kombination aus Experten, standardisierten Prozessen und modernen Technologien zu überwinden. Es ist ein innovativer und flexibler Ansatz, um die Projektabwicklung für alle Beteiligten zu optimieren.

ABB Adaptive Execution integriert Expertenteams, neue Technologien, agile Prozesse, gemeinsames Lernen und bewährte Methoden. So wird die Projektabwicklung für alle Akteure, die an großen Investitionsprojekten beteiligt sind, effizient.

IoT: Aus welchem Grund präsentierte ABB gerade jetzt das ABB Adaptive Execution? Gibt es hier auch einen direkten Zusammenhang zur angestrebten Energiewende und den neuen Klimazielen?
Lau: 2020 war ein Jahr der Umbrüche auf dem globalen Energiemarkt. Angesichts sinkender Ölpreise und der Herausforderungen, die sich aus den aktuellen Lockdowns und der steigenden Nachfrage nach nachhaltigen Energieinvestitionen ergeben, suchen die Unternehmen nach neuen Wegen, um Kosten, Zeitpläne und Risiken bei Großprojekten zu reduzieren. ABB Adaptive Execution macht sich die Vorteile der Digitalisierung zu Nutze und reagiert auf dieses Bedürfnis, damit Investitionsprojekte auch in der neuen Normalität gelingen können.

IoT: Und inwiefern hat die Covid-19-Pandemie einen Einfluss bei der Entwicklung gehabt bzw. erwartet sich ABB einen so genannten Push-Faktor ob der steigenden Nachfrage nach Digitalisierung?
Lau: Die Corona-Pandemie hat den Prozess sicherlich angeheizt und beschleunigt. Aber der Gedankenprozess begann schon viel früher. Wie können wir unsere Kunden am besten dabei unterstützen, das IoT in ihrer Produktionsanlage zum Leben zu erwecken? Das beginnt schon in der Planungs- und Engineering-Phase. Während der Lockdowns konnten wir einige Elemente testen und u.a. erfolgreich Remote-Engineering, Change-Management und sogar Remote Factory Acceptance Tests (FATs) durchführen.

IoT: Inwiefern kann ABB Adaptive Execution bei Industrie 4.0-Zielen konkret unterstützen?
Lau: Wenn Sie die Vorteile einer digital vernetzten Produktion nutzen wollen, müssen IT und OT Hand in Hand zusammengehen. Dies muss so früh wie möglich geschehen, um hohe Kosten und Inflexibilität zu vermeiden. Mit Adaptive Execution werden die ET-Daten (Engineering) von Anfang an mit den IT- und OT-Daten verknüpft. Damit wird ein zusätzlicher Hebel für die optimale Ausschöpfung der Betriebsdaten geschaffen. Die Plattform, um all diese Daten zu hosten und dem Anwender zur Verfügung zu stellen, ist ABB Ability Genix. Die Informationen stehen für Dashboards, im Kiosk und für den On-Demand-Abruf von Daten zur Verfügung und, was noch wichtiger ist, für die Erkennung von Anomalien, für die vorausschauende Wartung und für Opportunity Loss Indicators, um nur einige Anwendungen zu nennen.
Das macht die Produktion transparent, die Planung einfach und vermeidet Produktionsstillstände durch unvorhergesehene Anlagenausfälle. >>

Stefan Lau
Vertriebsleiter der Energy Industries Division von ABB in Deutschland

„Wenn Sie die Vorteile einer digital vernetzten Produktion nutzen wollen, müssen IT und OT Hand in Hand zusammengehen."

Offenes Ecosystem für die Automatisierung

Denken Sie Automatisierung mit uns neu

Vernetzung von IT und OT, Echtzeitausführung unabhängig von der Programmiersprache, Integration von Open Source Software, einfache Cloud-Integration sowie die freie Wahl Ihres favorisierten Programmier-Tools. Profitieren Sie von einer wachsenden Community und durch Apps von unserem digitalen Marktplatz.
Werden Sie Teil von PLCnext Technology:
www.plcnextcommunity.com

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

PHOENIX CONTACT
INSPIRING INNOVATIONS

© PHOENIX CONTACT 2021

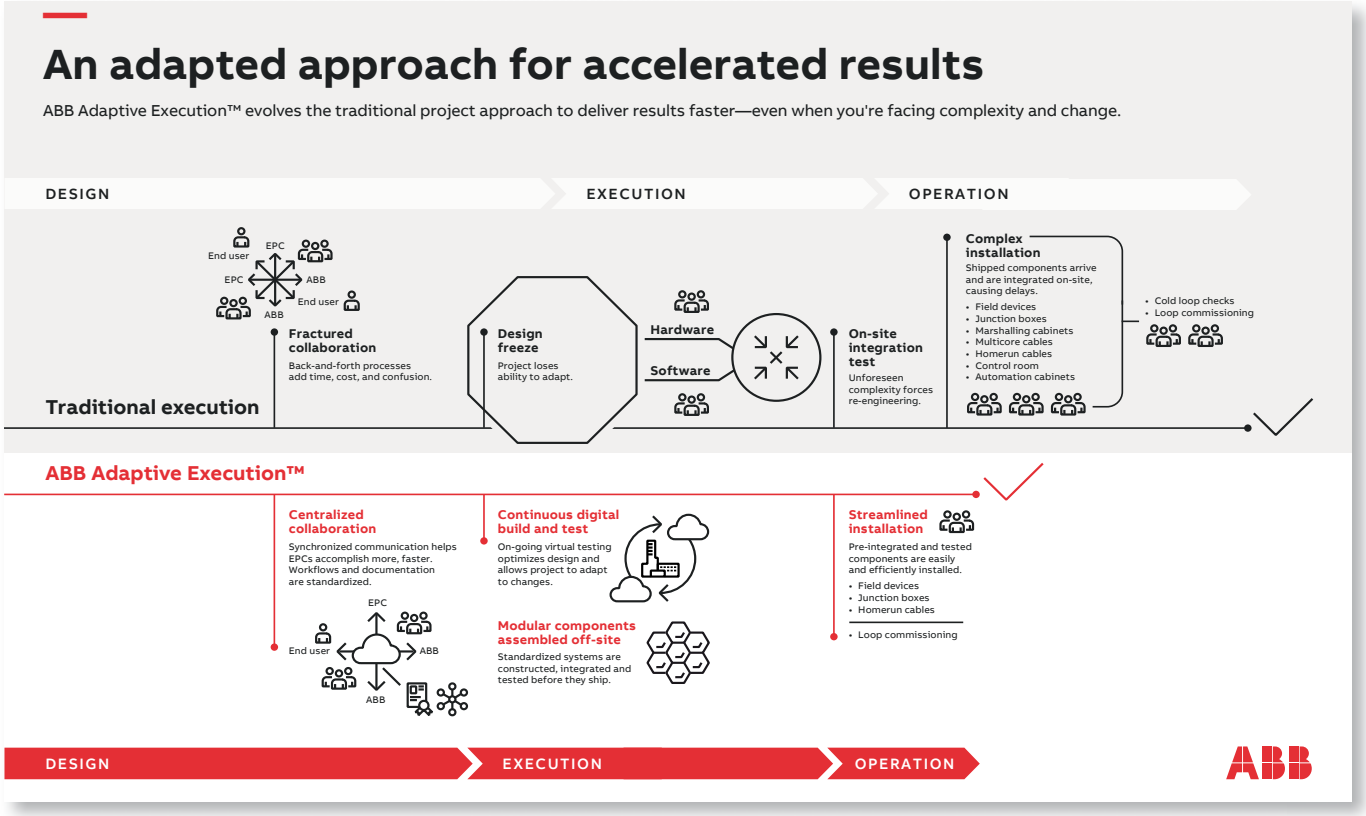


ABB Adaptive Execution integriert Expertenteams, neue Technologien, agile Prozesse, gemeinsames Lernen und bewährte Methoden.

IoT: Eine Bitkom-Studie aus 2020 besagt, dass durch die Digitalisierung bis 2030 umfangreiche Mengen an CO_2 eingespart werden könnten und diese demnach auch zum Klimaschutz beiträgt. Stimmen Sie dieser Aussage zu oder ist sie nicht eher widersprüchlich, da die Digitalisierung schlussendlich auch Energie benötigt?

Lau: ABB will aktiv zu einer nachhaltigeren Welt beitragen. Mit unserer Nachhaltigkeitsstrategie 2030 setzen wir uns aktiv für eine kohlenstoffarme Gesellschaft ein und arbeiten gemeinsam mit unseren Kunden und Lieferanten an der Umsetzung nachhaltiger Prozesse entlang unserer Wertschöpfungskette sowie über den Lebenszyklus unserer Produkte und Lösungen hinweg. Gleichzeitig wollen wir gemeinsam mit unseren Lieferanten und den Gemeinschaften, in denen ABB tätig ist, auch den sozialen Fortschritt vorantreiben. Den größten Einfluss auf die Reduzierung der Treibhausgasemissionen haben wir durch unsere innovativen Technologien, die den Energieverbrauch in der Industrie, in Gebäuden und im Transportwesen senken – Sektoren, die zusammen für fast drei Viertel des weltweiten Energieverbrauchs verantwortlich sind. Wir haben uns das ehrgeizige Ziel gesetzt, unseren Kunden zu helfen, ihre jährlichen CO_2-Emissionen bis 2030 um mehr als 100 Megatonnen zu reduzieren.
Das entspricht den jährlichen Emissionen von 30 Millionen Verbrennungsmotoren. So können beispielsweise unsere drehzahlvariablen Antriebe für Elektromotoren den Stromverbrauch um bis zu 25 Prozent reduzieren.

IoT: Das bedeutet konkret?

Lau: ... dass wir mit gutem Beispiel vorangehen wollen, indem wir CO_2-Neutralität in unseren eigenen Betrieben erreichen. Dies werden wir schaffen, indem wir vermehrt auf erneuerbare Energiequellen setzen, die Energieeffizienz in unseren Fabriken und Standorten verbessern und unsere Fahrzeugflotte auf elektrische oder andere emissionsfreie Alternativen umstellen.
Wir werden auch mit unseren Zulieferern in den Dialog treten, um unseren Einfluss auf die Reduzierung von Emissionen in der gesamten Lieferkette auszuweiten. Unsere digitalen Lösungen und Dienstleistungen sind definitiv ein Teil dieser Reise. Sie helfen Unternehmen, ihr Geschäft zu automatisieren, zu optimieren und zukunftssicher zu machen, um neue Höhen zu erreichen und nachhaltigen Fortschritt voranzutreiben.

IoT: Was erwartet sich ABB nun ganz gezielt bei den ABB-Lösungen wie Adaptive Execution für heuer, auch in Bezug darauf, dass Messen etc. nur eingeschränkt physisch stattfinden?

Lau: Im Oktober 2020 veranstaltete ABB ein virtuelles Kundenevent und eine virtuelle Pressekonferenz, um ABB Adaptive Execution weltweit vorzustellen. Ein spezielles „ABB Adaptive Execution Virtual Lab" wurde eingerichtet, um unseren Kunden aus aller Welt die Methodik zu präsentieren. Während der Live-Veranstaltung konnte man virtuell das ABB-Topmanagement treffen und in virtuellen Räumen die Kernattribute der Lösung erleben: Vision; Effektivität; Zusammenarbeit; Agilität und Effizienz. Das Lab ist auch jetzt noch auf Abruf verfügbar. Kunden können eine virtuelle, interaktive Tour durch unser Adaptive Execution Lab machen, um Demos anzusehen und die Inspiration hinter die sehr hochentwickelte Lösung für das Projektmanagement zu entdecken.

www.abb.com

Der Autor
Jelle Wieringa
... ist Security Awareness Advocate bei KnowBe4. KnowBe4 wurde vom IT- und Datensicherheitsspezialisten Stu Sjouwerman gegründet und unterstützt Unternehmen dabei, das Thema Sicherheit gezielt anzugehen, indem das Bewusstsein für Ransomware, Betrug etc. durch gezielte Sensibilisierungstrainings geschärft wird.

VORSICHT FALLE!

Was ist für Hacker naheliegender – wenn die Nutzung von E-Commerce steigt – als diesen Trend für Phishing-Kampagnen auszunutzen? Eben dies geschieht seit einiger Zeit vermehrt. Und weshalb? Die Covid-19-Krise und nicht nur das zurückliegende Weihnachtsgeschäft sorg(t)en dafür, dass viele Menschen ihre Einkäufe via Online-Bestellung erledigen.

Der Online-Versandhandel boomt und ist für viele eine Alternative geworden. Gleichzeitig wurde durch die Schließung des Handels aufgrund der Covid-19-Pandemie E-Commerce zu einer neuen, verstärkt genutzten Einkaufsmöglichkeit. Inzwischen lässt sich auch die Lieferung im Internet via Tracking verfolgen und wird oft über E-Mails dem Empfänger vorab angekündigt. Hierfür erhalten die Käufer bzw. Empfänger dann eine Nachricht mit einem Link zur Sendungsverfolgung.
Die Betrüger setzen genau hier an und fälschen solche E-Mails, die sie mit einem Phishing-Link versehen. Dieser leitet die Anwender auf eine ebenfalls gefälschte Webseite – die oft täuschend echt aussieht – und bittet darum, die Zugangsdaten, Zahlungsdetails oder andere personenbezogene Informationen einzugeben. Folgt ein Nutzer dieser Anweisung, wird er Opfer des Phishings und die Daten landen bei den Cyber-Kriminellen.

Obacht ist angesagt! Am liebsten wird derzeit das Transportunternehmen DHL für diese Zwecke missbraucht, wie unter anderem Nachforschungen von Check Point gezeigt haben. Die Sicherheitsforscher fanden heraus, dass die Anzahl solcher Betrügereien im Oktober 2020, verglichen mit dem September 2020, um 1.350 Prozent allein in Deutschland anstieg; in ganz Europa um 401 Prozent. Außerdem beobachteten sie im November 2020 eine Verdoppelung der Phishing-E-Mails, was wahrscheinlich auf die Sonderverkäufe rund um den Black Friday und Cyber Monday zurückzuführen ist.

Weiterhin bleiben solche Phishings relevant, in deren Zuge sich die Hacker als Zulieferer oder sogar Kunde eines Unternehmens ausgeben. Diese Erkenntnisse verdeutlichen erneut, wie wichtig eine gezielte Schulung der Mitarbeiter für Unternehmen ist, um Phishing abzuwehren. Denn die E-Mails gehen nicht nur an die privaten Postfächer der Menschen, sondern auch an die geschäftlichen, und eine unbedacht geöffnete Phishing-E-Mail kann für eine Firma schlimme Folgen haben – ob Datendiebstahl, Zugang zu Finanztransaktionen oder Einschleusung von Malware oder Ransomware.

Spezielle Kurse sensibilisieren Mitarbeiter. Online-Trainings-Kurse sind eine gute Methode, um die Angestellten auf allen Ebenen aufzuklären und ihr Bewusstsein für IT-Sicherheit zu stärken. Mithilfe einer Trainings-Plattform, die es erlaubt, Phishing aller Art zu simulieren und über verschiedene Module zur Schulung verfügt, lässt sich letzten Endes die Security Awareness im Unternehmen derart erhöhen und regelmäßig prüfen, dass eine echte menschliche Firewall aufgebaut werden kann. Denn die letzte Verteidigungslinie einer Firma stellen die Mitarbeiter dar und zum Schutz des Unternehmens, wie auch deren eigenem, sollten sie umfangreich gerüstet sein, um mit modernen IT-Bedrohungen umgehen zu können.

https://blog.knowbe4.com/author/jelle-wieringa

Bei international tätigen Kunden gibt es einen Trend hin zu vermehrtem Einsatz von Augmented Reality.

AUFWACHEN – UMDENKEN!

Im Interview mit IoT4 Industry & Business stellt Roman Oberauer, Vice President go to Market & Technical Services, NTT Ltd. in Österreich eindeutig klar, dass Österreich zwar auf dem richtigen Weg sei, bei der digitalen Transformation. Dennoch sei auch noch viel Luft nach oben vorhanden.

IoT4 Industry & Business: Kürzlich ist die Studie „Future Disrupted: 2021" mit den wichtigsten Prognosen zu aktuellen Technologietrends erschienen. Seit wann bringen Sie diese bei NTT Ltd. heraus und weshalb?
Roman Oberauer: Die Future Disrupted Reports gibt es seit dem Jahr 2016. Durch unsere langjährige Erfahrung am IT-Markt und unzählige Kundenkontakte können wir mit dem Report den Unternehmen einen Leitfaden liefern, damit sie die Vorteile der jeweiligen Technologien gut für sich nutzen können.

IoT: Und was sind für 2021 einem – nach dem „ersten Covid-19-Pandemie-Jahr" – wohl herausforderndem Jahr, die wesentlichen Kernaussagen der Studie?
Oberauer: Die Pandemie hat natürlich großen Einfluss auf die IT-Trends, allein schon wegen des veränderten Arbeitsumfeldes durch Homeoffice etc. Vor Ausbruch von Covid-19 haben unsere Studien gezeigt, dass die meisten Organisationen zwar die Notwendigkeit der digitalen Transformation sehen, es aber erhebliche Umsetzungslücken gab. Die Pandemie hat den Einsatz von Informationstechnologien deutlich beschleunigt.
Für das Jahr 2021 erwarten wir nun, dass sich der Wettlauf um eine effektive, digital fokussierte Kundenerfahrung beschleunigt, da diese für Unternehmen Priorität wird. Außerdem ist es an der Zeit, die Arbeitsplätze zu modernisieren und neue (hybride) Konzepte umzusetzen.

IoT: Was bedeutet das für die Sicherheit der Unternehmen?
Oberauer: Das Thema Security wird uns weiterhin begleiten, da es durch die rasante Umstellung auf Homeoffice bei vielen Firmen zu erheblichen Sicherheitslücken gekommen ist. Und steigende Datenmengen werden die Unternehmen auch künftig stark beschäftigen: Eine funktionierende Infrastruktur wird das Um und Auf: Hier geht der Trend Richtung APNs, um große Datenmengen in hoher Qualität übermitteln zu können.
Bei international tätigen Kunden sehen wir den Trend hin zu vermehrtem Einsatz von Augmented Reality. Nicht zuletzt durch Reisebeschränkungen ist es notwendig geworden, Fernwartungsservices auszubauen. Das gelingt zum Beispiel mit Datenbrillen, über die der Experte dem Techniker an der Maschine zugeschalten wird.

IoT: Die von der Studie erwähnten Zukunftsthemen setzen eine starke Digitalisierung bzw. einen entsprechenden Ausbau des Internets voraus. Wie schätzen Sie die vorhandenen Gegebenheiten für Österreich ein?

Oberauer: Österreich ist schon auf dem richtigen Weg, aber noch lange nicht am Ziel. Es gibt vielversprechende Initiativen, die hoffen lassen, wie zum Beispiel die Einführung von digitalen Amtswegen und den Ausbau des 5G-Netzes. Dafür muss aber der Zugang zu einem gut ausgebauten Internet in allen Regionen des Landes sichergestellt werden.
Viele Unternehmen haben ihre digitalen Möglichkeiten noch lange nicht ausgereizt, auch wenn Corona sicher ein Treiber war. Durch die Umstellung auf mobiles Arbeiten ist bei den Firmen das Bewusstsein jetzt geschärft. Da heißt es dranbleiben – und nicht nach der Krise in alte Muster zurückfallen.

IoT: Sie sprechen zudem in der Studie davon, dass der Datenumfang nur dann erfolgreich verarbeitet werden kann, wenn Strategien hierzu in den Unternehmen vorhanden sind. Welche Branchen sind auf das, was 2021 umgesetzt werden „muss", bestens vorbereitet?
Oberauer: Es gibt in Österreich Unternehmen aus allen Branchen, die schon vor der Krise ihren Fokus auf die digitale Transformation gelegt haben. Sie haben jetzt natürliche einen klaren (Wettbewerbs-) Vorteil. Doch auch Unternehmen, die sich erst in der Krise, mit digitalen Strategien auseinandergesetzt haben, sollten nicht verzagen und weiter daran arbeiten.

Die Pandemie hat großen Einfluss auf die Entwicklungen der IT.

IoT: Kommen wir noch einmal auf das Thema Security zurück. Zu viele Unternehmen „verzichten" nachwievor auf einen optimalen Schutz ihrer Daten. Weshalb?
Oberauer: Die Pandemie hat Cyber-Sicherheitsfragen sicher in den Mittelpunkt gerückt, doch es braucht vielfach auch noch Zeit, Versäumnisse aufzuholen. Unternehmen müssen Security noch stärker als „Enabler" ihres Geschäfts wahrnehmen und Security gleich von Beginn in ihren Lösungen mitdenken.

IoT: Welche Rolle spielen die Mitarbeiter dabei?
Oberauer: Die Mitarbeiter spielen eine zentrale Rolle, es liegt an den Unternehmen, Security-Bewusstsein zu schulen und kontinuierlich in den Fokus zu rücken. Für jeden Mitarbeiter sollen die möglichen Risken seiner Handlungen klar ersichtlich sein. Gerade in Zeiten von Homeoffce und mobile Working ist das ein großes Thema.
IoT: Abschließend bitte noch einen kurzen Ausblick: Welche Ziele haben Sie als NTT für 2021?
Oberauer: Wir haben uns neu aufgestellt, haben eine neue Geschäftsleitung und unser Portfolio klar positioniert. Wir wollen DER verlässliche Partner für große und mittelständische, vor allem internationale, Unternehmen und den öffentlichen Bereich sein. Unser Ziel ist es, unsere internationale Stärke auch in Österreich einzusetzen und zu zeigen, dass wir mit unseren lokalen Spezialisten den Kunden in der digitalen Transformation mit Experten zur Seite stehen. So können wir internationale Projekte lokal managen und weltweit koordinieren. (se)

https://hello.global.ntt/de-de/

Roman Oberauer
Vice President go to Market & Technical Services, NTT Ltd. in Österreich

„Viele Unternehmen haben ihre digitalen Möglichkeiten noch lange nicht ausgereizt, auch wenn Corona sicher ein Treiber war."

Die flexible Crossover-Lösung exOS bricht die Barriere zwischen IT und OT auf und verbindet beide Welten.

DAS WELTWEIT GRÖSSTE SOFTWARE-ÖKOSYSTEM

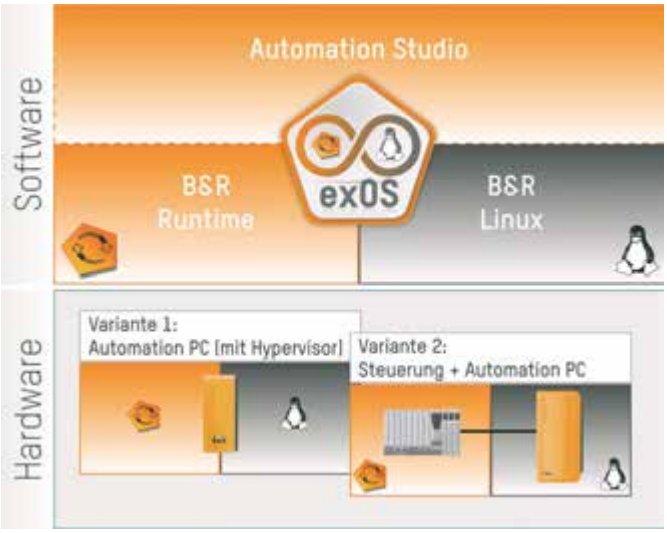
Wie finden IT und OT zusammen? Vor dieser Frage stehen alle Unternehmen, die Industrie 4.0 umsetzen wollen. Bisher gab es darauf keine wirkliche Antwort.

Ein Team ist immer nur so gut wie seine Mitglieder. Allerdings reicht es nicht aus, nur die Besten aus den unterschiedlichen Fachbereichen an einen Tisch zu setzen. Die Teammitglieder müssen auch die Möglichkeit bekommen, mit ihren unterschiedlichen Ansätzen und Arbeitsweisen eine gemeinsame Lösung zu erarbeiten und moderne Maschinenlösungen lassen sich nicht ohne Teamarbeit umsetzen.

Maschinenbauer benötigen zunächst IT- und OT-Experten, die in interdisziplinären Teams zusammenarbeiten. Nur so können sie die Möglichkeiten des Industrial IoT voll ausschöpfen und vernetzte Maschinen entwickeln. Allerdings prallen hier zwei Welten aufeinander: Während sich OT-Experten mit Maschinenentwurf, SPS-Programmierung und Maschineninbetriebnahme auskennen, sind IT-Experten mit höheren Programmiersprachen und Konzepten wie C++, Python und JavaScript vertraut und arbeiten mit Open Source-Software und Linux. Daher finden sie oft nur schwer einen gemeinsamen Lösungsansatz.

Die fertige Linux-Anwendung wird vom Entwickler einfach als exOS-Paket ins B&R-System importiert. Dadurch kann Automation Studio als zentrales Engineering-Tool verwendet werden.

Neue Wege der Gemeinsamkeit. Die Herausforderung liegt darin, die Hürde in der Zusammenarbeit zwischen IT- und OT-Welt zu überwinden und beide Welten optimal zu verbinden. „Mit dem Industrial IoT ist der Zeitpunkt gekommen“, sagt Stefan Bina, Product Manager Industrial IoT Network Solutions bei B&R. „Die Grenzen zwischen der IT- und OT-Welt müssen verschwinden.“ Die größte Schwierigkeit dabei ist, dass Steuerungssysteme aktuell nicht die volle Bandbreite an höheren Programmiersprachen ausführen können. Die Voraussetzung für die Verbindung von IT und OT muss daher sein, sämtliche Linux-Software für das Steuerungssystem zugänglich und verständlich zu machen.
Genau an diesem Punkt setzt B&R mit dem neuen enhanced crossover Operating System, kurz exOS, an. „Mit exOS überwinden wir die Hürde, die IT und OT bisher voneinander getrennt hat. Maschinenbauer können nun jede beliebige Linux-Software im B&R-System verwenden und so endlich die IT- und OT-Welt optimal verbinden. Damit erhalten Maschinenbauer Zugang zum weltweit größten Software-Ökosystem“, so Bina.
Mit exOS steht es jedem Linux-Softwareentwickler frei, in welcher Programmierumgebung (IDE) er den Programmcode entwickelt, kompiliert und debuggt. Anschließend lässt sich die Linux-Anwendung mit Hilfe von exOS einfach in das Steuerungssystem integrieren und Hand in Hand mit dem B&R-Echtzeitbetriebssystem Automation Runtime verwenden. „Das bietet den großen Vorteil, dass der Entwickler in seiner gewohnten Entwicklungsumgebung, zum Beispiel mit Eclipse oder Visual Studio, arbeiten und auf seine Erfahrungen und Expertise mit diesen Werkzeugen zurückgreifen kann“, erklärt er weiter.



Maschinenbauer können zwischen zwei unterschiedlichen Umsetzungsvarianten für exOS wählen.

exOS verfügt über zahlreiche integrierte Funktionen, mit denen sich hybride Maschinenapplikationen mit Steuerungs- und Linux-Anwendungen wesentlich einfacher erstellen lassen.

Ein zentrales Engineering-Tool. Die fertige Linux-Anwendung wird vom Entwickler einfach als exOS-Paket ins B&R-System importiert. Ab diesem Entwicklungsschritt kann Automation Studio als zentrales Engineering-Tool verwendet werden. Das Softwaremanagement und die Softwarediagnose gestalten sich so wesentlich einfacher und übersichtlicher. Zusätzliche Werkzeuge sind nicht notwendig. „Das heißt, nicht nur der Linux-Softwareentwickler, sondern auch der Ingenieur, der die Maschine in Betrieb nimmt, kann in seiner gewohnten Umgebung arbeiten, da die Crossover-Lösung exOS alle Ebenen vereint“, sagt Bina.
Neben der unkomplizierten Inbetriebnahme ist auch eine schnelle und einfache Wartung ein wesentliches Qualitätsmerkmal für smarte Maschinen. Servicetechniker müssen zum Beispiel bei einem Maschinenstillstand schnellstmöglich identifizieren, wo das Problem liegt und Rücksprache mit dem Maschinenbauer halten können. exOS bietet zudem umfangreiche Diagnosefunktionen für die Installation und Code-Ausführung. Das B&R-System zeichnet sämtliche Fehlermeldungen des Steuerungsbetriebssystems und der Linux-Anwendung durchgängig auf und stellt sie dem Anwender zur Verfügung. Darüber hinaus lassen sich Hardware-Komponenten einfach tauschen. Die Maschine ist so ohne Neuprogrammierung binnen Minuten wieder einsatzbereit.

Zukunftssichere Lösung. Die Crossover-Lösung von B&R verfügt über zahlreiche integrierte Funktionen. Damit lassen sich hybride Maschinenapplikationen mit Steuerungs- und Linux-Anwendungen wesentlich einfacher erstellen. Die integrierten Funktionen werden symmetrisch in Automation Runtime und Linux ausgeführt. Zu den Funktionen zählen unter anderem ein einheitliches Projektmanagement für Linux- und Steuerungsanwendungen in Automation Studio sowie eine automatische Übertragung der Linux-Anwendung von Automation Studio auf die Steuerung und die Linux-Umgebung. Darüber hinaus bringt exOS eine nutzerfreundliche API für einen leistungsfähigen Datenaustausch mit. Die API sorgt für eine einfache und gepufferte Prozessdatenkommunikation zwischen dem Steuerungsbetriebssystem und Linux und überträgt Daten konsistent im Millisekundenbereich.

www.br-automation.com

Die Autorin:
Carola Schwankner
... ist Unternehmensredakteurin bei B&R in Eggelsberg.

Interview

MEHR GESTALTUNGSMÖGLICHKEITEN

IoT 4 Industry & Business: Herr Bina, Sie sagen, die Grenzen zwischen IT und OT seien derzeit noch eine Hürde und müssen auf kurz oder lang verschwinden. Wie soll das Ihrer Ansicht nach funktionieren?
Stefan Bina: Maschinenbauer sind darauf angewiesen, dass ihre Experten aus IT und OT zusammenarbeiten. Nur wenn beide Bereiche optimal eingebunden sind, lassen sich die Möglichkeiten des Industrial IoT voll ausschöpfen und vernetzte Maschinen entwickeln. Deshalb ist es notwendig, eine Lösung zu finden, die beide Welten vereint und darüber hinaus auch die Inbetriebnahme der Maschinen sowie die Wartung und Instandhaltung vereinfacht.

IoT: Das bedeutet?
Bina: Mit der stetigen Zunahme der Rechenleistung industrieller Steuerungen, der Umstellung auf PC- oder ARM-Plattformen und der vierten industriellen Revolution steigt auch die Bedeutung von Linux in der Automatisierungstechnik. Viele der Aufgaben eines Automatisierungssystems können bereits jetzt auf einem Linux-basierten System bewerkstelligt werden.
Das Linux-Software-Ökosystem bietet eine Vielzahl an frei verfügbaren oder proprietären Softwarepaketen, wie Pfadplanungsbibliotheken für Robotersysteme, Machine Learning-Algorithmen zur Maschinenoptimierung oder übersichtliche Liniensteuerung mittels grafischer Programmierung im Baukastenprinzip.

IoT: Jetzt käme exOS von B&R ins Spiel. Was genau kann es?
Bina: exOS öffnet nun Maschinenbauern die Tür zu diesen Softwarepaketen. Konkret verbindet unsere Crossover-Lösung die zyklusbasierte Steuerungswelt mit der Event-basierten Linux-Welt über eine robuste Programmierschnittstelle. Diese Schnittstelle ermöglicht das Deployment, den schnellen Datenaustausch, die Zeitsynchronisierung und die Diagnose bei maximaler Flexibilität im Hardwaresetup.
exOS wird als Technologiepaket zur Verfügung gestellt und lässt sich einfach direkt über die B&R-Automatisierungssoftware Automation Studio installieren. Maschinenbauer können mit exOS das Know-how ihrer Entwickler und Ingenieure aus IT und OT voll ausschöpfen und hybride und adaptive Maschinenkonzepte mit einer kurzen Time-to-Market umsetzen.

IoT: Wie leicht ist die exOS-Lösung anzuwenden?
Bina: Mit exOS kann nun jede beliebige Linux-Anwendung im B&R-System verwendet werden. Jeder Linux-Softwareentwickler kann frei wählen in welcher Programmierumgebung er den Programmcode entwickeln möchte und mit exOS anschließend die Linux-Anwendung ganz einfach in das Steuerungssystem integrieren. Ab diesem Zeitpunkt gibt es nur mehr ein einziges Engineering-Tool, nämlich Automation Studio.

IoT: Ein klarer Vorteil?
Bina: Ja, denn das vereinfacht nicht nur Softwaremanagement und -diagnose, sondern auch die Wartung. Servicetechniker müssen zum Beispiel bei einem Maschinenstillstand schnellstmöglich identifizieren, wo das Problem liegt und Rücksprache mit dem Maschinenbauer halten können. Mit exOS werden sämtliche Fehlermeldungen der Linux-Anwendung durchgängig aufgezeichnet und sind jederzeit abrufbar.
Auch ein Hardwaretausch oder Maschinenupdates können schnell und einfach vorgenommen werden. Stillstandzeiten von Maschinen und Anlagen verringern sich dadurch deutlich. Somit können der Linux-Softwareentwickler, der Steuerungsprogrammierer und die Ingenieure, die die Maschine in Betrieb nehmen oder sie warten, in ihrer gewohnten Umgebung arbeiten. Das bietet einen größtmöglichen Grad an Gestaltungsfreiheit. Zudem verringert sich die Einarbeitungszeit der jeweiligen Mitarbeiter sehr deutlich oder entfällt komplett.

IoT: Der Weg zur smarten Fabrik nimmt auch mit den angebotenen Lösungen immer mehr Gestalt an. Wie weit sehen Sie bereits die Unternehmen in ihren Umsetzungen und war das erste Pandemie-Ausnahmejahr ein digitaler Förderer, auch was die Nachfrage der Lösungen betrifft?
Bina: Die Digitalisierung in den Fabriken ist bereits seit geraumer Zeit in vollem Gang. Nicht zuletzt ist die in den vergangenen Jahren deutlich gestiegene Nachfrage nach individualisierten Produkten ein wesentlicher Treiber. Die Pandemie hat diesen Trend sicherlich noch einmal verstärkt und gezeigt, dass Konsumenten Ware per Mausklick bestellen und möglichst schnell erhalten möchten.
Deshalb müssen Maschinen in smarten Fabriken vor allem adaptiv sein und innerhalb kürzester Zeit unterschiedliche Güter produzieren. Hier stoßen noch viele Unternehmen an ihre Grenzen, denn mit einem herkömmlichen Ansatz und den bekannten Konzepten, lassen sich die neuen Anforderungen hinsichtlich Adaptivität nicht mehr erfüllen. Die Unternehmen benötigen neue und flexible Produktionskonzepte sowie eine standardisierte und IT-/OT-konvergente Kommunikation zwischen den Maschinen und nicht zuletzt möglichst viel Freiheit in der Maschinenprogrammierung.
Diese Freiheit erhalten sie, wenn höhere Programmiersprachen wie C++, Python und JavaScript eingesetzt werden können – und genau an diesem Punkt kommt exOS und der damit verbundene Zugang zum weltweit größten Software-Ökosystem ins Spiel.

Stefan Bina
Product Manager Industrial IoT Network Solutions bei B&R

IHRE VERBINDUNG WIRD GEHALTEN

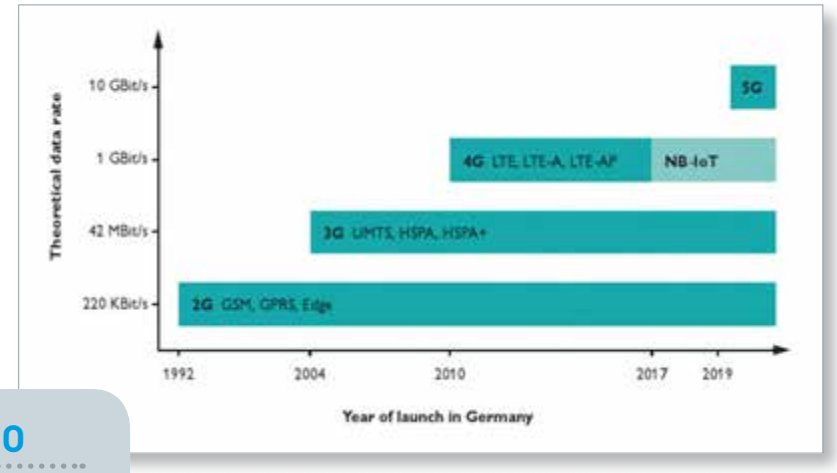
Prozesskommunikation gestört! Diese Meldung könnte bald auf den Bildschirmen vieler Leitzentralen zu sehen sein, wenn der jeweilige Provider die 3G-Technologie abgeschaltet hat und die per Mobilfunk angebundenen Außenstationen daher nicht mehr erreichbar sind. Was tun?

Mit dem Internet of Things (IoT), Industrie 4.0 und 5G werden derzeit zahlreiche neue Technologien diskutiert. Bei all den Vorteilen, die sie in Zukunft bringen, bleibt ein dann für die Anlagenbetreiber auftretendes Problem fast unbeachtet: In Deutschland etwa wird als erstes die 3G-Mobilfunktechnologie abgeschaltet. Warum aber? Der Großbuchstabe G steht für Generation und wird als Oberbegriff für die technischen Evolutionsstufen des Mobilfunks verwendet. Die analogen Vorläufer der ersten Generation – auch bekannt als A-, B- und C-Netz – waren durch teure, kofferraumgroße Endgeräte, inkompatible Netze und fehlende Massentauglichkeit gekennzeichnet. Die zweite Generation stellt das erste digitale Mobilfunknetz im heutigen Sinn dar. 2G wurde durch eine Arbeitsgruppe – die Groupe Spécial Mobile (GSM) – einheitlich spezifiziert. Es setzt sich aus dem D1-Netz der Telekom (ehemals Deutsche Bundespost), dem D2-Netz von Vodafone (seinerzeit Mannesmann) sowie dem späteren E1- und E2-Netz von Telefónica (früher E-Plus und o2) zusammen. 2G umfasst die Technologien GSM (Global System for Mobile Communication), GPRS (General Packet Radio Service) und EDGE (Enhanced Data Rates for GSM Evolution).

Mehr WWW, mehr Datenvolumen. Mit der zunehmenden Nutzung des Internets kam der Datenkommunikation eine stetig größere Bedeutung zu, sodass die Telefonie und der SMS-Versand nicht mehr die treibenden Kräfte der Weiterentwicklung waren. Zur Umsetzung der neuen Herausforderungen wurde mit der 3GPP (Third Generation Partnership Project) ein weiteres Gremium ins Leben gerufen, das den 3G-Standard mit den Technologien UMTS (Universal Mobile Telecommunications System), HSPA (High Speed Packet Access) und HSPA+ entwickelte. LTE (Long Term Evolution), besser bekannt als 4G, markierte schließlich den letzten großen Technologieschritt mit einer weiter gestiegenen Datenrate. Anfangs musste streng genommen von 3.9G gesprochen werden, da noch nicht alle Spezifikationen erfüllt wurden, was dann mit LTE Advanced und LTE Advanced Pro der Fall war. Zur vierten Generation gehören darüber hinaus aktuelle Technologien wie LTE-Cat-NB1 (NB-IoT) und LTE-Cat-M1 für das Internet of Things, die sich erstmals auf die datenarme Übertragung im Mobilfunknetz fokussieren.

Geringerer Netzausbau. Um zu verstehen, warum 3G als erster Standard vom Netz geht, gilt es zwei maßgebliche Aspekte >>

Historie der Mobilfunktechnik ab der zweiten Generation.



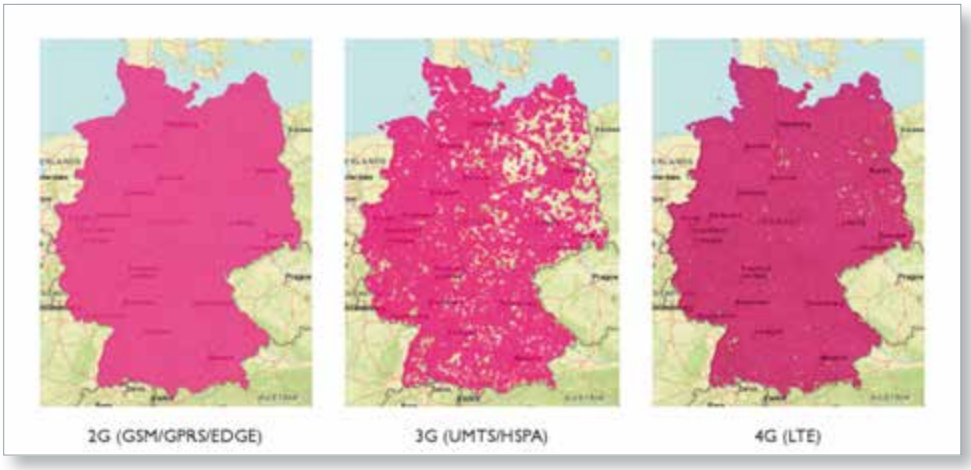
UMFASSENDES 4G-PORTFOLIO

Das 4G-Mobilfunkportfolio von Phoenix Contact stellt von einfachen Alarmierungs- und Schaltaufgaben über klassische Fernwirkapplikationen bis zur weltweiten Fernwartung von Maschinen und Anlagen für jede Aufgabenstellung eine passende Lösung zur Verfügung. Da eine Störungsbenachrichtigung der Ausnahmefall sein sollte, bietet sich hier eine eventorientierte Kommunikation über die Produktfamilie TC Mobile I/O an. Die Geräte informieren die Leitwarte oder den Mitarbeiter im Feld per SMS, E-Mail oder App. Die SMS-Technologie erweist sich bei einem niedrigen Datenvolumen noch immer als kostengünstigste Alternative und stellt daher auch weiterhin einen festen Bestandteil im LTE-Netz dar.
Für den kontinuierlichen, wirtschaftlichen Datenaustausch mit den Außenstationen via VPN und Fernwirkprotokoll eignen sich die Geräte der Baureihe TC Router am besten. Die Produktfamilien TC Cloud Client und TC mGuard fokussieren sich schließlich auf die Fernwartung der stetig höher automatisierten Produktionsanlagen im Maschinenbau. Neben einem zunehmenden Service durch die Spezialisten des Maschinenbauers benötigen derartige Applikationen aufgrund der steigenden Security-Anforderungen (IEC 62443 oder ISO/IEC 27001) turnusmäßige Software-Updates. Dazu müssen die IT-Netze des Maschinenbetreibers und -bauers sicher verbunden sowie die zahlreichen weltumspannenden VPN-Verbindungen gemanagt werden.

Phoenix Contact bietet für alle Anwendungsfälle von einfachen Alarmierungsaufgaben über zuverlässige Fernwirktechnik bis zur sicheren Fernwartung eine passende Lösung per 4G-Mobilfunktechnologie.

zu betrachten. Dies ist zum einen die Abdeckung der Netze. In Deutschland erweist sich das 2G-Netz als am besten ausgebaut und bildet daher ohne Investitionsbedarf das Rückgrat der Mobilfunkkommunikation. In der Funktion eines Fallback-Netzes bietet 2G die beste Lösung für die Telefonie (Notrufe und SMS) sowie bereits bestehende M2M-Applikationen. Als zweiter Aspekt kommt die Datenrate ins Spiel. Das 4G-Netz bedient den Consumer-Markt hier mit der notwendigen Bandbreite, während 3G mit HSPA+ lediglich 42 MBit/s zur Verfügung stellt. 2014 gab die Bundesregierung das Ziel aus, jedem Haushalt einen Internetzugang mit 50 MBit/s zugänglich zu machen. Weil diese Vorgaben 2015 bei der Frequenzversteigerung durch die Bundesnetzagentur mit 3G nicht zu erreichen waren, vernachlässigten die Provider den entsprechenden Netzausbau.
Doch auch vor 2014 kam die Erweiterung des 3G-Netzes nur schleppend voran. Der Grund hierfür lag in den Lizenzkosten bei der Versteigerung der UMTS-Frequenzen. Die damals gezahlten 100 Milliarden DM fehlten beim späteren Netzausbau. So erklärt sich, weshalb lediglich in 4G-Netze investiert wird und die LTE-Abdeckung schon heute das 3G-Netz aussticht. Schlussendlich hat das 3G-Netz seine Bedeutung verloren und die dafür verwendeten Frequenzräume können von den Netzbetreibern effektiver im 4G-Netz eingesetzt werden.

Sukzessiver Rückbau. In diesem Kontext passt der Begriff „Abschaltung“ eigentlich nicht. Mit Blick auf das Freiräumen von Frequenzbereichen muss eher von einem Rückbau gesprochen werden. Der Kunde verliert hingegen ab diesem Zeitpunkt den Anspruch auf die Verfügbarkeit des 3G-Netzes. Die Provider werden die Mobilfunkzellen sukzessive auf die neueren Technologien umrüsten. Ein Anlagenbetreiber kann also bereits kurz nach dem offiziellen Abschalttermin das Pech haben, dass sich seine 3G-Geräte nicht mehr in das Netz einwählen können. Die genauen Zeitangaben muss er direkt vom jeweiligen Netzbetreiber einholen, denn die Abschalttermine variieren von Anbieter zu Anbieter.
Die Telekom (D1-Netz) geht auf den erwähnten Anspruch schon in ihren allgemeinen Geschäftsbedingungen ein. In der Leistungsbeschreibung Mobilfunk heißt es: „Die dort aufgeführte Netztechnologie 3G […] im Mobilfunknetz der Telekom ist – vorbehaltlich einer Verlängerung – nur bis zum 31.12.2020 verfügbar.“ Eine solche schriftliche Aussage gibt es für das



Mobilfunkabdeckung der Telekom bei den jeweiligen Technologien; 3G konkurriert weder bei der Bandbreite noch bei der Abdeckung.

von Vodafone betriebene 2D-Netz noch nicht. Durch den Chief Technology Officer Johan Wibergh wurde lediglich kommuniziert, dass das Unternehmen eine 3G-Abschaltung in den Jahren 2020 und 2021 anstrebt. Am längsten wird die Technologie vom Telefónica-Netz unterstützt. Im Strategie-Update 2019 des Providers ist die 3G-Abschaltung erst für Ende 2022 vorgesehen.

Vorteilhafter 4G-Umstieg. Wie sollte ein Anlagenbetreiber vorgehen, damit die Kommunikationsverbindung zu seinen Außenstationen nicht unterbrochen wird? Zunächst ist zu überprüfen, ob 3G-Geräte für den Datenaustausch genutzt werden und die hier verfügbare Datenrate tatsächlich erforderlich ist. Bei einfachen Maschinendaten mit einem geringen Kommunikationsvolumen kann nämlich eine 2G-Verbindung noch ausreichend sein. Bietet das Mobilfunkgerät die Option, die Einwahl in das 3G-Netz zu verhindern, lässt sich durch einen einfachen Feldtest herausfinden, ob die Anlage weiterhin über das 2G-Netz erreichbar bleibt. Selbst wenn die Kommunikation der Applikation mit der Leitzentrale per 2G möglich ist, lohnt sich eine Betrachtung der neueren Technologien. Denn die aktuellen IoT-Netze – wie beispielsweise LTE-Cat-NB1 – können die Investition in neue Hardware unter Umständen durch geringere Verbindungskosten rechtfertigen. Möglicherweise lässt sich die Kombination aus Sensor, Steuerung, Netzteil und Router für eine einfache Pumpenanwendung sogar durch ein einziges batteriebetriebenes IoT-Gerät ersetzen. Ein klassischer 4G-Router eröffnet hingegen zusätzliche Optionen, etwa die Übertragung von Bildern einer Überwachungskamera. Neben der Hardware darf der Mobilfunkvertrag ebenfalls nicht außer Acht gelassen werden. Es ist davon auszugehen, dass Drittanbieter wie congstar oder Aldi Talk ihre Verträge um den LTE-Zugang erweitern, was die Anwender jedoch im Vorfeld klären müssen.

Zukünftige 5G-Verfügbarkeit. Auch wenn momentan hauptsächlich über 5G gesprochen wird, betrifft dieser Standard die heutigen Anlagenbetreiber noch nicht. 5G startet mit dem Fokus auf hohe Datenraten (Release 15). Um diese zu erreichen, verkleinern sich die Funkzellen und der Ausbau beschränkt sich daher zunächst auf den Bereich von Großstädten. Die nicht final spezifizierten Anforderungen an mMTC (Massive Machine Type Communications) oder uRLLC (Ultra Reliable Low Latency Communications) werden erst 2020 mit dem nächsten Evolutionsschritt (Release 16) umgesetzt oder sind schon durch die bestehenden IoT-Netzwerke abgedeckt. Derzeit lässt sich nicht abschätzen, wann industrietaugliche Seriengeräte kostengünstig erhältlich sind und die ländliche 5G-Abdeckung komplett vollzogen ist. Aktuelle Bestandsapplikationen, welche die neuen 5G-Funktionen nicht benötigen, brauchen sich im Rahmen der Abschaltung des 3G-Netzes also nicht mit dem Thema 5G zu beschäftigen.
Auf eine sofortige Unterbrechung der Prozesskommunikation müssen sich die Anwender somit nicht einstellen. Nach den offiziellen Terminen ab Ende 2020 schalteten die Provider die 3G-Funkzellen landesweit nicht ab, sondern bauten sie kontinuierlich zurück. Eine genaue Aussage, wann welche Station auf neuere Technologien umgerüstet werden muss, lässt sich folglich nicht treffen.

www.phoenixcontact.at/fernkommunikation

Mobile Network Operator (MNO)	Mobile Virtual Network Operator (MVNO)	Expected shutdown date
Deutsche Telekom (D1)	Telekom, congstar, EDEKA, freenetmobile, Klarmobil, callmobile, ...	End of 2020
Vodafone (D2)	Vodafone, 1&1, LIDL connect, OTELO, freenetmobile, Klarmobil, FYVE, callmobile, ...	2020 / 2021
Telefónica (E-Plus/O2)	O2, 1&1, ALDI Talk, Blau, BASE, Fonic, PremiumSIM, Klarmobil, smartmobil, ...	2022

Übersicht über die zu erwartenden Abschalttermine der Netzbetreiber.

HERAUSFORDERUNG DIGITALES ENGINEERING

Die digitale Transformation bietet dem Maschinenbau langfristig enorme Effizienzpotenziale – umso mehr, je früher die richtigen Weichen gestellt werden.

Effizientere Prozesse und eine kürzere Time-to-Market sind wesentliche Faktoren für den Maschinenbau, um sich im weltweit härter werdenden Wettbewerb zu behaupten. Die Anforderungen der Kunden stehen dem entgegen: Flexiblere Maschinen, die effizienter und leistungsfähiger sind, machen den Entwicklungsprozess aufwändiger und fehleranfälliger. Mit Hilfe digitaler Tools gelingt es schon heute, den Zeit- und Ressourceneinsatz im Engineering zu begrenzen. Doch sie versprechen noch mehr: In Zukunft können sie über den gesamten Lifecycle dazu beitragen, Abläufe zu vereinfachen, Kosten zu senken und damit das Dilemma des Maschinenbaus zu lösen.

Informationsfluss entscheidend. Für die Entwicklung einer Maschine ist ein bewährtes Prinzip die Modularisierung: erprobte Funktionseinheiten werden wiederverwendet und nicht immer wieder neu designt. Profitieren können Maschinenbauer und Anwender über weite Teile des Lifecycles: Vom Design über Programmierung und Inbetriebnahme bis hin zu Lagerhaltung und Ersatzteillogistik. Die wichtigste Voraussetzung, um auf Informationen aus vorangegangenen Projekten zurückgreifen zu können: dass diese in standardisierter Form verfügbar sind. Genau an dieser Stelle setzt der „Digitale Zwilling“ an. Er bildet physische Komponenten und Maschinen elektronisch ab und fungiert als Sammelpunkt für alle relevanten Informationen. Das Konzept ist unter dem Namen „Verwaltungsschale“ bereits ein Kernbestandteil im Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0), im internationalen Sprachgebrauch als Asset Administration Shell (AAS) bezeichnet.

Zwar wurden bereits vor drei Jahren wesentliche Schritte zur Standardisierung der AAS von der Plattform Industrie 4.0 verabschiedet. Doch erst langsam schließen sich die Lücken, die bislang einer durchgängigen Datennutzung im Weg stehen.

Moderne Design-Werkzeuge. Einen wesentlichen Beitrag dazu leistet Lenze zukünftig mit Werkzeugen und Apps, die das AAS-Konzept bereits heute anwendbar machen. Hier ist vor allem der Easy System Designer (ESD) zu nennen, der die ersten Engineering-Schritte wie Idee, Design und konkrete Entwicklung abdecken wird. Mit einem solchen webbasierten Werkzeug können alle am Planungsprozess beteiligten Personen der unterschiedlichen mechatronischen Fachdisziplinen die komplette Planung von Automationslösungen, vom Controller bis zur Antriebstechnik, inklusive der nötigen Applikationssoftware, durchführen.

Die Informationen, die dabei anfallen und in der AAS bezie-

hungsweise dem Digitalen Zwilling gesammelt werden, stehen auch in den folgenden Lifecycle-Phasen zur Verfügung. So sorgt Lenze mittelfristig mit passenden Schnittstellen dafür, dass beispielsweise Werkzeuge von Drittherstellern für Simulation und Virtual Commissioning darauf zugreifen können. Im Entwicklungsprozess können so Fehler schneller entdeckt und behoben werden, die Zeit für Auslieferung und Inbetriebnahme reduziert sich deutlich.

Smartes Engineering. Lenze leistet mit seinen Apps und Werkzeugen einen wesentlichen Beitrag zur durchgängigen Datennutzung. Ein neues Entwicklungsprojekt beginnt im ESD mit der Definition grundsätzlicher Maschinenfunktionen. Auf dieser Grundlage lässt sich bereits programmgestützt eine Machbarkeitsprüfung erstellen, die frühzeitig auf mögliche Probleme hinweist.
Beim Design werden Struktur der Applikationen und der I/O angelegt sowie die benötigte Steuerung festgelegt. Dabei können bereits vorhandene Lösungsmodule berücksichtigt werden. Auch bei diesem Schritt hilft das Planungswerkzeug bei der Machbarkeitsprüfung und deckt potenzielle Konflikte auf.
Für den OEM sind insbesondere die digitalen Assistenten eine wichtige Unterstützung. Die Auswahl von Komponenten, die Planung von Strukturen und das Aufspüren von Inkonsistenzen und potenziellen Problemen wird mit Hilfe der intelligenten Helferlein beschleunigt und vereinfacht. So wird der ESD zu einem smarten Entwicklertool.
Darüber hinaus legt der Easy System Designer den Grundstein für einen Digitalen Zwilling, also die Asset Administration Shell (AAS), die Struktur und Daten der Maschine als Single Point of Information enthält. Dazu zählen etwa die verwendeten Komponenten und ihre Eigenschaften, Informationen zur Software und noch vieles mehr. Auf diese Weise kann man auch später auf alle benötigten Informationen zentral und standardisiert zugreifen. Ein einheitliches Datenmodell eröffnet die weitere Nutzung auch in anderen Werkzeugen oder sogar in Tools anderer Hersteller.
Ein Beispiel dafür liefert das Lenze-Asset-Management. Das greift im späteren Betrieb genau auf diese Daten zu, beispielsweise wenn es darum geht, beim Ersatz einer Komponente die richtige Variante auszuwählen und Fehlbestellungen zu vermeiden. So vergrößert sich der Nutzen des Digital Engineering mittels AAS Schritt für Schritt.

Zentraler Mosaikstein der Digitalisierung. Digitales Engineering und Digitaler Zwilling sind nicht länger Theorie und auch kein Versprechen auf eine ferne, ungewisse Zukunft, sondern sind in der Realität angekommen. Sie können bereits praktisch eingesetzt werden und liefern einen nachweisbaren Mehrwert. Was nicht übersehen werden darf: Die Entwicklung ist noch lange nicht zu Ende, sondern bietet noch enormes Potenzial, wenn man beispielsweise auf eine durchgängige Nutzung der AAS und der darin enthaltenen Informationen denkt.
Ein weiterer Aspekt der zunehmenden Digitalisierung ist das Zusammenspiel in ganz unterschiedlichen Bereichen, das weitere Vorteile generiert. Etwa die einfachere Nutzung von Cloud-Services, die zur Optimierung von Fertigungsprozessen beitragen. Oder die intelligente Auswertung von Betriebsdaten, beispielsweise aus Antrieben, die zusätzliche Sensoren überflüssig machen. Und nicht zuletzt auch die erhöhte Flexibilität von Anlagen, in denen ganze Fertigungsmodule einfach per Plug & Produce ausgetauscht werden können.

www.lenze.com

Für den OEM sind insbesondere die digitalen Assistenten eine wichtige Unterstützung.

© Software Competence Center Hagenberg

Zu sehen ist das Projektteam von AI@Work.

ES **BEWEGT** SICH WAS

Mit knapp 500 Teilnehmern fand am 10. Dezember der 5. Summit Industrie 4.0 zum ersten Mal in virtueller Form statt. Es wurde aus dem Schumpeter Labor der TU Graz übertragen. Diesmal in Kooperation mit den beiden Standortagenturen, Steirische Wirtschaftsförderung SFG und Babeg Betriebsansiedlungs- und Beteiligungsgesellschaft.

Die Veranstalter hatten sich mit dem neuen virtuellen Format etwas ganz Besonderes ausgedacht und es gelang, mit knapp 500 Teilnehmern den 5. Summit Industrie 4.0 erfolgreich durchzuführen. Neu war nicht nur das virtuelle Format, auch wurden neben der Main Stage mit gewohntem Plattform Industrie 4.0-Programm zwei weitere thematische Schwerpunkte am Nachmittag gesetzt. Das Abschlussevent des Leitprojektes IoT4CPS zu Security im IoT-Kontext und das Kickoff-Event des Projektes Change2Twin zum Thema Digitaler Zwilling in der Produktion wurden in Parallelsessions näher beleuchtet.

Als internationales Partnerland konnte sich Australien präsentieren und deren Digitalisierungsstrategien anhand von konkreten Cases vorstellen. Auf die Frage hin weshalb ausgerechnet mit einem „am weitesten entfernten Land der Welt“ eine Partnerschaft eingegangen wurde antwortete Kurt Hofstädter, Vorstandsvorsitzender Plattform Industrie 4.0 Österreich. „Auch die Vernetzung mit internationalen Partnerplattformen wurde 2020 weiter voran-

Kurt Hofstädter,
Vorstandsvorsitzender Plattform Industrie 4.0 Österreich

„Die Vernetzung mit internationalen Partnerplattformen wurde 2020 weiter vorangetrieben.“

getrieben – mit Australien wurde erstmals ein Memorandum of Understanding mit einem außereuropäischen Partner unterzeichnet, der intensive Austausch mit den österreichischen Nachbarländern fortgesetzt und ein Blick weitab über die eigenen Landesgrenzen hinaus beschert einem des Öfteren einen besseren Blick auf das, was Digitalisierung alles bisher schon leisten kann. Für die eigene Strategie ist dies durchaus von Vorteil."

Digitalisierung nimmt Fahrt auf. Die aktuelle Situation hat der Digitalisierung einen weiteren kräftigen Schub gegeben, der in der Produktion durch Industrie 4.0 bereits seit einigen Jahren eingeläutet worden ist: Seit März 2020 hat sich der Mehrwert digitaler Komponenten, die in die Fertigung integriert werden, noch stärker bemerkbar gemacht – etwa durch die Möglichkeit, Maschinen über Remote Services aus der Ferne zu warten. Experten gehen davon aus, dass durch die Covid-19-Pandemie neue, lokalere Geschäftsmodelle und Marktplätze entstehen und die Produktion noch mehr nach Europa zurückverlagert wird – ein Prozess, der bereits vor einigen Jahren angestoßen wurde und hierzulande im 10-Jahresvergleich bis 2025 zusätzliche Produktion in der Höhe von 48 Mrd. Euro und 38 Mrd. Euro an Wertschöpfung generieren könnte.
Künstliche Intelligenz (KI) wird immer wichtiger, weil dadurch in großen Datenmengen Muster erkannt und komplexe, interdependente Systeme modelliert werden können. In Österreich setzen bereits drei Prozent der Produktionsbetriebe auf KI – bis 2022 soll sich dieser Anteil laut AIT vervierfachen. Die Ausgaben für KI betrugen in der Europäischen Union im Vorjahr 6 Mrd. Euro, bis 2025 wird von einer Steigerung auf 22 Mrd. Euro ausgegangen. KI entwickelt sich zunehmend zu einer Universaltechnologie, die präzisere Prognosen, Empfehlungen und Entscheidungen ermöglicht und die Produktivität steigert. Um das Potenzial von KI auszuschöpfen, sind ergänzende Investitionen in Daten, Kompetenzen und digitalisierte Arbeitsabläufe sowie Änderungen der organisatorischen Abläufe notwendig, wie die OECD festhält. Erfolgsentscheidend dabei ist, dass KI als „assistive Intelligenz" eingesetzt wird, d.h. den Menschen unterstützt und nicht ersetzt.

Forschung und Zusammenarbeit fördern. Die Digitalisierung hat heute bereits in viele Lebensbereiche Einzug gehalten, dieser Trend wird sich in den kommenden Jahren noch verstärken. „Grundvoraussetzung, um die Umbrüche durch die Digitalisierung für sämtliche gesellschaftliche Gruppen zum Erfolg zu führen, ist eine gemeinsame Stimme. Diese haben wir der produzierenden Industrie mit der Plattform Industrie 4.0 gegeben, die wir vor fünf Jahren mitgegründet haben. Ob eine Checkliste für den Einsatz von KI oder Ressourcen- und Energieeffizienz – gemeinsame und praxisnahe Lösungsansätze für die Digitalisierung, die uns alle betrifft, und andere Zukunftsthemen stehen dabei im Mittelpunkt", erklärte Christian Weissenburger, interimistischer Leiter der Sektion „Innovation und Technologie" im Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie (BMK).
Der Qualifikation der Arbeitnehmer kommt deshalb eine wichtige Rolle zu, wenn es um die Zukunftsfähigkeit der österreichischen Industrie geht. Beispielsweise richtet sich „Digital Pioneers – Dein freiwilliges digitales Jahr" speziell an junge Frauen: Das von der Plattform Industrie 4.0 und der Arbeiterkammer Vorarlberg ins Leben gerufene und vom AK DigiFonds finanzierte Projekt ermöglicht eine digitale Grundausbildung mit anschließender Praxiserfahrung und soll 2021 starten. Auch Forschung ist gerade im betrieblichen Kontext ein wichtiges Standbein, um die Innovationsfähigkeit zu erhalten.

Steirische Großprojekte. Die Steiermark setzt seit einigen Jahren konsequent darauf, die Chancen der Digitalisierung für Wirtschaft sowie Wissenschaft und Forschung zu nutzen. Auch in diesem Bereich wird eine steirische Stärke, die enge Zusammen- >>

© Plattform Industrie 4.0 Österreich/Harry Schiffer

V.l.: Zugeschaltet: LHStv.in Gaby Schaunig (Referentin für Digitalisierung und Technologie, Land Kärnten), Christian Weissenburger (Interimistischer Leiter der Sektion Innovation und Technologie im Bundesministerium für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie) und Barbara Eibinger-Miedl (Landesrätin für Wirtschaft, Tourismus, Regionen, Wissenschaft und Forschung, Land Steiermark);
live vor Ort v.l.: Josef Pesserl (Präsident Arbeiterkammer Steiermark), Stefan Rohringer (Vorstandssprecher für F&E der Industriellenvereinigung Steiermark) und Kurt Hofstädter (Vorstandsvorsitzender Plattform Industrie 4.0 Österreich)

arbeit zwischen Wissenschaft und Wirtschaft, forciert. So wird an der TU Graz gerade der Cybersecurity Campus etabliert, der seit 2019 Forschung, Ausbildung, Prüfung und Zertifizierung im Bereich IT-Sicherheit bündelt und bis zu 400 neue Arbeitsplätze schaffen soll. Ebenfalls an der TU Graz entsteht das Data House, das als Entwicklungszentrum für Datenanalyse und neue digitale Anwendungen nicht nur das „Institut für interaktive Systeme und Datenwissenschaften" der TU, das Kompetenzzentrum Know Center und den Science Park Graz, sondern auch Klein- und Mittelunternehmen aus dem Bereich Datenmanagement unter einem Dach vereinen soll.
Wirtschafts- und Forschungslandesrätin Barbara Eibinger-Miedl hierzu: „Gerade im heurigen Jahr haben wir durch die Corona-Pandemie einen regelrechten Digitalisierungsschub erlebt. Ich bin davon überzeugt, dass viele Trends gekommen sind, um zu bleiben."

Technologiekompetenz made in Carinthia. Zu den Aufgaben der Babeg Kärntner Betriebsansiedlungs- und Beteiligungsgesellschaft zählt es auch, Österreichs südlichstes Bundesland mit Projekten und Initiativen als einen national wie international sichtbaren Standort für Technologiekompetenz zu etablieren. Dabei stehen auch Themengebiete rund um die Digitalisierung im Fokus, bei denen idealerweise Bildung, Forschung und Wirtschaft miteinander vernetzt werden. Mit dem speziellen „Industrie 4.0-Programm" der Babeg werden Projekte, die die digitale Reife der Kärntner Industrie ankurbeln, initiiert und gefördert. Überdies wurden mit der Beteiligung der Babeg an der Joanneum Research Forschungsgesellschaft die Weichen für die „Forschungsachse Süd" gelegt und aufgrund dessen weitere Maßnahmen im Bereich F&E gemeinsam mit der Steiermark wie z.B. Silicon Alps Cluster, Silicon Austria Labs oder Digital Innovation Hub Süd auf- bzw. ausgebaut.
Mit dem 5G Playground Carinthia setzt die Babeg Impulse zur Entwicklung der Technologieregion Kärnten, die weit über die Grenzen des Landes ausstrahlen. Beim 5G-Playground handelt es sich um das modernste 5G-Testlabor für Forschung und Entwicklung in Österreich. Es steht Unternehmen und Forschungseinrichtungen zur Verfügung. Eine weitere Initiative ist die Coding School Wörthersee: Hier werden dringend benötigte junge Talente als Coder oder Developer in spezialisierten Intensivlehrgängen ausgebildet und laufend die aktuellsten Erfordernisse sowie Bedingungen der Branche miteinbezogen.
Kärntens Technologiereferentin LHStv.in Gaby Schaunig zeigte die große Bedeutung von begleitender Kompetenzvermittlung: „Es müssen gesellschaftspolitische, emotionale und soziale Fragen bearbeitet werden. In diesem Zusammenhang begrüße ich sehr, dass wir uns in diesem Summit mit dem Thema ‚Responsible Artificial Intelligence' beschäftigen."

Stefan Rohringer,
Vorstandssprecher für Forschung und Entwicklung der Industriellenvereinigung Steiermark

„Eines hat sich deutlich gezeigt: an der Digitalisierung in allen Facetten kommt niemand mehr vorbei."

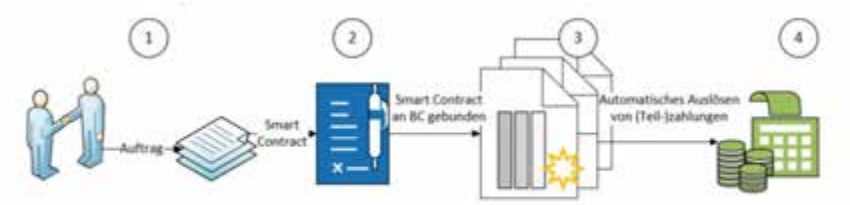
Jobmotor Industrie. Die Industrie ist der Jobmotor Österreichs: Mehr als die Hälfte aller Arbeitsplätze – 2,6 Millionen – werden hierzulande dadurch gesichert. Der Beitrag der österreichischen Industrie zur Wertschöpfung des Landes liegt mit fast 190 Mrd. Euro bei 55 Prozent. Damit das auch in Zukunft so bleibt, muss die heimische Industrie die Chancen der digitalen Transformation – Industrie 4.0 – nutzen und diesen Strukturwandel proaktiv mitgestalten. „Eines hat sich in den letzten Monaten deutlich gezeigt: an der Digitalisierung in allen Facetten kommt niemand mehr vorbei. Auch die Produktion profitiert vom verstärkten Einsatz smarter Lösungen: Fernwartung, Remote-Zugriffe auf Prozesse oder Big-Data-Lösungen, um Daten intelligent zu nutzen, sind hier nur einige Aspekte, um Industrie 4.0 in der Praxis voranzutreiben. Dabei spielt auch die weitere Qualifizierung der Mitarbeiter eine entscheidende Rolle", betonte Stefan Rohringer, Vorstandssprecher für Forschung und Entwicklung der Industriellenvereinigung Steiermark.

https://plattformindustrie40.at

« Zur Studie
„Zehn Thesen zur Zukunft digitaler Geschäftsmodelle für Industrie 4.0 in der Post-Corona-Ökonomie"

« Zur Studie
Strategic Research, Innovation and Deployment Agenda – AI, Data and Robotics Partnership

FERTIGUNGSOPTIMIERUNG **DANK BLOCKCHAIN**



Wie sich die Blockchain in der Fertigung einsetzen lässt, welchen Nutzen die neue Technologie bringt und wie Smart Contracts zukünftig das Business revolutionieren könnten, erläutert Digitalisierungsexperte Dipl.-Ing. Markus Nöbauer von der insideAx GmbH aus seiner Sicht.

Blockchain wird als einer der wichtigsten zukünftigen Schlüsseltechnologien gehandelt. Gartner sieht darin ein beachtliches Potenzial für die gesamte Wirtschaft. Die zentralen Vorteile der Blockchain sind die praktische Unveränderbarkeit der Daten, die Automatisierbarkeit mittels Smart Contracts und damit das Vertrauen der Nutzer in die Informationen und Prozesse.

Grundlage für den Einsatz von Blockchain ist eine hohe Datenqualität und Korrektheit. Die Informationen müssen naturgemäß digital verfügbar sein und etwa direkt an der Maschine per Sensoren und IoT-Anbindung oder per App am Tablet vom Produktionsmitarbeiter erfasst werden. Der Nutzen ist vielfältig: Anhand der Auswertung von Betriebsdaten lassen sich z.B. die Auftragsfertigung und die Qualitätssicherung optimieren sowie die Arbeitsabläufe für die Mitarbeiter vereinfachen. Wenn die gewonnenen Daten in die Blockchain geschrieben werden, können sie auch Kunden zur Verfügung gestellt werden – etwa Kennzahlen zu Qualität und Quantität. Damit kann der Kunde die Einhaltung seiner Qualitätskriterien bereits ab der Produktion nachvollziehen und dokumentieren.

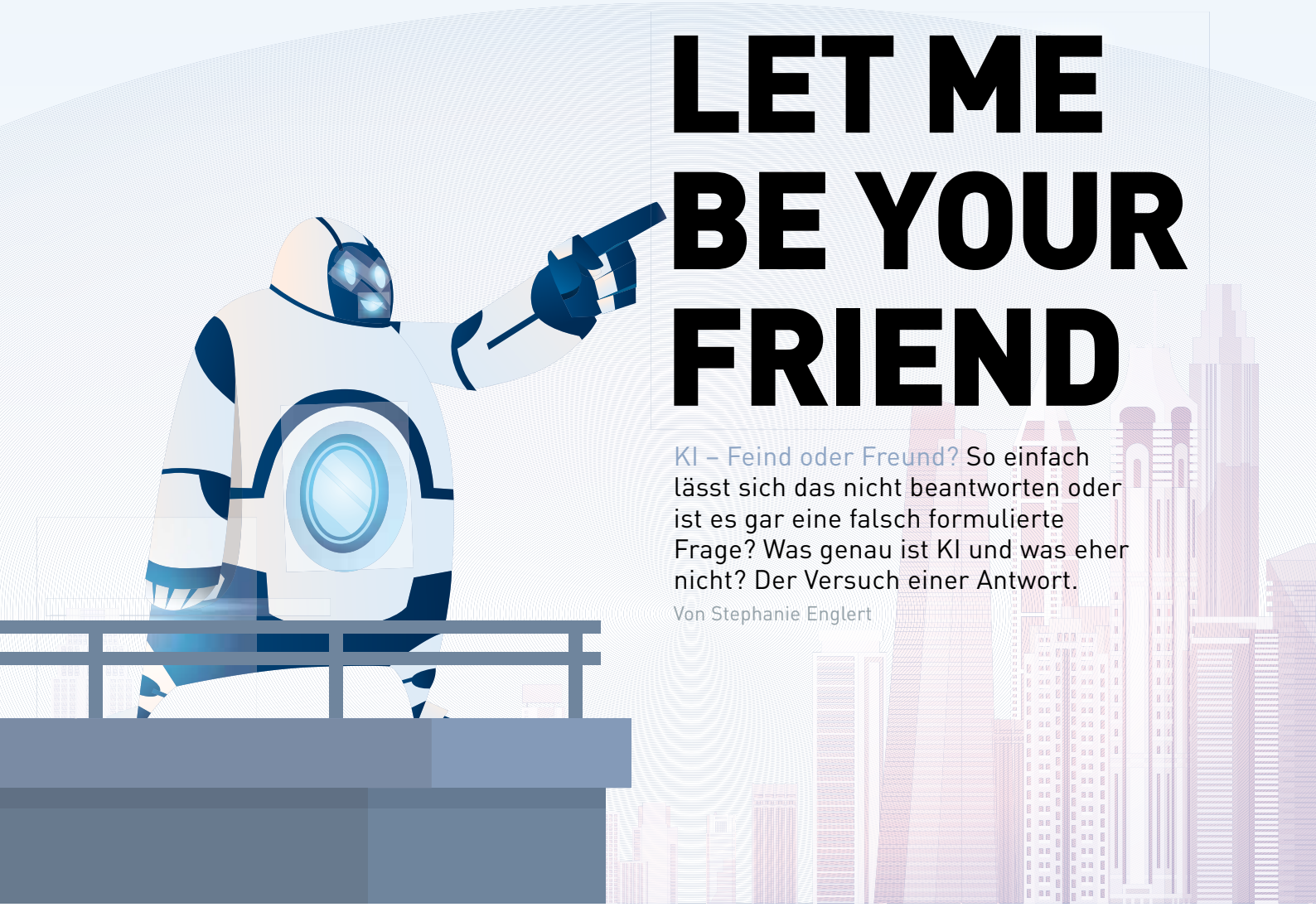
Einfachere, transparente Prozesse. Grundlegend für den Einsatz der Blockchain in der Produktion ist zunächst die Selektion, Bereinigung, Kategorisierung und Validierung der Daten sowie die Definition von relevanten Kennzahlen für die Zielgruppen. Die digitale Erfassung kann über eine App erfolgen, die den Produktionsauftrag komplett abbildet und auf Tablets zum Einsatz kommt. Oder mittels IoT-fähigen Sensoren direkt von Lager und Maschinen automatisch abgegriffen werden. Weitere Datenquellen sind z.B. das ERP- und PPS-System sowie die Qualitätssicherung. Nach dem Zusammenführen und Selektieren der erfassten Daten können diese vielschichtig genutzt werden. Mit dem System sind alle Produktionsabläufe klar dokumentiert und nachvollziehbar. Auch bei der planmäßigen Wartung hilft das System, weil es eine genauere Übersicht über Fertigung und Maschinen ermöglicht. Zusätzlich lassen sich die Prozesse verbessern und rasch Entscheidungen ableiten. Auch für den Kunden wird der gesamte Fertigungsauftrag transparenter.

Neue Anwendungen. Ein Smart Contract ist Programmlogik auf Blockchain-Basis, mit der sich der Lebenszyklus von Produktionsaufträgen abbilden lässt. Damit lassen sich der gesamte Zahlungsverkehr über die Blockchain in Form von Kryptowährungen wie Ethereum abbilden. In der Buchhaltung werden die Kryptowährungen wie eine Fremdwährung geführt und fügen sich nahtlos in die bestehenden Prozesse ein. Eine weitere Anwendungsmöglichkeit ist die Entwicklung neuer Geschäftsmodelle, wie Product as a Service. Dabei ändert sich die Rolle des Unternehmens vom Produzenten zum Dienstleister.

PaaS nutzt als Datenquelle typischerweise IoT-Lösungen, die es bereits von vielen Herstellern als Standardlösung gibt. Rohdaten, die über Sensoren erfasst werden, können damit für die Verwendung im PaaS-Modell vorbereitet und in der Blockchain gespeichert werden. Smart Contracts lassen sich zur Automatisierung der darauf aufbauenden Prozesse verwenden. Beispiele für solche Anwendungen sind die Abrechnung einer produzierten Menge in bestimmter Qualität, aber auch die Verrechnung von Mietautos nach gefahrenen Kilometern.

www.insideax.at

Der Autor:
Dipl.-Ing. Markus Nöbauer
... ist F&E-Verantwortlicher für Forschungsprojekte im Kontext von Business Software bei insideAx. Er hat an der Johannes Kepler Universität in Linz Informatik studiert und verfügt über zehn Jahre Erfahrung als Technology Consultant für Dynamics AX ERP-Systeme.



LET ME BE YOUR FRIEND

KI – Feind oder Freund? So einfach lässt sich das nicht beantworten oder ist es gar eine falsch formulierte Frage? Was genau ist KI und was eher nicht? Der Versuch einer Antwort.

Von Stephanie Englert

Dass digitale Technologien seit längerer Zeit die Arbeitswelt beeinflussen ist kein Geheimnis. Die fortschreitende Entwicklung von Technik hat auch Auswirkungen auf die Gesellschaft. Nehmen wir das Beispiel autonom fahrender Fahrzeuge. Kein anderes Thema erregt die Gemüter stärker. Kann ich einer „Maschine“ die alleinige Entscheidung im Straßenverkehr zutrauen und was, wenn ein Unfall, vielleicht sogar mit Todesfolge, passiert? In verschiedenen Feldversuchen hat man gesehen, dass dieses Szenario durchaus Realität werden kann. Wie weit sind die „Maschinen“ also und wo beginnt oder endet gar die Ethik?

Der VDI, Verein Deutscher Ingenieure, brachte es vor einiger Zeit auf den Punkt: „Künstliche Intelligenz ist nicht erst dann am Werk, wenn menschliche Eingriffe komplett überflüssig werden. Künstliche Intelligenz hat keine Moral und löst keine ethischen Konflikte. Künstliche Intelligenz kann Regeln anwenden, ändert sie aber nicht.“ Und Prof. Dr. Frank Flemisch vom Bonner Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie ergänzte in diesem Statement: „…die autonome Endstufe in allen Anwendungsfällen ist noch sehr weit in der Zukunft.“ Der Grund ist auch die einhergehende technische Voraussetzung, die geschaffen werden muss.

Große Datenmengen, verursacht durch den Einsatz von vielen Kameras und Sensoren bei dieser Technik, werden mit jedem Level des autonomen Fahrens mehr. In Folge muss auch mehr Rechenleistung gewährleistet werden. Es zieht alles einen gewissen „Rattenschwanz“ mit sich, den viele zunächst mit der Idee des autonom fahrenden Fahrzeugs wahrscheinlich noch gar nicht realisiert haben. Was für viele nur das reine Fahrzeug ist, ist für die Technik, die dahintersteckt, eine Mammutaufgabe mit all seinen Facetten.

Bernhard Moser
Research Director am Software Competence Center Hagenberg und Präsident der Austrian Society for Artificial Intelligence

„Daten sind Indizien und das ist die Basis!“

Wer trifft wann welche Entscheidung? Zu den ethischen Aspekten gesellt sich dann auch schnell folgende Frage: „Lässt sich in einem selbstlernenden System überhaupt noch nachvollziehen, welche Algorithmen zu welcher Entscheidung geführt haben?". Flemisch ergänzt weiters im VDI-Beitrag: „Wir können die Technik umfassend trainieren. Aber wir können dem Fahrer nicht so einfach vermitteln, welches Vertrauen angemessen ist."
KI-Methoden können demnach heutzutage sehr wohl, etwa in der Produktion, einen sinnvollen und ergänzenden Beitrag leisten, etwa um Verbesserungen zu eruieren und Varianten durchzuspielen. Aber sie bedürfen auch grundlegender rechtlicher Entscheidungen bzw. Gesetzgebungen und Grenzen, um eine sichere und auch faire Nutzung zu gewährleisten.

Wie alt ist KI? Die Geschichte der KI beginnt genau genommen schon Mitte der 50er Jahre – wenn nicht gar noch früher. Den Angaben zufolge nach fand als so genannte Gründungsveranstaltung der Künstlichen Intelligenz als akademisches Fachgebiet die Dartmouth Conference am Dartmouth College in Hanover (New Hampshire/USA) zu dieser Zeit statt. Dieser damalige Workshop mit dem Titel Dartmouth Summer Research Project on Artificial Intelligence wurde von John McCarthy im Rahmen eines von der Rockefeller-Stiftung geförderten Forschungsprojekts initiiert. Doch wie bereits erwähnt wurde weit vorher immer wieder die Kombination von Mensch und Maschine ins Gespräch gebracht (Julien Offray de La Mettrie und sein 1748 veröffentlichtes Werk L'Homme Machine). Und auch Namen wie Hubert Dreyfus oder Karl Popper aus den 70er Jahren haben einen Konnex zur Entwicklung von KI.
Künstliche Intelligenz gewinnt ohne Frage als Wachstumstreiber für Unternehmen immer stärker an Bedeutung. Doch für viele gibt es in diesem Bereich noch Aufholbedarf. Wie eine Studie des Beratungsunternehmens Accenture jüngst zeigte, glauben demnach 87 % der großen Unternehmen, dass KI zu einer signifikanten Transformation ihres Industriesektors führen wird, aber nur 42 % aller österreichischen Unternehmen etwa arbeiten aktiv mit ihr. KI ist, um es einmal klar zu sagen, kein Thema rein für Spezialisten, sondern für alle relevant und auf ganz unterschiedlichen Ebenen anwendbar. Und hier liegt oft auch das Problem.

Auf was kommt es an? Wird gerade in KMU oft davon gesprochen, dass der „geeignete Fachmitarbeiter" nicht am Markt oder gar im Betrieb vorhanden sei, vergessen viele dabei, dass es außer einer entsprechenden Ausbildung auf etwas ganz anderes beim KI-Einsatz ankommt. In einem persönlichen Gespräch zum Thema KI und Simulationen brachte es Harald Mutzke, Inhaber von SES (Simulation Expert Services) aus Nürnberg auf den Punkt. „KI-Einsätze können die Anzahl erforderlicher Simulationen reduzieren und somit bei einer konkreten Aufgabenstellung schneller zu geeigneten Lösungen führen. Die Frage ist doch: Welche Optimierung der Arbeitsvorgänge passt für meinen konkreten Fall bzw. Aufgabenstellung?"
Mutzke betonte auch, dass „bei einem noch so kleinen Problem, der Einsatz der KI durchaus Sinn macht und keinen Angriff auf bisherige Arbeitsweisen im Betrieb bedeutet, sondern eher die Optimierung der Prozesse im Raum steht." Hier ergänzt er in seinen Ausführungen weiters, dass man nicht von „einer optimalen Lösung ausgehen sollte, sondern immer mehreren, die durch Simulationen ans Tageslicht gebracht werden." >>

Roland Sommer
GF Plattform Industrie 4.0

„Wichtig ist immer, dass Maschinen keinen Menschen ersetzen werden. KI ist unterstützend gedacht, nicht als Konkurrenz zum Mitarbeiter."

Mutzke selbst sieht den Begriff KI auch als „Buzzword“ unserer Zeit, das vielerlei Unklarheiten mit sich bringe. Sein Ziel sei es grundsätzlich, folgenden Weg bei Kunden in der Beratung zu gehen:

1.) vom Visio Prozess-Modell automatisch
2.) zur Simulation
3.) zur automatischen KI-gestützten optimalen Gestaltung des Systems bzw. der Modellparameter wie Losgröße, Produktmix, Schichten, Personal etc. aber auch Automatisierungs- und Steuerungslogik, wo auch immer die konkreten Themen anstehen.

In der Praxis schaut selbst für Laien ein Einsatz von entsprechend zugeschnittener KI ganz anders aus als in der trockenen Theorie, bei der eben vielfach von Expertenwissen ausgegangen wird. Dies mag in komplexeren Prozessen auch stimmen, sollte aber wie erwähnt noch lang kein Hindernis sein, den Einsatz von KI zu fördern, unabhängig von der Unternehmensgröße und der Ausrichtung des Betriebes.

KI als allgegenwärtiges Thema. Auch die heuer ebenfalls im virtuellen Austragungsort gelandete CES startete im Jänner mit dem Thema KI. „Wir verbinden KI und Konnektivität zu AIoT, um die Energieeffizienz zu erhöhen und Corona zu bekämpfen“, sagte hierzu Bosch-Geschäftsführer Michael Bolle auf der CES. „AIoT bietet enormes Potenzial – wir nutzen dies bereits heute und bauen unser Engagement in Zukunft noch weiter aus.“ Unter dem Motto „Sustainable #LikeABosch“ präsentierte das Unternehmen auf der virtuellen Techmesse intelligente, nachhaltige Lösungen für die Bereiche Gesundheit, Wohnen und Mobilität. Zudem zeigte das Unternehmen einen Sensor, der unter anderem Luftgüte und relative Feuchtigkeit misst und somit Aufschluss über die Konzentration von Aerosolen in der Luft gibt – eine Angabe, die im Einsatz gegen Corona am konkreten Beispiel an Bedeutung gewonnen hat. Im Kampf gegen das Virus können auch Bosch-Sicherheitskameras unterstützen. Denn dank KI bieten sie die Möglichkeit, verschiedenste kundenspezifische Anwendungen umzusetzen.

KI im Arbeitsalltag. Und auch eine kurz vor Weihnachten von der Plattform Industrie 4.0 in Österreich initiierte virtuelle Veranstaltung zum Thema „AI@Work: Wie Mensch und Maschine in der Arbeitswelt voneinander lernen können, wenn sie zusammenarbeiten“ konkretisierte eines stark heraus: „Welchen Aufschwung KI derzeit erlebt, lässt sich an den EU-weiten Ausgaben ablesen: Während 2019 insgesamt 6 Mrd. Euro aufgewendet wurden, soll sich dieser Wert bis 2025 fast vervierfachen. Bis 2022 sollen bereits bis zu zwölf Prozent der heimischen Produktionsbetriebe KI-Anwendungen implementiert haben, wie das AIT prognostiziert, denn KI ermöglicht präzisere Prognosen, Empfehlungen und Entscheidungen, hilft dabei komplexe Herausforderungen zu bewältigen und steigert die Produktivität.“

Roland Sommer, Geschäftsführer der Plattform Industrie 4.0 sagte: „Oft gibt es vor allem in der Berufswelt aber noch Vorbehalte gegenüber KI, denen wir mit der Teilnahme am Projekt AI@Work entgegentreten wollen.“ Er ergänzte: „Wichtig dabei ist immer, dass Maschinen keinen Menschen ersetzen werden. KI ist unterstützend gedacht, nicht als Konkurrenz zum Mitarbeiter.“

Dies untermauerte auch Projektkoordinator Bernhard Moser, Research Director am Software Competence Center Hagenberg und Präsident der Austrian Society for Artificial Intelligence. „Ziel ist es“, so Moser, dass „sich jeder einen Reim aus seinen Unternehmensdaten machen kann und gezielt eine Anwendung dieser für Optimierungen eruiert“, so der Experte. „Daten sind Indizien und das ist die Basis!“

Aufbauend auf den Erkenntnissen von AI@Work wurde eine Roadmap für ein KI-Leitprojekt ermittelt, das noch mehr Projektpartner umfassen soll und strategisch wichtige Themen wie Maschinelles Lernen oder Knowledge Graphen, die verschiedene Daten grafisch vernetzen, näher beleuchten soll – beides Themen, die nicht ohne die Teamarbeit zwischen Mensch und Maschine auskommen.

Simon Hasler
IT Security und DevOps Engineer bei Rubble Master

„In der Baubranche ist die Digitalisierung der Maschinen noch oft weit am Anfang.“

Rubble Master nutzt KI. Wie der optimale Austausch zwischen Mensch und Maschine bereits funktionieren kann, erläuterte im Gespräch Simon Hasler, IT Security und DevOps Engineer bei Rubble Master in Oberösterreich – und zwar im Rahmen eines Use Cases. Das Unternehmen produziert Materialrecycling-Maschinen, die Einstellung für bestimmte Anwendungen gestaltet sich oft komplex – beispielsweise ist der optimale Zeitpunkt für Wartung und Austausch von Verschleißteilen nur sehr schwer vorherzusagen. Wünschenswert wäre eine Maschine, die die ideale Konfiguration selbst vorschlägt und durch ein Remote Monitoring-System vorausschauend gewartet werden kann.
Der Mensch müsste dazu KI-basierte Vorschläge bestätigen oder anpassen, regelmäßig sein Wissen in das lernende System einpflegen und die Maschinendaten überprüfen sowie intelligente Wartungstätigkeiten durchführen. Die Maschine wiederum müsste Umgebungs- und Eigendaten erfassen, durch KI unmittelbare Ergebnisse analysieren und mit anderen Maschinen kommunizieren, um die Baustelle ganzheitlich zu erfassen. Soweit so gut.
Er betonte darüber hinaus auf Nachfrage jedoch auch, dass „in der Baubranche die Digitalisierung der Maschinen noch oft weit am Anfang steht". Auch geeignete Studiengänge kämen erst allmählich ins Ausbildungsportfolio und entsprechend ziehe sich dieser Ausbildungsprozess des künftigen Personals hin.
Auf die abschließende Nachfrage, ob nun die Covid-19-Pandemie in all ihren Facetten ein Digitalisierungsbeschleuniger sei, bestätigten alle Teilnehmer der erwähnten Plattform Industrie 4.0-Veranstaltung diese Aussage. „Es kann nur von Vorteil sein, wenn diese Technik stärker Einzug in die Betriebe erhält, unabhängig von deren Größe und Aufgabengebiet", sind sich alle einig.

Wie setzt man nun aber KI am besten ein? Informationsveranstaltungen wie das vergangene Jahr virtuell ausgetragene Trevisto-Event namens „KI4KMU – wie die mittelständische Wirtschaft die Vorteile der Künstlichen Intelligenz nutzen kann" sorgen immer wieder für regen Gesprächsstoff. Wie bereits eingangs erwähnt stellen sich vor allem Unternehmen des Mittelstands häufig die Frage, ob ihre Datengrundlage für den Einsatz von KI ausreichend ist, wie sie erste Schritte gehen können und wie sie ihr Personal in die Lage versetzen, KI zu entwickeln und zu nutzen. Dies ist kein neu auftretendes Problem.
Jürgen Engler, Vorstandsvorsitzender von Trevisto aus Nürnberg, sieht dieses Problem sehr genau. Er erklärt: „Wir als Trevisto weisen immer wieder darauf hin, dass die Implementierung einer KI-orientierten Thematik alleine nicht ausreicht, um wirklich Mehrwerte zu erzielen. Ganz entscheidend ist immer, die Menschen, die damit arbeiten, auch mitzunehmen. Denn es entstehen oft Existenzängste („verliere ich jetzt meinen Arbeitsplatz?") oder KI wird ignoriert („was soll das denn besser können, als so, wie wir es immer schon getan haben?"). Und diese Fragestellungen entstehen immer nur dann, wenn abstrakt über KI gesprochen wird."
Aufgrund dieser Erfahrungen am Markt hat sich Trevisto immer darauf fokussiert, den wirklichen Nutzen darzustellen. Engler betonte auch das „leidige" Thema diverser digitaler Events, die entweder ausschließlich Anwendungen präsentierten, die beim besten Willen keine KI-Anwendung sind, oder es wird seinen Ausführungen nach leider „über Themen gesprochen, die viel zu weit weg sind, als dass man damit jetzt vorhandene Probleme lösen kann." Was rät Trevisto in solch einem Fall? Engler: „Wir

raten jedem Unternehmen, die Einführung von KI mit personalorientierter Begleitung durchzuführen. Der Veränderungsprozess muss von geeigneten Coaches begleitet werden und dies tunlichst von außerhalb des Unternehmens."
Doch was ist KI nun? Ein gutes KI-System kann sehr wohl von der menschlichen Expertise lernen und so schrittweise Aufgaben übernehmen. Und ob der enormen Datenmengen unserer Zeit kann KI hierbei ein freundschaftlicher Arbeitsbegleiter sein und einen Mehrwert bieten. Den Menschen ersetzen, wie so oft befürchtet, kann sie gar nicht, denn die soziale Kompetenz des Menschen ist mittels KI nicht ersetzbar. Stephen Hawkings sagte in seinem 1988 erstmals erschienen Buch „Eine kurze Geschichte der Zeit": „Intelligenz ist die Fähigkeit, sich dem Wandel anzupassen." Und genau so passiert es dann auch mit der Künstlichen Intelligenz.

www.fkie.fraunhofer.de
www.mutzke-ses.com
www.bosch.com
www.rubblemaster.com
www.plattformindustrie40.at
www.ces.tech
www.vdi.de
www.trevisto.de

SPATIAL COMPUTING KANN DIE INDUSTRIE TRANSFORMIEREN

Der Idee, den physischen Raum als integralen Bestandteil von computergestützten Erlebniswelten zu betrachten, begegnen wir im Consumer-Umfeld an vielen Stellen. Doch was kann diese Technik wirklich?

Sei es das Uber-Taxi, der Rasenmäher-Roboter oder die Anzeige über die Ankunft der nächsten U-Bahn: Wo immer Bewegungsabläufe optimiert werden können, ist Spatial Computing zur Stelle. So im weiten Feld der Navigation. Zwar geben wir mit Google Maps unseren Standpunkt preis, bekommen dafür aber den idealen Weg allen Staus zum Trotz zu unserem Ziel aufgezeigt. Im beruflichen Umfeld ist Spatial Computing für Lieferdienste von Waren oder Speisen von unschätzbarem Wert.

Spatial Computing birgt aber auch im B2B-Umfeld, etwa in der Fabrikplanung erhebliches Potenzial. Aber: Die räumliche Ausdehnung einer Fabrik muss entsprechend viel genauer erfasst werden und die Software deutlich mehr Optionen einbeziehen, auch Gefahrenzonen oder Rampen. Auch in der Intra- und Outbound-Logistik hat sich Spatial Computing seine Meriten verdient: Die am stärksten nachgefragten Produktgruppen werden in einem Lager so angeordnet, dass sie am schnellsten abtransportiert werden können.

Verschmelzung von digital und real. Kreative Entwickler sind derzeit dabei, Spatial Computing im Bereich der industriellen Anwendung auf die nächste Stufe zu heben. Durch die geschickte Kombination von Leading Edge-Technologien wie Augmented Reality (AR), Industrial Internet of Things (IIoT), Machine Learning und Sensorik lassen sich Fertigungsprozesse weiter optimieren, deren Design und Bedienung massiv vereinfachen. Detailkenntnisse über jeden noch so kurzen Prozessschritt offenbaren neue Einsichten und öffnen Tür und Tor für effizienteres und schnelleres Arbeiten, sparen Zeit und Energie.

Mit dem Einzug von IIoT ist der Einsatz von Bearbeitungszentren in den Fabrikhallen auf Basis von MES-Konzepten optimiert worden. Im Zuge der Einführung von Manufacturing Execution System (MES, auch: prozessnahe Produktionsfeinplanung) wurde die Überwachung der einzelnen Fertigungszellen zentralisiert, mehrere Maschinen parallel beobachtet und ihre Taktung aufeinander abgestimmt. Nun gilt es, die immer anspruchsvoller werdenden Tätigkeiten der Werker genauer mit den Maschinen-

Spatial Computing entwickelt auch den Digitalen Zwilling der Fabrik weiter.

Das Anwendungsfeld von Spatial Computing ist breit und birgt enormes Potenzial und Chancen.

Spatial Computing kann aufzeigen, wo Fehler passiert sind.

abläufen zu synchronisieren. Spatial Computing erlaubt es, Prozessanweisungen durch einen klaren räumlichen Bezug zu veranschaulichen und damit besser nachvollziehbar zu machen. Etwa bei der Programmierung der Industrieroboter.

Bisher werden diese umständlich über 2D-Interfaces programmiert („Teach-in"). Um diese komplizierte Programmierumgebung zu verstehen, ist eine langwierige Ausbildung nötig. Spatial Computing indes senkt die Abstraktionsebene des Teaching deutlich. Über ein Interface lassen sich Handlungsanweisungen intuitiv mit dem physischen Aktionsraum des Roboters verknüpfen. Etwa, indem der Roboter mit einer Armbewegung die Richtung vorgeben wird, oder Wegpunkte mit einem Smartphone platziert werden.

Wenn dann noch mehrere Maschinen und Roboter miteinander verkettet werden müssen, wird der Vorteil noch offensichtlicher: Spatial Computing kann aufzeigen, an welcher Stelle auf dem Shopfloor ein Fehler aufgetreten ist und eine AR-Anwendung dem Mitarbeiter den Weg dorthin aufzeigen. So lässt sich die Produktivität insgesamt signifikant steigern und die Frustration der einzelnen Werker aufgrund von an sich unnötigen Rückfragen deutlich senken.

Der Digitale Zwilling wird klüger. Neben den Maschinen können über Kameras auch die Bewegungen von Materialien, Werkzeugen und Werker nachverfolgt und ausgewertet werden. Waren bisher die tatsächlichen Arbeitswege der Mitarbeiter oder von Gütern weitgehend unbekannt, kann nun der komplette Produktionsablauf einschließlich der Montagearbeiten genau dokumentiert werden. So können Initiativen entwickelt werden, die sich dieses Wissen zunutze machen. Spatial Computing entwickelt damit den Digitalen Zwilling der Fabrik weiter. Künftig werden in Echtzeit nicht nur die Abläufe in der Maschine abgebildet, auch der Digitale Zwilling des Werkers lässt sich kreieren: Es kann präzise erfasst werden, wo sich eine Person gerade befindet, was sie tut und welche Fertigkeiten sie besitzt.

Ein anderer, bemerkenswerter Aspekt von Spatial Computing sind seine analytischen Fähigkeiten: Über sogenannte Spatial Heat Maps erhalten Unternehmen Einblicke, an welchem Ort während des Arbeitsablaufs sich die Arbeiter am häufigsten aufhalten, wo unverhofft Maschinenstillstand herrscht und welche Arbeitswege am meisten frequentiert werden. Räumlich verbesserte auflösende Kameras und Machine Learning haben ein komplett neues Anwendungsfeld entstehen lassen. Neue Kameratechnologien erfassen nicht nur eine 2D-Aufnahme, sondern auch Entfernungsinformationen.

Eine neue Ära in der Industrie ist eingeläutet. Mittels verketteter Kamerasysteme können komplette Produktionsstandorte aus der Ferne gesteuert werden. Interdisziplinäre Arbeitsgruppen können global auf Basis des Digitalen Zwillings so kollaborieren, als säßen sie in einem Raum zusammen – sie können sich selbst sehen und im virtuellen Beobachtungsraum des anderen bewegen.

PTC kennt das enorme Potenzial von Spatial Computing sehr genau und investiert in diese Technologie nachhaltig, wohl wissend, dass sie längst noch nicht ausgereizt ist. PTC stellt zum Beispiel die Vuforia Spatial Toolbox der Open Source Community zur Verfügung, damit diese eigene Programme entwickelt und voneinander lernt. Dabei arbeitet der Systemanbieter neben Partnern aus der Industrie mit Universitäten wie dem Massachusetts Institute of Technology (MIT) eng zusammen.

www.ptc.com

Der Autor:
Valentin Heun
... ist VP Innovation Engineering, Reality Lab bei PTC

ENTSCHEIDEN SIE!

Open Source-Software (OSS) wird bei Unternehmen immer beliebter. Warum? Es können Lizenzkosten eingespart werden und man kann sich unabhängig von großen Herstellern aufstellen. Doch es gibt auch Stolpersteine.

Die immense Bedeutung von Open Source-Software zeigt sich nicht zuletzt darin, dass mehr als zwei Drittel der deutschen Unternehmen diese bereits bewusst einsetzen. Bei den größeren Betrieben ab 2.000 Mitarbeitern sind es laut einer Studie des Branchenverbands Bitkom sogar 86 Prozent. Zudem enthalten mittlerweile fast alle Applikationen Open Source-Komponenten. Darunter fallen auch viele Anwendersoftware-Angebote, die wir täglich nutzen wie VLC, Firefox oder auch Spotify. Sogar der Edge Webbrowser von Microsoft basiert auf dem Open Source-Browser Chromium. Es sind vor allem drei Vorteile, die OSS in der Software-Landschaft so beliebt machen: Verfügbarkeit, Nachhaltigkeit und Transparenz.

1. Verfügbarkeit: Unabhängigkeit von einzelnen Herstellern

Unternehmen können Open Source-Software so lange und in der Form nutzen, wie es ihnen gefällt. Einmal veröffentlichte Quellcodes bleiben verfügbar, selbst wenn sich Lizenzbestimmungen künftig einmal ändern oder Hersteller vom Markt verschwinden. Auf diese Weise können sich Unternehmen also unabhängiger von einzelnen Anbietern machen. Das dt. Bundesministerium des Innern rät Behörden sogar aktiv dazu, Open Source einzusetzen. Denn Open Source befördert die digitale Souveränität der Unternehmen, der Bürger und des Staats. Plattformen wie GitHub dienen hierbei zum Austausch zwischen den mehr als 40 Millionen Entwicklern. Hier haben fast 70 Prozent der „Global Fortune 500"-Unterneh-

men im vergangenen Jahr einen Beitrag zu Open Source-Projekten geleistet. Der Erwerb von GitHub durch Microsoft im Jahr 2018 mit dem stolzen Preis von 7,5 Milliarden Dollar zeigt nicht zuletzt, welchen Wert man Open Source dort auch wirtschaftlich zumisst.

2. Nachhaltigkeit: Sharing Economy-Prinzip und Bildung

Riesige Quellcode-Pools liefern Unternehmen, unabhängig von Größe und Branche, die nötigen Bausteine für ihre Entwicklungen. Nach dem Prinzip der Sharing Economy leisten Unternehmen im Gegenzug sowohl finanzielle als auch aktive Beiträge – etwa indem sie die Software weiterentwickeln und selbst Code zurückgeben – und tragen so dazu bei, dass die Quellcode-Pools kontinuierlich gepflegt werden. Dieser Grundgedanke „nicht nur nehmen, sondern auch geben" ist elementarer Bestandteil des Open Source-Entwicklungsmodells.

Zudem leistet Open Source-Software auch einen unverzichtbaren Beitrag zur Ausbildung von zukünftigen IT-Experten. Deswegen nutzen viele Universitäten Open Source-Lösungen, da nur an diesen uneingeschränkt experimentiert werden kann. Open Source ist eben keine Black Box, sondern ermöglicht und ermutigt, zu analysieren, wie etwas umgesetzt wird.

3. Transparenz: Das sich selbst kontrollierende System

Bei Open Source liegt der Quellcode offen. Er ist für jede Person, die sich dafür interessiert, nutzbar. Auf diese Weise können Unternehmen sicher sein, dass keine versteckten Hintertüren eingebaut sind – denn die vielen Augen der Community hätten dies mit hoher Wahrscheinlichkeit bemerkt. Bei proprietärer Software hingegen kann niemand Eingriffe überprüfen, weshalb Nutzer allein auf das Vertrauen zum Hersteller angewiesen sind. Als sich selbst kontrollierende Systeme sind Open Source-Lösungen proprietärer Software in puncto Sicherheit also einen großen Schritt voraus.

Risiken abwägen und managen. Trotz offenem Quellcode und Entwicklungsmodell lassen sich auch bei OSS-Risiken nicht gänzlich ausschließen. Auch hier sind bereits Vorfälle durch kritische Fehler bekannt geworden. Ein Grund: Open Source-Komponenten werden zwar kontinuierlich weiterentwickelt, haben aber irgendwann einen sehr hohen Reifegrad erreicht. Dann arbeitet meist nur noch eine kleine Community an Updates und Patches für die Software. Ein gutes Schwachstellenmanagement ist also auch hier unabdingbar.

Eine weitaus größere Herausforderung ist jedoch der akute Fachkräftemangel. Nur die wenigsten Unternehmen verfügen über genug Inhouse-Spezialisten, um alle anfallenden Security-Aufgaben abzudecken. Insbesondere bei kostenlosen OSS-Angeboten gilt es, die Aktivitäten der Community stets im Blick zu haben, über wichtige Änderungen informiert zu bleiben und Patches zu testen und einzuspielen – eine Mammutaufgabe, für die internen Experten im Alltagsgeschäft oft nicht genug Zeit bleibt.

Darum lohnt es sich, für OSS Geld auszugeben. Wie lassen sich also die Vorteile von OSS nutzen und gleichzeitig Risiken vermeiden? Eine Lösung ist, auf kommerzielle Open Source-Angebote zurückzugreifen. Hier kümmert sich ein Dienstleister um Updates und Patches und entlastet die IT-Abteilung. So ist sichergestellt, dass Anwendungen stabil und sicher laufen und stets auf dem aktuellen Stand sind. Darüber hinaus sind Angebote von Dienstleistern oftmals speziell für das Unternehmensumfeld optimiert und bieten wichtige Zusatzfunktionen.

So enthält die kommerzielle Version der Schwachstellenmanagement-Lösung von Greenbone Networks etwa viele zusätzliche Schwachstellentests für Windows, Linux, Cisco-Komponenten oder ICS-/Scada-Steuerungen, die im Enterprise-Umfeld wichtig sind.

Ergo: Die Nutzung von IT bringt immer potenzielle Risiken mit sich – egal, ob es sich dabei um OSS oder proprietäre Produkte handelt. Beim Einsatz von Software wird es also immer nötig sein, ihr Verhalten zu beobachten, sie auf Schwachstellen zu scannen und diese zu schließen. OSS bringt Unternehmen viele Vorteile. Sie müssen jedoch abwägen, ob sie selbst das nötige Know-how und die zeitlichen Ressourcen für die Nutzung komplett kostenloser Versionen besitzen. Wer Open Source nutzen möchte und nicht auf ein übliches Support-Level verzichten kann und will, hat die Möglichkeit sich an Hersteller von Open Source-Produkten oder deren Partner zu wenden. Sie sorgen für sichere und stabil laufende Anwendungen, ohne die Inhouse-IT-Abteilung zu belasten. Auf diese Weise können Unternehmen die Vorteile von Open Source nutzen und dabei gleichzeitig Sicherheitsrisiken minimieren.

www.greenbone.net

Der Autor:
Elmar Geese,
COO bei Greenbone Networks
... ist seit Anfang 2020 Teil des Management-Teams von Greenbone und blickt auf eine langjährige Management-Erfahrung zurück. Zuletzt war er als CIO beim Berliner Gesundheits-Startup machtfit für deren SaaS-Plattform für betriebliches Gesundheitsmanagement verantwortlich.

Bild: © Greenbone

DIE MACHT DES WOLLENS

Dass mobile Anwendungen und der Umgang mit dem Internet in den afrikanischen Ländern sehr wohl weit fortgeschritten sind, vermuten zu wenige. Auf dem ersten digitalen AfricaCom- und AfricaTech-Festival Ende November 2020 verdeutlichten Experten aus den unterschiedlichsten Bereichen dies einmal mehr. Der Kontinent Afrika prescht digital vor.

Von Stephanie Englert

Alain Ebobissé, CEO Africa50, brachte es auf den Punkt: „Afrika braucht dringend einen Ausbau der regionalen und auch digitalen Infrastruktur, um in der afrikanischen Freihandelszone grenzüberschreitend optimal agieren zu können." Am AfricaTech-Festival sprach er als Keynote Speaker über genau diese „Bedeutung von Investitionen in die digitale Infrastruktur auf dem afrikanischen Kontinent, um das wirtschaftliche Wachstum voranzutreiben". Und viele Kollegen teilen seine Ansicht und seinen Appell. Denn obwohl es auf den ersten Blick so ausschaut, als ob nur ein Bruchteil der afrikanischen Bevölkerung Zugang zum Internet habe, muss dies bei insgesamt 55 Ländern differenzierter betrachtet werden.

Investitionen werden getätigt. GTAI (German Trade und Invest) meldete Anfang Februar, dass „für ein regionales Digitalisierungsvorhaben im südlichen Afrika und in Ostafrika bei der Weltbankgruppe ein Kredit und ein Zuschuss in Höhe von jeweils 125 Mio. US-Dollar beantragt wurde." Das Ziel des Projekts sei den Angaben zufolge der Ausbau der Reichweite von Breitbandnetzen, um dadurch die digitale Wirtschaft zu fördern. Doch auch im Westen Afrikas entwickeln sich seit Jahren einige Länder wie etwa Nigeria zu einer wirtschaftlich und digital repräsentativen Nation. Trotz ersichtlicher Armut auf der einen Seite weist das Land am Golf von Guinea auf der anderen Seite eine hohe Internet- und Mobilfunkpenetrationsrate laut GTAI auf: Demnach heißt es, dass im 1. Halbjahr 2020 nach Angaben der Nigeria Communication Commission (ICC) 143 Millionen Einwohner über einen Internetzugang verfügten, das sind etwa 60 Prozent der Bevölkerung. Im Jahr 2019 gab es 184 Millionen Mobilfunkanschlüsse, was einer Telekommunikationsdichte von 96 Prozent entspricht.

Mit der kürzlich verabschiedeten National Digital Economy Policy and Strategy (2020-2030) verfolgt die Regierung Nigerias den Angaben nach hochgesteckte Ziele. Die digitale Roadmap wird dabei auf acht Säulen gestützt, die die digitale Wirtschaftsentwicklung beschleunigen sollen. Dazu gehört die Schaffung eines regulatorischen Rahmens des IKT- und Digitalsektors sowie die Bereitstellung einer sicheren und zuverlässigen Infrastruktur. Darüber hinaus sollen entsprechende Ausbildungsmöglichkeiten für den Erwerb digitaler Kompetenzen geschaffen und Unternehmen, die im Bereich neuer Technologien tätig sind, besonders gefördert werden. Denn Afrika hat einiges vor.

Ein Name sticht beim Thema Digitalisierung in Westafrika ebenfalls ins Auge: Dr. Ayotunde Coker, Managing Director von Rack Center, einem Betreiber von Datenzentren in Nigeria. Coker weiß was er vorhat und weist eine 30-jährige internationale Karriere vor sowie eine Listung bei „the worlds most influential data economy leaders" im Data Economy Magazine in UK. Das Rack Center wurde 2012 gegründet und vermeldete Anfang Februar weitreihende Expansionspläne. Coker: „Wir sind stolz auf Qualität und Maßstab, beides Kriterien, die wir in der Region Westafrika erarbeitet haben, um de facto DAS digitale Datenzentrum für Westafrika zu sein."

Wirtschafts-Freihandelszone. Bei 54 (bzw. 55) Staaten und knapp 1,2 Mrd. Menschen gilt der afrikanische Kontinent als Wachstumsregion. Und um auch künftig beim Thema Warenwirtschaft noch flexibler agieren zu können, wurde die Panafrikanische Freihandelszone (AfCFTA) jetzt gegründet. Zu Beginn 2021 gab AfCFTA-Generalsekretär Wamkele Mene hierzu der FAZ ein Interview, in dem er sagte: „Es wird viele Jahre dauern, bis die Vereinbarungen über Handelserleichterungen, Transitregeln und die Zollzusammenarbeit konsequent umgesetzt sind. Das ist nicht in sechs Monaten oder einem Jahr zu schaffen. Wir haben die Harmonisierung der Zollverfahren, der Handelserleichterungen und des Transits erreicht. (…) Die Digitalisierung von Zollverfahren ist absolut nötig, aber es gibt Länder mit durchlässigen Grenzen oder Grenzen in sehr abgelegenen Gegenden. Auch dies wird einige Zeit in Anspruch nehmen, selbst wenn digitale Plattformen eingeführt werden.“ Dennoch sei der Schritt zur Digitalisierung ein wichtiges Muss im Gesamtkomplex.
Das Mobiltelefon spielt auf dem afrikanischen Kontinent als Kommunikations- und Informations- sowie Zahlungsmittel eine entscheidende Rolle. Letzteres ist inzwischen unumgänglich. Laut britischem Marktforschungsinstitut Ovum hatten 2016 etwa 300 Mio. Afrikaner ein Smartphone. Die Nutzeranzahl hat sich bis Ende 2019 auf 600 Mio. verdoppelt. Ende 2021 wird laut Studie mit einer Zahl von 900 Mio. bis 1 Mrd. Nutzern gerechnet.

Firmen investieren. Auf dem AfricaCom- und Tech-Festival im November war nicht zu übersehen, wer zu den bekanntesten Ausstellern gehörte, die sich allesamt vom sehr großen Potenzial des afrikanischen Marktes viel erhoffen. Microsoft, Huawei, Ericsson, AWS, IBM, Oracle, Orange – um nur einen Bruchteil der Namen zu nennen, die an vier vollbepackten Event-Tagen digital bei Vorträgen und in Foren vertreten waren – sind präsent vor Ort vertreten. Neben der IKT-Branche darf man auch die Notwendigkeit von IoT und 5G nicht vergessen.
Google kann entsprechend schon einen großen Coup vorweisen. Das Unternehmen eröffnete 2019 in der ghanaischen Hauptstadt Accra an der Westküste sein erstes afrikanisches AI-Forschungszentrum. Profitieren von dieser Technik könnte nicht nur die Landwirtschaft in Afrika. Moustapha Cisse ist dortiger Research Scientist und Head of Google AI Center und weist eine sehr umfangreiche Expertise vor. Abgesehen von seinem Studium der Mathematik und Physik erlangte er weiters einen PhD in Machine Learning und arbeitete bereits bei Facebook. Im Google AI Center kann er sein Wissen nun in vollem Umfang einsetzen und Accra zu einem bedeutenden digitalen Hotspot Afrikas mitentwickeln.
Festzuhalten ist: Afrikas Länder haben enormes unterschätztes Potenzial. Wer auf Netzwerken aus ist, muss nicht unbedingt immer nur die WKO aufsuchen. Eine Teilnahme am kommenden AfricaCom- und Tech-Event vom 8. bis 12. November 2021 lohnt sich ebenfalls, dann voraussichtlich wieder persönlich in Kapstadt. Davor, vom 11. bis 12. Mai 2021 findet virtuell das East AfricaCom statt.

https://www.faz.net/aktuell/wirtschaft/afcfta-generalsekretaer-ueber-die-neuen-regeln-fuer-mehr-freihandel-in-afrika-17126579.html

www.gtai.de
www.giz.de
www.rack-centre.com
www.worldbank.org
www.africatechsummit.com

Das Smartphone ist eines der wichtigsten technischen Mittel, um an dem Digitalisierungsfortschritt in den afrikanischen Ländern mit teilzuhaben.

https://www.youtube.com/watch?v=XSRw_-n0hKY&feature=emb_rel_pause

https://www.youtube.com/watch?v=LKeEHAfoWII

IM DIGITALEN FLOW

Es war wenig überraschend, dass es 2020 auch die hypermotion in Frankfurt/Main traf und diese Messe zu einer reinen Digitalveranstaltung wurde. Doch gerade bei Veranstaltungen, die inhaltlich stark Zukunftsthemen ausgerichtet sind, ist diese Lösung gar nicht so schlecht.

Die hypermotion 2020, die aufgrund der Covid-19-Pandemie-Bestimmungen auch im November noch rein digital stattfinden musste, stoß bei der Community auf großes Interesse. Der Inhalt der multimodalen Innovationsplattform, die an zwei Veranstaltungstagen mit zahlreichen Livestreams und interaktiven Modulen realisiert wurde, war schlussendlich bis 10. Dezember online zugänglich. Diesen Bonus gibt es bei reinen physischen Veranstaltungen in der Form nicht.

Die neuen, digitalen Angebote der hypermotion wurden von Ausstellern und Besuchern aus insgesamt 47 Ländern dann laut Veranstalter auch intensiv genutzt – rund 70.000 Page Views lautete die Bilanz nach wenigen Tagen. Mit 1.316 Unique Visitors, also registrierten Besuchern, waren 72 Prozent derer, die sich ein Ticket besorgt hatten, in den ersten drei Tagen bereits auf der Plattform aktiv. Das KI-gestützte Matchmaking hat allein an den zwei Tagen, an denen Live-Streams stattfanden, 824 Verbindungen generiert, infolgedessen über 750 Geschäftstermine vereinbart wurden. 237 Sessions fanden insgesamt statt, die von 8.190 Zuschauern verfolgt wurden, im Schnitt nahmen die User jeweils an sechs Sessions teil. Eine gute Bilanz.

Keynote Speaker Edward Snowden zog das Interesse an. Inhaltlich bot die hypermotion 2020 einiges an Highlights. Nicht zuletzt durch die Zusage von Edward Snowden, der zugeschaltet eine Keynote übernahm. Er betonte zum Thema Datenschutz, dass „eine vernetzte Welt die Menschen enger miteinander verbinde, aber auch Risiken mit sich bringt.“ Und in Zeiten von zunehmender Verlagerung der Aktivitäten ins WWW muss besonderes Augenmerk auf diese Entwicklungen gelegt werden.

In einer weiteren Keynote sprach Bestseller-Autor Marc Elsberg über die Auswirkungen auf systemische Infrastrukturen im Falle eines totalen Stromausfalls. Disruptive Konzepte wie Drohnenverkehr, IoT und additive Fertigungen lieferten neue Impulse für unser zukünftiges Transportsystem. Bei den Startup Pitches konnten Newcomer ihre innovativen Produkte und Ideen einer renommierten Jury präsentieren. RepairFix GmbH, D3 Technologies AG und DATAbility GmbH gingen dabei als Sieger hervor.

Der Vision mobility Think Tank sowie die Logistics Digital Conference (LDC!) des Huss-Verlags kamen in fünf Sessions, u.a. mit Experten von Hyundai Hydrogen Mobility AG, Bio-Hybrid GmbH, LEVC, Arvato Supply Chain Solutions SE und Vowag Cargo Bikes GmbH zu folgenden Ergebnissen: Der Straßenver-

Edward Snowden war als Keynote Speaker bei der ersten reinen digitalen hypermotion zu Gast.

2020 verlagerte sich die Veranstaltung rein ins Internet.

kehr kann zukünftig zu 100 Prozent auf Elektromobilität umgestellt werden. Firmenroller-Leasing-Modelle, Sharing-Angebote und der Einsatz von E-Transportern werden zunehmend auch im industriellen Raum zur Emissionsfreiheit und Energieeffizienz beitragen. Die Infrastruktur für Wasserstoff-Technik muss weitervorangetrieben werden, vor allem durch die Politik. KI-basierte Analysetools und mehr Transparenz innerhalb des Retourenmanagements können Warensendungen effizienter gestalten.

Veranstalter zufrieden. Detlef Braun, Geschäftsführer der Messe Frankfurt, zeigt sich nach der ersten rein digitalen Messe durchaus positiv und zuversichtlich und betonte abschließend: „Innovationen werden von Menschen gemacht, nicht von Maschinen. Nach der langen Phase des wirtschaftlichen Stillstands braucht es wieder B2B-Networkingplattformen. Es ist wichtig, dass wir miteinander in Kontakt bleiben und uns trotz Lockdown austauschen."
Auch Michael Johannes, Leiter des Geschäftsbereichs Mobility & Logistics bei der Messe Frankfurt, ist zufrieden mit dem Ergebnis: „In Windeseile haben wir die Themen der hypermotion digital umgesetzt, um die Vernetzung der Mobilitäts- und Logistikbranche weiterhin voranzutreiben. Wir freuen uns, dass unsere Partner sofort mit umgeschwenkt sind, was das Veranstaltungsformat angeht."

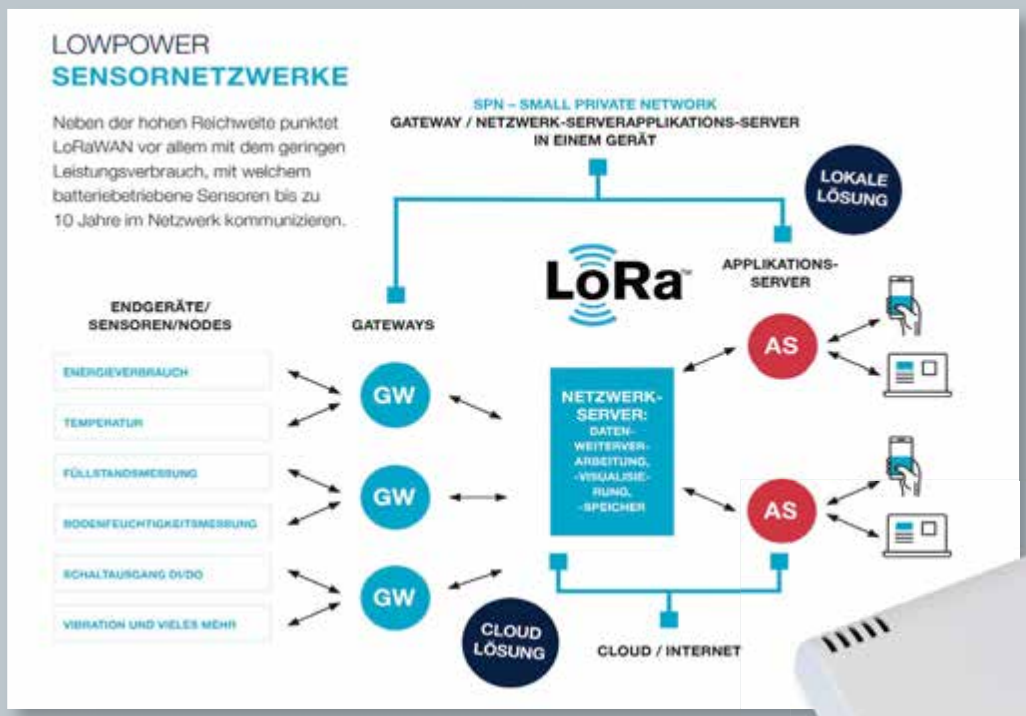
Aussteller zufrieden. David Bitzl, Sales und Business Development bei Siemens Mobility fügte zu seiner Erfahrung als Aussteller hinzu: „Wir haben die Möglichkeiten der digitalen hypermotion voll ausgenutzt. In Live-Streams konnten wir unser Portfolio vorstellen, daraus wertvolle Leads generieren und in zahlreichen Diskussionen per Videogespräch vertiefen." Und Tobias Buxhoidt (Gründer & CEO, parcelLab GmbH, Smart Solution Award-Preisträger 2019) hob hervor: „Ich fand es sehr professionell und bis jetzt die beste virtuelle Veranstaltung, an der wir teilgenommen haben." Ein klares Lob für die Veranstalter.

www.hypermotion.com

HYPERMOTION GOES DUBAI

hypermotion, das in Deutschland entwickelte Messeformat zum Thema Transformation und Zukunft des Verkehrs-, Logistik- und Mobilitätssektors durch Disruption, Dekarbonisierung und Digitalisierung, nimmt als zentrale Veranstaltung im Rahmen der Expo 2020 Kurs auf Dubai. Die hypermotion Dubai, die vom **2. bis 4. November 2021** im Dubai Exhibition Centre (DEC) ihre Pforten öffnen wird, findet parallel zur Expo 2020 statt – der ersten Weltausstellung im arabischen Raum unter dem Motto „Connecting Minds, Creating the Future".
Mit den wichtigen Unterthemen Mobilität, Nachhaltigkeit und Chancen wird die sechsmonatige Großveranstaltung Expo 2020 für einen erheblich größeren Anteil internationaler Besucher auf der hypermotion Dubai sorgen. Ebenso kann die Messe auf die Unterstützung von staatlichen und privaten Organisationen zählen, die sich an vorderster Stelle mit Mobilität und Logistik der Zukunft auseinandersetzen.
Von der Messe Frankfurt Middle East organisiert, arbeitet hypermotion Dubai 2021 mit dem internationalen Hafenbetreiber DP World als globalem Partner zusammen. Dazu sagte H.E. Sultan Ahmed Bin Sulayem, Group Chairman und CEO von DP World (Bild): „Die hypermotion bringt innovative Köpfe und Ideen für die Transformation der Mobilitäts- und Logistikbranche zusammen. Ob bei integrierten Logistikkonzepten, disruptiven Ideen oder digitalen Netzwerken: Die hypermotion gibt uns die Möglichkeit, mit Branchenkennern zusammenzuarbeiten, um eine Welt mit intelligenterem Handel und intelligenterer Logistik zu schaffen. Und: Dubai hat die Grenzen in puncto Innovation stets ausgelotet und diese Eigenschaft ist auch in der DNA von DP World festgeschrieben. Mit unserem Innovationsgeist konnten wir weltweit die Führungsrolle im Bereich intelligente End-to-End-Logistik übernehmen."

TECHNOLOGIE-NEWS



LoRaWAN SENSORIK MIT GROSSEN REICHWEITEN UND GERINGEM ENERGIEAUFWAND

Aus dem smarten Thema IoT entwickeln sich rasant Drahtlostechnologien, die möglichst energieeffizient sind und zugleich über große Reichweiten Daten übertragen können. Dabei gilt LoRaWAN, ähnlich wie Sigfox und Nb-IoT, als eine der Trendtechnologien für LPWAN (Low Power WAN). LoRaWAN (Long Range Wide Area Network) ermöglicht es, mit äußerst geringem Strombedarf Daten über lange Strecken zu senden und somit mehrere hundert batteriebetriebene Sensoren innerhalb eines Netzwerkes zu verwalten und Sensordaten zu verarbeiten.

LoRaWAN-Technologie. Ein LoRaWAN-Netzwerk besteht aus Nodes (Sensoren), Gateways und einem LoRa-Server. Die Sensoren senden in optimierten Intervallen Daten mittels LoRa an alle Gateways in der Umgebung, welche die Daten aufnehmen und an den Server, in die Cloud, weiterleiten. Dort können sie individuell weiterverarbeitet, visualisiert und gespeichert werden. Das Gateway dient als Schnittstelle zwischen den energieeffizienten LoRa-Sensoren und der leistungsstarken Anbindung zum Server. „Neben der hohen Reichweite dieser Funktechnologie punktet LoRaWAN vor allem mit dem geringen Leistungsverbrauch, mit welchem batteriebetriebene Sensoren bis zu zehn Jahre im Netzwerk kommunizieren," zeigt sich auch LoRaWAN-Experte Christoph Gattinger von BellEquip, dem niederösterreichischen Systemanbieter infrastruktureller Lösungen für den effizienten und sicheren Betrieb elektronischer Anwendungen, von dieser Technologie begeistert.

LoRaWAN-Vorteile. Mit LoRaWAN-Sensoren und -Gateways können intelligente (smarte) Monitoring-Lösungen für Gebäude- oder Maschinenüberwachung und vorausschauende Instandhaltung einfach integriert werden. Das Sortiment an LoRaWAN-Sensoren umfasst inzwischen Überwachungslösungen für Temperatur, Luftfeuchtigkeit, Licht, Bewegung, Vibration, CO_2, Geräusch, Anwesenheit und vieles mehr und zeichnet sich aus durch:

- hohe Reichweite und Gebäudedurchdringung
- batteriebetriebene Datenübertragung bis zu zehn Jahre
- 100te LoRa-Sensoren über 1 LoRaWAN-Gateway

Ein großer Vorteil der LoRaWAN-Gateways ist zudem, dass sich sowohl private als auch öffentliche LoRaWAN-Netzwerke mit Reichweiten bis zu 10 km aufbauen lassen. BellEquip Fazit: Das ist zukunftsfähige Technik, die verbindet.

Das Unternehmen BellEquip mit Sitz in Zwettl (NÖ) zählt zu den führenden Systemanbietern von infrastrukturellen Lösungen für den effizienten und sicheren Betrieb elektronischer Anwendungen in den Bereichen Remoteservice, Automatisierungs- und Kommunikationstechnik.

www.bellequip.at

TEAM NEU AUFGESTELLT

Der Gründer und Geschäftsführer des deutschen IT-Beratungs- und Dienstleistungsunternehmens **Scholderer GmbH,** Dr. habil. **Robert Scholderer**, ist neuer Vorsitzender des IT Service Management Forums (itSMF) in Österreich. Die online-tagende Generalversammlung wählte den deutschen Ingenieur und Unternehmer einstimmig zum Nachfolger von Martin Pscheidl, der nach acht Jahren im Amt nicht mehr kandidierte. Die Versammlung wählte außerdem einen neuen Vorstand des itSMF. Ihm gehören neben Scholderer als Vorsitzendem fünf weitere Mitglieder aus Österreich, Deutschland und der Schweiz an.

www.scholderer.de

EFFIZIENT IN DER CLOUD

Mit der TwinCat-IoT-Produktfamilie stellt **Beckhoff** bereits seit 2015 vielfältige Möglichkeiten für die IoT-Kommunikation zur Verfügung. Eine solche Datenübertragung in die Cloud oder zwischen vernetzten Maschinen eröffnet ein großes Steigerungspotenzial für die Produktionseffizienz. Dabei kann nun auch MindSphere, das Industrial IoT als Servicelösung von Siemens, eingebunden werden. Die Automatisierungssoftware TwinCat 3 kann als HTTP(S)-Client mit HTTP(S)-Servern kommunizieren, z.B. um über eine REST-API Daten auszutauschen.

www.beckhoff.at

UMFANGREICH ERNEUERT

Mit **abas** ERP 20 stellt der Karlsruher Softwarehersteller das bisher umfangreichste Upgrade seiner 40-jährigen Firmengeschichte vor, die kundenindividuellen Anpassungen bleiben dank der einzigartigen Architektur bestehen. Das neue Release setzt mit geschärften Leitplanken auf mehr Prozesssicherheit, bietet eine neue Dashboard-Technologie und integriert bisher kostenpflichtige Add-ons zu einem ERP-Gesamtpaket, ist aber weiterhin hoch individualisierbar. Der Schwerpunkt der neuen Version liegt auf der Erhöhung der Prozesssicherheit bei gleichzeitig maximaler Flexibilität, um Prozesse an unternehmensindividuelle Bedürfnisse anzupassen. Zudem sind nun 13 bisher aufpreispflichtige Funktionen im Standard-Lieferumfang enthalten: Beispiele sind die mobilen Anwendungen Warehouse für die Lagerverwaltung oder Shopfloor für die Betriebsdatenerfassung (BDE). Auch im Bundle integriert ist jetzt der „Elektronische Rechnungsversand" – wahlweise im nun unterstützten E-Rechnungsformat ZUGFeRD 2.1, das eine automatische Übergabe der Rechnungen an das Dokumentenmanagementsystem ermöglicht. Oder die „abas Dashboard" Technologie, die neben vorkonfigurierten Standard-Übersichten und Cockpits eine Erstellung nach individuellen Anforderungen im Dashboard Editor bietet – ohne jegliche Programmierung.

www.abas-erp.com

NEUER CHIEF TECHNOLOGY OFFICER

SAS, Anbieter von Lösungen für Analytics und KI, ernannte **Bryan Harris** (Bild) zum Executive Vice President und Chief Technology Officer (CTO). Harris war für SAS zuvor als Senior Vice President sowie Head of Engineering tätig und verfügt über mehr als zwanzig Jahre Erfahrung in der Entwicklung von Analytics, Enterprise-Search-Technologien, Distributed-Computing- und Cloud-Architekturen, zuletzt als Senior Leader der R&D-Abteilung von SAS. In jüngster Zeit war Harris maßgeblich an der Entwicklung der neuesten Generation von SAS Viya beteiligt und hat somit die Cloud-Strategie von SAS weiter vorangetrieben.

www.sas.at

SMART ERGÄNZT

Siemens erweitert seine Edge Applikation Analyze MyMachine/Condition um eine dazugehörige Mindsphere-Applikation und demonstriert damit, wie Edge Computing und Cloud Computing intelligent miteinander verknüpft werden. Die Sinumerik Edge-Applikation Analyze MyMachine/Condition erstellt anhand hochfrequenter CNC-Daten den mechanischen Fingerabdruck einer Werkzeugmaschine. In der Applikation können Anwender mithilfe flexibel konfigurierbarer Messreihen verschiedene Parameter wie Steifigkeit, Reibung und Umkehrspiel, in den einzelnen Achsen erfassen und auswerten. Die Messresultate können anschließend visualisiert und mit Referenzdaten verglichen werden.

Die neue ergänzende Mindsphere-Applikation zu Analyze MyMachine/Condition erlaubt nun maschinenübergreifende Vergleiche und Auswertungen. Warn- und Serviceschwellen können einzeln für jedes Asset visualisiert werden und die Zustände mehrerer Maschinen über einen längeren Zeitraum überwacht und visualisiert werden. Somit können Anwender auch Abweichungen über eine längere Zeit hinweg feststellen.

www.siemens.at

5G AUSBAUEN

Adlink Technology Inc. arbeitet mit Sageran Network Technology zusammen. Beide Unternehmen entwickeln gemeinsam End-to-End-Lösungen für offene 5G Open Radio Access Network (RAN). Die Partner richten dafür ein gemeinsames Labor für die Entwicklung integrierter 5G Edge-Lösungen auf Grundlage einer offenen Architektur für öffentliche und private Netze ein. Ziel ist es, Telekommunikationsdienstleistern eine verbesserte Hersteller-Interoperabilität, einen höheren Innovationsgrad sowie kontinuierliche Kostensenkungen zu bieten.

„5G RAN ist der wichtigste Infrastruktur-Baustein, um den Ausbau von 5G-Netzen voranzutreiben. Der Aufbau von 5G RAN auf kosteneffiziente, nachhaltige Weise ist ebenso wichtig wie die Bereitstellung von leistungsfähigen Netzwerken für Mobilfunkanbieter. Hier kommt 5G Open RAN ins Spiel", so Julian Ye, Director of Networking and Communications bei Adlink.

www.adlinktech.com

NEUE AUSRICHTUNG

Wie **SAP Österreich** kürzlich bekanntgab ist **Christina Wilfinger** neue Geschäftsführerin von SAP Österreich und löste hiermit Christoph Kränkl, der künftig für die strategischen Partner der SAP auf regionaler Ebene in Mittel- und Osteuropa verantwortlich ist, ab. Die erfolgreiche Businessfrau war in den vergangenen vier Jahren als Mitglied des Führungsteams bei Microsoft Österreich für den Lösungsvertrieb im Enterprise-Bereich verantwortlich. Ihr Hauptaugenmerk lag in der Umstellung von Kunden und Partnern auf das Cloud-Geschäft. Die gebürtige Steirerin hat Wirtschaftsingenieurwesen an der Technischen Universität Wien studiert und unterrichtet als Dozentin an der Donau-Universität Krems. Zudem war sie bereits bei SAP Österreich vor einigen Jahren tätig und kennt die Strukturen und einen Großteil des Teams sehr gut.

Die 38-Jährige ergänzte im Gespräch: „Veränderung ist immer eine Herausforderung. Gerade wenn wir als Unternehmen selbst den Wandel zur Cloud Company vollziehen, verstehen wir die Bedürfnisse unserer Kunden umso besser und können mit innovativen Angeboten punkten. Mit unserer neuen Strategie „Rise with SAP" bieten wir zudem eine ganzheitliche Business-Transformation, bei der die bestehenden ERP-Kernprozesse unserer Kunden in die S/4HANA Cloud-Plattform verlagert werden." Seit 1. Februar zeichnet zudem **Gregor Grindjan** als neuer Chief Operating Officer für SAP Österreich verantwortlich. Durch seine langjährige Erfahrung bei SAP und seine umfassende Expertise wird er gemeinsam mit der neuen Geschäftsführerin und dem ebenso neu aufgestellten Management-Team strategische Prozesse vorantreiben, um Kunden bestmöglich im Cloud-Business unterstützen zu können.

www.sap.com

IoT4 INDUSTRY&BUSINESS

ABGESCHLOSSEN

Mit 21. Dezember 2020 hat die **DCCS IT-Gruppe** sämtliche Anteile des Mainzer Software-Entwicklungsspezialisten **axenton** erworben. Damit wird der erfolgreiche Wachstumskurs des österreichischen IT-Business-Solutions-Unternehmens und der Marktausbau in Deutschland weiter fortgesetzt. Die axenton GmbH wird unter dem bestehenden Namen und in gleicher Rechtsform weitergeführt. Neuer Geschäftsführer von axenton ist **Wolfgang Mraz** (Bild), Miteigentümer und langjähriger CEO der DCCS IT-Gruppe. Gemeinsam mit dem axenton-Team wird er sowohl das Unternehmen als auch das Leistungsangebot für die Kunden kontinuierlich weiterentwickeln.

Der bisherige CEO Klaus Steidl zieht sich in den Ruhestand zurück, bleibt aber weiterhin beratend für das Unternehmen tätig.

www.dccs.at

FÜHRUNGSKRAFT

PTC ernannte **Troy K. Richardson** (Bild) zum Executive Vice President und Chief Operating Officer mit Wirkung zum 16. November 2020. Richardson ist eine erfahrene Führungskraft auf dem Gebiet der Unternehmenstechnologie und verfügt über mehr als drei Jahrzehnte Erfahrung als Vertriebs- und Betriebsleiter. Er hat dazu beigetragen, das schnelle Wachstum einiger der größten Marken der Softwarebranche voranzutreiben.

www.ptc.com

AUSZEICHNUNG ERHALTEN

Cloudflight, Softwareentwicklungsunternehmen und KI-Experte, wurde von der Wirtschaftskammer Österreich, Bezirksstelle Linz-Stadt, in der Kategorie „Innovation & Export" zum Unternehmen des Jahres 2020 gewählt. Die Award-Verleihung stand im Jubiläumsjahr, in dem die Auszeichnung bereits zum zehnten Mal verliehen wurde, unter dem Motto „Erfolgreich Herausforderungen meistern" und nahm damit direkten Bezug auf die Corona-Pandemie. Am Wettbewerb teilnehmen konnten alle Unternehmen mit Sitz in Linz, die vor dem 1. Jänner 2020 gegründet worden waren.
Cloudflight wurde mit dem Award für seine zahlreichen innovativen Projekte aus dem Bereich KI ausgezeichnet. Darüber hinaus wurde **Jörn Petereit**, COO von Cloudflight (Bild), in den Hauptvorstand des Digitalverbands Bitkom gewählt. Petereit ist ein ausgewiesener Transformations- und Technologieexperte mit über 15-jähriger Erfahrung in der digitalen Transformation. Vor seinem Eintritt in die Geschäftsführung von Cloudflight war der Manager Vice President IoT/M2M bei der Deutschen Bahn und Head of Strategic Cloud Projects & Service Strategy bei der QSC AG.

www.cloudflight.io

NEUE EIGENTÜMERSTRUKTUR

Die international tätige **technosert electronic GmbH** aus Wartberg/OÖ hat eine neue Eigentümerstruktur: technosert-Gründer **Ing. Johannes Gschwandtner** (li.i.Bild) übergab nach über 32 Jahren erfolgreichen Unternehmertums seine restlichen Firmenanteile an seinen Partner **Mag. Hermann Schübl** (re.i.Bild), der bereits seit Ende April 2020 Allein-Geschäftsführer ist.
Der Spezialist für Elektronikdienstleistungen in kleinen und mittleren Serien beschäftigt an seinen Standorten Wartberg ob der Aist und Linz-Pichling rund 150 Mitarbeiter. technosert ist spezialisiert auf innovative Lösungen in der Elektronikindustrie und führend in der Konzeption und Entwicklung, Testung und Assemblierung elektronischer Geräte bis hin zu Röntgenanalysen von Baugruppen und Bauelementen. Die Kunden von technosert sind international tätig und kommen aus unterschiedlichen Branchen: aus dem Auto- und Flugzeugbau, der Sicherheits- und Medizintechnik bis hin zur Satellitentechnik und Abwassermessung.

www.technosert.com

VÖSI UND ÖGV UNTER EINEM DACH

Der **VÖSI** (Verband Österreichischer Software Industrie) und der **ÖGV** (Österreichischer Gewerbeverein) arbeiten ab sofort unter einem Dach zusammen – Ziel ist „Digitaler Hotspot" und „Think Tank" für Gewerbetreibende und Industrie. Damit führt **Peter Lieber** (Bild), selbst Eigentümer der Software Unternehmen Sparx Systems und LieberLieber Software, seit 2014 VÖSI Präsident und seit Juni 2020 ÖGV-Präsident, nun zwei Verbände und vereint damit Unternehmertum und IT-Know-how in einer dynamischen Kooperation.

www.gewerbeverein.at
www.voesi.or.at

SCHNELL UNTERWEGS

Turck hat sein umfangreiches Drehgeberportfolio erweitert und bietet jetzt auch in der Efficiency und der Industrial Line Encoder mit IO-Link-Schnittstelle an. Damit sind neben den berührungslosen QR24-Drehgebern der Premium Line ab sofort auch in den anderen zwei Kategorien IO-Link-Modelle verfügbar. Die neuen Drehgeber unterstützen mit COM3 die aktuellste und mit 230,4 kBit/s schnellste IO-Link-Schnittstelle am Markt, mit der sich Regelkreise deutlich verbessern lassen. Die Encoder verfügen zudem über integrierte Temperatursensoren und geben bei Bedarf bereits vorverarbeitete Positionsdaten an IO-Link Master weiter. Mit ihren smarten Daten unterstützen die Geräte IIoT-Lösungen, beispielsweise zur vorausschauenden Wartung.

www.turck.at

MANAGERIN OPERATIONS ERNANNT

Claudia Schupp (Bild) ist ab sofort als Managerin Operations bei **Interxion**: A Digital Realty Company tätig. In dieser Position verantwortet die erfahrene IT Infrastructure & Application-Expertin den Auf- und Ausbau der Datacenter-Infrastrukturen am Wiener Standort. „Rechenzentren sind das Herz unserer digitalen Welt. Durch den Digitalisierungsschub, den Gesellschaft und Wirtschaft dieses Jahr erfahren haben, wird der Bedarf an hochverfügbaren, sicheren Datacentern als wichtigste Voraussetzung für Innovation weiter steigen. Aus diesem Grund brauchen wir herausragende Fachkräfte, um die steigende Nachfrage unserer Kunden bestmöglich adressieren zu können. Daher freut es mich besonders, dass wir mit Claudia Schupp eine Expertin für uns gewonnen haben, die nicht nur über umfassendes Rechenzentrums-Know-how, sondern auch über kaufmännische Expertise verfügt. Wir freuen uns schon sehr auf die Zusammenarbeit und wünschen ihr viel Erfolg für die neue Aufgabe", Martin Madlo, Managing Director bei Interxion Österreich. Die gebürtige Wienerin ist gelernte Industriekauffrau und akademische Exportkauffrau. Zu ihren beruflichen Stationen zählen unter anderem die Siemens AG Österreich, wo Claudia Schupp in unterschiedlichen Funktionen vom Controlling über die kaufmännische Leitung unterschiedlicher Business-Segmente bis hin zur Projektleitung beim Neubau des Rechenzentrums verantwortlich war, die Position als Abteilungsleiterin für das Operation Management des gesamten IT-Outsourcings bei der Atos IT Solutions and Services GmbH sowie jene als Abteilungsleiterin für die Betriebssteuerung IT bei der Raiffeisen Informatik GmbH.

www.interxion.com

IN DIE CLOUD

© Telekom

Die **Deutsche Telekom** und **Microsoft** haben eine Erweiterung ihrer bestehenden Partnerschaft angekündigt. Ziel ist es, Geschäftskunden aller Größenordnungen bei ihrer Cloud-Transformation zu unterstützen. Für viele Unternehmen ist die Cloud eine Chance, ihre IT-Kosten zu senken, die Flexibilität zu erhöhen und Innovationen zu beschleunigen. Doch um die Vorteile des Cloud Computing voll auszuschöpfen, ist auch ein skalierbares Hochleistungsnetz erforderlich, das die steigenden technologischen Anforderungen erfüllen kann.

Durch die Kombination der Cloud- und KI-Fähigkeiten von Microsoft mit dem Cloud Migration Framework und den Telekommunikationsdiensten der Telekom können Unternehmenskunden ihre Produktivität steigern, flexiblere und widerstandsfähigere Betriebsabläufe aufbauen und schneller neue Cloud-Angebote bereitstellen.

„Wir haben uns mit unserem langjährigen Partner Microsoft auf den Rahmen für gemeinsames strategisches Wachstum geeinigt. Darüber freuen wir uns sehr", sagte Adel Al-Saleh, Mitglied des Vorstands der Deutschen Telekom und CEO von T-Systems und ergänzt: „Diese Partnerschaft wird es uns ermöglichen, die Dienstleistungen für unsere Kunden zu verbessern. Auch bei der Digitalisierung und dem Netzausbau werden wir uns gegenseitig unterstützen".

www.telekom.com

DER WETTBEWERBSVORTEIL

Bild: © Capgemini

Unternehmen, die beim Dateneinsatz führend sind, erzielen 22 Prozent mehr Gewinn und pro Mitarbeiter 70 Prozent mehr Umsatz als ihre Wettbewerber. Trotzdem tragen datengestützte Entscheidungen erst in 38 Prozent der Organisationen zum Geschäftserfolg bei. Zudem vertraut nur jede fünfte Führungskraft den eigenen Daten. Zu diesen Ergebnissen kommt eine Studie namens **„The data-powered Enterprise: Why Organizations must strengthen their Data Mastery"** von **Capgemini**, für die weltweit jeweils 500 Führungskräfte aus den Fachbereichen und dem IT-Bereich von Unternehmen befragt wurden, die einen Jahresumsatz von mehr als einer Milliarde US-Dollar erwirtschaften.

Unternehmen müssen den Einsatz von Daten beherrschen, um Wettbewerbsvorteile zu erzielen. Laut Studie gelten diejenigen Unternehmen als datengetrieben, die ihre Daten selbständig erstellen, verarbeiten und dazu einsetzen können, um ihren Geschäftszweck zu erfüllen, Innovationen voranzutreiben und ihre Unternehmensziele zu erreichen. Allerdings verfügt aktuell nur jedes sechste Unternehmen (16 Prozent) über die erforderlichen Werkzeuge und Technologien sowie die entsprechende Datenkultur und -vision, um als datengetriebenes Unternehmen bezeichnet werden zu können.

Obwohl Unternehmen zuletzt Fortschritte gemacht haben, stellen nur die Hälfte (50 Prozent) von ihnen Daten bei der Entscheidungsfindung in den Mittelpunkt. Am häufigsten setzen Unternehmen aus den USA (77 Prozent) sowie Deutschland und Großbritannien (jeweils 69 Prozent) auf datengetriebene Entscheidungsprozesse.

Wirtschaftliche Vorteile. Datengetriebene Unternehmen schneiden bei Kennzahlen zu Kundenbindung, Betriebseffizienz und Kosteneinsparungen um 30 bis zu 90 Prozent besser ab. Zudem erzielen sie durch neue Produkte und Dienstleistungen eine 19-prozentige und damit um sieben Prozentpunkte höhere Umsatzsteigerung als andere Unternehmen.

Vier von fünf Unternehmen (83 Prozent), in denen die Daten als vertrauenswürdig gelten, gelingt es, ihre Datenbestände zu monetarisieren. Von den Unternehmen, deren Daten nicht als vertrauenswürdig angesehen werden, sind es nur 24 Prozent. Allerdings zeigt sich eine deutliche Diskrepanz zwischen der angenommen und der tatsächlichen Zufriedenheit bezüglich der Daten: Demnach vertraut nur jede fünfte Führungskraft im Geschäftsbereich den bereitgestellten Daten umfassend, nur etwa jeder vierte (27 Prozent) ist mit der Datenqualität zufrieden.

„Viele Unternehmen durchlaufen aktuell einen Transformationsprozess, bei dem die prozessorientierte Arbeitsweise zunehmend durch eine datengetriebene abgelöst wird. Das damit verbundene Potenzial und die wirtschaftlichen Vorteile wirklich datengetriebener Unternehmen verdeutlichen die Studienergebnisse eindrucksvoll. Entsprechend sollte sich jede Führungskraft eingehend mit der Datenstrategie seines Unternehmens befassen", so **Andreas Hornich** (Bild), Head of Insights and Data bei Capgemini in Österreich. „Allerdings zeigt die Studie auch, dass nur etwa jedes dritte Unternehmen datengestützte Entscheidungen gewinnbringend nutzt. Dies hängt oftmals mit dem Datenbewusstsein auf Geschäftsführungsebene zusammen, das entweder nicht ausgeprägt genug ist, oder zu sehr auf etwaige Risiken fokussiert, ohne die immensen Chancen mitzudenken."

www.capgemini.com

ZUR STUDIE

Für die Untersuchung befragte Capgemini technische Führungskräfte von 500 Organisationen aus Technologiebereichen wie IT, Informationsmanagement, Datenmanagement und -analyse sowie Business Intelligence. Zudem befragte Capgemini Führungskräfte aus verschiedenen Geschäftsbereichen von 504 Organisationen. Beide Umfragen wurden im August 2020 unter Unternehmen mit mehr als einer Milliarde US-Dollar Umsatz im letzten Finanzjahr durchgeführt.

Details zur Studie:

VERANSTALTUNGSKALENDER

MÄRZ

embedded world
1.-5.3.2021 | virtuell

Internet World Expo
8.-12.3.2021 | virtuell

ScaleUp 360° Big Data & Analytics Summit
9.-10.3.2021 | virtuell

Smart City Expo
15.-16.3.2021 | Dubai, hybrid

PI-Konferenz 2021
15.-19.3.2021 | virtuell

ScaleUp 360° Identity & Access Management
17.-18.3.2021 | virtuell

CloudFest
20.-25.3.2021 | virtuell

MarketsandMarkets IoT Virtual Summit
23.-24.3.2021 | virtuell

Ivalua Now Europe
23.-25.3.2021 | virtuell

5G Expo virtual
30.3.2021 | virtuell

APRIL

European Blockchain Convention
12.-16.4.2021 | virtuell

Hannover Messe digital
12.-16.4.2021 | virtuell

SCCS - Supply Chain Cyber Security Summit
14.-15.4.2021 | virtuell

Digital Transformation Week
20.-23.4.2021 | virtuell

DevOpsCon
20.-23.4.2021 | London, hybrid

ADV Data Governance Konferenz
22.-23.4.2021 | Wien

Ivalua Now America
27.-29.4.2021 | virtuell

Automatisierungstreff - IT & Automation
27.-29.4.2021 | Böblingen

MAI

Tech Jobs Fair Vienna
6.5.2021 | Wien

Techorama - Deep Knowledge IT Conference
17.-19.5.2021 | virtuell

Digital Transformation Expo
19.-20.5.2021 | Manchester

IT Security Summit
19.-21.5.2021 | virtuell

CloudTalk Online
26.-27.5.2021 | virtuell

More-IP
26.-27.5.2021 | Amsterdam

JUNI

Datacloud Global Congress
1.-3.6.2021 | virtuell

Twenty2X
15.-17.6.2021 | Hannover

Viva Technology
16.-19.6.2021 | Paris, hybrid

Cyber Week
20.-24.6.2021 | Tel Aviv

Rethink! IT Security
21.-22.6.2021 | Berlin, hybrid

IoT Evolution Expo
22.-25.6.2021 | Miami

ADDC - App Design & Development Conference
23.-25.6.2021 | Barcelona

WeAreDevelopers World Congress
28.-29.6.2021 | Berlin

MWC Barcelona
28.6.-1.7.2021 | Barcelona

JULI

Blockchance Europe
7.-9.7.2021 | Hamburg

SEPTEMBER

IoT Tech Expo Global
6.-7.9.2021 | London

EIC - European Identity and Cloud Conference
13.-16.9.2021 | München, hybrid

Hypermotion
14.-16.9.2021 | Frankfurt/Main

Industry of Things World
20.-21.9.2021 | Berlin

IT Security Summit
20.-22.9.2021 | Berlin

European Cloud Summit
27.-29.9.2021 | Mainz

OKTOBER

IoT Solutions World Congress
5.-7.10.2021 | Barcelona

it-sa
12.-14.10.2021 | Nürnberg

European Cloud Conference
26.-28.10.2021 | Nizza

Smart Country Convention
26.-28.10.2021 | Berlin

NOVEMBER

EHI Technologie Tage
9.-10.11.2021 | Bonn

SPS
23.-25.11.2021 | Nürnberg

VORSCHAU

IoT4 NR. 2 | Erscheinungstermin: **1. Juli 2021**

ZUKUNFT MESSE – 5G GEHÖRT DAZU

Noch heuer wird das Messegelände der Deutschen Messe in Hannover auf mehr als 1,4 Millionen m² zum ersten 5G-Messegelände Europas. Dafür hat der Veranstalter von internationalen Investitionsgütermessen eine Frequenzzuteilung im Bereich 3,7-3,8 GHz der Bundesnetzagentur erhalten und wird in Summe 30 Hallen und Gebäude sowie das gesamte Freigelände zu einem der größten 5G-Areale Europas ausbauen. Dr. Jochen Köckler, Vorsitzender des Vorstandes der Deutschen Messe AG schaut somit sehr zuversichtlich in die digitale Zukunft.

ZUKUNFT CLOUD?

Alle Welt spricht von Clouds und in Zeiten vermehrten Homeoffices nimmt der Bedarf ebenfalls zu, die Daten an einem sicheren Ort abzuspeichern. Doch was können die unterschiedlichen Angebote? Was wird geboten? Der Schwerpunkt Cloud Computing zeigt Highlights und Schwachstellen auf.

OFFENLEGUNG (gemäß Mediengesetz § 25, Absatz 1-3)

Medieninhaber: Technik & Medien Verlagsges.m.b.H.,Traviatagasse 21-29/8/2, 1230 Wien.

Geschäftsführer: Thomas Lunacek

Unternehmensgegenstand: Herausgabe von periodischen Fachzeitschriften für die Industrie u.a.

Gesellschafter: Thomas Lunacek. Das Unternehmen befindet sich zu 100 Prozent in seinem Besitz.

Grundlegende Ausrichtung: IoT4 Industry & Business ist eine unabhängige Fachzeitschrift für die Industrie- und IT-Branche sowie alle Branchen, die mit IoT (Internet of Things/ Internet der Dinge) in Berührung kommen.

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.

5. Jahrgang
©2021 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.

IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

Zum kostenlosen Abo

HABEN SIE NOCH FRAGEN?

Stephanie Englert, Chefredaktion
s.englert@technik-medien.at

Gudrun Lunacek, Vertrieb und Marketing
g.lunacek@technik-medien.at

IoT4 INDUSTRY&BUSINESS

Security | Big Data | Cloud |
Realtime IoT | Künstliche Intelligenz |
Menschen im Gespräch | Innovationen | ...

... Impulse für Fortschritt

TECHNIK & MEDIEN VERLAGSGMBH

www.iot4industry.info

Zuverlässigkeit steigern. Flexibilität vorantreiben. Integration vereinfachen.

RocketLinx
A Pepperl+Fuchs Brand

RocketLinx® Ethernet-Switches

- Ethernet-Switches mit vollem Funktionsumfang für höchste IT-Sicherheit und maximale Performance
- Individuelle Netzwerkkonfiguration durch Kombination aus Gigabit-RJ45- und SFP-Glasfaser-Ports in einem einzigen Gerät
- Ausgelegt auf Zuverlässigkeit: Netzwerkredundanz, robuste Metallgehäuse und erweiterter Temperaturbereich

Mehr Informationen unter
pepperl-fuchs.com/pr-rocketlinx

Your automation, our passion.

PEPPERL+FUCHS