IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

3|2021
Erscheinungstermin:
16. November 2021
www.iot4industry.at

3 x jährlich

# NONSTOP KOOPERATIVES ANLAGEN-ENGINEERING

**Mit der Plant Solution von Engineering Base bietet Aucotec ein Höchstmaß an Durchgängigkeit, vom R&I bis Arbeitsblatt, von Process Design bis Automation**

Im Fokus
**KEINE ZEIT FÜR SECURITY?**

Im Fokus
**ATTACKED! WAS NUN?**

Im Gespräch
**DAS KALKULIERBARE RISIKO**

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

OPC UA

IO-Link

# Technologien perfektionieren. Kommunikation revolutionieren. Sensorik 4.0 ermöglichen.

## IO-Link-Master mit OPC UA-Schnittstelle

- OPC UA-Schnittstelle für zukunftsorientierte IoT-Lösungen im Zeichen von Industrie 4.0
- MultiLink – Parallele Steuerungs- und Cloudkommunikation bietet höchste Flexibilität in Automatisierungssystemen
- Einfache Konfiguration über Webbrowser durch integrierten Webserver und IODD-Interpreter

**www.pepperl-fuchs.com/pr-iot-master**

Your automation, our passion.

PEPPERL+FUCHS

# SERVUS!

Wer könnte es schöner sagen als Peter Alexander, der einst sang: *„Es kommt für alles schon einmal die Endstation (…) Sag beim Abschied leise Servus, nicht Lebewohl und nicht Adieu. Diese Worte tun nur weh, doch das kleine Wort Servus ist ein lieber letzter Gruß, wenn man Abschied nehmen muss. (…) Sag beim Abschied leise Servus und gibt´s auch kein Wiedersehen, einmal war es doch schön.“*

**Jetzt fragen Sie sich,** was dieser Wiener Klassiker mit der aktuellen Ausgabe vor Ihnen zu tun hat? Nun: Zum einen könnte man den Konnex zu Cyberangriffen durchaus herstellen, denn einmal gehackt, sind für die meisten Unternehmen die Daten erst einmal „futsch“, Zugriffe gesperrt und wohl oft auch das Konto leer. Cyberkriminalität nimmt rasant zu, nicht erst seit der Pandemie, und in diesem einen Moment, wenn die scheinbar sichere Email sich als unsicher herausstellt, nehmen die Betroffenen sicher vorerst einmal „Abschied“ von Daten, gesicherten Produktionsabläufen uvm. Zum anderen ist es auch so, dass man sich vielleicht ein wenig von dem Gedanken verabschieden muss, dass es „den sicheren Mitarbeiter“ gibt. Menschen machen Fehler, ein Glück. Und KI, Avatare, Roboter und Co., ihnen allen fehlt eines wiederum: das Menschliche.

**In den vielen zurückliegenden Gesprächen** der vergangenen fünf Jahre, die der Titel **IoT4 Industry&Business** nun schon besteht, habe ich eine Reihe von Erkenntnissen dazu gewonnen. Zu den unterschiedlichsten Themen gab es viel zu besprechen und für den Leser aufzubereiten. Ich habe gezählt: In 130 Interviews durfte ich Fragen stellen, zuletzt auch mittels Zoom und Co., durfte staunen, nachfragen und auf diversen IoT-Events auch durchaus erleben. AR, HoloLens, LiveHacking ... alles ist für das Erleben da und das Verstehen.

**Und Informationen rund um die Digitalisierung** reißen ja zum Glück nie ab, das hat auch die Pandemie nicht geschafft – im Gegenteil. Als 2016 die Idee zum Titel entstand, bin ich auf der Cebit in Hannover vielen „Machern“ über den Weg gelaufen. Eine Begeisterung für Produkte und Inhalte bekommen Sie nur zwischenmenschlich, und diese formiert wiederum Inhalte. Dafür kann ich mich heute auf diesem Weg nur bei allen herzlich bedanken! Zum Jahresende verlasse ich auf eigenen Wunsch den Technik&Medien Verlag und somit auch das IoT4 Industry&Business. Es hat viel Spaß gemacht: Dankeschön dafür – auch an das Team – und Servus!

**Stephanie Englert**, Chefredakteurin

# INHALT
## NOVEMBER 2021

### Coverstory

**Nonstop kooperatives Anlagen-Engineering**
Mit der Plant Solution von Engineering Base bietet Aucotec ein Höchstmaß an Durchgängigkeit, vom R&I bis Arbeitsblatt, von Process Design bis Automation

**www.aucotec.at**

**Lesen Sie mehr ab Seite 28!**

### IM FOKUS


**6 Attacke!**
**8 News Security**
**14 Gelungener Restart**
**16 Es kann jeden treffen**
**20 „Keine Zeit für Security" rächt sich bald einmal** | Kai Zobel, Imperva
**23 Gastkommentar** | Warum brauchen Unternehmen eine Vision?
**24 Gastkommentar** | Welchen Security-Level würde Ihr Automatisierungssystem erreichen?
**26 Attacked!** | Roman Oberauer, NTT


### IM GESPRÄCH


**28 Coverstory** | Nonstop kooperatives Anlagen-Engineering von FEED bis zum Anlagenbetrieb
**32 Digitalisierung ist nicht nur eine E-Mail** | Andreas Dangl, Fabasoft
**34 Datensicherheit für die Industrie**
**35 Gastkommentar** | Geregelte IT-Verhältnisse
**36 Allheilmittel IoT-Plattformen?** | Marcel Möstel, tresmo
**39 „Meine Leidenschaft für die digitale Welt wurde mir in die Wiege gelegt"** | René Blaschke, B&R
**40 Das kalkulierbare Risiko** | Daniel Metzger, Cloudera
**42 Gastkommentar** | OEE und IIoT


### SECURITY | BIG DATA | CLOUD COMPUTING


**44 Das sensible System schützen**
**46 LoRaWAN-Überwachungslösungen vor allem bei Kommunen immer mehr gefragt**
**47 News**


### STÄNDIGE RUBRIKEN


**49 Veranstaltungen**
**50 Impressum | Vorschau**


**3 x jährlich**

**20**
Der Mitarbeiter als Firewall? Mehr Investitionen in Aufklärung und Angriffsabwehr? Vielleicht ist das, was offen kommuniziert wird, noch lange nicht das, was für eine wirklich funktionierende Abwehr von Cyberangriffen ausreicht oder gar intern wirklich ausgeübt wird. Doch wann wird es soweit sein, dass Unternehmen den richtigen Weg einschlagen, um ihre Daten ausreichend zu schützen? Im Gespräch mit Kai Zobel, Area Vice President EMEA Central bei Imperva, kam ein erster Eindruck zutage, der zum Nachdenken anregen sollte.

**26**
Cyberattacken nehmen zu. Die Seite der Angreifer wird gefühlt immer professioneller und es ist ein Business daraus entstanden. Im Interview mit Roman Oberauer, Vice President Go to Market & Innovation bei NTT Ldt., wurde klar, dass der Wissensabstand zwischen Angreifern und Angegriffenen kleiner wird, dennoch muss stärker gehandelt werden – jetzt und nicht erst dann, wenn es „zu spät" ist.

**36**
Allheilmittel IoT-Plattformen? Als Head of Solutions von tresmo ist Marcel Möstel verantwortlich für das Lösungsportfolio und dessen stetige Weiterentwicklung sowie die Kundenberatung rund um innovative IoT-, Cloud- und App-Lösungen – und die Nachfrage nach diesen Lösungen wächst nicht erst seit der Pandemie. Seit 2012 begleitet tresmo Kunden unterschiedlichster Branchen und Unternehmensgrößen in engen Partnerschaften auf dem Weg zu eigenen digitalen Produkten und Services. Im Gespräch mit ihm gab es aufschlussreiche Erkenntnisse.

PASSWO

# ATTACKE!

Man gewöhnt sich an vieles. Doch gewöhnt man sich wirklich auch an Cyberangriffe? Oder schärfen diese nicht viel mehr den Blick jedes Einzelnen bei vermeintlichen Spams inklusive unseriöser Anhänge – vor allem am Arbeitsplatz.

Von Stephanie Englert

Die vermehrte Nutzung von digitalen Angeboten und die Etablierung des so genannten Homeoffice haben uns eines in den vergangenen zwei Jahren gezeigt: Cyberangriffe finden täglich statt. EY kam Anfang diesen Jahres zu folgendem Ergebnis: „Fast jedes vierte österreichische Unternehmen hat in den letzten fünf Jahren konkrete Angriffe auf Daten entdeckt – es gibt eine hohe Dunkelziffer“ und: „Mehr als jedes zweite Unternehmen hat zu wenig Budget im Kampf gegen Cyberangriffe – dennoch fühlen sich 89 Prozent grundsätzlich sicher.“ Was bedeutet das im Arbeitsalltag?

EY führt in seiner Untersuchung wie folgt aus: „Wie bereits in den Jahren zuvor zielen die mit Abstand meisten Hackerangriffe auf die IT-Systeme ab (40 %). Insbesondere der Datendiebstahl durch eigene Mitarbeiter ist ein Risikofaktor für heimische Unternehmen: Bei fast einem Viertel (23 %) wurden Beschäftigte zu diesem Zweck von Wettbewerbern abgeworben, bei jedem Fünften (21 %) begingen die eigenen Mitarbeiter Datendiebstahl.“ Diese Aussagen sollten die Verantwortlichen aufwecken, denn wenn die Investition in die eigene Belegschaft insofern endet, als dass sie dem Unternehmen im Umkehrschluss Schaden zufügt, kann in Zukunft nur durch strengere IT-Maßnahmen ein geregelter Arbeitsalltag stattfinden. Denn wir bewegen uns seit Jahren hin zu vermehrter Digitalisierung. Industrie 4.0, IoT uvm. bilden die Basis für den wirtschaftlichen Erfolg, jedoch mit welchen Begleiterscheinungen? „Mehr als jedes zehnte Unternehmen (11 %) in Österreich wurde bereits mindestens einmal Opfer eines Ransomware-Angriffs mit dem Ziel der Erpressung von Lösegeld“, so ein weiteres Ergebnis der EY-Cyberstudie 2021.

**Nichts zu essen, kein Tanken.** Mit den Cyberangriffen auf die Lebensmittel-produzierende Industrie wurde vielen von uns zuletzt verstärkt deutlich gemacht, dass ein Angriff auf die IT nicht nur einen Ausfall von Systemen bedeutet, die uns im Alltag nicht tangieren. Ende Juni diesen Jahres fiel die drittgrößte Molkerei Österreichs einem Cyberangriff zum Opfer – eine Woche stand die Produktion still. Zwei Tage später mussten in Folge einer der größten Hackangriffe der vergangenen Jahre über 800 Supermarktfilialen in Schweden geschlossen werden. Auch Angriffe auf US-Benzinpipelines waren in den Schlagzeilen. Den Cybersecurity-Experten Markus Seme, einen der Geschäftsführer von BearingPoint Austria, haben diese Angriffe dazu veranlasst, gemeinsam mit dem israelischen Unternehmen Check Point, einen praxisorientierten Leitfaden zur schnellen und effektiven Erhöhung der Cybersicherheit für Unternehmen aus Industrie und Produktion zu gestalten. „Konkret liefert das Handbuch Lösungen und Konzepte zur schnellen und effektiven Erhöhung der Cybersicherheit für Unternehmen aus Industrie und Produktion“, heißt es offiziell.

Doch die größte Schwachstelle ist und bleibt der Mensch selber. Inwiefern man diesen zu einem „guten, vertrauenswürdigen Mitarbeiter“ machen kann, was uns künftig noch erwarten wird oder auch, wie Unternehmen doch auf der „sichereren Seite stehen könnten“ weiß niemand so genau. Einige Möglichkeiten sind jedoch in dieser Ausgabe nachzulesen und der Glaube an eine bessere Welt, schwindet bekanntlich zuletzt.

**www.ey.com/at**
**https://info.deepinstinct.com**

# OHNE KATASTROPHEN-SZENARIEN KEIN RISIKOMANAGEMENT MÖGLICH

Bild: © MelzerPR

Die Zunahme an Bedrohungen durch Cyberattacken halten Unternehmen über alle Branchen und Industrien hinweg in Atem. Somit ist man als CEO oder CFO gut beraten, sich über versicherbare und nicht versicherbare Risiken Gedanken zu machen. Auch die Versicherer selbst sehen sich neuen Szenarien gegenüber ausgesetzt. Auf Einladung der **Vienna Insurance Group** kamen kürzlich hochrangige Executives zusammen, um sich über aktuelle Trends im Risikomanagement und Zukunftsszenarien auszutauschen.

**Änderungen spürbar.** „Die Zukunft hat sich verändert", stellte Isabella Mader (Bild), CEO des Excellence Institutes und Executive Advisor des Global Peter Drucker Forums, einleitend fest. „Neu ist, dass ohne Katastrophenszenarien kein Risikomanagement mehr möglich ist. Denn es wird klar, dass nicht jedes Risiko versicherbar ist." Um Betriebsausfälle bestmöglich zu minimieren, müsse man sich im Prozessmanagement auch die vor- und nachgelagerten Prozesse gut anschauen, erläuterte hierzu Hermann Obermair (Bild li.), Senior Vice President und Division Manager Automation beim Anlagenspezialisten Andritz: „Wir schauen uns alle Produktionsprozesse von der Beschaffung bis hin zur Fertigung ganz genau an. Nur durch genaues Monitoring kann ich Standzeiten, beispielsweise aufgrund von Überbelastung eines Teiles, vorhersehen und minimieren. Diese Stillstände in der Produktion werden beim Risikomanagement leider noch häufig vergessen."

**Lieferketten halten.** Der – partielle – Ausfall von Supply Chains und die damit verbundenen Lieferschwierigkeiten beschäftigen gerade die fertigende Industrie sehr. Mader: „Die Engpässe durch geschlossene Häfen in China stellen die Firmen vor die Aufgabe, ihre Sourcing-Strategien zu überdenken. Fällt uns die Abhängigkeit von Fernost jetzt auf den Kopf und wäre eine teilweise Rückkehr zu lokalen bzw. europäischen Lieferanten vielleicht doch die bessere Strategie?"

**IT-Käseglocke funktioniert nicht.** „Das Problem bei der ganzen Cybersecurity-Debatte ist, dass sich alle auf IT-Security konzentrieren und nicht auf die OT-Security. Wenn ein IT-Techniker sagt, das Unternehmen sei durch Firewall usw. wie unter einer Käseglocke geschützt, glauben Sie das bloß nicht", mahnte Obermair. „Jedes Update einzelner Steuerungssoftware muss überprüft werden. Denn via VPN-Tunnels kann ein Cyberangreifer meist unerkannt einfach in die Fertigungshalle spazieren und großen Schaden anrichten." So könne es passieren, dass plötzlich Maschinen miteinander kommunizieren, die das vorher noch nicht taten. „Wenn Sie über Cybersecurity in der Produktion nachdenken, schauen Sie sich jedes kleinste Teil der Produktion an und sind Sie nicht verwundert, wenn die Käseglocke nicht funktioniert."

## VEREINBARUNG GESCHLOSSEN

**Stormshield** und **Allnet GmbH Computersysteme,** Value-Add-Distributor mit Niederlassungen in Deutschland, Österreich und der Schweiz, gaben bekannt, dass sie eine Vereinbarung über den Vertrieb von Stormshield-Produkten im DACH-Gebiet geschlossen haben. Die Vereinbarung betrifft die Vermarktung des gesamten Lösungsportfolios des zum Luft- und Raumfahrtriesen Airbus gehörenden Cybersicherheitsanbieters durch die Allnet GmbH. Dabei handelt es sich um drei Produktfamilien, die nahtlos miteinander interagieren, um die Umsetzung von mehrstufigen Sicherheitsstrategien zu vereinfachen.

**www.stormshield.com**

IoT4 INDUSTRY&BUSINESS

## CYBER-BILDUNG

Das **Department Informatik und Security** der **FH St. Pölten** besetzte Anfang Juli diesen Jahres die Leitung des Studiengangs IT Security neu. **Jochen Hense** (Bild), Experte im Bereich Softwarearchitektur und Security, übernahm den Bachelor Studiengang und bringt langjährige Führungserfahrung in der Privatwirtschaft und Expertise im Hochschulbereich in seine neue Position ein. „Die Gewährleistung von sicheren Prozessen im Wirtschaftsleben, aber auch im privaten Bereich ist eine der zentralen Herausforderungen in unserer digitalisierten Gesellschaft. Umso wichtiger ist es, mit einer praxisnahen und zukunftsorientierten Ausbildung Personen auszubilden, die dieser Aufgabe gewachsen sind", betont Jochen Hense. „IT Security an der FH St. Pölten bietet eine hervorragende Ausbildungsmöglichkeit mit einem starken Bezug zur Praxis. Ich freue mich sehr, aktiv an der Weiterentwicklung des Studiengangs mitarbeiten zu können."

Erfreut über die Bestellung von Jochen Hense zeigt sich auch Simon Tjoa, Leiter des Departments Informatik und Security und betont: „Mit der Kombination aus praxisnahem Unterricht und wissenschaftlichen Erkenntnissen bieten wir unseren Studierenden alle Möglichkeiten für eine erfolgreiche Karriere im Security-Bereich." Die 360-Grad-Ausbildung in allen wesentlichen Schwerpunkten der IT-Security bereitet Studierende optimal auf die Berufswelt vor. Der Studienplan setzt dabei auf eine Mischung aus Informatik, Management und Teamwork unter den Studierenden.

**www.fhstp.ac.at**

Bild: © Jochen Hense

| FB12-14G |

# EtherCAT P: reduziert Verkabelung und Aufwand

Ultraschnelle Kommunikation und Power auf einem Kabel

EtherCAT P integriert in einem 4-adrigen Standard-Ethernet-Kabel die EtherCAT-Kommunikation sowie die System- und Peripheriespannung. Das I/O-System für EtherCAT P in Schutzart IP 67 nutzt die Vorteile von EtherCAT P voll aus: Material- und Montagekosten sowie der benötigte Bauraum in Schleppketten, Kabeltrassen und Schaltschränken werden deutlich reduziert. Die kompakten und robusten I/O-Module decken ein breites Signalspektrum ab: von Standard-Digital-I/Os bis zur komplexen Analog- und Messtechnik. Hinzu kommen über 100 weitere Komponenten für EtherCAT P. Jetzt informieren!

Scannen und alles über Wettbewerbsvorsprung mit EtherCAT P erfahren

New Automation Technology BECKHOFF

## WARNHINWEIS – GERECHTFERTIGT?

„Benutzen Sie kein Windows, weil es ein Sicherheitsrisiko darstellt", rät jetzt aktuell **Marc Ruberg**, einer der bekanntesten White Hacker Deutschlands. Der Kernphysiker und Informatiker ist Verantwortlicher für das Hochschulnetz des Landes Baden-Württemberg, stimmberechtigtes Mitglied im Chaos Computer Club (CCC) und aktives Mitglied im Diplomatic Council, einem globalen Think Tank mit Beraterstatus bei den Vereinten Nationen (UNO). Die Hackerszene, in der er als „ruby" bekannt ist, kennt er wie kaum ein anderer.

Für die Gefahrenlage im Internet macht Marc Ruberg drei Mitspieler verantwortlich: die Cyberkriminellen, die staatlichen Geheimdienste und die von den Digitalkonzernen wie Facebook verwendeten Algorithmen zur Meinungsmache durch Künstliche Intelligenz. Es kann jeden treffen, warnt er: Im Jahr 2020 wurden in Deutschland 108.404 Straftaten im Bereich Cyberkriminalität erfasst. „Das ist nur die Spitze des Eisbergs", ist sich Ruberg sicher, die Dunkelziffer schätzt er auf über 90 Prozent.

**Geheimdienste bedenklicher als die Kriminellen?** Noch bedenklicher als die Cyberkriminellen stuft er die Rolle der staatlichen Geheimdienste ein. Statt bei Sicherheitslücken in Standardsoftware zu warnen, nutzen die Cyberagenturen von Staaten häufig die Schwachstellen selbst aus und potenzieren damit die Gefahrenlage, weiß der White Hacker. Der größte bekannte Cyberangriff namens „WannaCry", bei dem mehr als 230.000 Computer in 150 Ländern infiziert wurden, ging unmittelbar auf die US-amerikanische National Security Agency (NSA) zurück, die sich eine Software zur Ausnutzung von Lücken in Microsoft Windows von Hackern hat klauen lassen. „Die USA, China, Russland, Israel und Nordkorea marschieren mit ganzen Cyberarmeen durchs Internet", so Ruberg. Nordkorea würde durch den fortwährenden Diebstahl von Kryptowährungen im großen Stil sein Staatsbudget maßgeblich finanzieren, schätzt der Experte.

**Es wird munter gehackt.** Kritisch weist Marc Ruberg darauf hin, dass auch die Bundesrepublik Deutschland gleich in mehrfacher Hinsicht als Hacker im Netz unterwegs ist, unter anderem mit der Cyberspionage-Behörde ZITiS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich). „Das beste oder wohl eher schlimmste Beispiel für ein deutsches Spionageprogramm ist der Bundestrojaner", sagt Ruberg. Es handelt sich dabei um ein staatliches Spionageprogramm, das von deutschen Behörden auf die Rechner von verdächtigen Bundesbürgern und sonstigen Personen geschmuggelt wird, um diese zu überwachen. „Dem Vernehmen nach bedarf es dazu einer richterlichen Anordnung, aber so genau wissen das nicht einmal Insider", behauptet Ruberg. Er sagt: „Die unklare Sachlage hängt damit zusammen, dass das Bundesverfassungsgericht zu dem Urteil gelangt ist, dass der Bundestrojaner Grundrechte verletzt. Folglich wird seitdem jedweder Einsatz verschleiert."

Ruberg hat unter anderem das Buch „Cyber War – die digitale Bedrohung" geschrieben. Das 244 Seiten starke Buch ist 2021 auf Deutsch bei Diplomatic Council erschienen.

**www.diplomatic-council.org/de**

## ERNANNT

**Kudelski Security,** die Cybersicherheitssparte der Kudelski-Gruppe, hat Tony de Bos zum Vice President Services für EMEA bekanntgegeben. De Bos verfügt über mehr als 20 Jahre Berufserfahrungen in den Bereichen Cybersecurity, Datensicherheit und digitale Transformation. Umfangreiche strategische und unternehmerische Führungskompetenzen hat er durch die Gründung und Führung global erfolgreicher Technologie- und Dienstleistungsunternehmen erlangt.

**www.nagra.com**

## TRANSPARENZ GEFORDERT

**Kaspersky** aktualisiert sein Produktportfolio Kaspersky Industrial CyberSecurity und bietet nun ein zentralisiertes Management-Dashboard für die Orchestrierung aller Sicherheitsabläufe der OT-Infrastruktur an. Dieses visualisiert alle geographisch verteilten Assets und reichert diese mit Informationen zu Vorfällen und Vorfallanalyse an. Durch die Integration von Kaspersky Industrial CyberSecurity für Nodes und Kaspersky Industrial CyberSecurity for Networks können Daten zu Störungen an Endpoints und im gesamten Netzwerk in Echtzeit kombiniert werden. Des Weiteren bietet das Portfolio nun Abwehrmechanismen gegen Brute Force und Exploits im Rahmen von Netzwerkattacken sowie erweiterte Datengrundlagen für Vulnerability- und Patch-Management.

Für zwei Drittel der Industrieunternehmen zählen ein Mangel an Sichtbarkeit und Verwaltbarkeit von komplexen IT- und OT-Infrastrukturen zu den größten Herausforderungen. Um die Infrastruktur entsprechend schützen zu können und Transparenz zu erhalten, benötigen sie eine einheitliche Plattform für das Management von Sicherheitsrichtlinien, Schutz sowie Informationen zu allen Sicherheitsvorfällen. Die Kaspersky Industrial CyberSecurity Management Konsole steht ab Dezember 2021 im Kaspersky Security Center zur Verfügung.

**www.kaspersky.de**

## LÖSUNG: PASSWORTLOSE MULTIFAKTOR-AUTHENTIFIZIERUNG

Credential Stuffing ist eine stark wachsende Bedrohung für die Datensicherheit. Dabei wird versucht, mit von diversen Online-Services gestohlenen Login-Daten (engl. „Credentials") in ein System einzudringen, um an noch profitablere Daten im Account zu gelangen. Die beste Strategie, dieser Gefahr zu begegnen, ist zugleich die unkomplizierteste: Cyberkriminellen den Zugang zu jeglichen Login-Daten zu entziehen, indem gar keine verwendet werden. Mit der passwortlosen Multifaktor-Authentifizierungsplattform **VeridiumID** haben somit groß angelegte Hackerattacken keine Chance auf Erfolg.

Credential Stuffing ist im Vergleich zu anderen Angriffen sehr effizient. Die Trefferquote ist durch tatsächlich existierende Passwörter wesentlich höher als bei Brute-Force-Attacken, die auf zufällige Passwort-Kombinationen zurückgreifen. Und auch im Vergleich zu Social Engineering ist die „Erfolgschance" größer: Beim Credential Stuffing können Hunderte verschiedener Onlineservices gleichzeitig attackiert werden, während beim Social Engineering der Angriff meist auf eine einzige Plattform beschränkt ist.

Da eine wirklich sichere Passwortverwaltung aufwändig und mühsam ist, bleiben Lösungen, die im Lauf des Authentifizierungsprozesses auf Kennwörter zurückgreifen, ein Sicherheitsrisiko: Für jeden Dienst sollte ein eigenes, starkes Passwort kreiert werden, doch oft wird aus Bequemlichkeit dieselbe Kombination von E-Mail-Adresse und Passwort für verschiedene Online-Services verwendet.

**Kein Passwort – kein Problem. Rainer Witzgall** (Bild), Country Manager DACH des international tätigen Cybersecurity-Software-Herstellers Veridium, hat eine Lösung für das Problem: „Eine Multifaktor-Authentifzierung, die ohne Passwörter auskommt, ist die sicherste Möglichkeit, um Credential Stuffing zu entgehen. Unsere Authentifizierungsplattform VeridiumID verwendet KI-basierte Verhaltensbiometrie als einen der nötigen Faktoren. Als zweiter Faktor reicht bereits der Besitz eines Smartphones oder Tablets aus – dank der speziellen Nutzung der Biometrie, die in allen handelsüblichen mobilen Geräten bereits integriert ist. Passwörter sind hier in keiner wie auch immer gearteten Form

für den Identifizierungsprozess nötig, nicht als Hashwert, nicht als Klartext, weder unverschlüsselt noch verschlüsselt."

VeridiumID nutzt das unverwechselbare individuelle Bewegungsmuster einer Person und setzt Bewegungsimpulse wie die Flüssigkeit und Geschwindigkeit der Bewegungen oder die Stärke des Drucks auf den Screen mittels Künstlicher Intelligenz in Daten um.

**www.veridiumid.com**

## NEUE STUDIE

**Trend Micro,** Anbieter von Cybersicherheitslösungen, veröffentlichte kürzlich neue Studienergebnisse. Daraus geht hervor, dass in großen österreichischen Unternehmen durchschnittlich 29 verschiedene Sicherheitslösungen zum Einsatz kommen. Angesichts dieser hohen Zahl fällt es Security Operation Centern (SOC) immer schwerer, Warnungen zu priorisieren und Sicherheitsrisiken effektiv zu kontrollieren. Die global durchgeführte unabhängige Studie zeigt auf, dass SOC-Teams, die mit der Erkennung von und Reaktion auf entstehende Sicherheitsbedrohungen beauftragt sind, erheblichen Herausforderungen gegenüberstehen. Die große Anzahl von weltweit durchschnittlich 29 verschiedenen Sicherheitslösungen im Unternehmen (in Österreich ebenfalls 29) erschwert ihnen die Priorisierung. In globalen Fir-

men mit über 10.000 Mitarbeitern steigt die Anzahl der im Einsatz befindlichen Security-Tools sogar auf 46 an.

**Alarmierend.** Über die Hälfte (58 Prozent) der Befragten aus Österreich (51 Prozent weltweit) gab an, dass die Lösungen zwar innerhalb des Unternehmens im Einsatz sind, SOC-Teams die Informationen und Daten jedoch nicht für ihre Analyse nutzen. „Das Ausufern von Security-Tools ist in globalen Unternehmen jeder Größenordnung immer häufiger zu beobachten. Mit Blick auf Incident Detection und Response können damit jedoch steigende Kosten einhergehen", betont Richard Werner, Business Consultant bei Trend Micro.

Für die Studie befragte Sapio Research insgesamt 2.303 IT-Security-Entscheider aus 21 Ländern weltweit – 100 aus Österreich. Darunter sind Führungskräfte, die SOC-Teams leiten (85 Prozent) und solche, die SecOps aus ihrem IT-Security-Team heraus managen (15 Prozent). Alle Befragten arbeiteten in Unternehmen mit über 250 Mitarbeitern, mit der Ausnahme von Norwegen (über 10 Mitarbeiter), Dänemark (über 25 Mitarbeiter), Österreich und Belgien (je über 100 Mitarbeiter).

**www.trendmicro.com**

## LÜCKEN BEI ABSICHERUNG

**Semperis** gab jetzt die Veröffentlichung der ersten Ausgabe des Active Directory Security Halftime Report bekannt. Der Bericht befasst sich mit der Welle von Angriffen und Schwachstellen bei Identitätssystemen – vom Angriff auf Colonial Pipeline bis hin zum Windows-Druckspooler-Leck – und bietet Expertenempfehlungen zur Festigung der Identitätssicherheitsstrategie, die über viele Jahre hinweg durch Konfigurationsfehler und Kompetenzmängel aufgeweicht wurde.

„Active Directory steht nach wie vor im Mittelpunkt jeder Identitätsverwaltung – es ist in den meisten Unternehmen das Herzstück der Identitätsplattform –, jedoch hat sich das Umfeld radikal verändert", sagt Mickey Bresman, CEO bei Semperis. „Die sichere AD-Konfiguration hat vor 15 Jahren noch keine große Rolle gespielt, und viele Empfehlungen aus der damaligen Zeit haben sich als unsicher erwiesen und wurden seitdem vollständig revidiert. Aus vielen der damals begangenen Fehler sind die Probleme geworden, die Unternehmen heute beheben müssen."

**Kompetenzmängel.** Darüber hinaus weist Bresman auf Kompetenzmängel hin zu einer Zeit, in der vor allem Identitäts- und Sicherheitsteams mit dem Schutz vor Cyberangriffen betraut sind. „Möglicherweise kennen sich Ihre Mitarbeiter mit AD extrem gut aus, denken aber eher von den Betriebsabläufen her", sagt Bresman. „Oder Ihre Mitarbeiter sind mit Red-Teaming und Sicherheit umfassend vertraut, aber keine AD-Experten. Es ist nicht einfach, Personen zu finden, die über Kompetenzen in beiden Bereichen verfügen."

Angesichts der eskalierenden Cyberangriffe auf Identitätssysteme hebt der Active Directory Security Halftime Report die Bereiche hervor, auf die sich IAM-Teams (Identity & Access Management), Sicherheitsteams und CISOs, die für den Schutz dieser Systeme in Unternehmen verantwortlich sind, konzentrieren müssen.

**Praxisanleitungen.** Mehr als zwei Drittel des Berichts bestehen aus Praxisanleitungen von erfahrenen Experten für digitale Identitäten zur Vermeidung von Cyberangriffen auf Identitätssysteme, aber auch zur Minderung ihrer Folgen und zur Wiederherstellung nach Angriffen. Identitätssysteme sind weiterhin ein vorrangiges Ziel für Cyberkriminelle, obwohl Schwachstellen umfassend bekannt sind – vor allem in Active Directory, dem zentralen Identitätsspeicher bei 90 % der Unternehmen weltweit. Auch wenn die Bedrohungslandschaft ständig größer wird, können Unternehmen ihre Sicherheitsstrategie verbessern, indem sie methodisch die bekannten identitätsrelevanten Schwachstellen identifizieren und in Angriff nehmen, die im Active Directory Security Halftime Report behandelt werden. „Unabhängig davon, welche Systeme und Assets lokal und in der Cloud betrieben werden, muss jedes Unternehmen den Identitätsspeicher schützen", erklärt Bresman. „Identität wird beim Schutz vor Angreifern auch weiterhin eine entscheidende Rolle spielen."

**www.semperis.com**

## WATCHGUARD ERWEITERT CLOUD-PLATTFORM

Nach der Mitte des Jahres erfolgten erfolgreichen Integration der Endpoint Security-Lösungen von Panda hat **WatchGuard Technologies** seine Sicherheitsplattform WatchGuard Cloud abermals erweitert: Ab sofort können nun auch die Wlan-Produkte von WatchGuard an gleicher Stelle online administriert werden. Dadurch ergibt sich nicht zuletzt für Managed Service Provider die Möglichkeit, weitreichende Security-Leistungen auf Basis einer zentral verwaltbaren Plattform, die alle Technologien von WatchGuard integriert, anbieten zu können. Dies umfasst auch die ebenfalls ab heute verfügbare neue Gerätegeneration WiFi 6-fähiger Access Points (AP), die Anwendern verbesserte Konnektivität, zusätzliche Leistung und erstklassige Sicherheit bringt.

„Der MSP-Markt wächst weiterhin in rasantem Tempo. Das veranlasst Partner dazu, nach zentralisierten Lösungen zu suchen, die ihnen die Bereitstellung und Verwaltung der Services vereinfachen und gleichzeitig ein Höchstmaß an Sicherheit bieten. Dank ‚Wi-Fi in WatchGuard Cloud' und den neuen Access Points können Managed Service Provider nun auch Wlan-Leistungen bieten, die auf einem gesamtheitlichen Ansatz aus maximaler Sicherheit und Performance basieren. Jetzt ist wirklich unser komplettes Technologie-Portfolio rund um Firewall, Endpunktschutz, MFA und Wlan in der Unified Security Platform integriert", so Andrew Young, Senior Vice President of Product Management bei WatchGuard. „Da Wlan in vielen Unternehmen mittlerweile unverzichtbar ist, bietet MSP noch mehr Potenzial zum Ausbau der Geschäftsaktivität bei gleichzeitiger Senkung der Aufwände."

**www.watchguard.com**

## FABRIKWEITE VERNETZUNG

Die Industrial IoT Edge-Software Cybus Connectware ist ab sofort für Kunden der Automatisierungsplattform ctrlX Automation von **Bosch Rexroth** im ctrlX Store erhältlich. Cybus Connectware stellt den vollumfänglichen und automatisierbaren Datenfluss zwischen Shopfloor und IT her und ergänzt damit die modulare Steuerungsplattform ctrlX Core um wertvolle System- und Geräte-Konnektivität. Die Kollaboration zwischen IT und OT beschleunigt den kulturellen Wandel in der Fertigungs- und Produktionsindustrie auch über Unternehmensgrenzen hinweg. Sowohl Bosch Rexroth als auch Cybus haben OT/IT-Kollaboration frühzeitig als Innovationstreiber erkannt und verfolgen die gemeinsame Mission, Grenzen zwischen OT und IT aufzuheben.

„Der Grad der Automatisierung schreitet in allen Branchen stetig voran. Das erfordert Lösungen, die die Vernetzung mit verschiedensten Systemen ermöglichen und sich nahtlos in die bereits bestehende digitale Infrastruktur einfügen. In Cybus Connectware sehen wir die Software, mit der diese Offenheit und Flexibilität vorangetrieben wird. Darum freuen wir uns, dass Cybus auf unserer Automatisierungsplattform ctrlX Automation vertreten ist", begrüßt Hans Michael Krause, Director Product Management ctrlX World, den neuen Partner Cybus.

**www.ctrlx-automation.com**

## KOOPERATION

**Siemens** und Zscaler Inc., führend in Cloud-Sicherheit, arbeiten zusammen, um Kunden den sicheren Zugriff vom Arbeitsplatz im Büro oder mobil auf Operational Technology (OT)-Systeme und -Anwendungen im Produktionsnetzwerk zu ermöglichen. Dadurch können Anwender beispielsweise qualitätssichernde Maßnahmen oder Diagnosen aus der Ferne durchführen. Damit das OT-Netzwerk keinem erhöhten Bedrohungspotenzial ausgesetzt wird, haben Siemens und Zscaler das OT-Konzept „Defense-in-Depth" mit der Zero Trust-Architektur erweitert. Aufbauend auf dem „Least Privilege Access"-Prinzip autorisiert Zero Trust nur anwendungsspezifische Zugriffe, für die überprüfte Berechtigungen auf Basis der Anwenderidentität und des Kontexts vorliegen. In Kombination mit den vorhandenen OT-Sicherheitsmechanismen, wie Zellenschutz-Firewalls, lässt sich so ein granulares Zugriffskonzept umsetzen. Zudem lassen sich dadurch weiterhin die Anforderungen der Produktion nach Verfügbarkeit und Echtzeitfähigkeit erfüllen. Umgesetzt wird dies durch die Installation des App-Connectors des cloudbasierten Remote Access-Service Zscaler Private Access (ZPA) auf einem Docker-Container auf der lokalen Verarbeitungsplattform Scalance LPE von Siemens, wodurch eine Zugriffslösung für industrielle Umgebungen entsteht.

**www.siemens.at**

BUXBAUM
Member of the Softing Group

VIELFÄLTIGE LÖSUNGEN. SEIT 1996

25 JAHRE

BUXBAUM AUTOMATION GmbH
Telefon +43/720/704 560
office@myAUTOMATION.at
www.myautomation.at

Bild: © Nuernberg Messe | Frank Boxler

# GELUNGENER **RESTART**

Die it-sa ist zurück und wurde vom 12. bis 14. Oktober in Nürnberg erneut zum Treffpunkt der IT-Sicherheitsexperten und -entscheider. Neben der Wiedersehensfreude stand das Thema der zunehmenden Cyberangriffe und den Gegenmaßnahmen im Mittelpunkt. Von Mag. Barbara Sawka

Mit 274 Ausstellern aus 18 Ländern und rund 5.200 Fachbesuchern aus 28 Ländern freuen sich die Verantwortlichen der it-sa 2021 über das erste Wiedersehen nach dem Corona-bedingten Aussetzen im vergangenen Jahr. „Die it-sa 2021 war ein voller Erfolg: Wie in der aktuellen Situation erwartet, kleiner als die letzte Veranstaltung, für die teilnehmenden Unternehmen aber ein äußerst wirkungsvolles Marketing-Instrument" resümiert Frank Venjakob, Director it-sa. „Die Aussteller der it-sa 2021 sind begeistert über die hohe Qualität der Kontakte und intensive Fachgespräche zu konkreten Projekten. Wir freuen uns sehr über dieses positive Feedback aus zahlreichen persönlichen Gesprächen", so Venjakob.

**Bewusstsein wächst.** IT-Sicherheit ist wichtiger denn je, darüber waren sich die Teilnehmer der Messe mit Blick auf die Zunahme von Cyberangriffen einig. Zwar steige das Bewusstsein für IT-Sicherheit, ebenso die Ausgaben in Deutschland, wie der Digitalverband Bitkom zur it-sa berichtete. Es gelte aber, Strukturen zu schaffen, die das weitere Wachstum des IT-Sicherheitsmarktes fördern. So forderte Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation, die Stärkung des Cybersicherheitssektors im europäischen Wirtschaftsraum. Der Markt für IT-Sicherheit in Europa leide im internationalen Vergleich unter einer Finanzierungslücke von mehr als vier Milliarden Euro jährlich.

**Messe-Highlights im Forenprogramm.** Über 130 Beiträge zu unterschiedlichen Themen verzeichnete das Vortragsprogramm der vier Foren auf der it-sa 2021. Sie waren auch in diesem Jahr wahre Publikumsmagneten. Zusätzlich zu drei deutschsprachigen Foren bot das englischsprachige International Forum zusätzliches Fachwissen auch für diejenigen, die selbst nicht vor Ort sein konnten: Parallel zur it-sa in Nürnberg wurde das Programm auf der Online-Plattform it-sa 365 übertragen. Auch wer nicht vor Ort auf der it-sa sein konnte, hatte so Gelegenheit, die englischsprachigen Beiträge und Messe-Highlights wie die Special Keynote oder die Verleihung des UP@it-sa Award online zu verfolgen. Das Forenprogramm wird nach der it-sa auf der Plattform it-sa 365 reingestellt und damit auch nach der Messe online abrufbar sein.

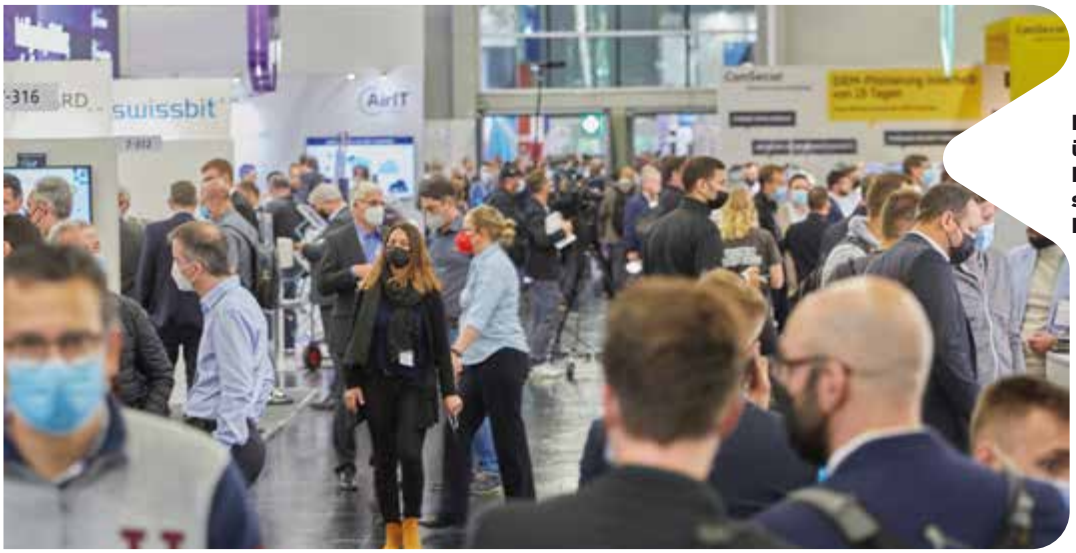



Bild: © Nuernberg Messe | Thomas Geiger

**Die it-sa 2021 freut sich über einen gelungenen Restart mit 274 Ausstellern und rund 5.200 Fachbesuchern.**

**Special Keynote von KI-Pionier Chris Boos.** Die Keynote der it-sa 2021 hielt Hans-Christian („Chris“) Boos. Der Experte für Künstliche Intelligenz sprach über die Bedeutung der Technologie für aktuelle und zukünftige Security-Anwendungen. Er appellierte an sein Publikum, sich der Verantwortung bei der Entwicklung von KI-basierten Security-Tools bewusst zu sein. Der zunehmende Einsatz von Künstlicher Intelligenz läutet den Abschied vom Industriezeitalter ein, so seine These. Systeme, die zur autonomen Entscheidung fähig sind, werfen dabei nicht nur neue ethische, moralische und rechtliche Fragen auf. Es ergeben sich auch neue Herausforderungen für die IT-Sicherheitsforschung und -entwicklung. Mit seinem Vortrag „AI will end the Industrial Age – Let’s find some love for the future!“ setzte Chris Boos die Reihe der Special Keynote-Vorträge auf der it-sa fort. Persönlichkeiten wie Edward Snowden, die IT-Sicherheitsexpertin Paula Januszkiewicz oder Maximilian Schrems nutzten in der Vergangenheit den letzten Messetag bereits für eine Bestandsaufnahme in Sachen Datenschutz und -sicherheit.

**Startups im Fokus – UP@it-sa Award für XignSys.** Mit der Sonderfläche Startups@it-sa, einer Panel-Diskussion sowie der Verleihung des UP@it-sa Awards förderte die it-sa 2021 junge Unternehmen. Preisträger des begehrten Startup-Awards für Bewerber aus dem DACH-Raum ist die Firma XignSys aus Gelsenkirchen. Den Preis erhält das XignSys-Team für die Entwicklung einer innovativen Authentifizierungslösung, die eine einheitliche und zukunftssichere Basis für sämtliche digitale Transaktionen schafft. Für Anbieter und Nutzer gleichermaßen. Auf Basis Smartphone-basierter und passwortloser Authentifizierungssoftware, die als einzige Lösung flexibel in jeder Art von Transaktion genutzt werden kann, kombinieren XignSys hohe Sicherheit (bestätigt durch das BSI) mit maximaler Nutzerfreundlichkeit und absoluter Flexibilität – ideal zum Beispiel für die Anforderungen in der Smart City. Und all das auf Basis deutscher Technologie unter Berücksichtigung europäischer Sicherheitsansprüche.

**Onsite und online.** Als ganzjährige Erweiterung der it-sa Expo&Congress riefen die Veranstalter der Fachmesse 2020 die digitale Dialogplattform it-sa 365 ins Leben. IT-Sicherheitsanbieter präsentieren sich hier mit Unternehmensprofilen und Produktinformationen sowie in Online-Vorträgen. Auf Anbieterseite verzeichnet die Plattform aktuell zusätzlich zu den 274 Profilen aller Aussteller der it-sa 2021 weitere 77 Company Profiles. Seit dem Start im Oktober letzten Jahres hat sich die Zahl der registrierten User fast verdoppelt: Von rund 2.900 Registrierungen nach den Launch Days stieg die Zahl auf mittlerweile bereits mehr als 5.500. Während der it-sa wurde die Plattform intensiv genutzt – zur Messevorbereitung und zur Anbahnung von realen Kontakten: Rund 1.500 Chatnachrichten wurden im Laufe der Messewoche über die Plattform verschickt. „Zur Messelaufzeit konnten wir nochmals einen deutlichen Zuwachs der Userzahlen verzeichnen. Das zeigt, wie gut sich onsite und online mit dem attraktiven Angebot auf it-sa 365 verzahnen lassen“, erklärt Frank Venjakob. Für IT-Sicherheitsverantwortliche und -entscheider bleibt die it-sa 365 auch nach der Messe eine Anlaufstelle für Informationen und Expertise zum Thema Cybersicherheit. Mit weiteren Ausgaben der IT Security Talks knüpfen die Veranstalter der it-sa am 15. und 16. März 2022 sowie vom 17. bis 18. Mai 2022 an das erfolgreiche Konzept an, wichtige IT-Sicherheitsfragen in Online-Vorträgen zu beleuchten. Die nächste Ausgabe der it-sa findet vom 25. bis 27. Oktober 2022 im Messezentrum Nürnberg statt.

**www.it-sa.de**

**Chris Boos appellierte im Rahmen seiner Keynote an sein Publikum, sich der Verantwortung bei der Entwicklung von KI-basierten Security-Tools bewusst zu sein.**

Corona hinterlässt nicht nur gesundheitliche Spuren, es macht auch blinde Flecken in Sachen Cybersecurity sichtbar. Die Angriffe sind massiv gestiegen, die Gründe sind vielfältig: unsicheres Homeoffice, zu hohes Vertrauen in Lieferketten aber auch die zunehmende Professionalisierung der Cyberkriminellen. Von Mag. Barbara Sawka

# ES KANN JEDEN TREFFEN

Sämtliche Studien sind sich einig: die Wahrscheinlichkeit digital angegriffen zu werden, war noch nie so hoch wie in diesem Jahr. Die Angriffe steigen befeuert durch die zunehmende Digitalisierung einerseits und andererseits aufgrund der Tatsache, dass sich Cyberkriminalität zu einem regelrechten Geschäftsmodell entwickelt hat. Man könnte es fast schon als Pandemie der anderen Art bezeichnen, die während der Covid-19-Krise ausgebrochen ist. Betroffen sind neben IT-Dienstleistern aktuell sehr häufig auch physische Lieferketten und kritische Infrastruktur. Die Lösegeldforderungen steigen rasant, und auch die Kunden gehackter Unternehmen bleiben nicht verschont. Erschreckend: Ransomware-Tools werden mittlerweile wie kommerzielle Dienstleistungen verkauft, Service inklusive.

Cyberkriminelle müssen dazu auch nicht mehr sonderlich technisch versiert sein, um Chaos anrichten zu können. Eine Entwicklung, wie man sie auch schon bei Malware erlebt hat. Denn cyberkriminelle Gangs haben ihr Malware as a Service-Modell weiter ausgebaut und bieten dabei richtige Schritt-für-Schritt-Anleitungen an, wie man auch durch die Kompromittierung der Angriffsziele Profit schlagen kann, sagen die Experten von Acronis, einem Anbieter von Cyber Protection-Lösungen.

Bild: © BMI/G. Pachauer

**Mag. Dr. Franz Ruf, MA**
**Generaldirektor für die öffentliche Sicherheit**
**MA - Sektion II (Generaldirektion für die öffentliche Sicherheit)**

„Cybercrime ist in den letzten zehn Jahren von einer kriminalistischen Randerscheinung zu einem Hauptproblem geworden."

Bild: © Radar Cyber Security

**When Fiction meets Reality: Ali Carl Gülerman, CEO Radar Cyber Security und Bestseller-Autor Marc Elsberg waren gemeinsam auf Spurensuche durch aktuelle Szenarien und Bedrohungen im Bereich Cyber Defense.**

Auch der Cybercrime-Report des Bundeskriminalamtes vom August dieses Jahres verzeichnet einen Anstieg von insgesamt 26,3 % an angezeigten Delikten im Vergleich zu 2019. „Es gibt nur mehr wenige Bereiche, auch in der traditionellen Kriminalität, in denen Digitalisierung und IT keine Rolle mehr spielen“, so Mag. Dr. Franz Ruf, MA, Generaldirektor für die öffentliche Sicherheit. „Cybercrime ist in den letzten zehn Jahren von einer kriminalistischen Randerscheinung zu einem Hauptproblem geworden. Deshalb ist Cybercrime auch eine Priorität in der Sicherheitsstrategie des Innenministeriums.“

**Jeden Tag ein Angriff.** Basierend auf den Ergebnissen einer unabhängigen Umfrage unter 3.600 IT-Managern und Remote-Mitarbeitern von kleineren und mittleren Unternehmen (in 18 Ländern auf der ganzen Welt) geht im Cyber Readiness Report von Acronis hervor, dass 53 % der globalen Unternehmen ein falsches Gefühl von Sicherheit haben, wenn es um Lieferkettenangriffe geht. Trotz der weltweit bekannten Angriffe auf vertrauenswürdige Software-Anbieter (wie Kaseya oder SolarWinds) glauben dennoch über die Hälfte der IT-Führungskräfte, dass die Verwendung einer „bekannten und vertrauenswürdigen Software“ ein ausreichender Schutz wäre – was diese Unternehmen zu einem leichten Ziel macht.
Drei von zehn Unternehmen berichten, dass sie mindestens einmal pro Tag mit einem Cyberangriff konfrontiert werden, ähnlich wie im letzten Jahr. Allerdings geben diesmal nur noch 20 % der Unternehmen an, gar nicht angegriffen worden zu sein, was gegenüber 2020 (mit damals 32 %) ein deutlicher Abfall ist. Das Ausmaß der Angriffe nimmt also zu. Die häufigsten Angriffsarten erreichten in diesem Jahr ein Rekordniveau, was insbesondere Phishing-Angriffe betrifft, die noch häufiger vorkommen und nun mit 58 % die häufigste Angriffsart darstellen. Auch Malware-Angriffe haben 2021 weiter zugenommen: in diesem Jahr wurden sie von 36,5 % der Unternehmen entdeckt (im Gegensatz zu 22,2 % in 2020).
„Die Cybercrime-Branche hat sich in diesem Jahr als gut geölte Maschine erwiesen, die auf bewährte Angriffstechniken wie Phishing-, Malware- oder DDoS-Angriffe zurückgreift. Die Bedrohungsakteure weiten ihre Ziele immer stärker aus, während die Unternehmen durch die wachsende Komplexität der IT-Infrastruktur behindert werden“, sagt Candid Wuest, Vice President des Bereichs Cyber Protection Research bei Acronis. „Nur wenige Unternehmen haben sich die Zeit genommen, um ihr IT-Arsenal mit einer integrierten Data Protection- und Cybersecurity-Lösung zu modernisieren. Die Bedrohungslandschaft wird weiterwachsen – und Automatisierung ist der einzige Weg zu mehr Sicherheit, geringeren Kosten, höherer Effizienz und weniger Risiken.“

>>

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

**Blinder Fleck.** IT-Sicherheit steht in Österreich eine häufig vorherrschende Unwissenheit über die entscheidenden Schutzmaßnahmen sowie die größten Cyberrisiken gegenüber. Allen voran mögliche Bedrohungen durch Dritte, die zu häufig durch die Komplexität und Vernetzung von Partner- und Lieferantenbeziehungen verdeckt werden. Das zeigen die für Österreich geltenden Ergebnisse der „Global Digital Trust Insights Survey 2022“ von PricewaterhouseCoopers kurz PwC, im Zuge derer weltweit mehr als 3.600 CEOs und Führungskräfte qualitativ befragt wurden. „Die Entwicklungen in den letzten Jahren haben die Bedeutung der IT-Sicherheit ins Rampenlicht gerückt. Doch man kann nicht schützen, was man nicht kennt. So haben viele österreichische Unternehmen enorme Schwierigkeiten dabei, ihre Risiken durch Dritte – wie Lieferanten – im eigenen Umfeld zu erkennen. Gerade die Vorfälle der jüngeren Vergangenheit haben gezeigt, dass potenzielle Angreifer immer das schwächste Glied in der (Liefer-)Kette auswählen, um das Unternehmen lahm zu legen. Bei einer fehlenden Einbindung von Dienstleistern in die eigene Risikobetrachtung werden diese Risiken zumeist falsch oder gar nicht bewertet”, erklärt Georg Beham, Cybersecurity & Privacy Leader bei PwC Österreich. So gaben nur 35 % der befragten heimischen Unternehmen an, dass sie das Risiko von Datenschutzverletzungen durch Dritte systematisch erheben und über ein gutes Verständnis der vorhandenen Risiken verfügen. Bei Technologieanbietern oder IoT-Spezialisten haben lediglich 17 % ein angemessenes Verständnis für diese Risiken. Ein großer blinder Fleck, den Cyberkriminelle sehr wohl kennen und ausnutzen. Entgegen dem weltweiten Trend wird in Österreich immer noch zu sehr auf Lieferanten vertraut, ohne sich ein unabhängiges Bild zu machen. Die Durchführung von umfassenden Due-Diligence-Prüfungen im Rahmen von Dienstleister-Beauftragungen wird von mehr als 80 % der Befragten als nicht erforderlich betrachtet. „Ich fürchte, dass wir besonders bei österreichischen KMU Aufholbedarf haben und in der Vergangenheit wenig gemacht bzw. zu viel gespart wurde. Wir sind keine Insel der Seligen, sondern Teil des globalen Cyberspace. Daher rate ich allen Unternehmen – auf gut österreichisch – nicht jammern, sondern anpacken“, meint Jimmy Heschl, Head of Digital Security bei Red Bull als einer der Befragten der Studie im Interview.

Bild: © PwC Österreich

**Georg Beham**
**Cybersecurity & Privacy Leader bei PwC Österreich**

„CEOs wollen nicht nur im Ernstfall, sondern frühzeitig und aktiv bei der strategischen Festlegung und Erreichung von Cyberzielen eingebunden werden.“

**Die Tücken des Homeoffice.** Teleworking, Remote-Working oder Homeoffice – die Bezeichnungen sind unterschiedlich, das Problem identisch. Auch künftig werden Mitarbeiter von zu Hause aus arbeiten, Meetings oder Einstellungsgespräche aus der Ferne geführt werden. IT-Teams müssen Lösungen für den Mangel an Hardware, die wachsende Komplexität, den erhöhten Bedarf an IT-Support und bessere Cybersecurity-Lösungen finden. Der Acronis Cyber Readiness Report hält auch die drei größten technischen Herausforderungen fest, die weltweit von Remote-Mitarbeitern genannt werden: Wlan-Konnektivität, Verwendung von VPN und anderen Sicherheitsmaßnahmen sowie fehlender IT-Support. Einer von vier Remote-Mitarbeitern verwendet keine Multi-Faktor-Authentifizierung und wird so zu einem leichten Phishing-Ziel (die häufigste Angriffsart 2021). Im Durchschnitt ist jeder fünfte Remote-Mitarbeiter stark von Phishing-Angriffen betroffen und erhält monatlich weit über 20 Phishing-E-Mails. Wobei 71 % der Befragten bestätigten, dass dies Monat für Monat der Fall ist. Solche Angriffe mithilfe von Cybersecurity-Schulungen besser zu erkennen, ist von entscheidender Bedeutung, um nicht nur Unternehmen, sondern auch private Vermögenswerte schützen zu können.

**Zu viel Zeit – zu wenig Information.** Die Studie von PwC lässt zusätzlich eine falsch wahrgenommene Sicherheit auf Vorstandsebene erkennen. Während in Österreich 50 % der befragten CEO ihrerseits eine frühzeitige und aktive Einbindung bei der strategischen Festlegung und Erreichung von Cyberzielen sehen, teilen lediglich zehn Prozent ihrer führenden Mitarbeiter diese Einschätzung und erkennen die Einbindung der CEO primär bei der Behandlung von konkreten Cybervorfällen (46 %). „Eine rein passive Information an den CEO bei strategischen Cybersecurity-Entscheidungen vermittelt ein falsches Gefühl von Sicherheit. Dabei kann ein proaktives Engagement auf Vorstandsebene den entscheidenden Unterschied ausmachen. Wie unsere Studie zeigt, erzielten Unternehmen mit sehr engagierten CEO, die ihre Führungskräfte in hohem Maße unterstützen, in den letzten zwei Jahren erhebliche Fortschritte bei ihren Cybersecurity-Programmen“, so Experte Georg Beham. Als weiteres Problem erkennt Beham, dass wesentliche Elemente zur Umsetzung einer datenbasierten Entscheidungsgrundlage in Österreich meist unzureichend vorhanden sind. Cyberkriminelle seien bereits seit Monaten in das Unternehmens-Netzwerk eingedrungen und hätten

**Die Cyberangriffe steigen, drei von zehn Unternehmen sagen, dass sie mindestens einmal pro Tag mit einem Cyberangriff konfrontiert sind.**

ausreichend Zeit sich überall auszubreiten. „Das wäre fast so, als wenn man in einem Einfamilienhaus eine Alarmanlage montiert, aber vergisst diese einzuschalten. Hier lohnt es sich für heimische Unternehmen einen Blick auf die weltweiten Vorreiter zu werfen, denn Datenanalyse ist auch in der Verteidigung des eigenen Unternehmens eine entscheidende Macht“, empfiehlt Georg Beham.

**Präventivarbeit immens wichtig.** Europa befindet sich mitten im digitalen Wandel: die Europäische Kommission hat „Europas digitale Dekade“ ausgerufen und will mit klaren Vorgaben einen entschlossenen Kurs auf ein digital gestärktes Europa bis 2030 setzen. Doch die zunehmende Digitalisierung birgt Gefahren, die sich massiv auf die analoge Welt auswirken können: Seien es zuletzt Hacker-Angriffe im Mai 2021 auf die größte Pipeline der USA und die irische Gesundheitsbehörde oder ein Vorfall in einem kroatischen Umspannwerk Anfang des Jahres, der Europa an den Rand eines Strom-Blackouts führte. „Die Angriffe nehmen zu. Sei es durch einzelne Hacker, die organisierte Kriminalität oder durch Staaten. Aber nicht nur quantitativ wird der Druck stärker, auch die Qualität der Angriffe ist massiv gestiegen. Es vergehen oft Wochen und Monate zwischen Infiltration und dem eigentlichen Hack. Die Diebe sind aber nicht völlig unsichtbar und wir können sie mit unseren Methoden entdecken, wenn davor Präventivarbeit geleistet wurde“, berichtet Ali Carl Gülerman, CEO von Radar Cyber Security im Rahmen einer virtuellen Informationsveranstaltung Anfang Juni zusammen mit Beststeller-Autor Marc Elsberg. Es gäbe derzeit einen rasant wachsenden Markt für Cyberkriminalität und die Experten von Radar Cyber Security erkennen bei Cyberangriffen mittlerweile Businessmodelle mit ausgeklügelter Arbeitsteilung. Man bestellt im Darknet einen Angriff auf das gewünschte Ziel, das dann erpresst wird. Den Gewinn teilt man sich mit den Hackern. Je bedeutsamer eine Branche für die Gesellschaft ist, desto drastischer die Auswirkungen. Bei erfolgreichen Cyberangriffen auf Krankenhäuser kann es etwa sein, dass lebensrettende Operationen nicht stattfinden können.

Software alleine kann das Problem nicht lösen: „Wir müssen uns auf eine Steigerung der Resilienz in der kritischen Infrastruktur konzentrieren und auf regelmäßige Cybersecurity-Übungen mit Szenario-Trainings setzen. Leider können wir einmal erfolgte Hacks nicht mehr rückgängig machen – deshalb ist die Präventivarbeit so wichtig. Und das Thema ist kein Spleen von IT-Verrückten. Denn neben den Lieferketten oder Cash-Systemen von Unternehmen und Organisationen kann es in gewissen Branchen wie dem Lebensmittel-Einzelhandel bis hin zur massiven Verunsicherung der Bevölkerung durch Lieferengpässe gehen. Und damit kann man Politik machen. Mit Cybersecurity schützen wir deshalb auch unsere europäischen Werte“, so Ali Gülerman.

Dieses erschreckende Szenario hat Marc Elsberg bereits 2012 in seinem Roman „Blackout“ verpackt. Zwar fiktiv, aber dennoch dank fundierter Recherche sehr nah dran an einer möglichen Realität. „Die IT-Infrastruktur ist mittlerweile zum sensiblen Nervensystem unserer gesamten Gesellschaft geworden. Unzählige Systeme hängen voneinander ab und sind miteinander verbunden. Bereits eine kleine Störung in einem Teilbereich kann massive Auswirkungen auf die Funktionsfähigkeit und Belastbarkeit des Gesamtsystems bewirken. Wir haben seit dem Erscheinen meines Buches vor zehn Jahren noch immer nicht gelernt, vernünftig mit dieser Tatsache umzugehen und strapazierfähige Fall-Back-Systeme zu entwickeln. Es ist wohl wie in der Liebe: Man weiß erst, was man hatte, wenn man es verloren hat“, so Marc Elsberg.

**www.acronis.com**
**www.allianz.at**
**www.bundeskriminalamt.at**
**www.pwc.com**
**www.radarcs.com**

Daten schützen – erste Ansätze beginnen schon bei der Sensibilisierung von Mitarbeitern.

# „KEINE ZEIT FÜR SECURITY“ RÄCHT SICH BALD EINMAL

Der Mitarbeiter als Firewall? Mehr Investitionen in Aufklärung und Angriffsabwehr? Vielleicht ist das, was offen kommuniziert wird, noch lange nicht das, was für eine wirklich funktionierende Abwehr von Cyberangriffen ausreicht oder gar intern wirklich ausgeübt wird. Doch wann wird es soweit sein, dass Unternehmen den richtigen Weg einschlagen, um ihre Daten ausreichend zu schützen?
Im Gespräch mit Kai Zobel, Area Vice President EMEA Central bei Imperva, kam ein erster Eindruck zutage, der zum Nachdenken anregen sollte. Von Stephanie Englert

**IoT 4 Industry & Business: Herr Zobel, in einer aktuellen Studie zum Thema „Sicherheit von Datenbanken“ heißt es, dass weltweit 46 Prozent aller On-Premise-Datenbanken anfällig für Angriffe, mit durchschnittlich 26 Schwachstellen pro Datenbank sind. Wie kommt es zu einer derart beunruhigenden Entwicklung bzw. wo liegen die Schwachstellen und wie kann man dem entgegenwirken?**
**Kai Zobel:** Fakt ist: Trotz steigender Ausgaben für Cybersecurity nehmen Angriffe und kompromittierte Datensätze weiter zu. Das Kernproblem liegt allerdings nicht wie man vermuten könnte an unentdeckten Schwachstellen. Bei den meisten CVEs (Anmerkung: Common Vulnerabilities and Exposures) handelt es sich um bekannte Schwachstellen, für die es bereits Patches gibt. Den IT-Teams fehlt jedoch die nötige Zeit, regelmäßige Patches durchzuführen.

**IoT: Was bedeutet das in Folge?**
**Zobel:** Das spielt Hackern in die Karten und so sind gerade Schwachstellen von öffentlichen Datenbanken ein leichtes Ziel, denn Angriffe sind hier mit noch weniger Aufwand verbunden. Über Tools wie Shodan suchen sich Angreifer verwundbare Ziele, um sich dann Exploit-Codes zu beschaffen. Das funktioniert über Repositories wie ExploitDB, die Hunderte von Exploit-POC-Codes enthalten. Von dort aus kann der Angreifer das Exploit von überall aus ausführen, da die Datenbank eine öffentliche IP-Adresse hat.

**IoT: Was kann man tun?**
**Zobel:** Entgegenwirken kann man diesem beunruhigenden Trend, indem man seine IT-Teams bestmöglich unterstützt: Mit mehr Manpower und ausgefeilteren Cybersecurity-Tools.

**IoT: Weiters heißt es – wie in so vielen anderen Studien und Gesprächen – dass Unternehmen das Sicherheitsrisiko oft schlecht einschätzen. Müsste nach so vielen Erfahrungsjahren und durch die zunehmenden Telearbeiten (durch die Pandemie) die Gefahr hinsichtlich möglicher Angriffe nicht längstens weitreichend bekannt sein? Wie erklären Sie sich nach wie vor diesen „schlechten" Umgang mit Daten und die nicht angepasste Sensibilität der Betroffenen?**

**Zobel:** Während Unternehmen öffentlich betonen, wie viel sie in die Sicherheit investieren, zeigen unsere umfangreichen Untersuchungen, dass die Probleme weiterhin fortbestehen. Allzu oft vernachlässigen Unternehmen die Datenbanksicherheit, weil sie sich auf systemeigene Sicherheitsmechanismen oder veraltete Prozesse verlassen. Leider wird auch intern zu selten umgesetzt, was nach außen hin propagiert wird.

**IoT: Weshalb der „Trend" zu On-Premise-Datenbanken trotz Risiken?**

**Zobel:** Unternehmen möchten die Kontrolle ihrer sensibelsten Daten nicht aus der Hand geben und setzen daher lieber auf lokale Datenbanken als auf Cloud-Datenbanken. Im Vergleich zu Cloud-Datenbanken gelten On-Premise-Datenbanken als vermeintlich sicherer, aber unsere Studie zeigt, dass diese Annahme nicht unumstritten ist.
Viele überschätzen hier ihre aktuellen Fähigkeiten und Abwehrsysteme. Bei Cloud-Datenbanken hingegen gewährleistet zum Großteil der Provider die Sicherheit der Daten und Backups und kümmert sich gleichzeitig noch um die schnelle Einspielung von Updates.

**IoT: Nach wie vor werden auch Wege des Phishings und der Malware für einen Angriff genutzt. Wie weit hinkt hier bei den Mitarbeitern die Aufklärung dem Status Quo der Gefahrenlage Ihrer Meinung nach hinterher?**

**Zobel:** Die meisten Mitarbeiter sind sich nicht bewusst, dass sie die erste und wichtigste Firewall ihres Unternehmens sind. Leider versuchen Hacker daher immer wieder dieses schwächste Glied in der Kette auszunutzen. Die Techniken werden dabei immer raffinierter, sodass Phishing-Attacken als solche von vielen Mitarbeitern gar nicht erkannt werden. Unternehmen bieten hier zwar Basis-Schulungen an, diese müssten aber ebenso oft aktualisiert werden, wie Hacker ihre Angriffs-Methoden ändern. Zu wenig Unternehmen investieren bisher die nötige Zeit, um ihre Mitarbeiter bestmöglich auf Phishing-Angriffe vorzubereiten, daher die hohe Erfolgsquote bei Cyber-Kriminellen.

**IoT: Gibt es „regionale" oder eher „Branchen-Unterschiede" bei der Häufigkeit der Attacken?**

**Zobel:** Die regionale Analyse zeigt erhebliche Unterschiede zwischen den einzelnen Ländern: Die Anzahl an gefährdeten Datenbanken ist in Deutschland mit 19 Prozent deutlich geringer als in Ländern wie Frankreich (84 Prozent), Australien (65 Prozent) oder Singapur (64 Prozent). Hinsichtlich der Anzahl an Schwachstellen pro Datenbank im Durchschnitt besetzen deutsche Datenbanken mit 64 Schwachstellen die oberen Ränge. Nur Frankreich (72), China (74) oder Mexiko (70) weisen im Durchschnitt mehr Schwachstellen pro Datenbank auf.

**IoT: Wie wird sich Ihrer Erfahrung nach die Angriffs-Situation in den kommenden Jahren entwickeln?**

**Zobel:** Die Migration von Daten in Cloud-Datenbanken ist nach wie vor hoch. Dennoch setzen die meisten Unternehmen weiterhin auf On-Premise-Datenbanken, insbesondere dort wo die sensibelsten Daten gespeichert werden. In Anbetracht der Tatsache, dass fast jede zweite On-Premise-Datenbank anfällig ist, werden die gemeldeten Datenschutzverletzungen aller Voraussicht nach weiter ansteigen und auch die Tragweite dieser Fälle wird zunehmen.
IT-Sicherheitsteams sollten sich deshalb auf ein beunruhigendes und noch nie dagewesenes Jahr einstellen. Bis Ende 2021 werden rund 40 Milliarden kompromittierte Datensätze prognostiziert – das sind mehr als doppelt so viele wie im letzten Jahr.

**IoT: Vielen Dank!**

**Zur Studie >>**

**Kai Zobel,**
**Area Vice President EMEA Central Imperva**

„Die Migration von Daten in Cloud-Datenbanken ist nach wie vor hoch. Dennoch setzen die meisten Unternehmen weiterhin auf On-Premise-Datenbanken."

**Die Welt ist angreifbar, vor allem was Cyberattacken angeht, haben Angriffe stark zugenommen.**

## ÜBER DIE STUDIE

Imperva, Inc., ein Unternehmen im Bereich Cybersecurity, präsentierte in einer aktuellen Studie aus diesem Jahr umfangreiche Ergebnisse zur Fragestellung der Sicherheit von Datenbanken. Diese besagt, dass weltweit 46 Prozent aller On-Premise-Datenbanken anfällig für Angriffe, mit durchschnittlich 26 Schwachstellen pro Datenbank sind. Die Längsschnittstudie scannte dafür über fünf Jahre hinweg fast 27.000 Datenbanken.
Mehr als die Hälfte (56 Prozent) der gefundenen Schwachstellen wurde gemäß den Richtlinien des National Institute of Standards and Technology (NIST) als „hoch" oder „kritisch" eingestuft. Die Studienergebnisse deuten darauf hin, dass viele Unternehmen der Sicherheit ihrer Daten eine geringe Priorität einräumen und routinemäßiges Patching vernachlässigen. Einige der CVEs (Common Vulnerabilities and Exposures) blieben laut den Cybersecurity-Experten drei oder mehr Jahre auf den lokalen Datenbanken unerkannt.

**Keine Sicherheitsvorkehrungen im Fokus.** „Während Unternehmen öffentlich betonen, wie viel sie in die Sicherheit investieren, zeigen unsere umfangreichen Untersuchungen, dass ihre Maßnahmen meistens nicht erfolgreich sind", konstatiert Elad Erez, Chief Innovation Officer bei Imperva. „Allzu oft vernachlässigen Unternehmen die Datenbanksicherheit, weil sie sich auf systemeigene Sicherheitsmechanismen oder veraltete Prozesse verlassen. Und obwohl wir weiterhin eine starke Verlagerung hin zu Cloud-Datenbanken beobachten, ist die besorgniserregende Realität, dass die meisten Unternehmen weiterhin auf On-Premise-Datenbanken setzen, wo sie dann ihre sensibelsten Daten speichern. In Anbetracht der Tatsache, dass fast jede zweite On-Premise-Datenbank anfällig ist, werden die gemeldeten Datenschutzverletzungen aller Voraussicht nach weiter ansteigen und auch die Tragweite dieser Fälle wird zunehmen."

**Webanwendungen als Einfallstor für Attacken auf Datenbanken.** Bei nicht öffentlich zugänglichen Datenbanken greifen Hacker auf eine Vielzahl von Tools wie SQL-Injektionen (SQLi) zurück, um Schwachstellen in Webanwendungen auszunutzen, die mit der Datenbank verbunden sind. In den letzten Jahren ist diese Angriffsart zu einer ständigen Bedrohung für Unternehmen geworden – fast 50 Prozent der Sicherheitsverletzungen hatten ihren Ursprung in der Anwendungsebene. Unabhängig davon können Angreifer Phishing und Malware einsetzen, um im internen Netzwerk Fuß zu fassen und dann auf die anfällige Datenbank überzugehen.

Noch größer ist die Bedrohung für öffentliche Datenbanken, denn Angriffe sind hier mit noch weniger Aufwand verbunden. Angreifer können über Tools wie Shodan verwundbare Ziele suchen und Exploit-Codes über Repositories wie ExploitDB beschaffen, die Hunderte von Exploit-POC-Codes enthalten. Von dort aus kann der Angreifer das Exploit von überall aus ausführen, da die Datenbank eine öffentliche IP-Adresse hat.

**Ziel sind personenbezogene Daten, Anmeldedaten und Kreditkarten.** Angesichts der Anzahl von Schwachstellen in On-Premise-Datenbanken ist es nicht verwunderlich, dass die Anzahl der Fälle von Datenverlusten im 12-Monats-Durchschnitt um 15 Prozent gestiegen ist. Eine Analyse der Datenschutzverletzungen seit 2017 zeigt, dass es sich bei der Mehrheit der gestohlenen Daten um personenbezogene Daten (74 Prozent) handelt; Anmeldedaten (15 Prozent) und Kreditkartendaten (10 Prozent) sind jedoch ebenfalls lukrative Ziele.

**www.imperva.com**

# WARUM BRAUCHEN UNTERNEHMEN EINE VISION?

Warum sollten Sie als Unternehmer eine Vision haben? Worin besteht der Unterschied zwischen Zielen, die Sie erreichen möchten und einer großen Vision? Als Unternehmensleitung ist es sehr wichtig, ein Denken in sehr großen Linien zu haben.

Die Visionärin Stefanie Brings lebt ganz nach dem Motto „Mit großen Visionen in eine erfolgreiche Zukunft". Doch was sind überhaupt Visionen? Dabei geht es um die Mentalität und den großen Sinn, warum Sie einer bestimmten Sachen nachgehen. Erfolgreiche Visionäre wissen längst, dass man mit einer großen Leidenschaft ein Ziel verfolgen muss. Das Herzblut und die wahre Identität für eine bestimmte Sache sind sehr wichtig, damit Sie als Unternehmer erfolgreich sind. Ihre Vision als Unternehmen kann zum Beispiel lauten: „Freier und glücklicher durch Mobilität", „Pünktlich und sicher an ihr Ziel" oder „Glücklich und gelassen im Ruhestand." Eine Vision muss Ihrer Firma der Erreichung von Umsatz- oder Ertragsziele stets übergeordnet sein. Wichtig ist es auch dazu ein passendes Bild dafür zu entwickeln, das alle Mitarbeiter kennen.

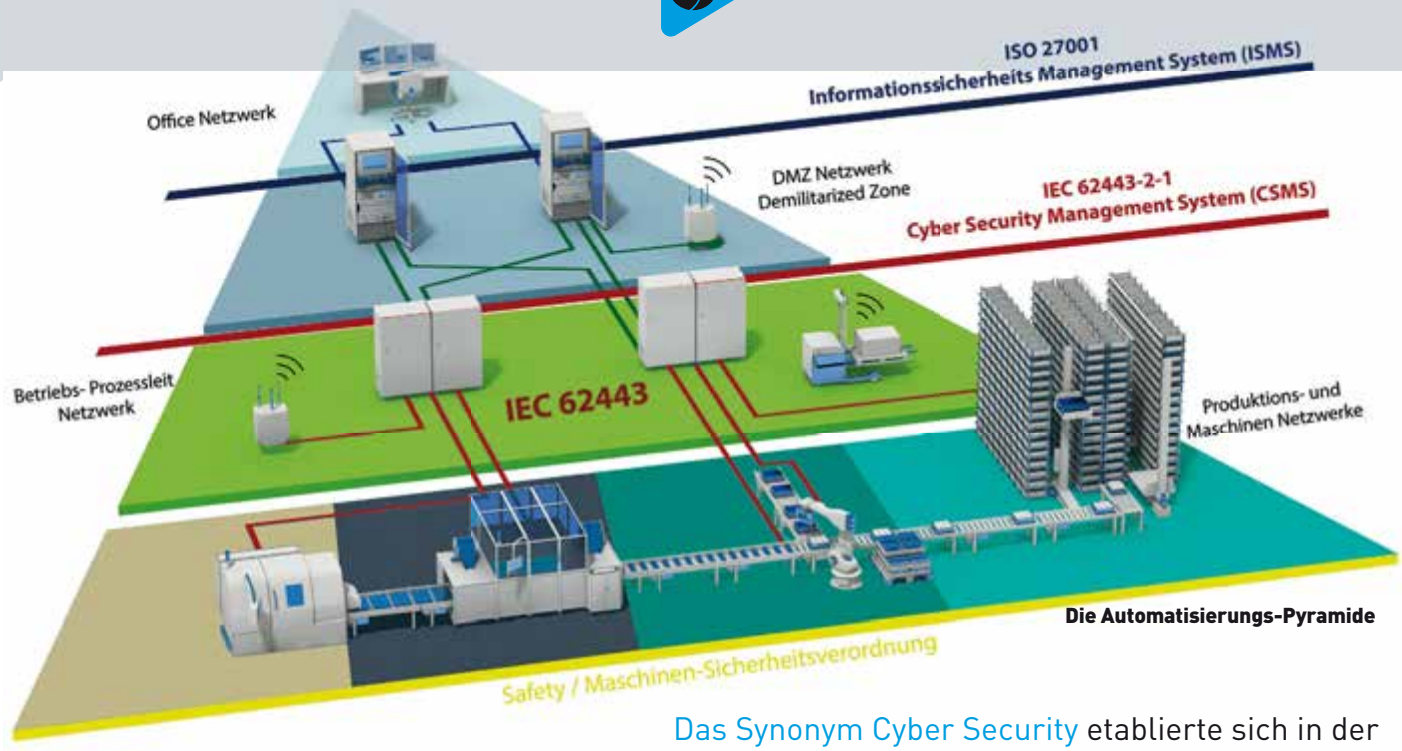
**Müssen die Mitarbeiter die Vision kennen?** Jeder in der Crew muss sich mit der Vision intensiv beschäftigen und sollte mit vollem Herzblut dahinterstehen. Bei einer gelebten Vision handeln alle Mitarbeiter in die gleiche Richtung. Aus diesem Grunde muss, wenn Sie als Chef ein Vorstellungsgespräch mit vakanten Bewerbern führen, unbedingt die Vision zur Sprache kommen. Nur dann wird sich ein Mitarbeiter auf Dauer in Ihrer Firma wohlfühlen und produktiv sein. Sie haben noch keine Vision? Dann gilt: Entwickeln Sie Ihre Vision in Ruhe und geben sich Zeit. Dies ist ein Prozess. Kopieren Sie keine anderen Unternehmensleitbilder oder orientieren Sie sich nicht nur an der Konkurrenz. Hören Sie auf sich und auf Ihre innere Stimme.

Die Visionärin:
**Stefanie Brings**
... ist Beraterin und Coach und hat eine Mentaltraininerausbildung.

**Machen Sie Ihre Vision lebendig.** Der ehemalige Apple-Chef Steve Jobs hat seine Vision der Einfachheit von Technik zu einem Markenzeichen gemacht. Dieses hat sich bis heute erfolgreich auf dem gesamten Markt weltweit durchgesetzt. Jeder überzeugte Apple-Nutzer weiß, dass alle Geräte der Firma hervorragend miteinander kombiniert werden können. Doch auch junge Unternehmer und Startups sollten wissen, welche große Vision sie mit ihrer Firma verfolgen – und das auf Dauer. Eine Vision kann, muss aber nicht der Öffentlichkeit zugänglich gemacht werden. Wenn sie gelebt wird, strahlt sie automatisch nach Außen und zieht Kunden an. Da die Worte Vision, Mission oder Philosophie des Unternehmens nicht einheitlich definiert werden, sollten Sie sich von den unterschiedlichen Begriffen nicht verwirren lassen. Wichtig ist, dass Sie wissen, welch´ große Vision Sie als Chef mit Ihrem Team verfolgen!

**Normen und Werte sind in vielen Visionen enthalten.** Egal, welche Vision Ihnen wichtig ist: Das Große und Ganze im Unternehmen sollte sehr wohlüberlegt ausgewählt werden. Als Unternehmensleitung sollten Sie nicht nur innovativen Trends folgen, die gerade einmal einer „Challenge der heutigen Zeit" entsprechen. Visionäre denken langfristig. Sie haben es sich auf die Fahnenstange geschrieben, dass sich mit der dementsprechenden Vision die Firma auch noch in fünf, zehn, 20 oder 50 Jahren identifizieren kann. Eine Vision verbindet Sinn und Gewinn. Wenn diese gelebt wird, verbunden mit Werten und entsprechender Führungskultur, steigt die Produktivität und Identifikation der Mitarbeiter und das strahlt nach Außen und zieht Kunden an (auch wenn die Kunden die Vision nicht kennen). Dies führt zu Kundenempfehlungen und letztlich steigen auch die Umsatzzahlen. Zudem sind solche Unternehmen z.B. auch durch das positive Betriebsklima attraktiv für gute Fachkräfte.

**https://visionaeres-management.com**




**Die Automatisierungs-Pyramide**

Das Synonym Cyber Security etablierte sich in der Industrie unter anderem, um den Blick auf die besonderen Anforderungen hinsichtlich der Anlagen-Verfügbarkeit sowie Safety oder Atex-Normen der Industrie sichtlich zu schärfen. Ein Überblick von Erich Kronfuss.

# WELCHEN SECURITY-LEVEL WÜRDE IHR AUTOMATISIERUNGSSYSTEM ERREICHEN?

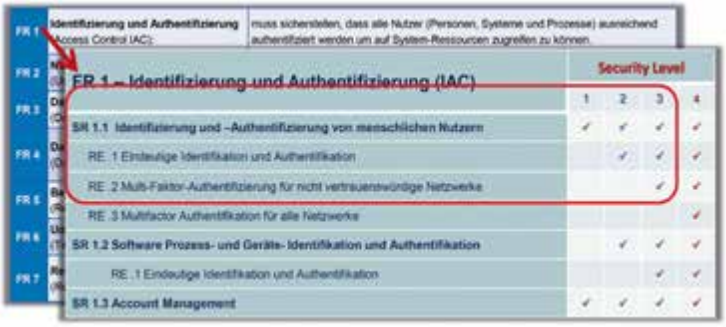
Risikobewertungen von Produktionsanlagen gehen von anderen Angriffsvektoren aus als jene der konventionellen IT. Um OT-Risiken zu identifizieren, bemessen und bewerten zu können muss der prozessuale Ablauf von Industriesystemen verstanden werden. HMI (Anzeige/Touch-Panel) in Produktionsanlagen verfügen oftmals nur über ein Single-User-Betriebssystem. Hier gibt es standardmäßig keine Microsoft User/Rechte-Verwaltung.

Bei einem 24/7-Betrieb einer Produktionsanlage mit HMI-Steuerung müssten alle Maschinenführer das gleiche Kennwort/PIN kennen, um im Notfall eingreifen zu können. Hier können keine konventionellen IT-Datenschutzmaßnahmen zur Anwendung kommen. Auch das Bundesamt für Sicherheit in der Informationstechnik schreibt in seinen Empfehlungen zu Authentisierungsmechanismen in der Produktion: „Anders als in der konventionellen IT sind mit Blick auf die besonderen Anforderungen hinsichtlich Verfügbarkeit und Safety solche Sperren aber beispielsweise erst nach 20 statt bereits nach drei Fehlversuchen vorzunehmen."

**Über was sprechen wir?** Wir sprechen hier über Cyber Security im IACS-Bereich (Industrielle Automatisierungs- und Steuerungssysteme). Diese umfasst einen sehr großen Anwenderbereich wie im Anlagenbau, Prozessindustrie, Energieversorgung, Gebäudeautomatisierung, Wasserwirtschaft, Bahnindustrie, Telekommunikation, Maschinenbau, Automotive u.v.m. Die Unternehmen messen, regeln und steuern mittels elektrotechnischer Systeme (SPS/PLC-Sensoren und -Aktoren) deren Anlagen oder Fahrzeuge.

Die International Electronical Commission (IEC) ist das Normierungsgremium für Normierungen im Bereich der Elektrotechnik und der Elektronik und entwickelt somit auch Normen für Security im IACS-Bereich. Im Rahmen der Arbeitsgemeinschaft „World Standards Cooperation" der ISO, IEC und ITU werden Normen die z.B. die Elektrotechnik betreffen ausschließlich durch die IEC ausgearbeitet.

ISO-Gremien entwickelten mit der ISO 27001 ein ISMS zur Prüfung der Informationssicherheit konventioneller IT. IEC-Gremien entwickelten mit der IEC 62443 Part 2-1 ein CSMS zur Prüfung der IACS-Cyber-Security im OT-Bereich. Dies zeigt auch die unterschiedliche Ausrichtung des ISMS der ISO, dieses steht für Informationssicherheitsmanagement-System, wobei das CSMS „Cyber Security Management-System" der IEC den Fokus auf Cyber Security, also den Schutz von Automatisierungssystemen und IT-Prozessen, beschreibt.



| | | Security Level | | | |
|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 |
| FR 1 | Identifizierung und Authentifizierung Access Control (IAC): muss sicherstellen, dass alle Nutzer (Personen, Systeme und Prozesse) ausreichend authentifiziert werden um auf System-Ressourcen zugreifen zu können. | | | | |
| | FR 1 – Identifizierung und Authentifizierung (IAC) | | | | |
| | SR 1.1 Identifizierung und –Authentifizierung von menschlichen Nutzern | ✓ | ✓ | ✓ | ✓ |
| | RE. 1 Eindeutige Identifikation und Authentifikation | | ✓ | ✓ | ✓ |
| | RE. 2 Multi-Faktor-Authentifizierung für nicht vertrauenswürdige Netzwerke | | | ✓ | ✓ |
| | RE. 3 Multifactor Authentifikation für alle Netzwerke | | | | ✓ |
| | SR 1.2 Software Prozess- und Geräte- Identifikation und Authentifikation | | ✓ | ✓ | ✓ |
| | RE. 1 Eindeutige Identifikation und Authentifikation | | | ✓ | ✓ |
| | SR 1.3 Account Management | ✓ | ✓ | ✓ | ✓ |

**Bei einem Security-Level 3 würde für ein nicht vertrauenswürdiges Netzwerk eine 2-Faktor-Authentifizierung vorgegeben sein.**

**Eine Norm.** Die IEC 62443 stellt in deren Norm Cyber Security-Anforderungen an Betreiber, Integratoren und Automatisierungskomponenten (Hard- und Software). Weiters umfasst diese auch noch das Konzept der „Defense in Depth" um Sicherheitsmaßnahmen in Bezug auf Anlagensicherheit, Netzwerksicherheit bzw. Systemintegrität abzustufen. Ein weiteres Kernthema dieser Norm ist die Segmentierung und kontrollierte Zusammenführung von Netzwerken. Diese Segmente werden entsprechend einer Risikobeurteilung klassifiziert und somit einem Security-Level zugeordnet. Zunächst erfolgt eine technisch machbare und sinnhafte Segmentierung von Anlagen oder Maschinenbereichen nach logischer oder räumlicher Zusammengehörigkeit von Komponenten. Weiters erfolgt eine Klassifizierung nach der zu erwarteten Stärke eines Angreifers, welche in einem vierstufigen SL (Security-Level)-Modell nominiert ist. Diese SL korrespondieren nicht mit den vier SIL aus der IEC 61508 (Safety), auch wenn diese sehr ähnlich klingen mag.
**SL 1:** zufälliges Ausnutzen von Schwachstellen durch Fehlverhalten
**SL 2:** vorsätzliches Ausnutzen von Schwachstellen unter Einsatz von einfachen Mitteln und geringer Motivation
**SL 3:** durchdachtes Ausnutzen von Schwachstellen mit adäquaten Mitteln und moderatem Aufwand
**SL 4:** zielstrebiges Angreifen mit hohem technischen Know-how, hochwertigem Equipment und hohem Zeitaufwand
Anhand des Ergebnisses der Bedrohungs-/Risikoanalyse wird aus den sieben grundlegenden Anforderungen (FR) des IEC 62443 Security-Konzepts der Umfang der Security-Maßnahmen – entsprechend der Security-Level – abgeleitet. Bei einem Security-Level 3 würde für ein nicht vertrauenswürdiges Netzwerk wie einer Fernwartung eine 2-Faktor-Authentifizierung etwa mit einem SMS-Einmalpasswort vorgegeben sein.

**Welcher Security-Level würde nun erreicht?** Mit diesem Security-Konzept können Sie bereits die Bewertung Ihres Automatisierungssystem durchführen. Die Norm nimmt hier aber auch noch Rücksicht auf den Status und die Umsetzbarkeit solcher Maßnahmen.
**SL-T =** Ziel-Security-Level, Ergebnis der Bedrohungs-/Risikoanalyse
**SL-A =** Erreichter Security-Level, im Gesamtsystem erreichter und messbarer Security-Level
**SL-C =** Umsetzbarer Security-Level, Security-Level, den ein Gerät oder System erreichen kann

Um abschließend einen Gesamtüberblick über alle Security-Maßnahmen messbar zu machen, gibt es noch den Maturity-Level (1-4) als Reifegrad der organisatorischen Prozesse und Einhaltung organisatorischer Richtlinien sowie den Prodection-Level (1-4), der Auskunft über die gesamtorganisatorische Cyber Security geben soll.
Um all diese Fragen qualifiziert beantworten zu können, gibt die Norm auch Vorgaben zur Qualifikation eines IACS Service Providers, also eines zertifizierten IACS Cyber Security-Dienstleisters, vor. In Österreich wurde Phoenix Contact durch den TÜV-Süd als erster nach IEC 62443-2-4 zertifiziert und bereits rezertifiziert.

**Abgrenzung der OT-Security IEC 62443 zur IT-Security ISO 27000.** Die Normreihe IEC 62443 berücksichtigt auch Anforderungen anderer Industrienormen wie Safety, also dem Schutz von Menschen und Umwelt noch vor den Security-Zielen der Verfügbarkeit, Integrität und Vertraulichkeit von Daten. Es werden konkrete Anforderungen an Automatisierungssysteme gestellt (FR) sowie auch Anforderungen an den zertifizierten Integrator nach IEC 62443-2-4. Security-relevante Komponenten (Hard- und Software) wie SPS oder Firewall werden entsprechend der geforderten Security-Level getestet und nach IEC 62443-4-2 zertifiziert. Die Normenreihe ISO 27000 bietet einen generischen, prozessorientierten Ansatz sowie allgemeine Vorgaben und Rahmenbedingungen.

**www.phoenixcontact.at**

Der Autor
**Erich Kronfuss**
**... ist IEC-Experte des Österreichischen Verbands für Elektrotechnik und in der Funktion als stv. Vorsitzender der Arbeitsgruppe IACS Security der TSK MR65 an der Entwicklung der IEC 62443 Norm mit beteiligt. Kronfuss ist als IoT-Security-Spezialist bei Phoenix Contact Österreich tätig.**

# ATTACKED!

Cyberattacken nehmen zu. Die Seite der Angreifer wird gefühlt immer professioneller und es ist ein Business daraus entstanden. Im Interview mit Roman Oberauer, Vice President Go to Market & Innovation bei NTT Ldt., wurde klar, dass der Wissensabstand zwischen Angreifern und Angegriffenen kleiner wird, dennoch muss stärker gehandelt werden – jetzt! Von Stephanie Englert

**IoT 4 Industry & Business: Herr Oberauer, Sie sagen, dass Hacker immer professioneller agieren. Was sind die Gründe für diese Entwicklungen und gleichzeitig stellt sich mir noch die Frage: Weshalb agieren die „Opfer" inzwischen nicht auch professioneller?**

**Roman Oberauer:** Zunächst einmal ist es nicht so, dass die Unternehmen bzw. die Menschen schlechter werden, was die Cyberabwehr betrifft. Die Angreifer lernen nur sehr schnell dazu, handeln rasch und entwickeln immer wieder neue Angriffsstrategien. Das sind Top-Experten, die sich leider für die falsche Seite des Gesetzes entschieden haben.

Die Pandemie und die damit verbundene Umstellung auf hybrides Arbeiten hat den Hackern extrem in die Hände gespielt, weil dadurch große Sicherheitslecks entstanden sind. Hier ist man als Unternehmen natürlich besonders gefragt, Schritt zu halten und noch stärker auf die Security-Themen zu fokussieren.

**IoT: Es wird aber immer wieder betont, dass sich Cyberkriminelle zu einem professioneller werdenden Netzwerk entwickeln bzw. es bereits sind. Ist – überspitzt formuliert – dieser Arbeitgeber für den IT-Nachwuchs attraktiver anstatt auf der anderen Seite, also der der „Angegriffenen", zu arbeiten?**

**Oberauer:** Ich glaube, im Leben geht es oft darum, sich für die richtige Seite zu entscheiden. Ich bin davon überzeugt, dass es für den überwiegenden Teil des IT-Nachwuchses nicht in Frage kommt, auf die illegale Seite zu wechseln.

Aber natürlich hat das Verbotene immer seinen Reiz und es wird immer Personen geben, die sich davon angezogen fühlen. Auf der legalen Seite – also auf Unternehmensseite – gibt es viele interessante Tätigkeitsfelder, gerade im Security-Bereich. Mit Penetrationstests kann man beispielsweise genauso testen, wie sicher Unternehmen sind, ohne ihnen wirklich zu schaden.

**IoT: Wie kann das Darknet von Unternehmen für die eigene Sicherheit gezielt genutzt werden? Ist das möglich?**

**Oberauer:** Es ist für Unternehmen enorm wichtig, das Darknet nicht zu ignorieren und in ihre IT-Beobachtungen miteinzubeziehen. Im besten Fall übernimmt das der IT-Dienstleister, der das Unternehmen betreut. Unsere NTT-Experten kennen die Methoden der Hacker und können durch die ständige Beobachtung des Darknets oft Angriffe frühzeitig verhindern bzw. rechtzeitig Gegenmaßnahmen ergreifen.

**IoT: Was sind in diesem Zusammenhang die immer häufiger in Gesprächen auftauchenden Honeypots?**

**Oberauer:** Honeypots sind ein entscheidendes Tool zur Bekämpfung von Cyberattacken. Das bedeutet so viel, dass man unter einem Honeypot fiktive Angriffspunkte zu verstehen hat, die

Hacker anziehen sollen. Durch Attacken auf diese Schnittstellen lernen wir viel über aktuelle Methoden und Vorgehensweisen der Kriminellen und können unser Kundensysteme dementsprechend sichern. Wir haben weltweit mehr als 1.500 sogenannter Honeypots in 23 Ländern installiert. Auf Basis der Erkenntnisse aus den Honeypots kann NTT monatlich rund 10.000 neue Angriffsmuster identifizieren und in die Cyberabwehr bzw. in die Erkennungssysteme einspielen.

**IoT: Wie groß können denn eigentlich Imageschäden nach gelungenen Cyberangriffen für die betroffenen Unternehmen werden? Dadurch, dass auch Ihren Aussagen nach, fast „jedes" Unternehmen heutzutage angegriffen werden wird, müsste doch gleichzeitig das Verständnis am Markt groß sein, wenn es „wieder" jemanden trifft?**

**Oberauer:** Es ist so: Die Pandemie hat gezeigt, wie wichtig es ist, sich mit Security- und Cloud-Themen auseinanderzusetzen. Denn nur mit standardisierten, aber individuell zugeschnittenen Lösungen, kann mein Unternehmen resilient, also widerstandsfähig gegen mögliche Angriffe werden. Das gilt für KMU genauso wie für Großkonzerne.

Der sprunghafte Anstieg der Attacken zeigt, dass die Hacker oftmals leider die Nase vorne haben und viele Unternehmen so rasch wie möglich nachrüsten müssen. Betriebe müssen laufend an ihren Systemen arbeiten und sie weiterentwickeln. Das Thema Cybersecurity muss in allen Branchen, und hier vor allem auch bei Lieferketten, eine höhere Priorität bekommen. Denn es ist klar: Gelingt ein Cyberangriff und die Produktion wird dadurch lahmgelegt, kann ein dauerhafter Reputationsschaden entstehen. Und dieser Schaden ist wohl der größte und langfristigste, mit dem die Firma leben muss.

**IoT: Allgemein gefragt: Investieren die Unternehmen (in Österreich) immer noch zu wenig in die Ausweitung der Security-Maßnahmen?**

**Oberauer:** Bei vielen großen Konzernen ist Cybersecurity zum Glück bereits ein Top-Management-Thema. Nur wer gut geschulte Experten bei der Hand hat, die im Ernstfall schnell handeln können, kann den Schaden so gering wie möglich halten. Es bewährt sich jedenfalls, die IT-Security an einen externen Dienstleister wie NTT abzugeben oder einen externen Partner zumindest einzubinden.

Der Aufwand, der mittlerweile für Cybersicherheit betrieben werden muss, ist enorm und kann nur von Experten übernommen werden. Durch die externe Expertise braucht es nur mehr eine kleine eigene IT-Abteilung und auch Kosten für aufwändige Infrastruktur und Software können dadurch minimiert werden.

**IoT: Wie sehen Sie die Entwicklungen bzgl. der Angriffe und der Professionalität der Angreifer am hiesigen Markt bzw. auch global betrachtet für die kommenden Jahre?**

**Oberauer:** Cyberkriminalität bleibt und wird mit fortschreitender Digitalisierung steigen, das ist unumstritten. Die Zeit der Script-Kiddies ist längst vorbei und Cyberkriminelle arbeiten als professionelle Anbieter im Darknet. Das bedeutet, dass im Grunde jeder Attacken kaufen kann. Von speziellen Einzelangriffen bis hin großangelegten Denial of Service-Attacken oder Ransomeware-Attacken. Drei wesentliche Faktoren im Aufbau einer Abwehrstrategie sind und bleiben weiterhin wichtig:

1. Früherkennung von Anomalien (via Software und auch durch Menschen)
2. Globale Sicht auf die Cybercrime-Aktivitäten
3. Redundante Sicherheitssysteme

Ein Restrisiko bleibt aber immer und es geht in der Cybersecurity vor allem darum, das Risiko so weit wie möglich zu minimieren und sich als möglichst unattraktives Ziel – weil gut abgesichert – darzustellen. Stellen Sie sich vor: Ihr Nachbar hat eine Alarmanlage und Sicherheitsschlösser und Sie nicht. Wo wird es ein Einbrecher eher versuchen...?

**IoT: Vielen Dank!**

**https://hello.global.ntt**

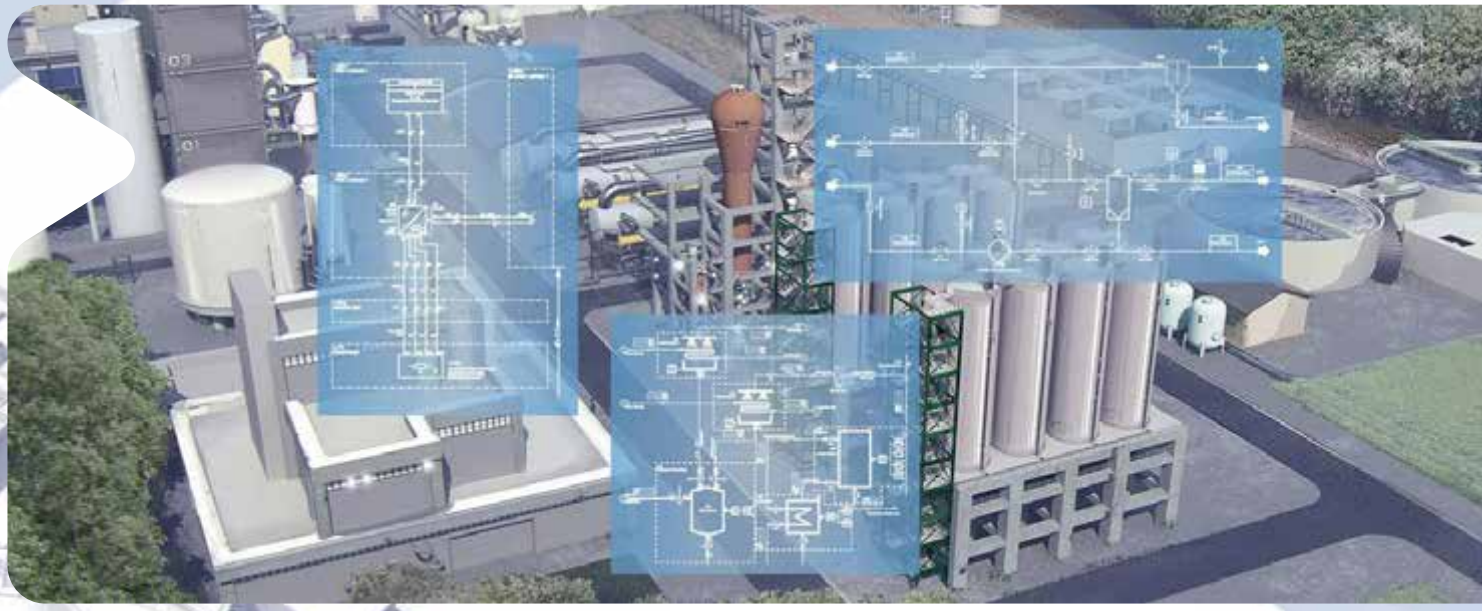
**Roman Oberauer,**
**Vice President Go to Market & Innovation bei NTT Ldt.**

„Es ist für Unternehmen enorm wichtig, das Darknet nicht zu ignorieren und in ihre IT-Beobachtungen miteinzubeziehen."

Bilder: Aucotec AG

# NONSTOP KOOPERATIVES ANLAGEN-ENGINEERING VON FEED BIS ZUM ANLAGENBETRIEB

Der Anlagenbau ist geprägt durch Teilanlagen sowie durch mittelgroße bis sehr große Projekte mit einer Vielzahl anspruchsvoller Engineering- und Management-Aufgaben. Dabei darf die Qualität nicht auf der Strecke bleiben. Das gehört zur üblichen Herausforderung im Anlagen-Engineering.
Mit der Plant Solution von Engineering Base bietet Aucotec ein Höchstmaß an Durchgängigkeit, vom R&I bis Arbeitsblatt, von Process Design bis Automation – mit allen Vorteilen für den Techniker und das Management.



**Mit der Plant Solution von Engineering Base bietet Aucotec ein Höchstmaß an Durchgängigkeit, vom R&I bis Arbeitsblatt, von Process Design bis Automation – mit allen Vorteilen für den Techniker und das Management.**

## Coverstory

Projekte in der Prozessindustrie sind geprägt von hoher Komplexität von Anlagen und großem Zeit- und Kostendruck. Die entscheidende Aufgabe ist es, den Überblick über die enormen Datenmengen im Engineering zu behalten, um alle am Prozess beteiligten Gewerke und Experten nahtlos kooperieren zu lassen – besonders wenn diese an verschiedenen Standorten sitzen.

Das R&I-Schema (oder: P&ID) als Ergebnis des Prozess-Design ist der Ausgangspunkt für alle weiteren Engineering-Disziplinen und erfordert daher ein Höchstmaß an Aktualität und Zuverlässigkeit. Jede Änderung muss für alle anderen klar erkennbar und nachvollziehbar sein.

Anlagenbauer nutzen Front End Engineering Design (FEED), um wichtige Entscheidungen zu fällen und die Kosten realistisch einzuschätzen. Denn die Simulation der FEED-Phase gibt Aufschluss über wichtige Fragestellungen: Wie erreiche ich am effektivsten die gewünschte Funktionalität? Welche Technologie sichert mir das beste Kosten-Nutzen-Verhältnis?

Die Herausforderung dabei: Häufig müssen tausende von Daten per Hand aus dem Simulationstool ins Engineering-System übertragen werden. Der Vorgang fordert Zeit, erzeugt Aufwände und ist darüber hinaus anfällig für Fehler. Außerdem wiederholt sich das Prozedere, denn schließlich sollen verschiedene Szenarien gegeneinander verglichen werden.

**Intelligente Verknüpfung mit der Simulation spart Zeit.** Für einen kooperativen, disziplinübergreifenden und durchgängigen Plant Design-Prozess bietet Aucotec die datenbankgestützte, objektorientierte Plattform Engineering Base (EB). Das Basic Engineering-Paket startet mit einfacher, hocheffizienter Process-Flow-Diagram (PFD)-Konfiguration anhand vordefinierter Module. Die intelligente Verknüpfung von Simulation und Engineering führt darüber hinaus zu drastischen Zeit- und Aufwandsersparnissen von FEED-Phasen. Das komfortable Handling verschiedener Szenarien erleichtert deren präzisen Vergleich – inklusive Dokumentation und Kalkulation. Dabei werden Process Design, FEED, Instrumentation & Control, Electrical, Cause & Effect und Automatisierungsunterstützung in einer einzigartigen Lösung vereint. EB bietet beispielsweise eine intelligente Verknüpfung zu gängigen Simulationstools, etwa zu Aspen. Selbst Simulationen mit Pro II oder eigens kon- >>

**Engineering Base von Aucotec ermöglicht nonstop kooperatives Anlagen-Engineering von FEED bis zum Anlagenbetrieb – ein Anlagenleben lang.**

figurierte XLS-Kalkulationen können eingebunden werden. Das PFD und die Arbeitsblätter von EB übernehmen die Simulationsberechnungen automatisiert und zeigen das Ergebnis des jeweiligen Szenarios an: vom groben Fließschema bis zur Materialbilanz. So können unterschiedliche Szenarien im intelligenten Datenmodell parallel abgelegt und miteinander verglichen werden. Daraus resultierend lassen sich Angebote einfacher und schneller erstellen, die Datenqualität erhöhen und Übertragungsfehler vermeiden. Durch die erheblich verkürzte FEED-Phase lassen sich pro Szenario mehrere Wochen Zeit einsparen.

**Zentrales Process Design.** Das Process Design startet mit dem Aufbau eines groben PFDs oder dem Ergebnis der FEED-Phase (Front End Engineering Design), also dem „Gewinner-Szenario", das in der Simulation das Optimum ergeben hat. Dabei sorgt die Datenzentrierung von EB dafür, dass selbst global verteilte Planungsteams immer auf dem aktuellen Stand der Anlagendokumentation bleiben.
EB arbeitet auf Basis eines regelbasierten P&ID. Regeln, die z.B. für eine bestimmte Rohrleitung gelten, wirken sich automatisch auf alle in dieser Leitung verbauten Geräte aus. Außerdem kann die Rohrleitungsdarstellung durch zusätzliche Informationen wie Fließrichtung, durchfließende Medien, Temperaturen und Drücke ergänzt werden.

**Die Vorteile liegen ganz klar auf der Hand:**

- Übergreifende Synergie und einzigartige Durchgängigkeit beim Process Design,
- automatische Fehlererkennung und -markierung,
- automatische rohrklassengerechte Komponentenauswahl,
- einfache Leitungssegmentierung,
- schneller Überblick durch „schlaue" Rohre mit sämtlichen Hintergrundinformationen,
- automatische Erstellung von Materialstücklisten.

**Cause & Effect-Tabellen für die Inbetriebnahme-Phase.** Um diese Tabellen zu erstellen, müssen Logik-Diagramme, R&I-Schemata und andere Unterlagen aus den beteiligten Engineering-Disziplinen und unterschiedlichen CAE-Tools durchforstet werden. Da diese Tabellen zusätzlich sehr umfangreich sind, erfordert ihre Erstellung viel Zeit und birgt Potenziale für Fehlerquellen.
EB übernimmt das sonst sehr aufwändige Zusammenführen von Informationen aus den verschiedenen Bereichen. Nach den Cause & Effect-Festlegungen der einzelnen Disziplinen erstellt die Plattform eine Cause & Effect-Tabelle für jeden gewünschten Operations-Modus.
Die einzigartige Durchgängigkeit von EB ermöglicht erheblich automatisierte Abläufe mit außergewöhnlicher Konsistenz und Qualität der Tabellen für verschiedene Betriebsmodi und Szenarien. Ein anwenderfreundliches Cause & Effect-Engineering wird durch Filter und Übersichten gewährleistet. Ebenso lassen sich die Daten einfach im Excel-Format als Standard-Matrix exportieren. Die einzigartige Konsistenz der Cause & Effect-Tabellen bleibt dank der Verbindung der Disziplinen in der gemeinsamen Datenbasis auch bei paralleler Erstellung für Process Design (R&I), Instrumentierung und Automation. Das ermöglicht nicht nur eine beschleunigte Änderungskoordination, sondern auch ein lückenloses Revisionsmanagement mit Änderungsverfolgung und Dokumentation der Cause & Effect-Historie.

**DCS-Portal – Brücke zum Leitsystem.** Leitsysteme (DCS – Distributed Control System) sind die Gehirne einer Anlage. Sie regeln den Betrieb mit allen Funktionen und verarbeiten dazu laufend Informationen aus der Anlage. Vorausgesetzt, dass das Leitsystem alle relevanten Parameter aus dem Anlagen-Engineering kennt. Da aber die Automatisierer oft erst am Ende der Workflow-Kette zum Einsatz kommen, stehen sie dann unter erheblichem Zeitdruck bei der Programmierung. Änderungen während dieser Phase bereiten erhebliche Probleme, wenn nicht

**Cause & Effect-Tabellen ermöglichen erheblich automatisierte Abläufe mit außergewöhnlicher Konsistenz und Qualität für verschiedene Betriebsmodi und Szenarien.**

alle Beteiligten auf eine gemeinsame Datenbasis zugreifen können. Zur Lösung dieser Problematik bildet EB die sichere Brücke zwischen Anlagen-Engineering und Leitsystem-Programmierung. Die relevanten Parameter werden direkt übergeben und gehen automatisch in die Programmierung ein, sogar wenn mehrere unterschiedliche DCS-Systeme – auch gleichzeitig – im Einsatz sind. Dafür stellt das Portal effiziente Schnittstellen für alle gängigen Systeme zur Verfügung. So kann das Automatisierungs-Engineering wesentlich beschleunigt werden. Auch die schnelle und sichere Übernahme von Änderungen steigert letztendlich die Effizienz, Geschwindigkeit und Qualität, die EB nicht nur Automatisierern, sondern auch EPCs und Betreibern bietet.

**Wartung: Mobilität ist Trumpf.** In weiterer Folge bietet EB mit seiner Maintenance-Lösung Wartungsverantwortlichen, Management und Technikern ein umfassendes Paket mit fehler- und zeitsparenden Funktionen.

Nach der Inbetriebnahme endet in der Regel der Einsatz herkömmlicher Engineering-Systeme. Schließlich ist die Planung abgeschlossen und damit die Aufgabe erledigt. Doch im laufenden Betrieb ergibt sich immer wieder die Notwendigkeit von Änderungen – und mit ihr leider oft auch einige Probleme.

Die zentrale Frage lautet: Wie kommen die zuständigen Techniker an den wirklich aktuellen Stand der Dokumentation mit allen relevanten Daten? Hochpreisige CAx-Tools zu verwenden, ist keine Lösung, weil sie Anforderungen an die Hardware stellen, die nicht zur üblichen Wartungs-Praxis passen. Außerdem brauchen Abteilungs- und Betriebsleiter nicht nur die aktuelle Dokumentation, sondern auch den Maintenance-Plan der Anlage.

Im Fokus des Maintenance-Pakets von EB steht eine wichtige Anforderung an effektive Wartung: Datenmobilität. Servicemitarbeiter haben jederzeit, vor allem bei spontanen Notfällen – ohne langes Ordner-Durchforsten flexiblen Zugriff auf alle aktuellen und relevanten Anlagendaten. Mit einer Web-basierten Anwendung wird der Service noch deutlich flexibler. Dafür hat Aucotec die Maintenance App entwickelt. Dabei ist EB die Brücke von der App zu SAP-PM (Plant Maintenance), aber auch zu anderen Systemen für das Planungsmanagement. Durch die Cloud-Technologie hinter den Maintenance-Lösungen greift der Service-Techniker stets auf die aktuellen Daten und Dokumente der Anlage zu. Damit erfüllt EB auch die Anforderungen von Industrie 4.0 durch Predictive Maintenance.

**www.aucotec.at**

**Dank Datenmobilität haben Servicemitarbeiter jederzeit, vor allem bei spontanen Notfällen – ohne langes Ordner-Durchforsten, flexiblen Zugriff auf alle aktuellen und relevanten Anlagendaten.**

Der Ansatz, dass jeder glaubt, er muss alles selbst machen, führt zum Kollaps und eine wirklich digitalisierte Welt wird dadurch nicht geschaffen.

Bild: © Busakorn, Pongparnit, Moment, Getty Images

# DIGITALISIERUNG IST NICHT NUR EINE E-MAIL

Die Stolpersteine liegen im Kopf, sagt Andreas Dangl, Business Unit Executive für Cloud Services bei Fabasoft, mit Blick auf die Umstellung auf digitale Geschäftsprozesse. Ein weiteres Hindernis seien der Fachkräftemangel und das Silodenken. Es gibt aber auch Positives zu berichten: die Potenziale wären enorm. Von Mag. Barbara Sawka

**IoT 4 Industry & Business: Digitalisierung ist das Wort der letzten beiden Jahre. Wie digital sind die österreichischen Unternehmen geworden?**

**Andreas Dangl:** Man muss hier einen großen Unterschied machen: interne Prozesse zu digitalisieren, ist ja noch halbwegs trivial. Denn im eigenen Unternehmen hat man im Wesentlichen nur eine Entscheidungsstruktur. Dennoch ist auch hier noch definitiv Luft nach oben.

Wir haben gerade zu Beginn der Pandemie gesehen, dass nicht alles so reibungslos funktioniert hat. Der viel komplexere Weg ist es, unterschiedliche Unternehmen in einem gemeinsamen Prozess zu verankern. Dies ist um einiges aufwändiger, und viele Unternehmen stehen dabei noch ganz am Anfang. Die großen Unternehmen sind aufgrund ihrer globalen Aktivitäten schon weiter.

Und gerade KMU müssen verstehen, dass Digitalisierung nicht bedeutet, nur eine E-Mail zu verschicken. Es geht darum, einen Prozess in Bezug auf eine Freigabe, eine Überprüfung, eine Genehmigung, eine digitale Unterschrift mit Externen durchgängig zu realisieren. Das ist genau die Aufgabe von Fabasoft. Mit unserer Plattform, der Fabasoft Business Process Cloud, sind wir genau die Drehscheibe, die alle Informationen so aufbereitet, dass sie in einer ganzheitlichen Sicht zur Verfügung stehen. Jedes Dokument und jede Information befindet sich in einem Fluss, in dem die unterschiedlichsten Beteiligten Daten erstellen, bearbeiten, lesen oder nutzen können.

**IoT: Was scheint der größte Hemmschuh auf dem Weg zur Digitalisierung zu sein?**

**Dangl:** Es gibt unzählige Schlagworte wie Industrie 4.0 oder

Internet of Things. Vieles ist dabei in erster Linie auf die Produktion ausgerichtet. Wir unterstützen mit unserem Angebot primär den gesamten Administrationsprozess rund um die eigentlichen Industrie 4.0-Prozesse. Darauf haben viele einfach noch keinen Fokus gesetzt. Meistens geht es nur um die Smart Factory, in der alles komplett automatisiert und digital ist. Das ist natürlich extrem wichtig und zukunftsträchtig.
Daneben gibt es noch die ganz klassischen Verwaltungsabläufe, in denen Prozesse entsprechend dokumentiert werden müssen, in denen es gilt, Compliance-Vorschriften zu beachten, Genehmigungen mit hunderttausenden von Dokumenten für einen Anlagenbauer zu organisieren und zu administrieren, um am Ende die automatisierte Smart Factory zu realisieren.
Viele Unternehmen haben noch nicht erkannt, wie viel Potenzial im Dokumentenmanagement in Hinblick auf die Produktivität liegt. Wir richten uns mit unserem Angebot stark an den Maschinen- und Anlagenbauer, die noch oft in Silos denken. Da geht es um „meine" und „deine" Daten, um „mein" und „dein" System. Die Hindernisse liegen mehr im Kopf des Managements oder jener Personen, die die Entscheidungen treffen. Das sind die größten Stolpersteine.

**IoT: Sie bieten Ihre Services über eine Cloud an. In den letzten Jahren erkennt man wieder einen Trend zum eigenen Rechenzentrum. Was sind die Vorteile Ihres Cloud-Angebotes?**
**Dangl:** Wenn Transparenz gegeben ist, dann gibt es aus meiner Sicht keinen großen Unterschied, ob Daten im eigenen Rechenzentrum oder in einer Cloud liegen. Fabasoft verfolgt bei seinem Cloud-Angebot ganz konsequent das Konzept der Zertifizierungen und Audits auf höchstem Niveau. Bei einem eigenen Rechenzentrum haben wir eine natürliche Transparenz. Man kann hineingehen und nach dem Rechten sehen.
Wir beauftragen Zertifizierungsstellen, etwa namhafte Wirtschaftsprüfer, die verifizieren und dokumentieren, dass das Leistungsversprechen eines Cloud-Anbieters den jeweiligen Zertifizierungskriterien entspricht und insbesondere Qualität, Datenschutz und IT-Sicherheit gegeben sind.

**IoT: Sie haben Transparenz angesprochen. Sind Sicherheit und Transparenz ein Gegensatzpaar?**
**Dangl:** Nein, eigentlich nicht. Sicherheit ist ein Fundament, das gegeben sein muss. Transparenz bedeutet, dass für mich ersichtlich ist, wer auf Informationen zugreifen darf und wer worauf zugegriffen hat. Wenn Sie ein E-Mail verschicken, ist es weder für Sie als Absender noch für den Empfänger klar, wer letzten Endes alles mitliest. Das ist das Problem bei der Transparenz. Es geht darum zu verstehen, was mit der Information passiert und ob ich noch die Kontrolle darüber habe. Das verstehe ich unter dem Begriff Transparenz: nachzuvollziehen, wer zu welchem Zeitpunkt Zugriff auf eine Information gehabt hat.

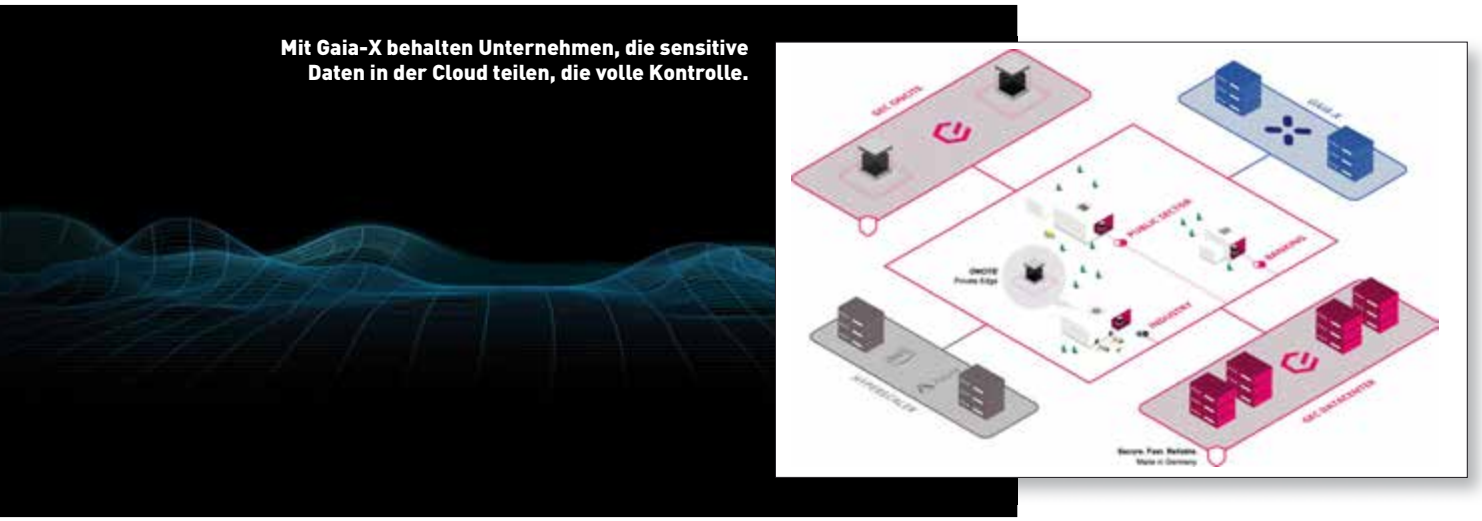
**IoT: Viele Cloud-Dienste werden in Abo-Systemen angeboten. Macht es Fabasoft mit seinen Angeboten ebenso?**
**Dangl:** Mit einer Cloud ist ganz grundsätzlich ein Abo-Modell verbunden, das entsprechend leistungsorientiert oder nutzenbasiert funktioniert. Indem Unternehmen keine Kapitalinvestitionen treffen müssen, minimiert sich die Eintrittshürde. In ein Rechenzentrum mit eigener Infrastruktur und Software-Lizenzen zu investieren, bedeutet sehr viel initialen Aufwand.
Mit der Cloud arbeitet man generell über einen Skalierungseffekt. Das hat für den Kunden den Vorteil, dass er erstens keine Kapitalinvestitionen treffen muss und zweitens, dass er klein beginnen kann, ganz im Sinne des Proof of Concept. Ein Abo-Modell bietet die Chance, relativ einfach und ohne riesige Summen in die Hand zu nehmen, Dinge ausprobieren zu können, was gerade im Bereich innovativer und disruptiver digitaler Prozesse oft notwendig ist. Wir unterstützen diesen agilen Ansatz unserer Kunden.

**IoT: Was sehen Sie aktuell oder in den nächsten Monaten als die größte Herausforderung für Fabasoft?**
**Dangl:** Meine größte persönliche Herausforderung ist es, genügend Ressourcen zu haben. Ganz ehrlich, wir haben derzeit einen extremen Mangel an Fachkräften. Und das liegt auch an einer Eigenheit der Industrie. Jeder will seine eigene Cloud aufbauen oder seine eigene Digitalisierungsstrategie auf die Beine stellen und konsumiert dabei aus dem Pool der wenigen Fachkräfte, die am Markt sind. Da sind wir wieder bei den schon angesprochenen Stolpersteinen im Kopf.

**www.fabasoft.com**

**Andreas Dangl**
**Business Unit Executive für Cloud Services bei Fabasoft**

„Mit unserer Plattform Fabasoft Business Process Cloud sind wir die Drehscheibe, die alle Informationen so aufbereitet, dass sie in einer ganzheitlichen Sicht zur Verfügung stehen."



Mit Gaia-X behalten Unternehmen, die sensitive Daten in der Cloud teilen, die volle Kontrolle.

# DATENSICHERHEIT FÜR DIE INDUSTRIE

Die Initiative Catena-X hat sich die Entwicklung eines einheitlichen Industriestandards zum Ziel gesetzt. Große Player und Mittelständler haben sich dem neu gegründeten Automotive Network angeschlossen – dabei ist auch die German Edge Cloud.

Es geht um nichts weniger als um die Zukunft der deutschen und europäischen Automobilindustrie. Der Aufbau von offenen B2B-Industrieplattformen soll den Informationsaustausch zwischen den OEMs, Lieferanten sowie Kunden digitalisieren und damit: vereinfachen, sicherer machen und neue, datengetriebene Geschäftsmodelle auf die Straße bringen. Voraussetzung sind einheitliche Industriestandards. Hier setzt Catena-X an.

Die Initiative arbeitet an einem offenen, skalierbaren Netzwerk auf Basis Gaia-X für den sicheren, unternehmensübergreifenden Datenaustausch in der Fahrzeugindustrie. Mitglieder wie BMW, Mercedes Benz, Robert Bosch, SAP SE, Siemens, ZF und German Edge Cloud (GEC) wollen mit der entstehenden B2B-Plattform die deutsche Automobilindustrie für den internationalen Wettbewerb stärken. Das Netzwerk soll der europäischen Fahrzeugindustrie und ihren Partnern offenstehen und vor allem auch mittelständische Zulieferer integrieren. Basis der Datenplattform ist eine souveräne Infrastruktur: Gaia-X. So ist sichergestellt, dass die Unternehmen, die sensitive Daten in der Cloud teilen, die volle Kontrolle darüber behalten.

**German Edge Cloud mit Lösungen.** Für Datenschutz und Datensouveränität steht auch die GEC als Pionier der Branche. Ihre Lösungen unterstützen besonders datenintensive und performancekritische Anwendungen in der Industrie 4.0. Die Friedhelm Loh Group ist mit ihrer Tochtergesellschaft GEC Mitbegründer von Gaia-X. German Edge Cloud ermöglicht die heute erforderliche Datensouveränität u.a. mit ihrem Produkt Oncite. Das Edge-Cloud-Rechenzentrum mit industriellen Software-Applikationen ermöglicht echtzeitfähige, produktionsnahe Anwendungen und gleichzeitig eine sichere Anbindung an bestehende Cloud-Lösungen und trägt zum Aufbau einer sicheren europäischen Dateninfrastruktur bei.

**Industrie stärken.** Mit dem Engagement in der Allianz Catena-X will die German Edge Cloud die Brücke zwischen Gaia-X-Konzepten und praxisrelevanten Anwendungsfällen der Automobilindustrie bauen. „Wir möchten zunächst die Machbarkeit und die Vorteile von unternehmensübergreifender Datennutzung in der Lieferkette über die Realisierung erster Leuchtturmprojekte, beispielsweise zur Nachverfolgbarkeit von Bauteilen, demonstrieren. Außerdem werden wir als mittelständischer Vertreter der Ausrüster-Seite den Transfer der Konzepte in den produzierenden Mittelstand aktiv betreiben“, erklärt Dieter Meuser, CEO Cloud & Industrial Solution der German Edge Cloud. Dr. Sebastian Ritz, CEO Cloud & Edge Computing der German Edge Cloud, sagt: „Mit dem Beitritt zum Catena-X Automotive Network gehen wir einen weiteren wichtigen Schritt, um deutschland- und europaweit Plattform-Standards für den sicheren Datenaustausch und den Aufbau neuer Geschäftsmodelle in der Industrie zu etablieren. Diese Initiative wird die internationale Wettbewerbsfähigkeit der Automotive-Branche maßgeblich stärken.“

**www.gec.io**

# GEREGELTE IT-VERHÄLTNISSE

Wer ein Rechenzentrum zukunftssicher planen, betreiben und erweitern möchte, hat mit der DIN EN 50600 einen Leitfaden durch den Dschungel der europäischen Vorgaben zur physikalischen Sicherheit sowie zur Versorgungssicherheit.

Egal wohin man schaut, es geht um die Digitalisierung. Gleich ob kleines oder großes Unternehmen, öffentliche Institution oder staatliche Verwaltung – ohne IT geht es nicht mehr. Dass Daten unternehmensrelevant sind, ist mittlerweile allen klar. Und dass Daten geschützt werden müssen ebenfalls. Ob man das in einer Cloud oder in einem eigenen Rechenzentrum machen soll, ist eine Frage, die jeder nur nach seinen jeweiligen Anforderungen beantworten kann. Die großen Unternehmen betreiben meist ihr eigenes Rechenzentrum und lagern vorwiegend Dienste wie z.B. Backup oder Exchange in die Cloud aus. Kleinere Unternehmen gehen eher zu einem externen Anbieter, um die eigenen Ressourcen zu schonen.

Wenn es allerdings um die Planung eines eigenen Rechenzentrums geht, stehen Verantwortliche vor zahlreichen Fragen. Entsprechen die vorhandenen räumlichen Möglichkeiten den Anforderungen für einen sicheren Betrieb? Sind nötige Erweiterungen in Zukunft einfach umsetzbar? Genügen Stromversorgung, Klimatisierung und Sicherheitsvorkehrungen den Anforderungen und Vorschriften? Besonders die Ansprüche an die Sicherheit, Verfügbarkeit sowie die Größe der Rechenzentren hat sich in den letzten Jahren verändert. Bei den IT-Verantwortlichen ist auch das entsprechende Bewusstsein vorhanden. Aber wer kann beurteilen, ob die Gebäudestruktur, die Stromversorgung und Umgebungsbedingungen, Verkabelung und Sicherheitssysteme aufeinander abgestimmt sind und einem neuen Rechenzentrum nichts im Weg steht?

**Europäisches Regelwerk.** Um ein Rechenzentrum entsprechend den eigenen Wünschen und Anforderungen zu bauen, sowie gesetzlichen Vorschriften gerecht zu werden, mussten sich Errichter und Betreiber bislang mit verschiedenen Richtlinien behelfen. Eine Norm für die Gesamtbetrachtung von Rechenzentrums-Infrastrukturen fehlte die längste Zeit. Es gab zwar Planungsleitfäden und Unternehmensstandards, diverse Normen zum Stand der Technik in einzelnen Gewerken und Bereichen. Da diese nicht einheitlich waren, waren sie auch nicht vergleichbar. Damit wurde die Notwendigkeit ein einheitliches europäisches Regelwerk zu schaffen sehr deutlich. Mit der Errichtung der DIN EN 50600 hat die europäische Normungsgesellschaft Cenelec diesen Zustand beendet.

Seit 2016 bietet die EN 50600 die notwendige Unterstützung für die Betreiber von Rechenzentren oder Cloud-Infrastrukturen sowie für deren Kunden. Diese können ihre IT-Infrastrukturen mittels diesem europäischem Leitfaden zukunftssicher planen, betreiben und erweitern. Mit der EN 50600 gibt es einheitliche europäische Vorgaben zur physikalischen Sicherheit sowie zur Versorgungssicherheit im Rechenzentrum. Sie ist in die vier Bereiche allgemeines Konzept, physische Aspekte von baulichen Fragen des Gebäudes bis hin zu Energie-, Verkabelungs- und Sicherheitsaspekten, Management und Effizienzaspekte wie KPIs, Energieverbrauch und erneuerbare Energien unterteilt. Darin enthalten sich auch Angaben für die Planung der Baukonstruktion, Elektroversorgung, Klimatisierung, Verkabelung sowie die Sicherheitssysteme und sie beschreibt auch die Anforderungen für den Betrieb.

Allerdings ist die Norm rechtlich nicht bindend, sondern nur eine Empfehlung. Der TÜV übernimmt anschließend die Zertifizierung, die vor allem für Unternehmen wichtig ist, die als Zulieferer etwa in der Automobilindustrie gelistet werden wollen.

**www.seccon.cc**

Der Autor

**Christian Schupfer**

**... ist Geschäftsführer der Seccon IT-Sicherheitstechnik GmbH. Das Unternehmen übernimmt den kompletten Rechenzentrumsbau und die Planung von EDV-Infrastrukturen von der Konzepterstellung, über die Detailplanung bis zur Realisierung von Rechenzentren und Serverräumen nach DIN EN 50600.**

# ALLHEILMITTEL IoT-PLATTFORMEN?

Als Head of Solutions von tresmo ist Marcel Möstel verantwortlich für das Lösungsportfolio und dessen stetige Weiterentwicklung sowie die Kundenberatung rund um innovative IoT-, Cloud- und App-Lösungen – und die Nachfrage nach diesen Lösungen wächst nicht erst seit der Pandemie. Seit 2012 begleitet tresmo Kunden unterschiedlichster Branchen und Unternehmensgrößen in engen Partnerschaften auf dem Weg zu eigenen digitalen Produkten und Services.

Von Stephanie Englert

**IoT 4 Industry & Business: IoT-Plattformen sind das „Allheilmittel" für erfolgreiche IoT-Lösungen – ja oder nein?**

**Marcel Möstel:** Leider ist eine IoT-Plattform – im Idealfall standardisiert und sofort einsatzbereit – nicht das Zaubermittel für die Bereitstellung erfolgreicher IoT-Anwendungen. Es braucht viele kleine Schritte zum Erfolg, denn die IoT-Plattform ist tatsächlich nur ein kleiner Bestandteil der eigentlichen IoT-Lösung. Mit ERP- oder CRM-Systemen, Analytik, Geschäftslogik, Anwendungen, Apps, Gateways und natürlich den Produkten, die miteinander kommunizieren müssen, benötigen Unternehmen noch eine ganze Menge mehr als die Plattform selbst für den eigentlichen digitalen Erfolg.

Außerdem dürfen die beteiligten Akteure aus Vertrieb, Marketing, Support und Technik, einschließlich der Betreiber für die gesamte Lösung, die Partner für die Implementierung und die Nutzer, die im besten Fall vom Endergebnis profitieren sollen, nicht vergessen werden. Man stellt sich IoT-Vorhaben am besten wie eigene Unternehmungen innerhalb des Unternehmens vor, denn es geht hier oft nicht nur um IT.

**IoT: Auf was müssen Kunden achten, wenn sie sich für den Einsatz von IoT-Plattformen entscheiden?**

**Möstel:** Geht es an den Aufbau und die Konzeption der eigentlichen Plattform, stellen sich einige Fragen, über die sich Unternehmen vorab bewusst werden sollten: Hören wir auf den

Markt oder unsere Intuition? Nutzen wir eine Standard-Applikation oder eine auf uns zugeschnittene Lösung? Und essenziell – Stichwort Make-or-Buy: Machen wir das Ganze selbst oder geben wir das Projekt in die Hände erfahrener Expert:innen?

**IoT: Gibt es Unterschiede je nach Firmengröße oder Branchen?**
**Möstel:** Letztlich ist jedes IoT-Projekt einzigartig, denn es geht immer darum, innovative Lösungen zu entwickeln, mit denen ein Kundenproblem gelöst wird bzw. der Anbieter einen neuen Mehrwert für seine Zielgruppe schafft. Daher gleicht kein IoT-Projekt dem anderen und es gibt so gut wie nie – weder für bestimmte Unternehmensgrößen noch für einzelne Branchen – pauschale Standardlösungen, die einfach aus der Schublade entnommen und in die Praxis umgesetzt werden können.

**IoT: Was zeichnet eine „optimale" IoT-Plattform aus?**
**Möstel:** Die "optimale" IoT-Plattform gibt es pauschal nicht, sondern richtet sich immer nach der jeweiligen Problemstellung und dem Mehrwert, den das Unternehmen für seine Zielgruppe generieren möchte. Die Frage nach der passenden Technologie und der richtigen Plattform sollte immer der Betrachtung des Kundennutzens nachgelagert sein. Wenn im Detail klar ist, was das Team für die Zielgruppe erreichen will, ergibt sich die technologische Lösung meist nahezu automatisch. Wollen die Verantwortlichen zum Beispiel für eine sehr technische Zielgruppe (z.B. die eigenen Servicetechniker) eine erste Condition-Monitoring-Lösung schaffen, dann darf durchaus mal geschaut werden, ob nicht bekannte Hardware- oder Regeltechnik-Hersteller schon eine kleine Out-of-the-box-Lösung anbieten.
Geht es aber im ersten Schritt darum, direkt auf die Kund:innen zuzugehen und eine marktreife Monitoring-Applikation anzubieten, kommt man schnell in komplexe Abwägungen, ob nicht eine erweiterbare Lösung auf Microsoft Azure oder AWS zukunftsweisender ist.

**IoT: Woran kann eine erfolgreiche Implementierung einer IoT-Lösung scheitern? Was sind die größten „Fehler", die gemacht werden. Kann man hier Pauschalisieren?**
**Möstel:** Es gibt fünf zentrale Hürden, an denen viele IoT-Projekte in der Praxis scheitern:

1. Wenn Unternehmen den Kundennutzen den technischen Anforderungen unterordnen, gerät der Business Value in den Hintergrund und es besteht die Gefahr, dass das Team an den Marktbedürfnissen vorbei entwickelt.
2. Bei den vielen technischen Buzzwords, die rund um IoT kursieren, entstehen oft versehentlich unterschiedliche Erwartungshaltungen bei verschiedenen Stakeholdern. Eine transparente, klare Kommunikation ist daher wesentlich, um Missverständnissen von Anfang an vorzubeugen.
3. Ohne starke Partner gelingen die wenigsten IoT-Projekte. Daher gilt es, diese rechtzeitig einzubinden und auf eine vertrauensvolle Zusammenarbeit zu setzen, in der alle mit dem gleichen Mindset an der bestmöglichen Kundenlösung arbeiten.
4. Die Kosten in IoT-Projekten verlaufen viel dynamischer als Unternehmen es von anderen Vorhaben gewöhnt sind. Daher gilt es, den gesamten Lebenszyklus einer IoT-Lösung bei der Budgetplanung zu betrachten.

**Marcel Möstel**
**Head of Solutions bei tresmo**

„Einige Entscheider werden schon mutiger und trauen sich, innovative Projekte anzugehen."

5. Steht das Management nicht zu 100 % hinter dem IoT-Projekt, ist es oft schon zu Beginn zum Scheitern verurteilt. Daher sollten Teams zunächst prüfen, ob sie sich auf den Rückhalt der Führungsebene verlassen können und sich direkte Kommunikationsebene etablieren lässt, auf deren Basis ein erfolgreiches Projekt gelingen kann.

**IoT: Sind sich viele Kunden nicht über ihr eigentliches Ziel/den Mehrwert, den sie erreichen wollen, bewusst?**
**Möstel:** Es besteht durchaus die Gefahr, dass Unternehmen über die Auswahl der passenden Technologie und die Bewertung unterschiedlicher Lösungen den Kundennutzen aus dem Fokus verlieren. Das kommt alleine schon durch die hohe Komplexität und ist eine große Gefahr für den Erfolg eines IoT-Projekts. Denn dieser steht und fällt mit dem generierten Mehrwert für den Markt. Daher tun Teams gut daran, das Ziel – die Generierung von Nutzen für die Zielgruppe – stets im Blick zu behalten.

**IoT: Inwiefern haben gerade die vergangenen Monate zu einer Bewusstseinserweiterung bei Unternehmen hinsichtlich IoT-Lösungen und -Nutzen etc. geführt?**
**Möstel:** In den letzten Monaten ist in vielen Unternehmen deutlich geworden, dass IoT-Lösungen dazu beitragen können, das eigene Geschäft noch erfolgreicher aufzustellen. Einige Entscheider werden schon mutiger und trauen sich, innovative Projekte anzugehen. Insbesondere das Thema Usability wird aktuell immer wichtiger. Das bedeutet konkret, auch Kund:innen im B2B-Umfeld eine professionelle UI und UX zu bieten.

**IoT: Sind die Teams/Mitarbeiter der Kunden/Unternehmen für eine IoT-Plattform gut aufgestellt bei Ihren Kunden oder scheitert es auch an deren „Know-how"? Wird hier eventuell falsch „gespart"?**

>>

**Möstel:** So verlockend die Herausforderung für Unternehmen sein mag, sich die passende technologische Lösung für ihren Nutzen selbst zu kreieren, so wenig rentabel ist es häufig. Wenn sie ein Problem erkennen, das sie für ihre Kund:innen lösen können, sind Betriebe viel besser beraten, sich an erfahrene Partnerunternehmen zu wenden und bestehende technologische Ansätze zu nutzen. Denn die Frage ist weniger: Können wir das selbst machen? als vielmehr: Sollten wir das selbst machen?
Auf dem Weg zur IoT-Plattform kann man aufgrund der heutigen technologischen Infrastruktur viele kluge Make-or-Buy-Entscheidungen auf unterschiedlichsten Ebenen treffen. Dafür muss man sich aber gut auf dem Tech-Markt auskennen.

**IoT: Kurz zwischengefragt: Worauf sollten Unternehmen bei der Auswahl des richtigen Partners denn überhaupt achten?**
**Möstel:** Im ersten Schritt lohnt es sich, genau zu hinterfragen, ob es sich beim jeweiligen Partner um einen Berater/Systemintegrator oder einen (eigenen) Lösungsanbieter handelt. Unabhängige Berater sind in der Praxis oft unbefangener und können sich besser auf den Kundennutzen konzentrieren und auf dieser Basis agnostisch die richtigen Lösungen entwickeln. Beim Lösungsanbieter haben Unternehmen oft einen operativen Vorteil, weil dort schon viele Prozesse um die eigene Lösung herum optimiert wurden. Was direkt zum zweiten Punkt führt: Für den Partner sollte – ebenso für das Unternehmen selbst – der Mehrwert für die Zielgruppe immer im Fokus stehen. IoT sollte nicht als Selbstzweck dienen, sondern einen echten Nutzen hervorbringen – sonst können Unternehmen auch darauf verzichten.
Außerdem ist der richtige Partner immer dazu in der Lage, trotz seines Know-how-Vorsprungs die technischen Zusammenhänge für das gesamte Projektteam verständlich zu kommunizieren. Nur so kann Missverständnissen rechtzeitig vorgebeugt werden. Da IoT-Projekte flexible Budgets, dynamische Zeitpläne und eine auf Veränderung eingestellte Unternehmenskultur erfordern, ist auch die Erfahrung ein wichtiger Faktor. Je mehr innovative Projekte das Team des Partners bereits begleitet hat, desto besser kann es dabei unterstützen, den Change im eigenen Unternehmen voranzutreiben.

> „In vielen Unternehmen sind IoT-Initiativen sowohl komplex als auch kulturell anspruchsvoll."

**IoT: Was können Sie für ein besseres Verständnis bei Kunden tun, so dass „erste" Fehler in Bezug auf IoT-Plattformen vermieden werden können und es mehr um den Mehrwert geht als um das Verständnis, was IoT-Plattformen eigentlich sind/können?**
**Möstel:** Jedes Unternehmen sollte sich in Innovationsprojekten zwei Schlüsselfragen stellen: Einerseits jene nach dem Ziel, andererseits die nach dem Mehrwert für den Markt. Dabei ist und bleibt der zentrale Faktor der Mensch. Die Technik ist nur ein untergeordneter Bestandteil von innovativen Projekten und maximal ein Mittel zum Zweck. Umso wichtiger ist es, dass die Verantwortlichen die Zielgruppe nicht aus den Augen verlieren. Dazu gehören sowohl die eigenen Mitarbeiter:innen, Kund:innen als auch Partner:innen. In vielen Unternehmen sind IoT-Initiativen sowohl komplex als auch kulturell anspruchsvoll und machen es notwendig, für solche Projekte ganz eigene Teams zu etablieren, die den hohen Anforderungen gerecht werden können. So kann die Entwicklung von wertvollen IoT-Lösungen, die einen signifikanten Anteil am Unternehmenserfolg haben, erfolgreich sein.

**IoT: Vielen Dank!**

**www.tresmo.de**

**Gerade bei IoT-Projekten sollte man auf den richtigen Partner setzen.**

# „MEINE LEIDENSCHAFT FÜR DIE DIGITALE WELT WURDE MIR IN DIE WIEGE GELEGT“

Für René Blaschke ist das Internet der Dinge nicht nur eine zukunftsweisende Technologie – es ist seine Leidenschaft. Schon seit seiner Kindheit interessiert er sich brennend für intelligente Technologien und digitale Trends. Als Head of Product Management, IoT bei B&R gestaltet er die Zukunft der Digitalisierung mit.

„Seit ich mich erinnern kann, haben mich Computer fasziniert“, So René Blaschke. Und diese Faszination hat nie nachgelassen: Bereits mit acht Jahren hat er seinen ersten PC bekommen. Kurz darauf hat er ihn komplett zerlegt und wieder zusammengebaut. „Es hat mich einfach interessiert was in dem PC-Gehäuse steckt.“ Mittlerweile hat Blaschke seine Leidenschaft zum Beruf gemacht und ist für das Produktmanagement des IoT-Portfolios von B&R verantwortlich. „Das ist eine ungemein spannende Aufgabe, denn der digitale Wandel zwingt viele Unternehmen dazu, ihre Geschäftsmodelle grundlegend zu überdenken“, sagt der IoT-Spezialist. „Wir unterstützen unsere Kunden dabei, gestärkt aus diesem Prozess herauszugehen.“

**Vom intelligenten Stromzähler zur intelligenten Maschine.** Vor seiner Zeit bei B&R war Blaschke in der Energiebranche tätig und hat sich unter anderem intensiv mit Smart Grids und Smart Metern auseinandergesetzt. „Ich bin quasi von der Energie 4.0 zur Industrie 4.0 gewechselt“, sagt Blaschke mit einem Augenzwinkern. „Dieser Wechsel ist weniger gravierend, als man vielleicht im ersten Moment denken mag, denn zwischen diesen beiden Welten gibt es viele Analogien“.
So hatte sich Blaschke zuvor mit intelligenten Energienetzen und deren Teilnehmern beschäftigt, während er heute die Kommunikation zwischen Maschinen und Anlagen im Blick hat. „Was für mich früher der Stromzähler war, ist heute die Maschine“, so Blaschke. „Es dreht sich alles um die intelligente Vernetzung aller Teilnehmer eines Systems. Die Konzepte, Methoden und Herausforderungen sind in beiden Welten sehr ähnlich.“ Noch heute beschäftigt sich Blaschke neben seiner Tätigkeit bei B&R mit Energie 4.0. Als Lektor an der Fachhochschule Salzburg hält er unter anderem Vorlesungen über Smart Grids und das Design von Systemarchitekturen.

**Neue Geschäftsmodelle entwickeln.** Seine Ausbildungen als Elektro-, Energie- und EDV-Techniker sowie sein Master im Bereich Informationstechnik & System-Management kommen dem 35-Jährigen bei seinen Aufgaben als Produktmanager zugute. „Wenn ich in eine Fabrikhalle komme, rede ich nicht nur theoretisch von Netzwerken und Kommunikation. Ich weiß, wie eine Maschine verkabelt wird und was in einem Schaltschrank passiert.“
So kann er die Herausforderungen der Kunden gut nachvollziehen. „Ein enger Austausch mit unseren Kunden ist mir besonders wichtig“, betont der IoT-Spezialist. „Wir reden offen über mögliche Schwächen im Prozess und finden auf diese Weise gemeinsam eine optimale Lösung.“ Darüber hinaus hat Blaschke auch einen Master im Bereich Betriebswirtschaftslehre. „Besonders spannend ist es, mit Kunden neue Geschäftsmodelle zu entwickeln und Dinge zusätzlich durch die Business-Brille zu betrachten.“

**Digitale Zukunft.** In naher Zukunft wird sich IoT innerhalb von B&R weiter zu einem zentralen Standbein entwickeln. „Wir werden für unsere Kunden eine neue Basis schaffen, die es ganz einfach macht, komplexe Daten zu beherrschen und Mehrwerte zu schaffen“, kündigt Blaschke an. Schon im Jahr 2018 habe die Produktentwicklung begonnen. In den nächsten Monaten soll mit einigen Pilotprojekten gestartet werden, kündigt Blaschke an.

**www.br-automation.com**

**René Blaschke**
**Head of Product Management, IoT bei B&R**

„Wenn ich in eine Fabrikhalle komme, rede ich nicht nur theoretisch von Netzwerken und Kommunikation.“

# DAS KALKULIERBARE RISIKO

Eine im vergangenen Jahr veröffentlichte Untersuchung namens „In zehn Schritten zum erfolgreichen Maschinellen Lernen im Unternehmen" besagt, dass Investitionen in diese Technologien sich durchaus für alle Betriebe und Betriebsgrößen früher oder später lohnen werden. Doch woran scheitern viele? Daniel Metzger, Regional Vice President Central & Eastern bei Cloudera, gibt Antworten. Von Stephanie Englert

Anwendungen für Künstliche Intelligenz (KI) und Maschinelles Lernen (ML) liegen in Österreich stark im Trend. Zu dieser Einschätzung kommt eine Studie von Cloud Provider Interxion, die Ende 2020 veröffentlicht wurde. Demnach nutzen fünf Prozent der heimischen Studienteilnehmenden KI bereits in verschiedenen Anwendungsfeldern. 18 Prozent setzen die Technologie in einem ersten Anwendungsszenario ein. Weitere 34 Prozent sind gerade dabei, KI zu testen. Unmittelbar vor diesem Schritt stehen 13 Prozent, die planen, KI kurzfristig anzuwenden.

Zudem wollen in den nächsten zwei Jahren 30 Prozent KI für einen ersten Anwendungsfall nutzen. Als größte Hindernisse bei der Implementierung führen die Studienautoren die Kosten (66 Prozent), den Mangel an technischer Expertise (56 Prozent) und die fehlende Einbettung in die Unternehmensstrategie (41,3 Prozent) an. In der Praxis gerät ein Unternehmen jedoch schnell in die Bredouille, soll es die Lücke zwischen dem Experimentieren mit ML und dem Einsetzen der Technologie in Produktionsumgebungen schließen.

**IoT 4 Industry & Business: In der vorliegenden Untersuchung heißt es: „In der Praxis gerät ein Unternehmen jedoch schnell in die Bredouille, soll es die Lücke zwischen dem Experimentieren mit ML und dem Einsetzen der Technologie in Produktionsumgebungen schließen." Wo genau liegen die Herausforderungen für Betriebe bzw. woran scheitern sie womöglich?**

**Daniel Metzger:** Um Machine Learning in Unternehmen erfolgreich umzusetzen, muss die Grundlage für ML – vorhandene Daten, Datenströme und die Fähigkeit, diese in großen Mengen zu speichern – gewährleistet sein. Für den konkreten ML-Einsatz

**Investitionen in Machine Learning und geeignetes Fachpersonal zahlen sich früher oder später für alle aus.**

ist es wichtig, zuvor bestehende Datensilos, die nur für einzelne Abteilungen verfügbar sind, aufzubrechen. So stellen Unternehmen die notwendigen Weichen für den ganzheitlichen Einsatz von ML-Technologien. Dabei bietet die Umsetzung in Produktionsumgebungen, beispielsweise hinsichtlich vorausschauender Wartung, vielversprechende Vorteile.

**IoT: Inwiefern?**
**Metzger:** Damit Unternehmen die angesprochenen Vorteile nutzen können, müssen sie über Fachkräfte verfügen, die nicht nur mit ML-Technologien, sondern auch mit der Produktionstechnik vertraut sind. Denn um vom Experimentieren mit ML zum konkreten Einsatz der Technologie in Produktionsumgebungen zu gelangen, gibt es bisher keine Musterverfahren.
Deshalb ist es für Unternehmen besonders wichtig, ihre eigenen Modelle zu verstehen und sie auch über die Experimentierphase hinweg fortlaufend anzupassen und kontinuierlich zu optimieren.

**IoT: Was bedeutet das für die Unternehmenn?**
**Metzger:** Es mag banal klingen, aber Unternehmen müssen auf die Funktionalität ihrer Modelle und ihr wirtschaftliches Potenzial vertrauen. Denn um wettbewerbsfähig zu bleiben, müssen Unternehmen KI-gestützte Erkenntnisse in die Tat umsetzen. Dabei zählt bereits der Versuch, andernfalls ist ein Scheitern des erfolgreichen Einsatzes von ML in Produktionsumgebungen vorprogrammiert.

**IoT: In der Studie heißt es auch, Scheitern gehöre dazu. So stellt sich mir die Frage: um welchen Preis? Wird bei derartigen Aussagen nicht später in der Praxis „sinnlos" Geld verspielt – Geld, das Unternehmen womöglich auch nicht „über" haben?**
**Metzger:** Dies ist ein Risiko, das Unternehmen eingehen müssen. Wobei es sich wie bereits bei der vorherigen Frage aufgezeigt um ein kalkulierbares Risiko handelt. Zum einen wird ML eine zunehmend wichtigere Rolle für Unternehmen einnehmen, um sich im digitalen Wettbewerb weiterhin behaupten zu können. Zum anderen trägt datengesteuertes Lernen entscheidend dazu bei, die Wettbewerbsfähigkeit auch zukünftig zu sichern.
Dabei ermöglicht ML Unternehmen ihre Kundenerlebnisse zu verbessern, ihre Effizienz zu optimieren und nicht zuletzt auch neue Geschäftsfelder und Einnahmequellen zu ermitteln. Wichtig ist dabei, dass die Unternehmen zu Beginn Einsatzbereiche definieren, zu denen sie die Fachkräfte haben und die Modelle genau definieren können, dann lässt sich ein mögliches Scheitern zumindest verringern. ,

**IoT: Könnten Sie noch konkreter werden anhand eines Beispiels?**
**Metzger:** Meine Annahmen können auch durch die IDG-Studie Machine Learning 2020 verdeutlicht werden: Rund 22 Prozent der ML-Projekte verschaffen laut dieser Unternehmen einen sofortigen Nutzen, weitere 22 Prozent nach vier bis acht Wochen. Nach drei Monaten können die meisten Betriebe, 27 Prozent, positive Effekte der ML-Lösungen verzeichnen.

**Daniel Metzger**
**Regional Vice President Central & Eastern bei Cloudera**

„Auf KI basierende, automatisierte Systeme werden zunehmend bei Entscheidungsprozessen in verschiedensten Anwendungsfeldern eingesetzt."

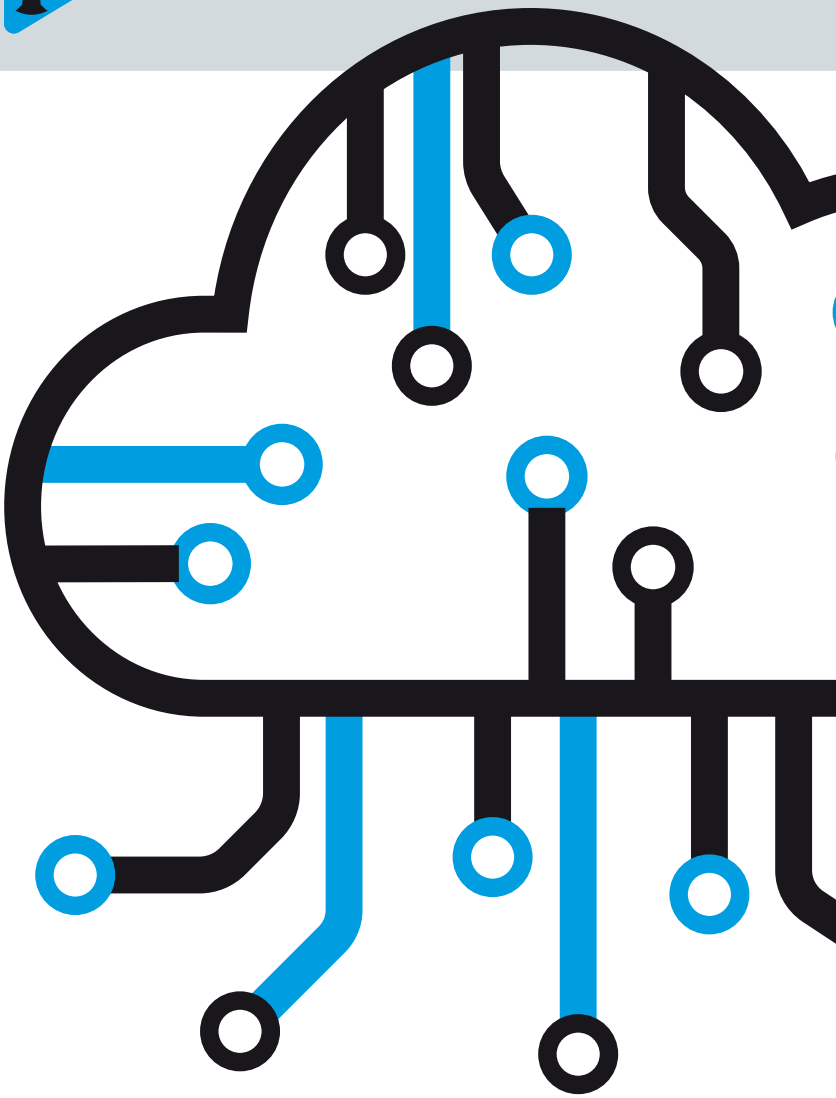
**IoT: Demnach machen Investitionen also Sinn?**
**Metzger:** Investitionen in die Technologie sind daher sicher nicht umsonst. Dabei ist die Größe der Unternehmen nachrangig, schließlich besitzen alle Betriebe interne und externe Daten, die insgesamt die Basis für datengetriebene Geschäftsmodelle bilden. Unternehmen, die in eine Datenstrategie investieren, sichern sich also langfristig einen Vorsprung gegenüber ihrer Konkurrenz.

**IoT: Weiters wird in der Studie das Thema „ethische KI" angesprochen. Inwiefern spielt diese eine Rolle in Betrieben und künftigen KI-Anwendungen?**
**Metzger:** Auf Künstlicher Intelligenz basierende, automatisierte Systeme werden zunehmend bei Entscheidungsprozessen in verschiedensten Anwendungsfeldern eingesetzt. Dass KI-gestützte Systeme verantwortungsvoll betrieben werden, muss auch für Unternehmen im Vordergrund stehen. Zwar gibt es noch keine allgemeingültigen Kriterien dafür, was ein System ethisch vertretbar macht, doch trotzdem müssen Unternehmen unbeabsichtigte Folgen im Auge behalten, nicht zuletzt, um Klagen zu vermeiden.
Schließlich können sie nur so gewährleisten, mögliche Verletzungen von Werten wie Fairness, Achtung der Privatsphäre und Transparenz zu vermeiden und weder Kunden noch anderen Personen zu schaden. Handeln Unternehmen dabei nachlässig, kann das sowohl rechtliche als auch rufschädigende und regulatorische Folgen für sie haben. Neben der Vermeidung dieser Risiken bringt das Achten auf ethische KI aber auch weitere Vorteile mit sich. Die für die Umsetzung ethischer KI sorgfältig eingesetzten Technologien, wie eine gute Überwachung und Steuerung, können das Geschäft positiv beeinflussen.

**IoT: Vielen Dank!**

**www.cloudera.com**

# OEE UND IIoT



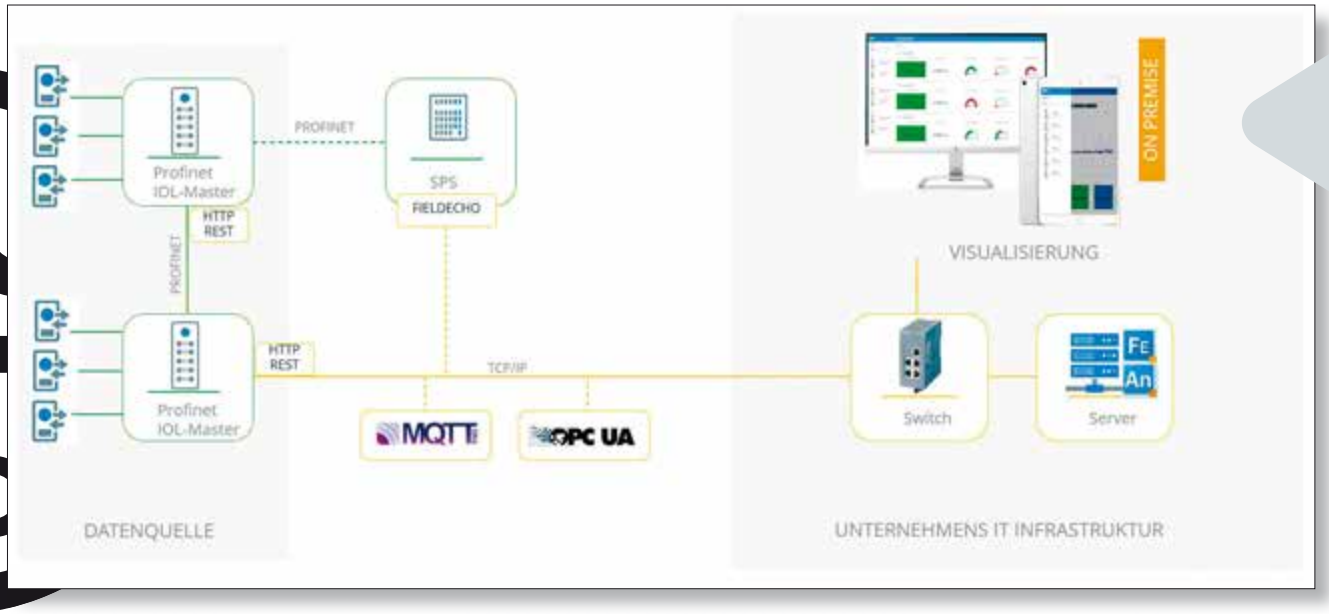
OEE und IIoT sind in aller Munde. Doch was bedeuten diese Begriffe und wie stehen sie zueinander in Bezug? OEE steht für Overall Equipment Effectiveness oder zu Deutsch: Gesamtanlageneffektivität. Die Kennzahl beantwortet die Frage „Wie effektiv arbeitet meine Anlage?“.

Für die eingangs erwähnte Berechnung werden drei Faktoren herangezogen: Verfügbarkeit, Qualität und Leistung. Die Verfügbarkeit sagt aus, in wieviel der geplanten Zeit tatsächlich produktiver Betrieb stattfindet. Die Leistung zeigt, wieviel Stück bezogen auf die geplante Anzahl tatsächlich produziert wurden. Die Qualität sagt aus, wie viele Teile bezogen auf die gesamte Produktionsmenge bei der Qualitätskontrolle bestanden haben. Erfasst man diese Daten mit den passenden Sensoren und multipliziert die drei Faktoren, ergibt dies die OEE. Soweit so gut – nur wo ist jetzt die Besonderheit und der Bezug zu IIoT?

IIoT steht für „Industrial Internet of Things“, also die Vernetzung von Geräten im industriellen Kontext. In der Praxis sieht das so aus, dass Sensoren über einen IO-Link Master (entsprechend einem digitalen I/O-Modul in klassischen Steuerungen) an eine SPS angebunden werden, damit diese mit Hilfe der Sensordaten den Prozess entsprechend steuern und regeln kann. Mittels Rest API – eine Schnittstelle, die der IO-Link Master unterstützt – kann auf Anfragen aus dem Netzwerk reagiert werden. Somit ist der „IIoT-Aspekt“ erfüllt. Die Anfrage sieht aus wie eine klassische URL und spezifiziert, welche Daten abgefragt oder geschrieben werden sollen. Die Antwort ist ein Textobjekt im sogenannten JSON-Format, das die gewünschten Informationen im Klartext enthält.

**Kommunikation gewährleistet.** Umgelegt auf unser Beispiel bedeutet dies, dass der IO-Link Master wie gewohnt via Profinet mit der SPS kommuniziert, aber zusätzlich z.B. über einen Switch auch in ein anderes Netzwerk mit eingebunden werden kann. Somit kann einerseits die SPS ungestört ihre Daten austauschen, und andererseits können die Sensordaten auch von anderen Geräten innerhalb des Netzwerks über die Rest API abgerufen werden. Beispielsweise einem ERP-System, einer Visualisierungssoftware, oder einem Programm zur Berechnung der OEE. Das hat den Vorteil, dass die SPS nicht in die Datenweitergabe involviert ist. Bezogen auf die Ermittlung der OEE in einer Anlage bedeutet das: Ein Computersystem kann die Sensordaten direkt über den IO-Link Master abfragen, anstatt den mühsamen Weg über die SPS zu gehen. Ebenso bedeutet das, dass eine SPS nicht für eine OEE-Ermittlung notwendig ist. Sind im bestehenden System beispielsweise keine Sensoren vorhanden, die Verfügbarkeit, Qualität oder Leistung messen können, dann können diese über einen IO-Link Master nachgerüstet werden, ohne diesen überhaupt mit der SPS verbinden zu müssen. Dies ist insbesondere dann ein Vorteil, wenn es um eine alte Anlage geht, die entweder keine SPS hat, oder das Motto „Never change a running system“ gilt.

**Daten auslesen.** In großen Anlagen kann es auch hilfreich sein, ein Tool wie Field Echo von Sick einzusetzen. Diese Software wird auf einem Computer installiert, der sich im selben Netzwerk wie die SPS befindet. Es muss lediglich ein einziger Funktionsblock von der SPS aufgerufen werden, dann können auf einen Schlag die Sensordaten aller IO-Link-Sensoren (herstellerunabhängig), die mit der SPS verbunden sind, über das Netzwerk ausgelesen werden. Der Computer, auf dem Field Echo installiert ist,




**Kommunikation im IIoT**

kann ebenso eine Rest API zur Verfügung stellen und somit Sensordaten für eine OEE-Auswertung oder andere Zwecke zur Verfügung stellen.

Diese Vernetzung bietet neben OEE-Berechnung noch viele weitere Möglichkeiten, vor allem hinsichtlich Wartung und Instandhaltung. Genauso wie Daten für eine OEE-Berechnung kann man auch Daten, die den Zustand der Sensoren und Aktoren aufzeigen, über die Rest API abfragen. Hier kommt der Vorteil von IO-Link-Geräten voll zum Tragen, diese liefern nicht mehr nur ein Schaltsignal, sondern z.B. Messwerte, Einstellungen, … und eben auch Diagnosedaten.

Nehmen wir eine Abfüllanlage als Beispiel. Hier werden oft Reflexionslichtschranken eingesetzt, um transparente Flaschen zu erkennen. Diese Sensoren werden auf einen Reflektor eingelernt und müssen anhand geringster Unterschiede in der Lichtdämpfung erkennen, ob sich zwischen Sensor und Reflektor eine Flasche befindet oder nicht. Wenn sich nun mit der Zeit Staub am Reflektor absetzt, wird der Sensor irgendwann fälschlicherweise schalten. Bei Sensoren mit klassischem Schaltausgang wird die Verschmutzung erst erkannt, wenn er dauerhaft schaltet. Derselbe Sensor mit IO-Link liefert einen sogenannten Quality-of-Run-Wert, der sensorintern berechnet wird und einen Indikator bietet, wie gut die Prozessqualität ist und ob eine Reinigung notwendig ist. So kann man frühzeitig und proaktiv, ohne Fehlverhalten oder ungeplantem Stillstand, reagieren.

**Kreativität zählt.** Es können aber nicht nur vorbereitete Sensorwerte verwendet werden, der Kreativität sind keine Grenzen gesetzt. Identifiziert man Sensoren oder Messstellen in einer Anlage, deren Daten in Bezug zueinander gesetzt eine Aussagekraft für den Anlagenzustand ergeben, so kann man diese unkompliziert und unabhängig von der SPS über das Netzwerk erhalten und auswerten. Durch diese Unabhängigkeit von der SPS ist es genauso bei alten Anlagen möglich. Werden z.B. mehrere Aktoren über eine Kette synchronisiert, so kann aus einer Veränderung des Timing-Verhaltens beispielsweise auf eine Kettenlängung geschlossen werden. Durch die Erfassung und Zählung von Markierungen auf einem Band und dessen Antriebsrolle kann Schlupf erkannt werden.

Die vielfältige Vernetzung industrieller Geräte hat das Potenzial, auf einfache Weise Daten zu verknüpfen, um unkompliziert und mit wenig Entwicklungsaufwand Zusatzinformationen zu erhalten. Sei es eine einfache Produktzählung für die Statistik, oder eine Lösung für Predictive Maintenance.

**www.sick.at**

Der Autor
**David Pescha**
... ist Market Application Engineer Presence Detection & Industrial Instrumentation bei Sick Österreich.

# DAS *sensible* SYSTEM SCHÜTZEN

Ali Carl Gülerman, CEO von Radar Cyber Security, betreibt in Wien das größte Cyber Defense Center Europas auf Basis einer eigenentwickelten Technologie. Er begab sich gemeinsam mit dem Bestseller-Autor Marc Elsberg (Blackout) kürzlich auf eine Spurensuche durch aktuelle Szenarien und Bedrohungen im Bereich Cyber Defense.

Cyberangriffe nehmen rasant zu. Die entscheidende Frage dabei ist: Was geschieht tatsächlich bei einem Cyberangriff und ist die aktuelle Bedrohungslage nur ein Hype oder bittere Realität? Der österreichische Schriftsteller Marc Elsberg führte in seinen Ausführungen vor einigen Monaten durch die dramatischen Phasen eines Strom-Blackouts und skizzierte dessen Auswirkungen auf die kritische Infrastruktur und unsere gesamte Gesellschaft. Das vom Erfolgsautor intensiv recherchierte und erlebbar gemachte Szenario in seinem Roman „Blackout" ist heute nicht mehr nur Fiktion, sondern mittlerweile zu einer ganz realen Bedrohung geworden, an der Europa zuletzt im Jänner 2021 haarscharf vorbeigeschrammt ist.

**Ali Carl Gülerman**
**CEO von Radar Cyber Security**

„Wir müssen uns auf eine Steigerung der Resilienz in der kritischen Infrastruktur konzentrieren."

„Die IT-Infrastruktur ist mittlerweile zum sensiblen Nervensystem unserer gesamten Gesellschaft geworden. Unzählige Systeme hängen voneinander ab und sind miteinander verbunden. Bereits eine kleine Störung in einem Teilbereich kann massive Auswirkungen auf die Funktionsfähigkeit und Belastbarkeit des Gesamtsystems bewirken. Wir haben seit dem Erscheinen meines Buches vor zehn Jahren noch immer nicht gelernt, vernünftig mit dieser Tatsache umzugehen und strapazierfähige Fall-Back-Systeme zu entwickeln. Es ist wohl wie in der Liebe: Man weiß erst, was man hatte, wenn man es verloren hat," so Marc Elsberg.

**Mit Cybersecurity die Digitalisierung sicher vorantreiben.** Europa befindet sich mitten im digitalen Wandel: Die Europäische Kommission hat „Europas digitale Dekade" ausgerufen und setzt mit klaren Vorgaben einen entschlossenen Kurs auf ein digital gestärktes Europa bis 2030. Doch die zunehmende Digitalisierung birgt Gefahren, die sich massiv auf die analoge

**Um Bedrohungen verantwortungsvoll und entschlossen zu begegnen, bedarf es einem digitalen Sicherheitsnetz.**

Welt auswirken können: Seien es zuletzt Hacker-Angriffe im Mai 2021 auf die größte Pipeline der USA und die irische Gesundheitsbehörde oder ein Vorfall in einem kroatischen Umspannwerk Anfang des Jahres, der Europa an den Rand eines Strom-Blackouts führte. In Anbetracht der aktuellen Ereignisse gewinnt das Thema Cybersicherheit immer mehr an gesellschaftlicher Relevanz. So definiert auch das österreichische Bundesheer in seiner jährlichen „Sicherheitspolitischen Jahresvorschau“ Cyberangriffe als eine hohe und aktuelle Gefährdung für das Gesamtsystem.

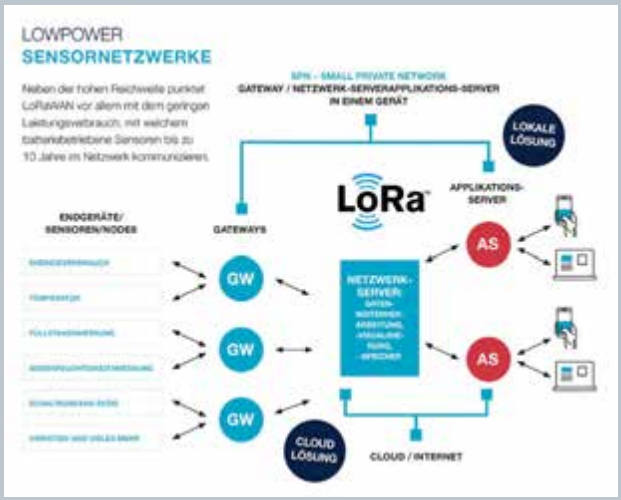
Um solchen Bedrohungen verantwortungsvoll und entschlossen zu begegnen, bedarf es einem digitalen Sicherheitsnetz. Ali Carl Gülerman, CEO von Radar Cyber Security, betreibt mit seinem Team das eingangs erwähnte größte Cyber Defense Center Europas auf Basis einer eigenentwickelten Technologie – mitten im Herzen von Wien. Egal ob Energie-, Finanz- oder Gesundheitssektor – tagtäglich wird mit State-of-the-Art-IT-Security „made in Europe“ die Sicherheitslage zahlreicher Einrichtungen in der kritischen Infrastruktur überwacht, vor Cyberangriffen geschützt und somit deren Stabilität garantiert. Zehn Jahre Erfahrung, umfassendes Know-how und österreichische Hoch-Technologie: Radar Cyber Security ermöglicht eine 360° Cyber Defense und analysiert permanent das aktuelle Sicherheitsrisiko der IT-Systeme in allen Branchen sowie im öffentlichen Dienst. Damit wird nicht nur die Erkennungszeit bei Angriffen massiv reduziert, sondern auch mögliche Sicherheitslücken werden rasch erkannt und geschlossen. Die europäische Technologie ist vom so genannten Patriots Act nicht betroffen und damit für US-amerikanische Verfolgungsbehörden nicht zugänglich.

**Einige Hundert Cyberangriffe pro Stunde.** „Die Angriffe nehmen zu. Sei es durch einzelne Hacker, die organisierte Kriminalität oder durch Staaten. Aber nicht nur quantitativ wird der Druck stärker, auch die Qualität der Angriffe ist massiv gestiegen. Es vergehen oft Wochen und Monate zwischen Infiltration und dem eigentlichen Hack. Die Diebe sind aber nicht völlig unsichtbar und wir können sie mit unseren Methoden entdecken, wenn davor Präventivarbeit geleistet wurde“, berichtet Ali Carl Gülerman. Es gibt derzeit einen rasant wachsenden Markt für Cyberkriminalität und die Profis von Radar Cyber Security erkennen bei Cyberangriffen mittlerweile Businessmodelle mit ausgeklügelter Arbeitsteilung. Man bestellt im Darknet einen Angriff auf das gewünschte Ziel, das dann erpresst wird. Den Gewinn teilt man sich mit den Hackern. Je bedeutsamer eine Branche für die Gesellschaft ist, desto drastischer die Auswirkungen. Bei erfolgreichen Cyberangriffen auf Krankenhäuser kann es etwa sein, dass lebensrettende Operationen nicht stattfinden können. Software alleine kann das Problem nicht lösen:

„Wir müssen uns auf eine Steigerung der Resilienz in der kritischen Infrastruktur konzentrieren und auf regelmäßige Cybersecurity-Übungen mit Szenario-Trainings setzen. Leider können wir einmal erfolgte Hacks nicht mehr rückgängig machen – deshalb ist die Präventivarbeit so wichtig. Und das Thema ist kein Spleen von IT-Verrückten. Denn neben den Lieferketten oder Cash-Systemen von Unternehmen und Organisationen kann es in gewissen Branchen wie dem Lebensmittel-Einzelhandel bis hin zur massiven Verunsicherung der Bevölkerung durch Lieferengpässe gehen. Und damit kann man Politik machen. Mit Cybersecurity schützen wir deshalb auch unsere europäischen Werte“, so Gülerman abschließend.

**www.radarcs.com**

TECHNOLOGIE-NEWS




# LoRaWAN-ÜBERWACHUNGSLÖSUNGEN VOR ALLEM BEI KOMMUNEN IMMER MEHR GEFRAGT

**Funk-Sensornetzwerke mit sehr geringem Energieverbrauch**

Innovative Konnektivitätslösungen wie LoRaWAN (Long Range Wide Area Network) sind auf dem Vormarsch und gehören zukünftig zu unserem Alltag. Die Technologie ermöglicht das energieeffiziente, kostengünstige und sichere Senden von Daten über lange Strecken hinweg. Auf diese Weise können tausende von batteriebetriebenen Sensoren innerhalb eines Netzwerks verwaltet und Sensordaten verarbeitet werden.

**Überwachungslösungen für Wasserversorgung, Kläranlagen, Müllcontainer und mehr.**

Die LoRaWAN-Technologie ist für die Entwicklung von intelligenten, sogenannten Smart Cities, maßgeblich. Aktuelle Anwendungsmöglichkeiten liegen in der Überwachung der Wasserversorgung, wo LoRaWAN für die Kommunikation zwischen Brunnen und Hochbehälter (Niveau und Schaltbefehle) oder für die Datenerfassung von Messschächten (Zählerstand und ev. Druck) zum Einsatz kommt. Eine weitere Anwendung von LoRaWAN ist die Regelung von Kläranlagen. Die Anbindung über Cloud oder lokales LoRaWAN sorgt hier für die zentrale Visualisierung der Anlagenzustände (Pumpwerke, Regenüberlaufbecken etc.). Zudem ist LoRaWAN in den Bereichen Regulierung des Straßenverkehrs, Parkraumüberwachung oder Monitoring der Straßenbeleuchtung ein heißes Thema. So kommt die Technologie bereits für die Datenerfassung, Visualisierung und Auswertung von Zählerständen (Energiezähler, Wasserzähler, Wärmemengenzähler usw.), Luftqualitätsmessungen (z.B. in Schulen, Kindergärten, Büros oder Sitzungsräumen) oder Wetterdaten (Wetterstationen) zum Einsatz.

„Die LoRaWAN-Technologie lässt sich sowohl im Innen- wie im Außenbereich problemlos anbringen und ist vielseitig einsetzbar, um eine effiziente und nachhaltige Überwachungs-Infrastruktur aufzubauen", zeigt sich Christoph Gattinger, der Experte für Umgebungsmonitoring & Sensorik aus dem Hause BellEquip, dem niederösterreichischen Systemanbieter infrastruktureller Lösungen für den effizienten und sicheren Betrieb elektronischer Anwendungen begeistert.

**Die Vorteile der LoRa-Technologie:**

- **NIEDRIGER ENERGIEVERBRAUCH:** Geringer Energieverbrauch und Batterielaufzeiten von bis zu zehn Jahren bei entsprechend technischem Design.
- **LOKALES/EIGENES NETZ:** Anders als bei SigFox, NB-IoT oder LTE M ist es mit LoRa möglich ein eigenes, lokales Netzwerk aufzubauen.
- **HOHE GEBÄUDEDURCHDRINGUNG:** Die schmalbandige LoRa-Technologie ermöglicht es Geräte in tiefliegenden Gebäudeteilen einzusetzen.
- **OPTIMIERTE BETRIEBSKOSTEN:** Mit einem LoRaWAN-Gateway können tausende Endgeräte verbunden werden. Die Hardware ist vergleichsweise kostengünstig.

**www.bellequip.at**

**Über BellEquip – 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.

Die BellEquip-Stärken lassen sich in sechs Bereiche zusammenfassen:

- M2M Router, IoT & Antennen
- KVM & Audio/Video Signalverteilung und -verlängerung
- USV, Energieverteilung und -messung
- Umgebungsmonitoring, Sensorik & IoT
- Industrielle Netzwerktechnik & WLAN
- Technik, Service, Support & RMA

Das Waldviertler Team, mit „Der Technik, die verbindet", realisiert auf Basis der breiten Produktpalette kunden- und bedarfsorientierte Lösungen mit großem Systemwissen und Hausverstand.

Weitere Informationen:
**Christoph Gattinger**
Vertrieb & technische Beratung
Umgebungsmonitoring, Sensorik & IoT
christoph.gattinger@bellequip.at

## NEUE PARTNER

**Rockwell Automation** gab kürzlich eine Partnerschaft mit **Kezzler AS**, einer cloudbasierten Plattform für Produktdigitalisierung und Rückverfolgbarkeit, bekannt. Hersteller werden dabei unterstützt, den Weg ihrer Produkte von der Rohstoffquelle bis zum Point of Sale oder darüber hinaus mithilfe von cloudbasierten Supply Chain-Lösungen zu erfassen, die sich auf die Rückverfolgbarkeit von Produkten konzentrieren. Das kombinierte Angebot ist ideal für Branchen wie Biowissenschaften, Lebensmittel und Getränke sowie verpackte Konsumgüter, die sich auf die Einhaltung gesetzlicher Vorschriften und die Erfüllung von Verbrauchererwartungen in Bezug auf beispielsweise Produktqualität, Sicherheit und Nachhaltigkeit konzentrieren.

**www.rockwellautomation.com**

## NEUES IIoT-GATEWAY MIT PLC-ERWEITERUNG

Die **IoTmaxx GmbH** aus Hannover steht für leistungsfähige und transparente Industrial IoT-Lösungen für den Mittelstand, die einfach zu handhaben sind. Die Hardwarebasis für die Konzepte zur Fernüberwachung und Fernwartung industrieller Anlagen bilden IIoT-Mobilfunk-Gateways aus eigener Entwicklung. Mit dem maxx GW4102 stellt das Unternehmen sein drittes robustes Industrial IoT-Gateway vor, das dank seiner PLC-Erweiterung weitere Kommunikationsoptionen und Anwendungsmöglichkeiten bietet.

Das Linux-basierte, frei programmierbare Industrie-Gateway maxx GW4102 für die Hutschienenmontage setzt auf höchste drahtlose Verfügbarkeit durch Kommunikation über Mobilfunk im LTE-4G-Netz sowie auf Netzredundanz über zwei SIM-Karten. Dank der Always online-Funktionalität führt das Gateway einen selbstständigen Verbindungsaufbau sowie im Falle eines Fehlers den eigenständigen Neuaufbau der Verbindung aus. So besteht jederzeit und von jedem Ort aus uneingeschränkter Zugriff auf das wartungsfreie Gerät.

**www.iotmaxx.com**

## DIGITAL PIONEERS BEGINNEN DUALE DIGITALE AUSBILDUNG

Nachdem beim Projekt „**Digital Pioneers** – Das freiwillige digitale Jahr" die Bewerbungsphase abgeschlossen ist, stehen nun die Teilnehmerinnen fest und starten ihre Ausbildung: 29 Frauen zwischen 17 und 27 Jahren aus Vorarlberg, Tirol und Oberösterreich werden im ersten Schritt digitale Skills vermittelt, bevor sie ab November einen Einblick in die Praxis bei namhaften Unternehmen erhalten. Digitale Kompetenzen werden heute in vielen Berufen und Branchen benötigt – von der Juristin über die Lehrerin bis hin zur Produktionsleiterin. „Digital Pioneers – Das freiwillige digitale Jahr", wurde von der Plattform Industrie 4.0 Österreich gemeinsam mit der Bundesarbeitskammer und dem Digital Campus Vorarlberg initiiert und in Kooperation mit dem BFI Oberösterreich, dem BFI Tirol und ABZ Austria umgesetzt. Alle verfolgen dabei ein Ziel: Jungen Frauen praxisorientiert den Weg in technische Berufe zu erleichtern.

**Unterschiedliche Branchen kennenlernen.** Bei „Digital Pioneers" können – unabhängig von Vorbildung – digitale Berufe in unterschiedlichen Branchen kennengelernt werden. Die Teilnehmerinnen erhalten neben fachlichen Kenntnissen und praktischen Erfahrungen in digitalen Berufen auch Einblick in aktuelle Trends in unterschiedlichen Unternehmen und Branchen. Die Pilotphase des Projekts in drei Bundesländern wird durch das Zukunftsprogramm der Bundesarbeitskammer finanziert. Das Projekt setzt sich aus zwei Modulen zusammen: In der Grundausbildung, die am 20. September 2021 in Tirol und Vorarlberg bzw. am 4. Oktober 2021 in Oberösterreich startete, werden Kenntnisse für den Einstieg in die digitale und technische Berufswelt vermittelt. Nach der Grundausbildung können die erworbenen Kenntnisse unternehmensseitig eingebracht werden: 23 namhafte oberösterreichische, Tiroler und Vorarlberger Unternehmen aus den unterschiedlichsten Branchen – vom Bildungsbereich über Industrie bis hin zu Marketing – konnten als Kooperationspartner gewonnen werden.

**www.digitalpioneers.at**

# PLATTFORM INDUSTRIE 4.0 ÖSTERREICH FÖRDERT WISSENSTRANSFER

Die **Plattform Industrie 4.0** weitet ihre grenzüberschreitenden Aktivitäten aus: Gemeinsam mit heimischen und slowakischen Kooperationspartnern wurde das Projekt Share 4.0 ins Leben gerufen, bei dem der Austausch zu neuen Technologien in der Produktion im Mittelpunkt steht. Im Rahmen dieses Projektes, das aus Mitteln des Kooperationsprogramms Interreg V-A Slowakei – Österreich finanziert wird, werden Best Practices ausgetauscht und Synergien genutzt, um die digitale Fertigung in beiden Ländern voranzutreiben. Die österreichischen Partner umfassen Fotec, Profactor und Forschung Burgenland. Von slowakischer Seite sind die Slovak Innovation and Energy Agency (SIEA), Institute of Materials and Machine Mechanics der TU Bratislava, Industry4UM und National Centre of Robotics der slowakischen Akademie der Wissenschaften mit an Bord.

**Smart Industry-Netzwerk soll entstehen.** Ziel ist es, durch das Projekt bis Ende 2022 eine nachhaltige und ergebnisorientierte Kooperation der Smart Industry-Schlüsselakteure in den beteiligten Regionen – Burgenland, Niederösterreich, Wien, Bratislava und Trnava – zu etablieren. Dadurch soll ein Smart Industry-Netzwerk für den dauerhaften Wissenstransfer entstehen.
Im ersten Schritt werden unter anderem Pilotprojekte mit KMU zu thematischen Schwerpunkten wie Robotik umgesetzt, aber auch Methodiken und Strukturen zur Dialogförderung zwischen Forschung, Wirtschaft und Verwaltung ausgetauscht.
Zudem wird im Rahmen eines Memorandum of Understanding eine gemeinsame Smart Industry-Plattform beider Länder aufgesetzt, die nicht nur relevante Stakeholder zusammenbringt, sondern auch zukünftige Kooperationen und eine strategische Zusammenarbeit mit weiteren europäischen Partnerregionen im Bereich der Forschung und Innovation ermöglichen soll. „Dieses Projekt kurbelt den grenzüberschreitenden Wissensaustausch zwischen der Slowakei und Österreich an, um ein wettbewerbsstarkes Smart Industry-Netzwerk im Herzen Europas zu initiieren. Entscheidend wird dabei auch sein, Entscheidungsträger aus Verwaltung, Politik, Forschung und Wirtschaft aus beiden Ländern ins Boot zu holen, um sie für den Einsatz von innovativen Technologien zu sensibilisieren – denn nur somit können resiliente und nachhaltige Produktionssysteme geschaffen werden", ist **Roland Sommer** (Bild), Geschäftsführer der Plattform Industrie 4.0 Österreich, überzeugt.

**www.plattformindustrie40.at**

## ERNANNT

**Thomas Wenger** (Bild) ist neuer Area Vice President für Zentraleuropa bei PTC. Seit rund 20 Jahren erfolgreich für PTC tätig, übernimmt er in seiner neuen Position die Verantwortung für den Vertrieb in Deutschland, Österreich und der Schweiz. Ein Schwerpunkt seiner künftigen Tätigkeit wird unter anderem auf der weiteren Vertikalisierung der Organisation liegen, mit besonderem Fokus auf den Branchen Mobility, Lifesciences, Prozessindustrie, Elektronik und Hightech sowie des Maschinen- und Anlagenbaus. Während seiner langjährigen Laufbahn bei PTC hatte Thomas Wenger Positionen im Bereich Sales, als Regional Director und Senior Regional Director sowie Vice President inne, bis er schließlich zum Area Vice President befördert wurde. Im Rahmen seiner bisherigen Stationen bei PTC hat Thomas Wenger zahlreiche bedeutende Projekte gewonnen, maßgeblich bei Großkunden der Automobilindustrie. Wenger studierte Elektrotechnik mit Schwerpunkt Automatisierungstechnik an der TU München. Nach dem Studium begann er seine Karriere als Projektingenieur bei Siemens Anlagentechnik. Im Anschluss wechselte er in den Vertrieb der österreichischen Firma Keba AG, die im Bereich der Automatisierungstechnik tätig ist, bevor er daraufhin bei PTC seine erste Stelle antrat.

**www.ptc.com**

# VERANSTALTUNGSKALENDER

## NOVEMBER

**ScaleUp 360° Industry of Things**
**16.-17.11.2021 |** virtuell

**AIBC Europe**
**16.-18.11.2022 |** Malta

**European Cyber Week**
**16.-18.11.2021 |** Rennes

**Smart City Expo World Congress**
**16.-18.11.2021 |** Barcelona, hybrid

**Blockchain Week**
**16.-20.11.2021 |** Rom, hybrid

**ScaleUp 360° Intranet**
**17.-18.11.2021 |** virtuell

**AIIM Forum Europe**
**18.11.2021 |** London

**AI in Manufacturing**
**22.-23.11.2021 |** Berlin, hybrid

**Cloud Expo Europe**
**23.-24.11.2021 |** Paris

**Digital Transformation Week Europe**
**23.-24.11.2021 |** Amsterdam

**IoT Tech Expo Europe**
**23.-24.11.2021 |** Amsterdam
**30.11.-1.12.2021 |** virtuell

**SPS**
**23.-25.11.2021 |** Nürnberg

**ScaleUp 360° Big Data**
**24.-25.11.2021 |** virtuell

**ScaleUp 360° IT Security**
**24.-25.11.2021 |** virtuell

**DigITS**
**27.-28.11.2021 |** virtuell

**European Cloud Summit**
**29.11.-1.12.2021 |** Düsseldorf

## DEZEMBER

**Blockchance Europe**
**2.-4.12.2021 |** Hamburg, hybrid

**IBC**
**3.-6.12.2021 |** Amsterdam, hybrid

**IT-Tage**
**6.-9.12.2021 |** virtuell

**Connected Germany**
**7.-8.12.2021 |** Mainz

**WorldCIS - World Congress on Internet Security**
**7.-9.12.2021 |** virtuell

**Digital Manufacturing Day**
**8.12.2021 |** virtuell

**Cloud Expo Europe**
**8.-9.12.2021 |** Frankfurt/Main

**ICIIOTS - Int. Conference on Industrial Internet of Things Security**
**9.-10.12.2021 |** London

**ICCS - Int. Conference on Cyber Security and Privacy in Communication Networks**
**9.-10.12.2021 |** Cardiff

**DevTernity**
**10.-11.12.2021 |** virtuell

**CANS - Int. Conference on Cryptology and Network Security**
**13.-15.12.2021 |** Wien

**ScaleUp 360° Legacy IT**
**14.-15.12.2021 |** virtuell

## JÄNNER 2022

**CES**
**5.-8.1.2022 |** Las Vegas, hybrid

**Hybrid Cloud Congress**
**11.1.2022 |** virtuell

**KickStart Europe Conference**
**24.-25.1.2022 |** Amsterdam

**Cybertech Global**
**25.-27.1.2022 |** Tel Aviv

## FEBRUAR

**Cisco Live**
**7.-11.2.2022 |** Amsterdam

**Internet World Expo**
**22.-23.2.2022 |** München, hybrid

**MWC - Mobile World Congress**
**28.2.-3.3.2022 |** Barcelona

## MÄRZ

**Cyber Intelligence Europe**
**1.-3.3.2022 |** Oslo

**Big Data & AI World**
**2.-3.3.2022 |** London

**Cloud & Cyber Security Expo**
**2.-3.3.2022 |** London

**Rethink! IT Security**
**10.-11.3.2022 |** Berlin, hybrid

**embedded world**
**15.-17.3.2022 |** Nürnberg

**CloudFest**
**22.-24.3.2022 |** Europa-Park Rust

**Data Natives**
**22.-24.3.2022 |** Berlin, hybrid

**Fiberdays22**
**23.-24.3.2022 |** Wiesbaden

**CyberTech Global**
**28.-30.3.2022 |** Dubai

## APRIL

**CSIT - Computer Science and Information Technology**
**11.-12.4.2022 |** Istanbul

# VORSCHAU

## IoT4 NR. 1-2022 | Erscheinungstermin: 17. März 2022

## AUTOMOTIVE UND KI

Künstliche Intelligenz gewinnt für die Automobilindustrie immer mehr an Bedeutung. Während sich die Öffentlichkeit hauptsächlich für den Einsatz beim autonomen Fahren interessiert, wird KI längst auch in anderen Bereichen wie Engineering, Produktion, Supply Chain oder Mobilitätsdienstleistungen angewandt. Mit KI kann die Automobilproduktion über die gesamte Wertschöpfungskette optimiert werden – für Hersteller und Zulieferer ist hier noch viel Luft nach oben. Doch was bedeutet das? **Stefan Hussmann**, Leiter des Geschäftsbereichs Automotive & Transportation bei adesso, zieht Bilanz.

## BLACKBOX NEURONALES NETZWERK

In zunehmend selbstfahrenden Autos sind zuverlässige Convolutional Neuronal Networks (CNN) essenziell. Denn mit ihrer Hilfe soll KI automatisch andere Verkehrsteilnehmer erkennen. Je selbständiger ein Auto aber fährt, desto größer werden die Anforderungen an die Sicherheit der Algorithmen. Um Menschenleben zu schützen, ist daher ein tiefes Verständnis der Klassifizierung dieser neuronalen Netzwerke notwendig. Ein CNN arbeitet allerdings per se als Blackbox, die komplexen Entscheidungswege sind also schwer nachzuvollziehen, wodurch eine Bewertung der Sicherheitsrisiken schwierig ist. Wir berichten über dieses Thema.

## 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

TECHNIK & MEDIEN VERLAGSGMBH

www.iot4industry.info

# DIE ADAPTIVE MASCHINE
## Ihr Wettbewerbsvorteil

In einer Welt der kleinen Losgrößen, kurzen Lebenszyklen und des Online-Handels bleiben Sie mit der adaptiven Maschine profitabel – der ersten Maschine, die sich dem Produkt anpasst.

| Aktuelle Herausforderungen | Adaptive Maschinenlösungen |
| --- | --- |
| Individuelle Konsumwünsche | Produktion auf Bestellung |
| Höhere Variantenvielfalt | Formatwechsel ohne Stillstandszeiten |
| Kurze Produktlebenszyklen | Einfache Neukonfiguration mit digitalem Zwilling |

B&R ermöglicht die Umsetzung der adaptiven Maschine bereits heute – mit einer perfekt abgestimmten Gesamtlösung aus intelligenter Track-Technologie, Robotik, Vision und digitalen Zwillingen.

**Holen Sie sich Ihren Wettbewerbsvorteil:**
**www.br-automation.com/adaptive**

PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP