www.iot4industry.at

IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

Erscheinungstermin: 23. März 2023 **1 | 2023**

3 x jährlich

Weidmüller eröffnet den einfachen Weg zum Industrial IoT

ALLES KANN – NICHTS MUSS

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

TECHNIK & MEDIEN VERLAGSGMBH

Security
VERTRAUEN IST GUT, KONTROLLE IST BESSER

Im Gespräch
WIR MÜSSEN DRAUSSEN BLEIBEN

Im Gespräch
KI UND DER UNIVERSALGELEHRTE

Mehrlagig scannen.
Inbetriebnahme revolutionieren.
Kosten minimieren.

R2300
3-D-LiDAR-Sensor

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

www.pepperl-fuchs.com/pr-R2300

SMART AUTOMATION AUSTRIA
23.-25.05
Standnr. 125

Your automation, our passion.

PEPPERL+FUCHS

Liebe Leserin, lieber Leser,

Die Versuchung war groß dieses Editorial von ChatGPT schreiben zu lassen. Warum? Weil es faszinierend ist der Künstlichen Intelligenz beim Denken zuzusehen und ich ganz begeistert bin, was ihr alles so einfällt. Warum dann doch nicht? Weil nicht alles, was ChatGPT schreibt richtig ist und schon gar nicht meinem Schreibstil entspricht. Noch nicht jedenfalls. Aber wer weiß, vielleicht kann man eines Tages seine persönliche KI mit seinem eigenen Stil füttern. In den Sozialen Medien wird bereits die Frage gestellt, ob die KI der schreibenden Zunft oder den Marketern dieser Welt die Arbeit wegnehmen wird. Ich habe eine schöne Antwort dazu gelesen: „Nein, ChatGPT wird niemandem die Arbeit wegnehmen. Das werden jene übernehmen, die gelernt haben mit der KI richtig umzugehen." Also prinzipiell will ich persönlich niemanden die Arbeit wegnehmen, ich möchte aber mit Sicherheit zu jener Gruppe gehören, die dieses Werkzeug – und im Moment ist es nichts anderes – richtig gut beherrscht. Die ersten Erfahrungen sammle ich bereits. Ich lasse mir z.B. Einleitungen und Überschriften vorschlagen, um sie dann ganz in meinem Stil zu adaptieren. Zeit spare ich damit in jedem Fall sehr viel.

Und Zeit ist doch generell ein wichtiges Thema. Mehr Zeit für all jene Dinge zu haben, die Spaß machen, Nutzen stiften und einen Mehrwert haben. Das bedeutet auch seine Arbeit effektiver und effizienter zu gestalten. Und am besten geht das mit Standardisierung und Automatisierung. Das betrifft nicht nur Produktionsbetriebe, sondern auch jeden Schreibtischtäter. Und da sind wir wieder beim Thema: Nimmt uns die Technik die Arbeitsplätze weg? Nein, sagen die Experten. Denn wenn uns einfache monotone Arbeiten von Robotern, Maschinen oder Künstlichen Intelligenzen abgenommen werden, sind wir Menschen frei für kreative und sinnstiftende Tätigkeiten.

Jetzt zum Heft. Wie in der letzten Ausgabe angekündigt, haben wir unsere Themen breiter aufgestellt. Es gibt nicht mehr nur das EINE Fokusthema im Heft. Jetzt ist jede Ausgabe für jedes Thema offen. Für ein bisschen Ordnung sorgen die Übertitel: IoT, Cloud, Digitalisierung, Security und KI. Was sich nicht geändert hat, sind unsere Interviews. Diesmal gibt es wieder sehr interessante Gesprächspartner, mit denen ich über weit mehr gesprochen habe, als dann hier Platz finden konnte. Davon haben Sie werte:r Leser:in jetzt leider nichts, ich habe aber wieder einmal viel gelernt. Ein Gespräch hat mich besonders beeindruckt. Nämlich das mit Reinhard Birke von NTT Data. Er hat es geschafft, unserem Gespräch eine beinahe philosophische und gesellschaftspolitische Wendung zu geben. Und genau das mag ich an den Interviews für das Heft besonders gerne. Sie ermöglichen den Blick über den Tellerrand der Unternehmen und ihre Produkte hinaus in Richtung Zukunft.

Und damit wünsche ich Ihnen viel Spaß beim Lesen dieser Ausgabe,

Ihre
Barbara Sawka

INHALT
MÄRZ 2023

Coverstory

Ob Energiemanagement, Prozessoptimierung, Condition Monitoring, Remote Access oder Predictive Maintenance – Daten müssen erfasst, vorverarbeitet und schlussendlich analysiert werden, um einen Mehrwert zu erzielen. Weidmüller zeigt seinen Kunden als „Enabler from Data to Value" einen einfachen Weg ins Industrial IoT.
www.weidmueller.at

Lesen Sie mehr ab Seite 6!

IoT
10 Gut zu wissen | Gastkommentar Siniša Mitrović, Cloudera
12 Am Sprung zur 6. Generation | Bosch gestaltet Grundlagen für 6G mit
14 Die Kraft von Factory Edge | Red Hat fördert offene Standards
16 Mit Micro-Data-Center-Lösungen von der Digitalisierung profitieren | Gastkommentar Ian-Hendrik Hannemann, Rittal
18 Gegen das große Rauschen | OT-Security kommt nicht einfach per Feenstaub, sagt Kay Ernst, Otorio
22 Es wächst zusammen, was zusammengehört | Copa-Data weiß wie OT und IT zusammenwachsen

SECURITY
24 Cybersecurity in Frauenhand | Europäische Initiative „Women4Cyber" auch in Österreich
26 Wir müssen draußen bleiben | Kevin Börner, Deep Instinct, über Deep Learning als Maßnahme zur Cybersecurity
28 Vertrauen ist gut, Kontrolle ist besser | Zero Trust als Konzept gegen Cyberattacken

DIGITALISIERUNG
30 Gegen den Verzicht | Thomas Lutzky, Phoenix Contact Österreich setzt auf Technik gegen steigenden Energieverbrauch
34 KI und der Universalgelehrte | Für Reinhard Birke sind die Digitalisierungs- und IT-Prozesse im Unternehmen die reinste Positivspirale
38 So wie Berg und Prophet | BearingPoint bringt die Daten zu den Mitarbeitern

KÜNSTLICHE INTELLIGENZ
40 Die zwei Seiten von ChatGPT | Die KI ist bei Hackern und Betrügern bekannt
42 Künstliche Intelligenz hebt Datenschätze | Heubach zieht mit Festo AX maximalen Wert aus seinen Daten
45 Smarte Ampeln | Fußgängerampeln regeln mittels KI den Verkehrsfluss

CLOUD
46 Cloud & Security | Bei allen Vorteilen der Cloud darf Security nicht fehlen
47 Supermarkt der Zukunft | Datenbasiertes Energiemanagement hilft Rewe beim Sparen
48 Mehr Kontrolle | Studie von Capgemini Research Institute zeigt Treiber für Cloud-Souveränität

50 Impressum | Vorschau

3 x jährlich

IoT4 INDUSTRY&BUSINESS

18

Gegen das große Rauschen

OT-Security kommt nicht einfach per Feenstaub ins Unternehmen, sagt Kay Ernst, Regional Sales Director DACH von Otorio. Und bei der Furcht vor Angriffen ist eine Fokussierung auf die Supply Chain zu beobachten. Wenn man es allerdings schafft die Risiken zu erkennen und zu beheben, ist man schon einen riesigen Schritt weiter. Wie das gelingen kann, erzählt er im Gespräch.

28

Vertrauen ist gut, Kontrolle ist besser

Frank Limberger Data & Insider Threat Security Specialist bei Forcepoint „Die Gefahr von Cyberattacken war wohl lange nicht so hoch wie jetzt und das wird sie aller Voraussicht nach auch bleiben." Der Zero-Trust-Ansatz folgt daher dem Credo „Vertraue niemandem, verifiziere jeden" und verbessert damit die Cybersicherheit in modernen IT-Umgebungen. Bei diesem Ansatz wird grundsätzlich allem und jedem misstraut und verlangt, dass der komplette Datenverkehr geprüft wird und dass sich Nutzer, Geräte, Anwendungen und andere Einheiten bei jedem Zugriff auf Systeme oder Daten authentifizieren müssen.

34

KI und der Universalgelehrte

Als Positivspirale bezeichnet Reinhard Birke, General Manager NTT Data DACH AT, die Digitalisierungs- und IT-Prozesse im Unternehmen. Und die IT generell als Multifunktionswerkzeug, das in alle Schlösser passt. Warum er sich keine Sorgen um die Zukunft macht und warum er sich ein anderes Bildungssystem wünscht, erzählt er im Interview.

ALLES KANN – NICHTS MUSS

Ob Energiemanagement, Prozessoptimierung, Condition Monitoring, Remote Access oder Predictive Maintenance – Daten müssen erfasst, vorverarbeitet und schlussendlich analysiert werden, um einen Mehrwert zu erzielen. Weidmüller zeigt seinen Kunden als „Enabler from Data to Value" einen einfachen Weg ins Industrial IoT.

Die Vernetzung und Digitalisierung der Prozesse bis an den Rand des Netzwerks, den „Edge“, bieten den Unternehmen wettbewerbsentscheidende Vorteile: transparente und aktuelle Informationen, hohe Flexibilität in den Prozessen, die Möglichkeit zu vorausschauenden Entscheidungen und damit Zeit- und Kosteneinsparungen – und nicht zuletzt eine gesteigerte Qualität der Prozesse. Dies wird nicht nur zu einem exponentiellen Wachstum an Datenvolumen führen, sondern auch bisher zentrale IT-Funktionalitäten und Entscheidungsprozesse an die dezentralen Edge-Komponenten verlagern. Dies wiederum bedingt eine digitale Vernetzung unterschiedlichster Systeme und Lösungen. Was in der Theorie nur vorteilhaft klingt, ist es in der Praxis auch – doch die Umsetzung ist (noch) nicht so einfach. Denn viele Vorteile, die eine durchgängige Smart Factory in puncto Flexibilität, Kosten- und Energieeffizienz bieten könnte, lassen sich aufgrund herstellerspezifischer Automatisierungssysteme nicht nutzen. Was in der IT heute Voraussetzung für eine am Markt erfolgreiche Lösung ist, nämlich die problemlose Kompatibilität zu Fremdsystemen, ist in der OT noch lange nicht Standard: Inkompatibilitäten der proprietären Lösungen und teure Wartungen und Nachrüstungen der Anlagen sind für die Anwender oft die Folge. Zudem mussten viele Unternehmen in den letzten Monaten feststellen, dass eine herstellerbezogene Lösung wenig Möglichkeiten bietet, bei Störungen in der globalen Lieferkette einfach auf einen anderen Komponentenhersteller auszuweichen.

IoT 4 Industry & Business: IoT ist ein großer Begriff. Weidmüller spricht vom „Easy way to IoT“. Was bedeutet das?
Milena Krstic: „The easy way to IoT“ bedeutet, dass wir unsere Kunden auf ihrem Weg IoT-Projekte umzusetzen begleiten. Wir haben dafür die notwendige Hardware, aber auch die erforderliche Software. Wir wollen den Kunden den Einstieg in die IoT-Welt bestmöglich leicht machen, damit sie sehr schnell an ihre Ziele kommen.

IoT: Viele fürchten den zeitlichen und organisatorischen Aufwand und natürlich auch die Kosten bei IoT-Projekten.
Krstic: Das ist verständlich. Wir können aber klein bei bestehenden Anlagen starten, die wir ganz easy nachrüsten. Selbst wenn es hier durch die bestehenden Systeme bestimmte Vorgaben gibt. Wir kennen diese Herausforderungen sehr gut. Nicht jede Schnittstelle kommuniziert mit einer anderen Schnittstelle. Dafür haben wir Enabler, die uns dabei helfen, die Produkte miteinander zu verbinden. Wir haben sehr viele Konnektoren für die unterschiedlichen Systeme – und das ist auch ein USP, den wir bei Weidmüller mitbringen. Sollte ein Connector vielleicht noch nicht an Bord sein, können wir ihn im Zuge des Projektes gemeinsam mit den Kunden entwickeln.

ResMa® unterstützt wirkungsvoll alle Aufgaben für ein effizientes und aktives Energiemanagementsystem und reduziert damit den notwendigen Personalaufwand erheblich.

Ein Betriebssystem für Industrial IoT und Automatisierung.
Je enger IT- und OT-Welt verschmelzen, desto größer wird der Wunsch der Anwender, die Abhängigkeit von bestimmten Herstellern zu durchbrechen. Weidmüller bietet ihnen nun eine Softwareplattform für IIoT und Automation, die offen, flexibel und unabhängig ist. Das Automatisierungsbetriebssystem u-OS basiert auf offenen, etablierten Standards wie Linux, Container-Technologie oder OPC UA (Open Plattform Communications Unified Architecture) und ermöglicht die Einbindung von Apps. u-OS ist damit einfach erweiterungsfähig und unterstützt Automatisierer durch bedienerfreundliches Engineering, Systeme individuell und webbasiert zusammenzustellen. Das macht Anwender und deren Kunden unabhängig, flexibel und zukunftsfähig. >>

Jürgen Kitzler
Automation Sales Engineer Weidmüller Österreich

„Wenn man unser Credo ‚Enabler from Data to Value‘ ernst meint, dann kann man nicht einfach nur die Hardware zur Verfügung stellen. Unser Credo erfordert ein gesamtes Lösungsportfolio für den Markt.“

u-OS ist das neue, offene Betriebssystem von Weidmüller. Es vereint die Automatisierung mit den Möglichkeiten des Industrial IoT auf nur einem Gerät und ist für Edge-Computing-Lösungen geeignet. u-OS ermöglicht eine effiziente Datenvorverarbeitung und präzise Steuerung direkt an der Maschine.

u-OS vereint die Stabilität von Automatisierungslösungen mit den Möglichkeiten des IIoT auf nur einem Gerät und bietet für Automatisierer und IT-Programmierer eine offene und flexible Lösung, die die digitale Vernetzung unterschiedlichster Systeme auf einfache Weise erlaubt. Zwar gibt es bereits Ansätze zu übergreifenden Automatisierungsplattformen, aber auch bei diesen muss sich der Anwender an den Vorgaben des Anbieters orientieren – Lösungen von Drittanbietern einzubinden, ist beispielsweise nur sehr aufwendig möglich.

IoT: Weidmüller hat sich in den letzten Jahren vom Produkt- zum Lösungsanbieter entwickelt. Jetzt kommt ganz viel Software dazu. Wird Weidmüller jetzt ein Softwarehaus?
Jürgen Kitzler: Nein das nicht. Auch wenn wir ein großes Team an Softwareentwicklern haben. Aber wenn man unser Credo „Enabler from Data to Value" ernst meint, dann kann man nicht einfach nur die Hardware zur Verfügung stellen. Unser Credo erfordert ein gesamtes Lösungsportfolio für den Markt.

IoT: Was ist das neue u-OS genau?
Kitzler: u-OS ist das Betriebssystem für unsere Steuerungen und Edgegeräte wie ein IPC oder IoT-Gateway. Genau wie man es von den verschiedenen App Stores am Handy kennt, ist u-OS die Plattform, egal ob es Richtung Automatisierung oder IoT geht, ob Visualisierung, Fernwartung oder Rolloutmanagement. Wir verfolgen bei der Implementierung den Nocode-Ansatz, Programmierkenntnisse sind nur anwendungsspezifisch notwendig. u-OS wird die Basis aller IoT- und Automatisierungskomponenten von Weidmüller sein um den Zugang in die IT- und OT-Welt sehr einfach zu machen. Und die Möglichkeit jederzeit seine Projekte zu erweitern, erlaubt es unseren Kunden und natürlich auch deren Kunden, ihr System individuell und webbasiert zusammenzustellen. Alles kann – nichts muss.

IoT: Jeder verwendet gerne Schlagworte. Bei u-OS sind es offen, flexibel und unabhängig. Wie erfüllt Weidmüller diese drei Begriffe tatsächlich mit Leben?
Kitzler: u-OS setzt auf offene, etablierte Standards wie Linux, der Container-Technologie oder OPC UA und ermöglicht es damit Weidmüller-Apps, eigene oder 3rd-Party-Apps einzubinden. Das macht den Anwender unabhängig. Denn damit ist er in der Lage, auch auf andere Anbieter zurückzugreifen, die auch Automatisierungsplattformen oder Apps anbieten. Linux als offener Standard ist deshalb Voraussetzung, weil es wichtige Eigenschaften für den Einsatz im Automatisierungsumfeld verbindet: sehr gute Echtzeitfähigkeit, eine große Community und durch den offenen Quellcode den Schritt Richtung Hardwareunabhängigkeit.

Schnelle Bereitstellung von Softwarelösungen. Die Container-Technologie als offener Standard erlaubt es, eine Anwendung mit all ihren Abhängigkeiten in einem einzigen Paket zu bündeln. Damit lassen sich selbst komplexe Software-Releases automatisiert und schnell bereitstellen. Das eliminiert viele Fehlerquellen beim Installieren und Updaten, verringert den Zeitaufwand und spart Kosten. Mit dem von u-OS genutzten Docker-Containern über Portainer lässt sich das System einfach und ohne Programmierkenntnisse auf die kundenspezifischen Bedürfnisse konfigurieren. Und OPC UA ist ein offenes Industrie-Kommunikationsprotokoll, das einen plattformunabhängigen, zuverlässigen und sicheren Informationsaustausch zwischen Geräten unterschiedlicher Hersteller ermöglicht. Aus der Nutzung dieser offenen Standards ergibt sich mit u-OS die Möglichkeit, Laufzeitsysteme von Drittanbietern auf der Softwareplattform auszuführen. Ein Beispiel dafür ist CODESYS®, das größte herstellerunabhängige Ökosystem in der Industrieautomatisierung. CODESYS® (Controller Development System) ist ein hardwareunabhängiges Programmiersystem nach IEC61131 zur Erstellung, Projektierung, Dokumentation, Visualisierung und Konfiguration von Steuerungsapplikationen. Zudem erlaubt das integrierte Engineeringtool u-create web zusätzlich die Umsetzung einfacher Automatisierungsaufgaben auf Funktionsbausteinbasis.

Maßgeschneiderte Anpassung durch Apps. Über Apps – von Weidmüller, von Drittanbietern oder anwendereigene – lassen sich neue Funktionen flexibel ergänzen und die ganze Welt der industriellen Automatisierung und des IoT erschließen. Mit dem Betriebssystem u-OS verschmelzen auf diese Weise zukünftig und unkompliziert unterschiedliche industrielle Welten: Beispielsweise kann PROCON-WEB, eine hochperformante, webbasierte Visualisierungslösung, einfach als App auf der offenen Steuerung installiert werden. u-OS verbindet Industrial IoT und Automatisierung, Partner mit deren Anwendern, die Cloud mit den Daten und industrielle Ökosysteme miteinander. Anwender, die auf Open-Source-Automatisierung statt herstellergebundener Systeme setzen, profitieren davon in mehrfacher Hinsicht. Sie stellen sich dank offener, digitaler Vernetzung produktiver, flexibler und effizienter auf.

Energie sparen in der Produktion. Der Einsatz von Energie und Ressourcen in der industriellen Produktion ist ein Kostenfaktor, der mit zunehmender Automatisierung an Bedeutung gewinnt. Durch die Verknüpfung von Ressourcenmanagement und IIoT kann die notwendige Transparenz, Prozesse nachhaltiger und wirtschaftlicher zu verfolgen gelingen. Mit dem Ressourcen- und Energiemanagement ResMa® bietet Weidmüller eine skalierbare Softwarelösung, die Daten über Connectoren zentral sammelt und eine Reihe intelligenter Auswerte- und Visualisierungsmöglichkeiten bietet, um Mehrwerte aus den Rohdaten zu erzielen. Ganz nach dem Motto „from Data to Value“.

IoT: Weidmüller hat eine Energiemanagementlösung. Was kann die neue Software?
Krstic: Mit dem Kauf des Softwareunternehmes GTI in 2018 ist die Software ResMa® in unser Produkt-Portfolio aufgenommen worden. Neben Energiedaten sammelt die Software Daten zum Gas-, Wasser-, Wärme- und Druckluftverbrauch. Da geht es zum einen um die Anzeige der Daten, aber natürlich auch um das Reporting. Man möchte ja nicht nur die Daten sammeln und visualisieren, sondern daraus Maßnahmen ableiten. Und die Reportings sind da ausschlaggebend. Man will schließlich wissen, wo man steht, um das als Basis zu nützen, gewisse Sachen besser zu machen. Mit ResMa® identifizieren wir zum Beispiel Potenziale bei der Energieeinsparung oder dem CO_2-Ausstoß. Man kann die Energieflüsse sogar auf einzelne Produkte runterbrechen oder Vergleiche zwischen unterschiedlichen Arbeitsschichten realisieren.

Dabei lassen wir den Kunden nicht alleine mit der Software, sondern leiten ihn in Form von Trainings und Workshops an. Was zu Demo-Zwecken sehr gut funktioniert, ist das Übertragen von händisch erfassten Daten, aus denen wir kleine Analysen machen, um dem Kunden ein Gefühl für die Software zu geben.

IoT: Können Sie uns ein Gefühl für ResMa® an Hand eines Beispiels geben?
Krstic: Wir haben bei einem Handelsunternehmen mit einigen 100 Geschäftsstellen europaweit unser Ressourcenmanagement aufgesetzt. Mittlerweile ist das eine Zeit lang im Einsatz. Da geht es „nur“ um die Beleuchtung, die Heizung und vielleicht ein bisschen Automatisierung in den Filialen. Die Software hat dabei geholfen, zu identifizieren wo und wann der Verbrauch stattfindet. Dank ResMa® konnten hier jährlich 2,5 Gigawattstunden an Energie eingespart werden. Das ist schon eine massive Zahl, bzw. ein halbes Kraftwerk, das hier eingespart wird.
Kitzler: Wir haben aktuell auch Kunden die den CO_2-Ausstoß einzelner Produkte und Chargen ermitteln und protokollieren was mit ResMa® recht einfach umsetzbar ist.

Effizientes Energiemanagement. Der Einsatzzweck von ResMa® ist vielseitig und umfasst unter anderem den Einsatz als Energiemanagementsoftware nach DIN EN ISO 50001, als Prozessoptimierung auf Basis von Produktionsdaten sowie die Integrationsmöglichkeit einer Prozessvisualisierung/HMI und eine Datenbereitstellung für externe Auswertemöglichkeiten wie beispielsweise KI-Tools. Der modulare Aufbau sowie vordefinierte Systemvarianten für bewährte ResMa® Use Cases ermöglichen eine flexible und schnelle Realisierung der Projekte – ob in Produktion, Industrie oder verteilten Infrastrukturen. Zudem erlauben offene Schnittstellen eine einfache und kostengünstige Integration in die bestehende IT-Umgebung.

www.weidmueller.at

Milena Krstic
Application Engineer Automation Weidmüller Österreich

„Mit ResMa® identifizieren wir Potenziale bei der Energieeinsparung oder dem CO_2-Ausstoß. Man kann die Energieflüsse sogar auf einzelne Produkte runterbrechen oder Vergleiche zwischen unterschiedlichen Arbeitsschichten realisieren.“

GUT ZU WISSEN

Siniša Mitrović, Regional Director Eastern Europe and Austria bei Cloudera, erklärt, warum Datenplattformen, Software as a Service (SaaS) und die Weiterbildung von Mitarbeitern immer wichtiger werden – und warum Kunden von Hyperscalern enttäuscht werden.

Der Fachkräftemangel hat die Tech-Branche weiterhin fest im Griff. Gleichzeitig ist die wirtschaftliche Lage angespannt. Trotzdem müssen Unternehmen mit ihrer Digitalisierung voranschreiten. Eine entscheidende Rolle spielt dabei die Fähigkeit, Daten zu nutzen. Wie gelingt das angesichts der wachsenden Herausforderungen?

Software as a Service wird immer wichtiger. Der Fachkräftemangel hält weiter an. Dadurch haben es Unternehmen schwer, IT-Experten und andere qualifizierte Mitarbeiter zu finden. Daher wird Software as a Service (SaaS) immer beliebter. Unternehmen erwarten von den Anbietern, dass diese mehr Verantwortung übernehmen. So können Firmen sich voll auf die Nutzung der Services konzentrieren und Konfiguration, Feintuning, Performance-Management und Optimierung anderen überlassen. Eine unverzichtbare SaaS-Anwendung ist Data Lakehouse. Sie speichert alle Daten, ob strukturiert oder unstrukturiert, in einem offenen Data Lake. Teams können dann für ihre Data-Science- und Business-Analytics-Projekte jederzeit auf sämtliche verfügbare Daten in der aktuellen Version zugreifen.

Föderierte Datenplattformen rücken in den Fokus. Ähnlich wie beim europäischen Cloud-Projekt Gaia-X werden wir auch im Bereich der Datenplattformen Initiativen sehen, die einen gemeinschaftlichen, sicheren Ansatz verfolgen. An Gaia-X arbeiten mehrere Länder zusammen, um Rahmenbedingungen für eine souveräne europäische Dateninfrastruktur aufzubauen und Innovationen zu schaffen. Ein solches föderiertes System ist keine einzelne Cloud, sondern verbindet viele Cloud-Anbieter und -Nutzer in einer transparenten Umgebung miteinander. Die Idee dahinter ist, die derzeitige Abhängigkeit von Cloud-Hyperscalern zu verringern. Organisationen wie der National Health Service, das Gesundheitssystem in Großbritannien und Nordirland, haben bereits Pläne zur Entwicklung einer föderierten Datenplattform vorgestellt, um große Datenmengen über mehrere Plattformen hinweg zu verwalten. Ein Unified-Data-Fabric-Ansatz zur intelligenten und sicheren Bereitstellung unterschiedlicher Datenquellen ist im Grunde ein föderiertes Datenmanagement-System im großen Stil. Indem es im Self-Service Zugriff auf Daten bietet – ganz gleich ob on premise oder in verschiedenen Clouds –, unterstützt es Unternehmen dabei, ihre Datenherausforderungen zu meistern.

Ernüchterung bei Hyperscaler-Nutzung. Die digitale Transformation ist ein Muss für alle Unternehmen, die ihre operative Agilität steigern, Innovationen vorantreiben und die Customer Experience verbessern wollen. In der Vergangenheit haben viele Entscheider dabei auf die Hyperscaler gesetzt und Milliardenverträge mit einer Laufzeit von drei bis fünf Jahren abgeschlossen. Nach und nach macht sich Ernüchterung breit. Unternehmen stellen fest, dass der gewählte Weg teuer ist und der Return on Investment deutlich später eintritt als erwartet. Sie entwickeln ein neues Bewusstsein für hybride Ansätze und erkennen, wie wichtig es ist, dass man Daten wieder aus einer Cloud zurückholen kann. Nicht zuletzt geht es auch um die Fähigkeit, flexibel auf Ereignisse zu reagieren, die außerhalb der eigenen Kontrolle liegen – zum Beispiel, wenn sich Datenschutzrichtlinien ändern und Unternehmen diese umsetzen müssen. Wir werden daher sehen, dass immer mehr Kunden nach Alternativen zu Hyperscalern suchen. Um es mit dem Bild der Analysten von Gartner zu beschreiben: Wir befinden uns ganz oben an der Kurve eines Hype-Zyklus. In den nächsten beiden Jahren werden wir den Scheitelpunkt überschreiten, sodass Hyperscaler auf den Tiefpunkt zusteuern und zunehmend unter Druck geraten, da Kunden eine Amortisierung ihrer Investitionen erwarten.

Die Tech-Branche wird sich weiter konsolidieren. Unternehmen wollen ihre Prozesse weiter vereinfachen. Anstatt mit vielen verschiedenen Herstellern wollen sie lieber mit Partnern zusammenarbeiten, die mehrere Services aus einer Hand anbieten. Daher wird sich der Technologiesektor 2023 noch stärker konsolidieren. Zahlreiche Anbieter verlieren gerade rasant an Marktwert. Viele kleinere und neu gegründete Unternehmen werden reif für eine Übernahme sein, weil sie womöglich unterbewertet sind oder seit ihrem Börsengang an Wert verloren haben. Wer Synergien mit solchen kleineren Unternehmen und Start-ups entwickelt, um sein Produktportfolio zu erweitern, wird sich dadurch Vorteile verschaffen können.

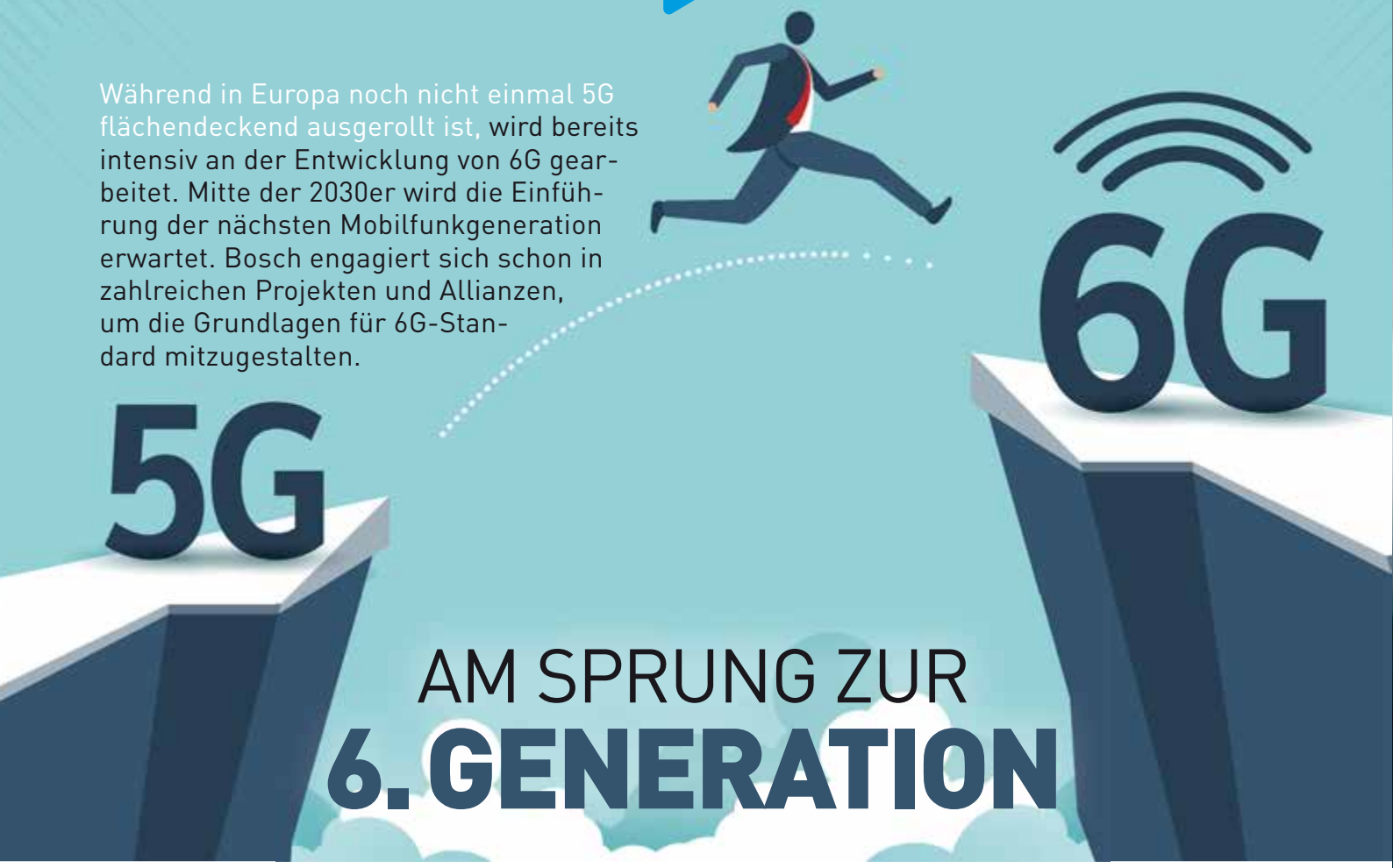
Upskilling wird überlebenswichtig. Der Fachkräftemangel hat sich im vergangenen Jahr weiter zugespitzt und ein Ende des Trends ist nicht in Sicht. Wie die Wirtschaftskammer Österreich im IKT Statusreport #6 festgestellt hat, fehlen in den nächsten fünf Jahren bis zu 30.000 IT-Fachkräfte in Österreich. Stellen bleiben lange unbesetzt, was nicht nur Digitalisierungsprojekte ausbremst, sondern im Ernstfall ganze Unternehmen gefährdet. Da es auch zu wenig Hochschulabsolventen mit spezialisiertem Daten-Know-how gibt, ist es von entscheidender Bedeutung, die bestehende Belegschaft besser zu qualifizieren. Weiterbildungs- und Umschulungsprogramme werden in den kommenden Jahren zum Schlüssel für künftiges Wachstum und Entwicklung. Eine wichtige Rolle spielen dabei Künstliche Intelligenz (KI) und Machine Learning (ML). Indem die Technologien zeitaufwendige Standard-Tätigkeiten übernehmen, gewinnen Mitarbeiter mehr Freiraum für komplexere Aufgaben. Unsere Studie „Limitless – The Positive Power of KI“ zeigt: 80 Prozent der Wissensarbeiter finden, dass ihnen KI und ML die Arbeit erleichtern und übernehmen dank dieser Verbesserung gerne neue Aufgaben.

www.cloudera.de

Der Autor
Siniša Mitrović
... ist Regional Director Eastern Europe and Austria bei Cloudera

Der Fachkräftemangel hält weiter an. Dadurch haben es Unternehmen schwer, IT-Experten und andere qualifizierte Mitarbeiter zu finden. Daher wird Software as a Service (SaaS) immer beliebter.

Während in Europa noch nicht einmal 5G flächendeckend ausgerollt ist, wird bereits intensiv an der Entwicklung von 6G gearbeitet. Mitte der 2030er wird die Einführung der nächsten Mobilfunkgeneration erwartet. Bosch engagiert sich schon in zahlreichen Projekten und Allianzen, um die Grundlagen für 6G-Standard mitzugestalten.



AM SPRUNG ZUR 6. GENERATION

Weltweit nehmen Forschung und Entwicklung für den zukünftigen Mobilfunkstandard 6G an Fahrt auf. Unternehmen und Staaten investieren massiv in diese Technologie. Bosch engagiert sich umfassend auf nationaler wie internationaler Ebene in Projekten, Kooperationen und Initiativen, um wichtige Grundlagen für die 6G-Technologie zu erarbeiten. „6G wird weit mehr sein als eine reine Infrastruktur für Vernetzung, es wird autonom fahrenden Autos, intelligenten Städten und vernetzten Industrien einen enormen Effizienzschub geben. Deswegen ist 6G für Bosch ein strategisch wichtiges Technologiefeld“, sagt Dr. Andreas Müller, der bei Bosch 6G-Aktivitäten bündelt und leitet. Im Unternehmen befassen sich derzeit rund 40 Mitarbeitende mit der 6G-Technologie. „In den kommenden zwei Jahren werden es voraussichtlich doppelt so viele sein“, so Müller. Gegenwärtig investiert Bosch einen mittleren siebenstelligen Betrag in die Forschung und Entwicklung von 6G.

Netze mit sechstem Sinn. Die nächste Mobilfunkgeneration wird unter anderem neue Funktionalitäten ähnlich zu Radar-Sensoren integrieren. Mit 6G wird es möglich sein, die Position von Objekten im Abdeckungsbereich des Netzes zu erfassen – und zwar ohne, dass diese Objekte mit einem Funkmodul ausgestattet sein müssen. 6G wird extrem hohe Datenraten von bis zu einem Terabit pro Sekunde ermöglichen, bei gleichzeitig sehr geringen Latenzzeiten in der Größenordnung von rund 100 Mikrosekunden – das ist vier Mal schneller als ein Blitzeinschlag. Dadurch wird es beispielsweise mithilfe digitaler Zwillinge möglich sein, Fertigungsabläufe aus der Realität in einer virtuellen Welt ohne zeitliche und räumliche Einschränkung zu überwachen und zu simulieren. Experten gehen davon aus, dass der erste 6G-Standard voraussichtlich im Jahr 2028 fertiggestellt sein wird. In den vergangenen Monaten wurden in Europa zahlreiche 6G-Projekte ins Leben gerufen.

Umfassendes Bosch-Engagement. Bosch bringt seine Expertise und Erfahrung in derzeit fünf öffentlich geförderte Projekte ein. Hierbei zielen die Projekte „6G-ICAS4Mobility“, „Komsns-6G“ und „6G-Brains“ primär auf die Integration von Kommunikation und sensorbasierter Umfeld-Erkennung. Bei erstgenanntem Projekt hat Bosch die Konsortialführerschaft übernommen. Neben der Betrachtung von relevanten Szenarien für den Straßenverkehr sollen Erkenntnisse aus der Projektarbeit insbesondere auch als technische Grundlage für Anwendungen im Bereich vernetzter Drohnen sowie im Bereich Industrie 4.0 etwa für fahrerlose Transportsysteme dienen. Bei den Projekten „6G-Anna“ und „6G-Shine“ stehen neue Vernetzungsstrukturen im Fokus. Diese sollen zukünftige E/E-Architekturen in Fahrzeugen oder Roboterzellen in der Industrie effizienter gestalten. Zudem beteiligt sich Bosch aktiv auch an frühen Diskussionen und Aktivitäten zu künftigen Mobilfunkstandards innerhalb verschiedener Industrieallianzen. Bei der „5G Automotive Association (5GAA)“ etwa arbeiten führende Unternehmen aus der Automobil- und Telekommunikationsbranche zusammen, um Lösungen für die Mobilität der Zukunft zu entwickeln. Bei der „5G Alliance for Connected Industries and Automation (5GACIA)“ legen Industrieunternehmen ihren Fokus auf die Vernetzung von Maschinen und Anlagen.

www.bosch.com

MESSE MÜNCHEN

Versteht die KI nur Daten oder auch Business?

HIER FINDEN SIE DIE ANTWORTEN. AUTOMATICA 2023

automatica

The Leading Exhibition for Smart Automation and Robotics

27.–30. Juni 2023 | München

automatica-munich.com

VDMA

Robotik + Automation

DIE KRAFT VON FACTORY EDGE

In der Fertigung gewinnt die Umsetzung innovativer Industrie-4.0- und IoT-Szenarien zunehmend an Bedeutung. Das entscheidende Hilfsmittel dabei ist Factory Edge. Mit diesem Konzept kann die produzierende Industrie die Fertigungs- und Logistikprozesse entscheidend optimieren.

Edge Computing ist branchenübergreifend ein Trendthema. Zentrale Treiber im produzierenden Gewerbe sind Industrie-4.0-Projekte. Dabei geht es um Themen wie IoT, Künstliche Intelligenz, Robotik, Augmented und Virtual Reality, Blockchain, 3D-Druck, Digitale Zwillinge oder 5G. Um Industrie-4.0-Konzepte erfolgreich umzusetzen, müssen umfangreiche Datenmengen schnell analysiert werden. Diese Aufgabe fällt zu einem großen Teil direkt an der Produktionslinie mittels Vernetzung der IT mit den Anlagen oder Steuersystemen an: also an der Factory Edge. Edge Computing unterstützt dabei die Verlagerung der Datenverarbeitung von zentralisierten Rechenzentren an diese verteilten Standorte. Im Fall von Factory Edge etwa an ein Device wie einen Roboter in der Fabrikhalle. Die Vorteile sind vielfältig. Wenn Rechenoperationen, einschließlich Datenverarbeitung und -analyse, näher an der Quelle durchgeführt werden, gibt es keine besonderen Anforderungen hinsichtlich Latenz oder Bandbreite. Außerdem werden durch die Reduzierung von Übertragungsverzögerungen auch Serviceausfälle vermieden. Dadurch erweist sich Edge Computing als ideale Basis für die Umsetzung von Industrie-4.0-Projekten im produzierenden Gewerbe. Eine Factory-Edge-Infrastruktur unterstützt auch eine stärkere Vernetzung von Fertigung und Logistik, sowie die Optimierung von Produktionskapazitäten und Logistikprozessen. Es können unter anderem auch potenzielle Fehler an der Montagelinie proaktiv entdeckt, die Produktqualität verbessert und mögliche Ausfallzeiten durch eine vorausschauende Wartung reduziert werden. Und selbst im Falle einer Beeinträchtigung der Kommunikationsverbindung mit einem zentralen Standort können einzelne Fertigungsanlagen weiter betrieben werden.

Veränderte Anforderungen. Voraussetzung für die Umsetzung einer Factory Edge mit der Neuordnung von Prozessen und der Datennutzung ist eine adäquate Systemlandschaft. Dazu zählen Sensoren, drahtlose Gateways, operative Dashboards oder agile Backend-Systeme. Vor allem aber bedeutet die Vernetzung und Digitalisierung in der Produktion eine Verknüpfung der IT mit den Anlagen oder Steuersystemen. Und daraus ergeben sich auch veränderte Anforderungen an die IT selbst. Für die Realisierung einer modernen Fertigungsumgebung ist eine IT-Infrastruktur erforderlich, die auf Containern, Kubernetes, agiler Entwicklung, Künstlicher Intelligenz und Machine Learning sowie Automatisierung basiert. Diese Technologien sind Komponenten einer offenen Hybrid-Cloud-Plattform wie etwa Red Hat OpenShift, die auch umfassende Edge-Implementierungen unterstützt.

Hybrid-Cloud-Infrastruktur als Fundament. Das Thema Factory Edge gewinnt auf breiter Front an Relevanz. So arbeitet etwa die Initiative OMP (Open Manufacturing Platform) an der Entwicklung von innovativen Industrie-4.0-Lösungen und IIoT (Industrial Internet of Things)-Anwendungen. Die von der BMW Group und Microsoft gegründete OMP, der auch Red Hat angehört, will durch Open Source und offene Standards die Digitalisierung der Produktion forcieren, gerade auch im Kontext der Factory Edge. Diese Technologien sind Komponenten einer offenen Hybrid-Cloud- oder Multi-Cloud-IT-Infrastruktur, die die Bereitstellung von Anwendungen in kurzen Entwicklungszyklen in einer dynamisch skalierbaren Umgebung ermöglichen. Mit einer Hybrid Cloud steht eine konsistente Plattform für Bare-Metal- und virtuelle Umgebungen sowie für Private und Public Clouds zur Verfügung. Selbstverständlich muss eine offene Hybrid-Cloud-Plattform auch umfassende Edge-Implementierungen unterstützen. Edge Computing muss damit zu einem integralen Bestandteil einer Open-Hybrid-Cloud-Strategie werden. Mit einer über alle Umgebungen hinweg konsistenten Plattform kann eine konsistente Entwicklungs- und Betriebserfahrung vom Core bis zum Edge etabliert werden. Eine Hybrid-Cloud-Plattform unterstützt auch die Portabilität von Applikationen. Dies ist wichtig, weil Fachapplikationen oft zentral entwickelt werden und dann in den verschiedenen Cloud-Umgebungen bis hin zu den Edge-Komponenten ausgerollt werden müssen. Aus technologischer Sicht haben sich hierbei auch im Edge- und IoT-Umfeld die Container-Technologie und Kubernetes als Container-Orchestrierungs-Framework für den Einsatz der Cloud-Services bis hin zu den Edge-Devices zunehmend bewährt.

Fazit. Generell wird Factory Edge die Basis für die Umsetzung innovativer Industrie-4.0- und IoT-Szenarien sein – und damit für effiziente und intelligente Geschäftsprozesse. Und die zugrunde liegende IT-Infrastruktur wird eine offene Hybrid-Cloud-Architektur sein, die die einheitliche Erstellung und Ausführung von Lösungen in Cloud-, On-Premises- und Edge-Umgebungen unterstützt.

www.redhat.com

IOT-LÖSUNG FÜR KLEINE GEBÄUDE

Connect Box, Teil des Siemens-Xcelerator-Portfolios, ermöglicht die Vernetzung, Überwachung und den Betrieb von kleinen bis mittelgroßen Gebäuden. Das macht den Betrieb effizienter, senkt den Energieverbrauch und unterstützt die Umsetzung der gesetzlichen Anforderungen an nachhaltige und gesunde Gebäude.

© Jcomp/freepik

Auch für kleinere und mittlere Gebäude, die bisher ohne Gebäudeautomation betrieben wurden, werden Energieeffizienz und Klimaneutralität immer wichtiger – zum einen aus Kostengründen, zum anderen, weil immer mehr behördliche Auflagen erfüllt werden müssen, die einen nachhaltigen Betrieb erfordern. In Europa unterstützt beispielsweise die EU-Richtlinie über die Gesamtenergieeffizienz von Gebäuden (EPBD) das Ziel der EU, bis 2050 einen klimaneutralen Gebäudebetrieb zu erreichen, und zwingt Gebäudebesitzer und -betreiber zum Handeln. Aus technischer Sicht bieten IoT-basierte Gebäudelösungen nicht nur die Voraussetzungen, um solche Anforderungen umzusetzen, sondern sie zahlen sich auch aus. Siemens Smart Infrastructure bringt mit Connect Box eine offene und benutzerfreundliche IoT-basierte Lösung für das Management kleiner bis mittelgroßer Gebäude auf den Markt. Die neueste Ergänzung im Siemens-Xcelerator-Portfolio bietet einen benutzerfreundlichen Ansatz zur Überwachung der Gebäudeperformance. Connect Box hat das Potenzial, die Energieeffizienz um bis zu 30 Prozent zu optimieren und die Raumluftqualität in kleinen bis mittelgroßen Gebäuden wie Schulen, Einzelhandelsgeschäften, Wohnhäusern oder kleinen Büros erheblich zu verbessern. Siemens Xcelerator ist eine offene digitale Business-Plattform, die Kunden dabei unterstützt, die digitale Transformation einfacher, schneller und skalierbar umzusetzen..

www.siemens.com

MIT **MICRO-DATA-CENTER-LÖSUNGEN** VON DER DIGITALISIERUNG PROFITIEREN

Mit der Umstellung auf eine immer smartere Produktion fallen immer höhere Datenmengen an, die sinnvoll verwaltet und verarbeitet werden müssen. Doch wo legt man kritische Daten am besten ab? Im Podcast „heise meets…" sprach Rittal-Experte und Global Portfolio Manager IT Projects Ian-Hendrik Hannemann über die Schwachstellen einer reinen Cloud-Lösung und die Vorzüge der RiMatrix Micro Data Center, sowie wann die Mikrorechenzentren „im Haus" sinnvoll sind und wie die Zukunft in Sachen Datenverwaltung aussieht.

Ein Micro Data Center ist im Prinzip nichts anderes als ein kleines Rechenzentrum, in dem Server, Speicher und IT-Technik überwacht, gekühlt und gesichert werden können. Ein Micro Data Center ist platzsparend und flexibel. Der Planungsaufwand gering, die Implementation sehr einfach. Zudem handelt es sich um ein modulares System, das jederzeit mit einem Rack erweitert werden oder als Erweiterung eines großen Rechenzentrums dienen kann – zum Beispiel dann, wenn ein Unternehmen mehrere Standorte hat. Darüber hinaus kann ein Micro Data Center dabei helfen, CO_2 und Energie einzusparen.

Der Trend der letzten Jahre geht eher in Richtung Verlagerung der Daten in eine Cloud. Dennoch spricht einiges dafür, bestimmte Daten wieder On-Prem zu verwalten. Bei der Echtzeitauswertung, beispielsweise perspektivisch in einer Smart Factory, werden die steigenden Datenmengen bei einer Cloud-Anbindung zunehmend zum Problem: Diese müssen erst einmal zu den großen Servern der Anbieter übertragen werden. Dabei geht kostbare Zeit verloren. Ein Vorteil von Micro Data Centern gegenüber einer reinen Cloud-Lösung sind die kurzen Latenzzeiten. Die Frage, die sich Unternehmen außerdem stellen sollten: Welche Daten will ich überhaupt an eine Cloud geben und welche sollten im eigenen Netzwerk bleiben?

Nachholbedarf in Sachen Datenkompetenz. Daten sind das Gold des 21. Jahrhunderts. Viele amerikanische Konzerne verdienen eine Menge Geld mit dem Verkauf von sensiblen Daten. Deshalb ist es wichtig, zumindest einen Teil der Daten zurück ins eigene Netzwerk zu holen und darüber die Hoheit zu haben. Ein wichtiges Thema dabei ist natürlich immer die Sicherheit. In erster Linie bietet ein Micro Data Center Schutz vor ungewollten physischen Zugriffen oder Umwelteinwirkungen, nicht vor Cyberangriffen.

Natürlich kann es aber auch beim Wiederaufbau einer IT-Infrastruktur nach einem Angriff helfen: Die Lösung ist schnell skalierbar, modular aufbaubar und hat kurze Lieferzeiten. Somit kann man schnell wieder den Betrieb aufnehmen.

EDGE MICRO DATA CENTER: IM BUNDLE SCHNELL KONFIGURIERT

Sie sind kompakt, leistungsstark und ein vollwertiges Zuhause für IT-Hardware. Rittal RiMatrix Micro Data Center bestehen aus abgestimmten OT-Komponenten für Rack, Power, Cooling, Monitoring und Security. Mit diesen fertig vordefinierten Bundles für Edge-Lösungen kann ein Rechenzentrum äußerst effizient geplant werden: zeitsparend, da alle Komponenten plausibel aufeinander abgestimmt sind, und energiesparend, da für jede Größe die optimal passende Kühllösung angeboten wird. Die RiMatrix Micro Data Center bleiben dennoch flexibel und können an veränderte Umgebungs- und Anwendungsbedingungen angepasst werden. Sie sind schnell realisierbar und stellen ohne aufwendige bauliche Veränderungen die komplette IT-Infrastruktur für z.B. Verwaltungen und Supermärkte bereit, können aber auch als Edge Data Center in der Produktion eingesetzt werden.

Optimal ist die Kombination. Da Prozesse zunehmend digitalisiert werden, werden künftig viele Unternehmen auf eine Kombination von Cloud-Edge-Lösungen setzen: Bei einer Cloud kann man von den großen Speichermöglichkeiten und Analysetools profitieren, Edge-Lösungen helfen dabei, die Latenz zu senken und die Hoheit über sensible Daten zurückzugewinnen. Im Bildungssektor oder einer Behörde kann ein kleines Micro Data Center die notwendige Rechenkapazität vor Ort zur Verfügung stellen und es besteht keine Gefahr, dass sensible Schüler- oder Stammdaten nach außen gelangen. Profitieren kann von solchen Lösungen aber so gut wie jede Branche – sowohl eine Supermarktkette mit mehreren Filialen als auch kleine Unternehmen, die ihre Produktion digitalisieren möchten.

www.rittal.at

Der Autor
Ian-Hendrik Hannemann
... ist Rittal-Experte und Global Portfolio Manager IT Projects

| EC12-15G |

Für die einfache Kommunikation mit der Cloud ...

... und die Steuerung komplexer Maschinen

Der Beckhoff IoT-Controller

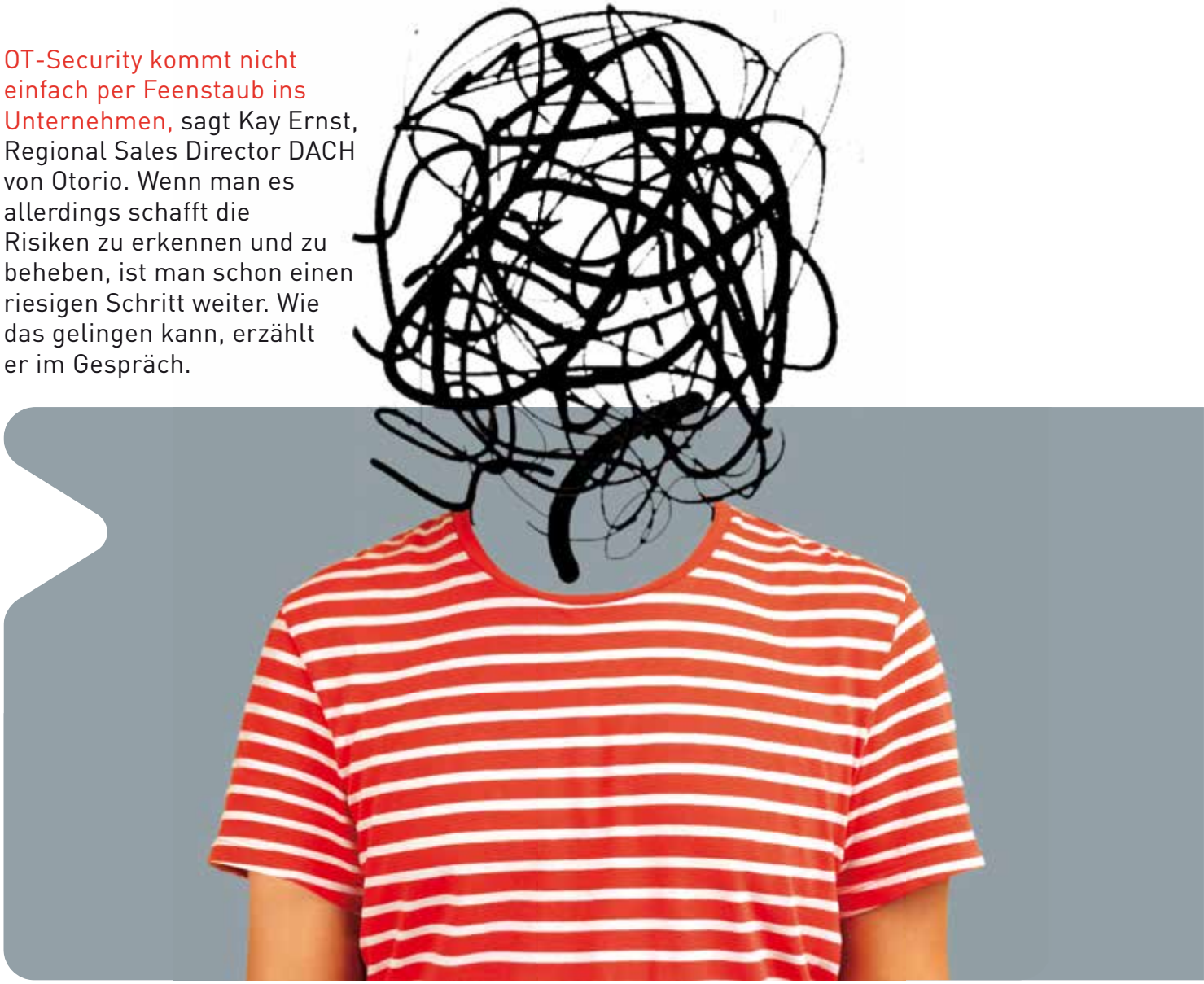
Mit den kompakten Embedded-PCs der CX-Serie und dem Softwaremodul TwinCAT IoT ermöglicht Beckhoff die Steuerung komplexer Maschinen mit gleichzeitiger Cloud und Big Data Connectivity. Dabei profitieren Anwender gleich doppelt vom Prinzip der offenen Steuerungstechnik: nach unten ins Feld durch variable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

Scannen und die Einsatzmöglichkeiten des IoT-Controllers erleben

HANNOVER MESSE
Halle 9, Stand F06

New Automation Technology BECKHOFF

OT-Security kommt nicht einfach per Feenstaub ins Unternehmen, sagt Kay Ernst, Regional Sales Director DACH von Otorio. Wenn man es allerdings schafft die Risiken zu erkennen und zu beheben, ist man schon einen riesigen Schritt weiter. Wie das gelingen kann, erzählt er im Gespräch.



GEGEN DAS GROSSE RAUSCHEN

IoT 4 Industry & Business: Gibt es Ihrer Meinung nach die vielzitierte Trennung zwischen OT und IT noch?

Kay Ernst: Das ist nach wie vor eine total relevante Frage. In den meisten Unternehmen gibt es diese Trennung. Und zwar nicht nur zwischen der Office-IT und der Produktionsseite, sondern auch innerhalb der OT. Denn in jeder Produktion gibt es unterschiedliche Bestandteile, wie die eigentlichen Automatisierungskomponenten, aber auch Netzwerk-, Security- und IoT- oder IIoT-Komponenten. Die Leute in der OT machen ihre Jobs seit 20 Jahren sehr tief, sehr detailliert und vor allem gut. Aber sie haben wenig Verständnis für die Security. Auf der anderen Seite stehen die IT-Leute, die Verständnis für die Security, dafür aber oft keines für die Bedürfnisse der OT-Seite haben. Es gibt aber Hoffnung auf Besserung. Denn es gibt einen Trend hin zu einer Gesamtverantwortung für den CISO oder den Chief Risk Officer. Und diese zentrale Verantwortung ist ein Schlüssel für erfolgreiche OT-Cybersecurity-Projekte. Das heißt aber auch: Der CISO hat künftig nicht nur eine technische, sondern er hat auch eine kulturelle Aufgabe zu erfüllen – nämlich die Teams zueinander zu führen.

IoT: Wo liegen aktuell die größten Treiber in der OT-Security?
Ernst: Wir haben letztes Jahr für unseren Cybersecurity Survey Report eine Gruppe von 200 Unternehmen befragt. Der Haupttreiber für die Maßnahmen ist tatsächlich als allererstes Compliance. Wer hätte das gedacht? Staatliche Vorgaben führen tatsächlich zu einer Verbesserung der Situation. Zweitens Wachstum. Den Unternehmen ist klar, dass sie nicht wachsen können, ohne Security intrinsisch miteinzubauen. Und erst an dritter Stelle kommt tatsächlich die Furcht vor Angriffen. Allerdings liegen diese drei Plätze sehr, sehr nahe beieinander. Bei der Furcht vor Angriffen ist eine Fokussierung auf die Supply Chain zu beobachten. Den Unternehmen ist bewusst, dass sie nicht nur auf die erste Schicht, sondern durchgängig auf die komplette Lieferkette schauen müssen. Das Bewusstsein wächst auf jeden Fall. Angriffe auf die OT-Infrastruktur waren bisher typischerweise Nation-State-Angriffe, sprich ein Land will die Infrastruktur von einem anderen Land schwächen. Dadurch, dass die Werkzeuge vereinfacht wurden bzw. jedem zur Verfügung stehen, kann jeder Angriffe auf die OT eines Unternehmens starten.

IoT: Otorio sagt, dass es nicht mehr darum geht einfach nur zu reagieren, sondern proaktiv zu sein. Wie macht man das?
Ernst: Unternehmen haben viel Geld und Know-how in Security-Maßnahmen investiert. Diese führen aber nicht immer zu einem wirklich kongruenten Endergebnis, das vom Betrachten einzelner Vorfälle, hin zu einem einheitlichen Risikomanagement geht. Denn das ist es, wohin Unternehmen im Grunde wollen. Sie wollen hin zu einem großen Bild. Und das fehlt noch. Das zu wissen, ist eine ganz, ganz entscheidende Erkenntnis. Security-Mechanismen erzeugen irrsinnig viel Rauschen. Selbst wenn ich ganz tolle Alarme durch Virenscanner, Detection-Systeme oder Firewalls habe, sobald es in der Produktion kein SOC (Security Operations Center) gibt, verhallen diese Alarme. Ein weiteres Problem der heutigen Verfahren ist: Sie helfen bei der Schadensminimierung post mortem. Sie helfen aber nicht bei beim Risikomanagement vorher. Ein Angriff erfolgt anhand einer Cyber Kill Chain. Egal ob auf die IT oder die OT, Otorio hilft dabei, dass man genaue Informationen über Schwachstellen innerhalb der gesamten Kette bekommt. Also weg vom Sehen der Einzelteile, hin zu einer kontextualisierten Betrachtung.

IoT: Wie bekommt man diesen Überblick?
Ernst: Auf der Produktionsseite gibt es jeden Tag tausende Alarme, Logeinträge, Events oder IDS-Meldungen. Das kann ein Mensch kaum bewerkstelligen. Und genau das ist es, was unsere Technologie RAM² korreliert und kontextualisiert. Sie zeigt jene Bereiche, die tatsächlich relevant sind und ein praktisch ausnutzbares Risiko darstellen. Ein grundsätzliches Problem bei der OT ist ja: Sie ist irrsinnig zerfasert. Es gibt allein für Automatisierungstechnik über 600 Hersteller. Es ist aber nötig, alles was es in der Produktion gibt, mit in die Security-Betrachtung aufzunehmen. Denn alles spielt eine Rolle. Daher gehört es zu unserem täglichen Geschäft, die vielen Anbieter zu integrieren. Ein großer Teil unserer Kollegen sind Forscher. Die machen nichts anderes, als sich den ganzen Tag Zugang zu Industrie-Komponenten zu verschaffen – entweder beim Proof of Concept beim Kunden oder durch Automatisierungstechnik-Anbieter, die uns bitten ihre Komponenten hinsichtlich Security zu prüfen. Daher hat Otorio einen sehr großen Wissensschatz. Und dieses Wissen fließt in unsere Technik ein.

IoT: Wie arbeitet ihre Technologie konkret?
Ernst: Jeder Anbieter von Automatisierungstechnik hat heute seinen eigenen digitalen Zwilling, der aber nicht quer über die gesamte Infrastruktur arbeitet. Wir erstellen genau diesen digitalen Zwilling, der ein Eins-zu-eins-Abbild der kompletten Produktion zeigt. Und dann wird er einer Angriffssimulation ausgesetzt. Wenn man schon mal einen Pen-Test in einer lebendigen Produktionsumgebung mitverfolgt hat, dann weiß man: Das ist super anstrengend. Denn der Pen-Tester ist limitiert, um die Produktion nicht lahmzulegen. Anders unser digitaler Zwilling. Den kann man testen, bis »

Kay Ernst
Regional Sales Director DACH von Otorio

„Egal ob auf die IT oder die OT, Otorio hilft dabei, dass man genaue Informationen über Schwachstellen innerhalb der gesamten Kette bekommt. Also weg vom Sehen der Einzelteile, hin zu einer kontextualisierten Betrachtung."

Die Trennung zwischen IT und OT ist nach wie vor ein relevantes Thema in den Unternehmen.

man wirklich alle Angriffsvektoren gefunden hat. Das ist ein kontinuierlicher Prozess. Und er ist automatisiert. Außerdem funktioniert unsere Technik autark, ohne Internetverbindung und ohne Verbindung in unser eigenes Netzwerk. Wenn ein neues Gerät oder eine neue Softwareversion hinzukommt und sich dadurch eine neue Risikosituation ergibt, wird auch das automatisch erkannt. Als logische Folge gibt es auch gleich Rat in Form von Playbooks. Und dieser Rat – und das ist ein großer Unterschied zur IT – lautet nicht: Spiele die folgenden Security-Patches ein. Wir haben einen anderen Zugang. Wenn eine ausnutzbare Schwachstelle in der Produktionsanlage entdeckt wird – etwa die Firewall lässt eine Ausnutzung zu, bei einem Remote Desktop Service musste bislang kein Passwort eingegeben werden – muss die mögliche Angriffskette eben dort vorne unterbrochen werden.
Ein angenehmer Bestandteil und damit weiterer Vorteil unserer Technologie kommt beim Thema Compliance zum Tragen. Es gibt professionelle Organisationen, die die Audits in den Unternehmen übernehmen. Allerdings gibt es dabei ein Problem: Wenn man ein halbes Jahr später wieder ein Audit machen lässt, dann kommt unter Umständen ein anderer Auditor, bei dem möglicherweise ein anderes Ergebnis herauskommt. Das heißt: Es ist einfach klug, sich beim Audit die technischen Informationen automatisiert zu holen. Das vereinfacht den Prozess irrsinnig und macht ihn schneller, objektiver und günstiger.

IoT: Auf Ihrer Website gibt es ein Erklärvideo zu RAM². Es wirkt so, als wenn alles wahnsinnig einfach funktioniert.
Ernst: Aufgrund der Komplexität der Dinge funktioniert OT-Cybersecurity nicht einfach per magischem Feenstaub. Ja, in der Theorie ginge es, wenn alle Anlagen von einem Hersteller sind und der Kunde eine Struktur hat. In der Praxis hat man immer heterogene Landschaften, auch noch aus unterschiedlichen Generationen. Und deswegen müssen solche Projekte gut vorbereitet angegangen werden. Es ist wichtig mit dem Kunden vorher über seine Infrastruktur zu sprechen und wie die Informationsgewinnung geschehen soll. Sobald unser System funktioniert, dann tatsächlich mit minimalem Wartungsaufwand. Aber es ist wie mit allen großen Sachen: Sie erfordern am Anfang einen gewissen Investitionsaufwand, um dann später großen Wert zu generieren und ganz wenig Pflegebedarf zu haben.

IoT: Was erwarten Sie vom heurigen Jahr hinsichtlich OT-Security?
Ernst: Es wird alles immer noch verbundener und es gibt immer noch mehr Helferlein, noch mehr Systeme, die aus Bequemlichkeitsgründen irgendwo schnell ohne spezielles Security-Bewusstsein ausgerollt werden. Das bedeutet, dass die Dimension von Gerätschaften, die Teil einer Risikobetrachtung sein müssen, weiter exponentiell steigen wird. Die Angriffe werden nicht weniger, Systeme werden komplexer und deswegen muss auch die Supply Chain immer intensiver betrachtet werden. Außerdem erwarten wir, dass die Regulierungen, die auf europäischer Ebene fixiert sind und noch auf nationaler Ebene umgesetzt werden müssen, einen großen Einfluss auf das Bewusstsein bei Unternehmen haben und das Thema OT-Security auf die Geschäftsführungstische heben werden. Auf der Habenseite – und das gibt mir Hoffnung – sehen wir den schon angesprochenen Trend, dass in der Produktion nicht mehr jeder siloartig für seinen eigenen Bereich verantwortlich ist, sondern dass es eine Person gibt, die für die Cybersecurity zuständig ist und die unterschiedlichen Abteilungen und Funktionen ansteuert. Das macht Cybersecurity-Projekte in der OT letztendlich erfolgreich.

www.otorio.com

File Read ermöglicht den Zugang zu Prozessdaten, die über XML-Dateien verfügbar sind.

© Softing Industrial

Die neue Funktion „File Read" der dataFeed OPC Suite Extended V5.25 ermöglicht den Zugang zu Prozessdaten, die über XML-Dateien verfügbar sind.

ZUGANG ZU XML

OPC ist der weltweit führende Interoperabilitätsstandard für einen sicheren und zuverlässigen Datenaustausch in der industriellen Automatisierung und in weiteren Anwendungen. Er stellt den lückenlosen Informationsfluss zwischen Geräten und Software-Anwendungen unterschiedlichster Hersteller sicher. Mit mehr als 20 Jahren Erfahrung in der OPC-Technologie und mit einer engen Arbeitsbeziehung zur OPC Foundation ist Softing der ideale Partner für alle OPC-Themen. Softing, mit Buxbaum Automation als Niederlassung in Österreich, entwickelt und vermarktet eine breite Palette von Entwicklungswerkzeugen und Endkundenprodukten, darunter Gateways für innovative und sichere IoT-Architekturen. Damit lassen sich sowohl in Bestandsanlagen als auch in neuen Werken modernste Lösungen für OPC-basierten und optimal auf individuelle Anforderungen zugeschnittenen Datenaustausch realisieren. Mit der dataFeed OPC Suite Extended erhalten Anwender ein Komplettpaket für OPC-Kommunikation und Cloud-Anbindung, mit dem auf die Steuerungen führender Hersteller und auf IoT-Geräte zugegriffen werden kann. Mit der neuen „File Read"-Funktionalität gewährleistet die Suite den Zugang zu Brownfield PLCs, Geräten und Maschinen, die Daten über XML-Dateien liefern.

Schnelle und einfache Datenintegration. File Read ermöglicht die schnelle und sichere Integration von Prozesswerten aus XML-Dateien in Anwendungen der Produktionssteuerung wie MES oder OEE über die Standardschnittstellen OPC Classic oder OPC UA. Die Produktionsdaten lassen sich außerdem über MQTT oder REST in IIoT-Cloud-Lösungen integrieren. Weiterhin besteht die Möglichkeit des Datenloggings zur Dokumentation, Analyse oder Verifizierung in einer separaten Datenbank.

Eine All-in-One-Datenintegrationslösung. Die dataFeed OPC Suite ermöglicht den Zugriff auf die Steuerungen führender Hersteller wie z.B. Siemens Simatic S7, Rockwell ControlLogix, B&R, Mitsubishi sowie auf Modbus-Steuerungen (z.B. von Wago). Sie fungiert als Gateway zwischen den beiden OPC-Standards, so dass bestehende OPC-Classic-Komponenten und -Anwendungen in moderne Industrie-4.0-OPC-UA-Lösungen eingebunden werden können. Die Übertragung von Produktionsdaten in IoT-, Cloud- oder Big-Data-Anwendungen erfolgt über die Protokolle MQTT und REST. Die Suite unterstützt die Speicherung von Produktionsdaten in einer Datei, in einer SQL-Datenbank oder in MongoDB und CouchDB. Dank der umfangreichen Datenvorverarbeitungsfunktionalität können Daten einfach und flexibel angepasst werden. Mit der OPC-UA-Reverse-Connect-Funktionalität gewährleistet die Suite außerdem eine sichere Kommunikation zwischen OPC-UA-Komponenten, die durch Firewalls oder DMZs getrennt sind.

https://myautomation.at

Der Autor

Dietmar Buxbaum

... ist Gründer und Geschäftsführer der Buxbaum Automation GmbH und steht für eine lange Reihe an gelungenen Projekten für industrielle Kommunikation, Identifikation und Bildverarbeitung. Ein Schwerpunkt des Unternehmens ist die kompetente Beratung, die Begleitung bei der Implementierung von industriellen Prozessen und Schulung.

ES WÄCHST ZUSAMMEN, WAS ZUSAMMENGEHÖRT

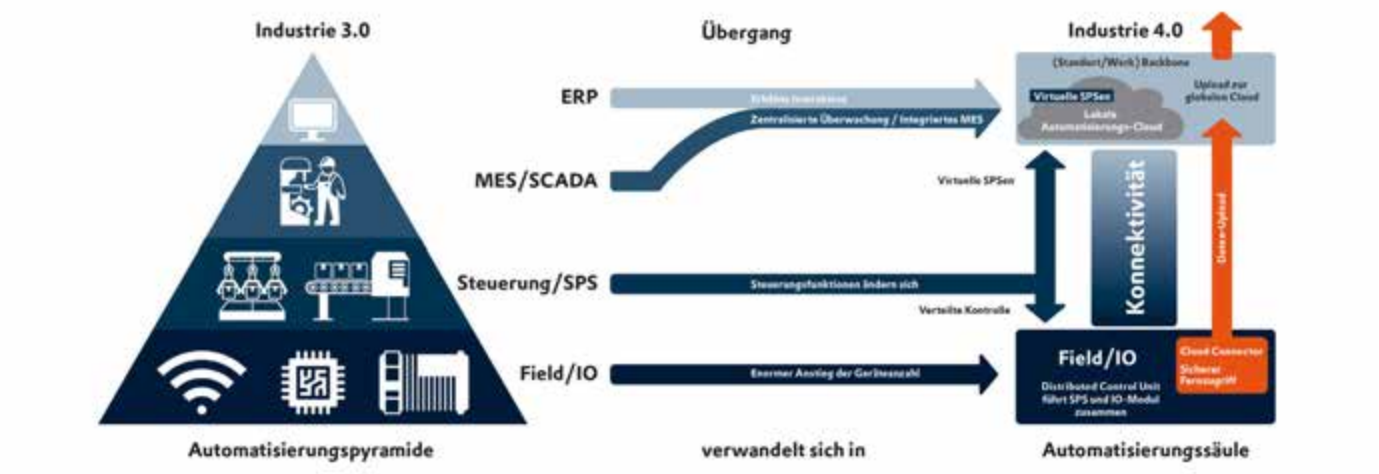
Die Welten der OT und der IT bewegten sich bislang in völlig unterschiedlichen Bahnen. Seit Kurzem nähern sich die Umlaufbahnen dieser beiden Astralkörper an. Was ist die Ursache? Und wie können Konvergenzen geglättet werden, damit es nicht zu unschönen Kollisionen kommt? Bei Copa-Data kennt man die Antworten.

Technologien zwischen IT und OT sind oftmals dieselben. Windows und Linux werden im OT-Umfeld verwendet, aber auch Netzwerkprotokolle wie TCP und UDP. Und darauf basierende Protokolle wie beispielsweise SOAP (Simple Object Access Protocol) als Basis von OPC UA, um zwischen Server und Client Daten auszutauschen. Das erklärte Ziel: Die Kosten der Fertigung senken. Einerseits soll das durch stärkere Automatisierung und effizientere Nutzung von Hard- und Software, andererseits durch die Optimierung des Betriebsablaufs geschehen, die aus der so genannten Datenanalyse resultiert. Dahinter stehen klare wirtschaftliche Interessen. Auch in der IT müssen Systeme rund um die Uhr bereitstehen, wenn es sich z.B. um Software für E-Commerce oder um SaaS-Angebote handelt. In der Finanzbranche gibt es sehr ähnliche Anforderungen, wie sie auch die OT kennt – Datenverlust kommt hier nicht in Frage. Finanzdaten sind zeitbasiert und die Frequenz von Kursschwankungen kann sehr hoch sein, ähnlich denen von Sensordaten in der OT.

Warum waren IT und OT bisher getrennt? IT ist auf die Interaktion zwischen Mensch und Anwendung gerichtet. Hier spielen Bruchteile von Millisekunden meist keine Rolle, da menschliche Prozesse Prozessverzögerungen tolerieren. Auch hat die Vertraulichkeit von Daten oft höhere Bedeutung als Verfügbarkeit und Datenintegrität. OT basiert dagegen auf der ereignisorientierten Interaktion zwischen Bedingungen und Prozesssystemen, was mitunter Regelkreise von zehn Millisekunden erfordert. Von Sei-

ten der Infrastruktur ist üblicherweise ein OT- und IT-Netzwerk notwendig, wodurch die netzwerkübergreifende Interaktion zwischen Anwendungen schwierig wird. Die meisten OT-Systeme wurden bislang isoliert betrachtet. Sie waren gar nicht dafür ausgelegt, aus der Ferne gesteuert zu werden. Zudem hat die OT direkte Auswirkungen auf die Realität, es kommen also Sicherheitsfragen hinzu, etwa beim Start einer Maschine oder beim Ausschalten eines Stromnetzes. Aus diesem Grund sind klare Schnittstellen zwischen beiden Netzwerken erforderlich.

Was hat die Cloud mit der IT/OT-Konvergenz zu tun? Beim Übergang von Industrie 3.0 auf 4.0 werden Softwaresysteme zusammengefasst, virtualisiert und in lokalen oder zentralen Cloud-Lösungen betrieben. Diese Transition und die Erweiterung der Landschaft der Anbieter machen es notwendig, technisch kompatibel zu sein. Sei es in Form von Schnittstellen oder der Unterstützung der Cloud. Wobei der Begriff Cloud oft inflationär verwendet wird. Es geht mehr darum, cloudkompatible Lösungen zu schaffen, sogenannte Cloud-native Software. Diese Art von



Wieso spielt in der OT die Sicherheit so eine große Rolle? In der IT ist es nicht immer üblich, hohe Investitionen in Hardware mit einer entsprechend langen Verfügbarkeit, kombiniert mit regulatorischen oder behördlichen Auflagen zu tätigen. Ein Server ist heute in der IT durch Virtualisierung schnell ersetzt, während die Dienste fast unterbrechungsfrei weiterlaufen. Im OT-Bereich ist dagegen Sicherheit wichtig. Das alles macht es sehr teuer, Updates von Software im OT-Bereich einzuspielen oder gar die Technologie zu wechseln. Verwendete Technologie sollte aus diesem Grund langfristig zur Verfügung stehen, sie sollte etabliert und damit möglichst frei von Kinderkrankheiten sein.

Welche Ziele verfolgt die IT/OT-Konvergenz? Es geht darum, die Prozesse zu optimieren. Das betrifft hauptsächlich den Produktionsprozess selbst, aber auch die Optimierung der Kosten von zum Beispiel IT-Hardware. Um Produktionsprozesse zu optimieren, muss man erst Daten haben. Dadurch findet man sich schnell in einem Geflecht aus verschiedenen Anforderungen wieder. Maschinen, die bereits seit Jahren in der Produktionshalle stehen, müssen nun plötzlich vernetzt werden. Software zur Datenanalyse muss neu angeschafft werden. Die verschiedenen Softwaresysteme sollen harmonisiert werden. Es macht Sinn, einen globalen Blick auf die OT-IT-Landschaft zu werfen. So müssen sich IT-Abteilungen immer stärker engagieren und letztlich auch Entscheidungen über Neuanschaffungen treffen. Die IT-OT-Konvergenz wird mehrere Auswirkungen haben. Technologische Produkte, die im IT-Bereich Stand der Technik sind, wandern mehr als zuvor in die OT-Netzwerke. So werden die IT-Abteilungen mehr und mehr die Anforderungen der OT verstehen.

Software kann man in öffentlichen oder privaten Cloud-Systemen betreiben und zentral oder lokal zur Verfügung stellen. Cloud-native Lösungen laufen üblicherweise auf dem Betriebssystem Linux, da es viele Vorteile hinsichtlich Wartung und Kosten gibt. Die Benutzerschnittstelle (UI) wird meistens webbasiert zur Verfügung gestellt. Kommunikationsprotokolle sind von Anfang an für die Kommunikation über die öffentliche Internetinfrastruktur gebaut, obwohl diese Protokolle natürlich auch lokal genutzt werden können.

Welche Einflüsse gibt es neben der IT/OT-Konvergenz? Der demografische Wandel und die Trends, die von der Generation Z ausgehen, machen sich bemerkbar. Einerseits gehen in den nächsten Jahren sehr viele Fachkräfte der Generation Babyboomer in den Ruhestand, andererseits drängen Mitglieder der Generation Z immer stärker in die Arbeitswelt. Das bedeutet, es geht langjährige Erfahrung verloren; eine Nachbesetzung ist aufgrund von Personalmangel schwierig. Die Generation Z ist die erste Generation, die komplett in der vernetzten Welt aufgewachsen ist. Sie setzt dieselben Maßstäbe an den Bedienkomfort von IT- und OT-Software in Unternehmen wie an die aus dem privaten Bereich.

Fazit. Es entstehen laufend neue OT-Anwendungsfälle. Dafür muss zuerst einmal die Ist-Situation erfasst werden. Das führt zu Systemen, die – allgemein gesprochen – Daten sammeln, zusammenfassen und für die Benutzer in passender Form zur Verfügung stellen. Auch die IT-Abteilungen werden zunehmend in die Entscheidungsprozesse über OT-relevante Software einbezogen. Deshalb muss die IT-Landschaft gesamtheitlich betrachtet werden.

www.copadata.com

CYBERSECURITY **IN FRAUENHAND**

Frauen wird landläufig wenig Interesse an sogenannten MINT-Berufen nachgesagt. Dass das nicht stimmt, zeigt die europäische Initiative „Women4Cyber", die jetzt Zuwachs durch ein Österreich-Chapter bekommen hat. Klares Ziel: den Wirtschaftsstandort Österreich weiblicher und cybersicherer zu machen.

„Cybersicherheit wird immer noch oft als männliche Domäne wahrgenommen. Mit ‚Woman4Cyber' möchten wir einen konkreten Beitrag dazu leisten, mehr Frauen für Berufe in diesem für Unternehmen und den Standort so wichtigen Bereich zu interessieren und das Mindset in der Bevölkerung nachhaltig zu ändern", betonte Martha Schultz, WKÖ-Vizepräsidentin und Bundesvorsitzende von Frau in der Wirtschaft, anlässlich der Kick-Off-Veranstaltung der neuen Cybersecurity-Plattform „Women4Cyber Austria" im November 2022. Das neue Frauennetzwerk hat ein klares Ziel: den Wirtschaftsstandort Österreich weiblicher und cybersicherer zu machen. Vor rund drei Jahren wurde die Dachorganisation „Women4Cyber" in Brüssel gegründet, um Frauen im Bereich der Cybersicherheit zu fördern und das Bewusstsein für eine gender-inklusive Cybersicherheits-Community zu erhöhen. Inzwischen umfasst das europäische Women4Cyber-Netzwerk Niederlassungen in 15 europäischen Ländern, darunter nun auch in Österreich. Im September des letzten Jahres haben die sechs Gründerinnen Verena Becker, Alexandra Horvath, Christina Bäck, Kristina Jovanovska, Stephanie Jakoubi und Ulrike Egger das Österreich-Chapter „Women4Cyber Austria" unter der Führung von Verena Becker eröffnet. „Gerade für Frauen bietet der Bereich Cybersicherheit eine unglaubliche Vielfalt an Möglichkeiten. Women4Cyber Austria will gezielt Mädchen zu technischen Ausbildungen ermutigen und Frauen z.B. mit Mentoringprogrammen unterstützen", hebt Becker die Chancen für Mädchen und Frauen hervor.

Internationales Netzwerk. Nachdem beim Österreich-Chapter „Women4Cyber Austria" die Außenwirtschaft Austria mit an Bo(a)rd ist, hat die Community Zugriff auf weltweite Aktivitäten. „Cybersecurity ist ein länderübergreifender Teamsport", zeigt sich Alexandra Horvath, Co-Founderin und Branchenmanagerin Technology für die Aussenwirtschaft Austria überzeugt und ergänzt: „Nur in einem internationalen Netzwerk, in dem sich die Communities kennen und Wissen austauschen, könne Cybersicherheit gelingen." Ziel der Initiative ist es, neben den geplanten nationalen Aktivitäten, auch das europäische Netzwerk und sogar darüber hinaus zu stärken. Das Angebot der Aussenwirtschaft Austria mit ihren weltweiten Niederlassungen bietet genau das: Von Internationalierungs-Unterstützung bis hin zur Vernetzung österreichischer Cybersecurity Expert:innen bei Inlandsveranstaltungen, Wirtschaftsmissionen, länderübergreifenden Webinaren und Zukunftsreisen. Alexandra Horvath ist dabei auch die richtige Ansprechperson, wenn es um B2B-Events und internationale Vernetzung geht. „Und auch Männer sind herzlich willkommen. Wir sind eine gender-inclusive Community", versichert Horvath, ganz nach dem Motto #schaffenwirgemeinsam.

Vernetzen Sie sich mit den Board Members und der wachsenden Community:

UNBEKANNTE ANGREIFER

Der „Global Perceptions on Threat Intelligence"-Bericht von **Mandiant** zeigt, dass 40 Prozent der befragten Unternehmen in Deutschland in den letzten 12 Monaten Opfer eines Cyberangriffs wurden – sieben Prozentpunkte mehr als weltweit gesehen. Um sich besser gegen Angriffe verteidigen zu können, ist es 77 Prozent der deutschen Umfrageteilnehmer wichtig, Informationen über die Vorgehensweise potenzieller Angreifer zu kennen. Dennoch erklären 81 Prozent der Befragten, dass sie die Mehrzahl der Entscheidungen hinsichtlich der Cybersecurity ohne Informationen zu den Angreifern getroffen werden. Nur 35 Prozent sind der Meinung, dass ihre Organisation überhaupt über ein umfassendes Wissen über die unterschiedlichen Hackergruppen und deren Taktiken, Techniken und Verfahren verfügt. 95 Prozent der deutschen Entscheidungsträger sind der Meinung, dass Cybersecurity-Strategien bei Verfügbarkeit neuer Threat Intelligence nicht schnell genug an die Gefahren angepasst werden. **Jens Monrad**, Head of Mandiant Intelligence, EMEA bei Google Cloud, empfiehlt daher: „Sicherheitsteams sollten sich Threat Intelligence aneignen, die vertrauenswürdig, zeitig und verwertbar ist und relevante Intelligence regelmäßig mit den entsprechenden Interessengruppen bis hoch zur Führungsebene teilen. Dann können Organisationen Security- und Geschäftsentscheidungen mit Einblick in die potenziellen Angreifer treffen."

www.mandiant.com

PARTNERSCHAFT FÜR CYBERRISK MANAGEMENT

Seit Januar 2023 ist das Technologie-Netzwerk **comTeam** neuer strategischer Partner von **Rimian**. Mit dessen Produkt „Lifeblood" können Unternehmen die geforderte Transparenz an ein Sicherheitsprofil zur Vorbeugung und zum Schutz von Angriffen, sowie zum Umgang damit gewährleisten. Die Geschäftsführung erhält die Möglichkeit, zu jedem Zeitpunkt einen exakten Überblick über Cyberrisiken auf die eigenen Prozesse zu haben – und das ohne jegliche IT-Vorkenntnisse. „Bereits nach der ersten Demo waren wir beeindruckt vom Potenzial der Lösung ‚Lifeblood'", erklärt **Sven Glatter**, Geschäftsführer von comTeam und führt weiter aus: „Damit hat Rimian ein effektives Tool geschaffen, das auf die Anforderungen unserer Zeit eingeht: Unternehmen sehen sich mit immer komplexer werdenden Bedrohungen ihrer IT-Infrastruktur und steigenden rechtlichen Anforderungen von Geschäftspartnern und Versicherungen konfrontiert. Rimian hat genau hierfür eine Lösung in der Hand, die nun auch die comTeam-Partner nutzen können, um ihre Dienstleistung auf ein neues Level zu bringen und sich deutlich vom Wettbewerb abzuheben."

www.comTeam.de
www.rimian.io

INDUSTRIELLE KÜNSTLICHE INTELLIGENZ.

THIS IS SICK
Sensor Intelligence.

Deep Learning von SICK eröffnet neue Wege in der Industrieautomatisierung. Bedienungsfreundlich in der Anwendung ermöglicht Deep Learning, in der Cloud künstliche neuronale Netze für SICK-Sensoren mit wenig Aufwand anhand von Beispielbildern zu trainieren.
Vor Ort – in Maschinen oder Anlagen – können die Sensoren anschließend selbst Objekte nach kundenspezifischen Kriterien bewerten und sortieren, auch wenn das natürliche Erscheinungsbild der Objekte variiert.
Wir finden das intelligent. www.sick.com/ai

WIR MÜSSEN

DRAUSSEN BLEIBEN

Wenn Deep Learning als Maßnahme zur Cybersecurity eingesetzt wird, dann lernt die KI die Guten von den Bösen zu unterscheiden und lässt Letztere gleich beim Eingang ins Unternehmen abblitzen. **Kevin Börner,** Distinguished Sales Engineer EMEA von Deep Instinct, erklärt im Interview die Methode.

IoT 4 Industry & Business: 2022 war das Jahr mit den meisten Cyberangriffen. Glauben Sie, dass sich die Angriffe auf einem hohen Niveau einpendeln oder wird dann 2023 das Jahr mit den meisten Angriffen sein?

Kevin Börner: Ich vermute tatsächlich Letzteres. Als ich vor gut zehn Jahren mit dem Thema Cybersecurity angefangen habe, hieß es schon damals, das sei das Rekordjahr der Angriffe. Und ich glaube, je mehr Anwendungen generell digital werden, desto größer ist die Angriffsfläche. Aber ich als unverbesserlicher Optimist gehe davon aus, dass wir es irgendwann schaffen, die geeigneten Schutztechnologien einzusetzen, die das Ganze in einer gewissen Art und Weise stagnieren lassen. Aber es bleibt abzuwarten, ob es tatsächlich so wird.

IoT: Deep Instinct hat einen Cyber Thread Report herausgebracht. Waren für Sie massive Überraschungen dabei oder haben Sie das genauso erwartet?

Börner: Aus unserer eigenen Blase heraus versuchen wir zu erzählen, dass es wichtig ist in Security und in neuartige Technologien zu investieren. Und es scheint so zu sein, dass das gerade im Bereich des Mittelstandes – aus welchen Gründen auch immer – noch nicht so angekommen ist. Denn es werden immer noch Unternehmen, von denen man das nicht unbedingt denken würde, Opfer von Cyberangriffen. Und wenn man sich die Hintergründe dazu anschaut – ein User hat auf eine E-Mail geklickt – könnte man denken: Na ja, das hätte man doch besser wissen können. Das ist es, was mich am meisten überrascht hat.

IoT: Welche weiteren Schlüsse ziehen Sie aus dem Report?

Börner: Wir sehen generell den Trend, dass wir einen größeren Grad an Automatisierung erreichen müssen. Es gibt eine Menge sehr, sehr guter Security-Werkzeuge, die Unternehmen sehr gut schützen können. Vor allem aufgrund des Fachkräftemangels sind diese aber extrem schwierig zu betreiben, da sie zu komplex sind und es an Know-how fehlt. Was wir sehen: Je einfacher selbst das komplexeste Produkt zu benutzen ist und je höher der Grad der Automatisierung ist, desto wahrscheinlicher ist es, dass es auch in seinem vollem Umfang eingesetzt wird und zu seinem vollen Potenzial entfaltet werden kann.

IoT: Deep Instinct bietet Cybersecurity auf Basis von Deep Learning. Wie funktioniert das konkret und auf welcher Basis lernt Ihr System?

Börner: Deep Learning ist an sich ein Teilbereich des sogenannten Maschinellen Lernens und das wiederum ist ein Teilbereich der Künstlichen-Intelligenz-Forschung. Bei Deep Learning geht es vor allem darum, ein bisschen die Wesensart und Denkweise des menschlichen Gehirns nachzustellen. Man spricht dabei von sogenannten Künstlichen Neuronalen Netzen, kurz KNN, die in der Lage sind, komplexe Muster und Beziehungen in sehr großen Datenmengen zu erkennen und daraus Vorhersagen treffen zu können. Das bietet eine ganze Reihe von Anwendungsfällen, die wir auch heute schon tagtäglich benutzen. Computer Vision zum Beispiel, also die Erkennung von Bildern oder das Einordnen von Bildern, wie etwa die Rückwärtssuche von Bildern bei Google. Ein anderes Anwendungsgebiet ist Spracherkennung, wie bei den Amazon- und Google-Geräten, mit denen Sie sprechen können. Und so gibt es eine ganze Reihe von Anwendungsgebieten, wie eben auch Cybersecurity. Bei Deep Instinct geht es vor allem um die Verhinderung von Angriffen durch Vorhersage. Wir haben vortrainierte Deep-Learning-Modelle, die bei uns in unseren Laboren mit Millionen von Daten trainiert werden. Auf einem Endgerät installiert können sie dann voll autonom agieren und Vorhersagen treffen. Etwa wenn eine neue Software auf den PC kommen soll, dann schaut sich das Deep-Learning-Modell diese Software an und kann aus seinem Wissensschatz auf eine Schadsoftware schließen und die Installation blockieren.

IoT: Wäre es möglich, das System zu hacken, um ihm schlechte Sachen zu lernen, damit es Schadsoftware absichtlich nicht als solche erkennt?

Börner: Egal in welchem Bereich der Cybersecurity man sich bewegt, es ist immer ein Kopf an Kopf Rennen zwischen dem Angreifer und dem Verteidiger. Im Bereich von Machine bzw. Deep Learning spricht man von adversarischen Methoden um die Systeme auszuheben oder auszutricksen. Beispiele können sogenannte Poisoning-Attacken sein. Wir härten unsere Modelle in besonderem Maße gegen diese und weitere Arten von Angriffen ab, durch die das Modell zu anderen Ergebnissen kommen könnte. Wir machen das zum einen dadurch, dass wir unsere Daten nur in unseren Laboren trainieren. Zum anderen ist es für denjenigen, der noch nie auf unser Modell geschaut hat, nicht nachvollziehbar oder überhaupt zu verstehen, wo man überhaupt vergiften muss, um ein anderes Ergebnis zu bekommen.

IoT: Sie müssen dem System ja gewisse Informationen zur Verfügung stellen, damit es lernen kann. Dabei macht der Mensch gewisse Vorgaben bzw. schafft einen gewissen Rahmen, in dem dieses Lernen stattfindet.

Börner: Das ist vollkommen richtig. Wir als Menschen müssen dem Modell vorgeben, was es eigentlich tun soll. Wir füttern unsere Modelle aber nicht mit völlig unstrukturierten Daten oder sagen dem Modell: Jetzt schau mal bitte bei Google, was es denn Neues an Schadsoftware gibt. Wir stellen dem Modell einen Katalog an Daten zur Verfügung. Da gibt es zwei Unterscheidungen. Man spricht einmal von Supervised Learning, bei dem man dem Modell klassifizierte Daten mitgibt und zum anderen von Unsupervised Learning, bei dem man dem Modell einen ganzen Haufen an Daten gibt und auf ein Ergebnis wartet. Bei Deep Instinct setzen wir auf Supervised Learning. Dabei treffen unsere Modelle am Ende zwei mögliche Entscheidungen: eine Software ist gut oder schlecht. Sie wird also blockiert oder zur Installation bzw. Ausführung freigegeben. Zur Sicherheit verwenden wir nie dieselben Daten für das Validieren die wir als Eingangsdaten verwenden. Wir trainieren mit völlig unterschiedlichen Daten.

IoT: Wie weit kommt ein Angreifer mit Deep Instinct, bevor er erkannt wird? Kann er tatsächlich nur an die Tür klopfen und dann heißt es schon: Du kommst hier nicht rein.

Börner: Ja, so kann man es tatsächlich sagen. Wir verhindern in über 99 % aller Fälle, dass der Angreifer überhaupt durch die Tür kommt. Und für das fehlende Prozent gibt es technische Sicherungsmaßnahmen. Das ist wie bei vielen Dingen und bei Cybersecurity ist das immer so, man versucht das Risiko zu minimieren. Es gibt keinen Schutz, der alles immer zu jederzeit absichern kann. Also versuchen wir es mit einer möglichst hohen Risikominimierung. Und das gelingt uns aus unserer Sicht mit Deep Learning relativ gut.

www.deepinstinct.com

Kevin Börner
Distinguished Sales Engineer EMEA von Deep Instinct

„Wir haben vortrainierte Deep-Learning-Modelle, die bei uns in unseren Laboren mit Millionen von Daten trainiert werden. Auf einem Endgerät installiert können sie dann voll autonom agieren und Vorhersagen treffen."

Roman Oberauer
Country Managing Director von NTT Ltd. in Österreich

„Eine hundertprozentige Sicherheit gibt es nie, aber der Zero-Trust-Ansatz hat sich als eine der effektivsten Strategien im Bereich der Cybersecurity etabliert."

VERTRAUEN IST GUT, KONTROLLE IST BESSER

In den letzten Jahren hat die Bedrohung durch Cyberangriffe weltweit zugenommen. Um Unternehmen und Organisationen vor solchen Attacken zu schützen, hat sich das Zero-Trust-Konzept als mögliche Lösung etabliert.

Kaum eine Woche vergeht ohne Berichte über einen neuen Cyberangriff auf ein namhaftes Unternehmen, die politisch oder wirtschaftlich motivierten Aktivitäten einer Hackergruppierung oder zumindest einer kritischen Schwachstelle in verbreiteten Systemen sowie ein Verweis auf den Fachkräftemangel in der Cybersicherheit. Die angespannte Bedrohungslage durch Cyberkriminelle verschärft sich zunehmend und Unternehmen sollten ihre IT-Sicherheitsmaßnahmen auf den Prüfstand stellen und anpassen. Ein sehr hohes Sicherheitsniveau verspricht der Zero-Trust-Ansatz. Er folgt dem Credo „Vertraue niemandem, verifiziere jeden" und verbessert damit die Cybersicherheit in modernen IT-Umgebungen, die durch mobile Arbeit, Homeoffice und den Einsatz von Cloud-Plattformen geprägt sind. Bei diesem Ansatz wird grundsätzlich allem und jedem misstraut und verlangt, dass der komplette Datenverkehr geprüft wird und dass sich Nutzer, Geräte, Anwendungen und andere Einheiten bei jedem Zugriff auf Systeme oder Daten authentifizieren müssen.

Effektivste Strategie. Nach wie vor verfolgen die meisten Organisationen das Prinzip „Erst bestätigen, dann vertrauen". Das heißt, wenn jemand die richtigen Nutzeranmeldedaten hat, darf er auf Webseiten, Apps oder Geräte zugreifen. Dies führt allerdings zu erhöhten Sicherheitsrisiken durch Datendiebstahl, Malware- und Ransomware-Angriffe. Heutzutage muss der Schutz innerhalb digitaler Infrastrukturen dort ansetzen, wo sich Anwen-

dungen, Daten, Nutzer und Geräte befinden. Gerade hier kommt Zero Trust ins Spiel. „Eine hundertprozentige Sicherheit gibt es nie, aber der Zero-Trust-Ansatz hat sich als eine der effektivsten Strategien im Bereich der Cybersecurity etabliert", erklärt Roman Oberauer, Country Managing Director von NTT Ltd. in Österreich. „Der Aufbau einer Zero-Trust-Architektur ist sicher kein Projekt, das sich nebenbei umsetzen lässt, aber es zahlt sich auf alle Fälle aus, hier Zeit und Ressourcen zu investieren. Wird es professionell implementiert, können Eindringlinge effizient erkannt und abgewehrt werden. Im Kampf gegen professionelle Cyberangriffe, bei denen herkömmliche IT-Sicherheitskonzepte inzwischen versagen, lohnt sich die Investition in Zero-Trust-Maßnahmen, um langfristig Kosten zu sparen und den Betrieb des Unternehmens aufrechtzuerhalten."

Vertraue niemandem – verifiziere jeden. „Die Gefahr von Cyberattacken war wohl lange nicht so hoch wie jetzt und das wird sie aller Voraussicht nach auch bleiben", erklärt Frank Limberger, Data & Insider Threat Security Specialist bei Forcepoint. „Unternehmen sollten deshalb Maßnahmen ergreifen, um den Schutz ihrer Daten und Systeme zu verstärken. Das Konzept der Zero-Trust-Security bietet ihnen dafür schlagkräftige Verfahren und Technologien." Einige Methoden und Technologien von Zero Trust können Unternehmen laut dem Security-Spezialisten vergleichsweise schnell implementieren und damit ihr Sicherheitsniveau kurzfristig deutlich erhöhen. Mittels Multi-Faktor-Authentifizierung werden etwa Zugangsberechtigungen zu Systemen durch mehrere unabhängige Merkmale überprüft. Dazu zählen etwa Passwörter, Token und biometrische Merkmale wie Fingerabdrücke. Besonders starke Verfahren fügen dem noch eine „Out of Band"-Methode hinzu, beispielsweise einen Code, der dem Nutzer per Push-Benachrichtigung auf sein Smartphone gesendet wird. Identitätsdiebstahl wird durch Multi-Faktor-Authentifizierung erheblich erschwert. Ein Zero Trust Network Access lässt Mitarbeiter und Geräte bei Remote-Zugriffen auf Anwendungen, Daten und Services nur bestimmte Netzwerkprotokolle verwenden. Außerdem haben sie auch nur Zugang zu Ressourcen, für die sie eine ausdrückliche Berechtigung besitzen. Im Gegensatz zu VPNs ist kein potenzieller Zugriff auf sämtliche Systeme und Daten möglich. Gelingt es Angreifern, in ein System einzudringen, können sie sich von dort aus nicht ungehindert im Unternehmensnetzwerk weiterbewegen. Einen ähnlichen Effekt hat das Prinzip des minimalen Zugangs dem Least Privilege Access. Unternehmen nutzen inzwischen viele Anwendungen und Services aus der Cloud, wodurch sich ihre Angriffsfläche deutlich vergrößert. Least Privilege Access stellt sicher, dass Nutzer nur auf Daten in der Cloud zugreifen können, die sie für ihre Arbeit auch wirklich benötigen. Angreifer können dadurch mit gestohlenen Anmeldedaten nur begrenzten Schaden anrichten. Auch Dokumenten, die Mitarbeiter aus dem Internet herunterladen oder als E-Mail-Anhang empfangen, wird grundsätzlich ein mitgeschickter Schadcode unterstellt. Bei Zero Trust Content Disarm and Reconstruction werden deshalb aus den Dokumenten die Informationen, bei denen schädliche Inhalte garantiert ausgeschlossen werden können, extrahiert. Anschließend setzt die Technologie daraus komplett neue Dateien im Ursprungsformat zusammen. Sie sind vollständig frei von ausführbarem Code und können dadurch auch keine Schadsoftware mehr enthalten. Ähnlich misstrauisch agiert die Remote Browser Isolation. Rufen Mitarbeiter eine Website auf, wird sie auf einen isolierten externen Browser in der Cloud geladen, der ein Abbild der Inhalte erzeugt und es auf die Browser der Mitarbeiter streamt. Sie bemerken keinen Unterschied, da sie aber keinerlei HTML-Code erhalten, werden sie vor potenziellem Schadcode bewahrt.

Vorhandene Lösungen einbeziehen. Unternehmen haben im Laufe der Jahre teils erhebliche Summen in IT-Sicherheit investiert. Die Sorge vorhandene Technologien vollständig zu ersetzen oder enorme Investitionen in neue Technologien ist unbegründet. Stattdessen sollte man bei der Planung bereits vorhandene Sicherheitspraktiken und -tools einbeziehen, rät etwa NTT. Viele Organisationen verfügen bereits über die notwendige Basis für eine Zero-Trust-Architektur. Das umfasst unter anderem Identitäts- und Zugriffsmanagement, Autorisierung, automatisierte Richtlinienentscheidungen, Patching von Ressourcen, kontinuierliches Monitoring durch Protokollierung und Analyse von Transaktionen, weitgehende Automatisierung von wiederholbaren, fehleranfälligen Aufgaben sowie Verhaltensanalysen und Threat Intelligence für einen besseren Schutz von Assets. Darauf aufbauend kann eine umfassende Zero-Trust-Architektur realisiert werden.

www.forcepoint.com
www.global.ntt

Frank Limberger
Data & Insider Threat Security Specialist bei Forcepoint

„Die Gefahr von Cyberattacken war wohl lange nicht so hoch wie jetzt und das wird sie aller Voraussicht nach auch bleiben."

GEGEN DEN VERZICHT

Thomas Lutzky, Geschäftsführer Phoenix Contact Österreich, spart im Gespräch nicht an Komplimenten an die österreichische Industrie in Sachen Digitalisierung. Um das Dilemma zwischen dem steigenden Energieverbrauch und Nachhaltigkeit zu meistern, setzt er auf Technik.

IoT 4 Industry & Business: Klima und Energie sind die Topthemen des Jahres. Bringt das für Phoenix Contact besondere Herausforderungen?

Thomas Lutzky: Wir engagieren uns schon lange in den Bereichen Energieerzeugung aus erneuerbaren Quellen, intelligente Energieverteilung und effizientes Energiemanagement. Durch die Klima- und Energieversorgungskrise ist der Bedarf nach effektiven Lösungen für die Elektrifizierung, Vernetzung und Automatisierung massiv gestiegen. Mit der zunehmenden Vernetzung sind auch die Möglichkeiten in der Anwendung deutlich größer geworden. Heute betrachtet man nicht mehr nur eine einzelne Maschine, sondern die gesamte Produktion, sektorübergreifend auch im Zusammenspiel mit dem smarten Gebäude. Daten sind das Fundament und die Voraussetzung Skalierungseffekte nutzen zu können.

IoT: Sie haben Vernetzung angesprochen. Alles vernetzt und verbindet sich. Häufig sind es aber Insellösungen, die die Hersteller anbieten. Wie schafft man hier Durchgängigkeit?

Lutzky: Erst das Zusammenspiel aller verbauten Komponenten und Gewerke ermöglicht es Produktionen und Gebäude kostengünstig und nachhaltig zu betreiben. Dazu braucht es einen ganzheitlichen Ansatz – von der Feldebene über die Automation bis hin zum Management und Betrieb. Wir führen Daten, die von unterschiedlichsten Systemen und in unterschiedlichsten Formaten in der bereits installierten Basis generiert werden, in einer zwischengeschalteten Ebene, unserem smarten IoT-Framework, zusammen. Damit kann der Anwender komfortabel weiterarbeiten und sofort Kosten sparen.

IoT: Ein schöner Satz von der Phoenix-Contact-Website: „Digitalisieren Sie jetzt." Wie einfach könnte Digitalisierung in der Produktion tatsächlich sein?

Lutzky: Es kommt immer darauf an, welche Schritte man setzen möchte. Die ersten kleineren Schritte sind tatsächlich sehr einfach. Im Rahmen unserer Initiative „Digital Factory Now" bieten wir Betreibern fertige Plug & Play-Lösungen

inklusive Software an, mit denen sofort Verbesserungen erzielt werden, ohne die bestehende CE-Zertifizierung der Maschine zu verletzen. Diese Lösungen lassen sich dann hochskalieren bis zur kompletten digitalen Fabrik. Bei uns in Österreich gibt es ganz hervorragende Produktionsunternehmen, die auch im internationalen Vergleich Vorreiter sind indem sie ihre Prozesse zu einem großen Teil schon digital abbilden und damit ihre Effizienz, Qualität und Produktivität steigern. Für alle, die sich weiter verbessern wollen, leisten wir mit ergänzender Beratung und Programmierung die entsprechende Unterstützung.

IoT: Wo liegen Ihrer Meinung nach die größten Herausforderungen, wenn Unternehmen digital werden wollen?
Lutzky: Es gibt immer eine Unsicherheit, ob der Weg, den man einschlägt, auch tatsächlich der Richtige ist. Wenn man einmal in eine bestimmte Richtung unterwegs ist, wird es schwierig oder teuer, wieder zurückzugehen, von Null zu starten und etwas Neues zu machen. Das Know-how in den Produktionsunternehmen wächst stetig, aber die Antwort auf die Frage, ob sich der angestrebte Effekt mit der jeweiligen Investitionsentscheidung einstellt, ist zu Beginn nicht immer eindeutig erkennbar. Bei Phoenix Contact haben wir mit der Kombination aus eigenem Maschinenbau und Produktion eine ausgezeichnete Ausgangslage Erfahrungen mit unserem Portfolio in beide Richtungen zu sammeln. Alles, was wir in unser Produkt und Dienstleistungsangebot aufnehmen, wurde zuvor in der eigenen Produktion auf Herz und Nieren getestet. Unsere eigenen Techniker gehen dabei sehr akribisch vor und hinterfragen alles kritisch. Erst wenn der jeweilige Digitalisierungsschritt bei uns intern bestanden hat, stellen wir die Lösung unseren Kunden vor. Von daher können wir jederzeit den Beweis antreten, dass unsere Lösungen funktionieren.

IoT: Mittlerweile werden nicht mehr nur IT- , sondern auch OT-Infrastrukturen angegriffen. Ist hier Bewusstsein vorhanden?
Lutzky: Die Zahl der Cyberangriffe, nimmt massiv zu und stellt heute ein großes Bedrohungsszenario dar. Vor einigen Jahren sind wir noch durchs Land gezogen und haben versucht das Bewusstsein dafür zu schaffen. Inzwischen ist es voll da. Was manchmal noch fehlt, ist der klare Weg OT-Security tatsächlich zu erreichen. Denn in der OT geht man von anderen Rahmenbedingungen aus als in der IT. Während auf der IT-Seite kurze Entwicklungszyklen alles sehr schnelllebig machen, ist es in der OT so, dass Maschinen über Jahrzehnte im Einsatz sein können. Hier gilt es laufend Updates am Bestand zu realisieren. Ein Aspekt, der Fachkenntnisse und Umdenken erfordert.

IoT: Wie glauben Sie, könnte man OT-Technikern am besten helfen?
Lutzky: Mit zunehmender Vernetzung und Digitalisierung von Anlagen und Produktionen erhöhen sich gleichzeitig auch die Anforderungen an ganzheitliche Sicherheitskonzepte. Menschen, Maschinen und Daten müssen bestmöglich geschützt werden. Zusätzlich gibt es immer mehr gesetzliche Vorgaben und Standards, die Unternehmen im Bereich OT-Security und der funktionalen Sicherheit einhalten müssen. Ich glaube, dass der Aufbau von Know-how der Schlüssel ist. Wir bieten »

Plug & Produce mit MTP[1]

Machen Sie Ihr Leben einfacher mit MTP in der Softwareplattform zenon:

- *Senkung der Produktionskosten um 40%*
- *50% schnellere Time-to-Market*
- *Hohe Innovationskraft sorgt für größere Wettbewerbsfähigkeit*
- *Größtmögliche Flexibilität der Anlagennutzung*

[1] Module Type Package (MTP), definiert nach VDI/VDE/NAMUR 2658, ist ein herstellerunabhängiger Standard zur Beschreibung von Prozessmodulen

www.copadata.com/mtp

zenon by COPA-DATA

dazu unterschiedliche Schulungen an, vom Tages- bis zum Wochenseminar mit anschließender TÜV-Prüfung.

IoT: PLCnext ist vom TÜV Süd zertifiziert worden. Was bedeutet das für Sie?

Lutzky: In der Automatisierung nimmt die IEC 62443 „IT-Sicherheit für industrielle Automatisierungssysteme" eine herausragende Rolle ein, da sie die Security aus der Perspektive des Betreibers, Systemintegrators und Geräteherstellers ganzheitlich betrachtet. Je mehr Produkte nach der IEC 62443 nachhaltig entwickelt werden, desto einfacher wird es für Betreiber und Systemintegratoren Security bei Integration und Betrieb von automatisierungstechnischen Anlagen umzusetzen und über den gesamten Lebenszyklus sicherzustellen. Ergänzend dazu wird die funktionale Sicherheit durch die Sicherheitsnormen IEC 61508, ISO 13849 und IEC 62061 beschrieben. Künftig müssen beide Sichten für erfolgreiche Automatisierungslösungen kombiniert werden und konsequenterweise rückt in der kommenden Maschinenrichtlinie der OT-Security-Aspekt durch die Forderung nach „Schutz gegen Verfälschungen" stärker in den Fokus. Als Experte für funktionale Sicherheit und OT-Security kombiniert Phoenix Contact diese Disziplinen in der PLCnext-Control-Technologie. Gegenüber dem TÜV Süd haben wir unsere Security-Kompetenz mit vielen Zertifikaten im Bereich der Prozesse für die Produktentwicklung, System-Design und Security-Services nachgewiesen und Ende 2021 die weltweit erste Zertifizierung einer Steuerung nach IEC 62443-4-2 (SL2 Feature Set) geschafft. Mit der Zertifizierung der Kombination aus OT-Security und bereits nach IEC 61508 SIL3-zertifizierter Safety-Hardware ermöglichen wir es unseren Kunden zukunftssichere Digitalisierungslösungen zu implementieren. Nach den erfolgreichen IEC 62443-4-1 ML3- und IEC 62443-4-2-Zertifizierungen unserer Axioline Controller ist OT-Security durch die Umsetzung des Secure Development Lifecycles für weitere Steuerungen der PLCnext-Control-Familie in der Breite unseres Portfolios angekommen.

IoT: Wir sind von so vielen negativen Nachrichten umgeben. Was könnte im heurigen Jahr positiv werden?

Lutzky: In der Branche haben wir allen Grund für Optimismus. Innovationen schreiten rasch voran und wir haben eine starke Dynamik bei den großen Trends. Denn es gilt die Transformation aktiv zu gestalten um unsere Wettbewerbsfähigkeit in Europa zu erhalten und die Klimakrise zu adressieren. Zudem nehmen viele Kunden große Auftragsbestände aus den letzten beiden Boomjahren mit ins heurige Jahr.

IoT: Kann Technik helfen ein nachhaltiges Leben zu ermöglichen?

Lutzky: Ja, denn es kann nicht unser Anspruch sein, mit Verzicht durchs Leben zu gehen. Vielmehr gilt es durch Investitionen in erneuerbare Energien den vermehrten Bedarf zu leistbaren Konditionen zu decken und ergänzend durch technisch-organisatorische Maßnahmen CO_2 zu reduzieren. Ein Aspekt, der künftig auch in Ausschreibungen für große Projekte eine wesentliche Rolle spielen wird. So sind Unternehmen schon aus eigenem Geschäftsinteresse gefordert, sich dazu intensiv Gedanken zu machen und an Lösungen zu arbeiten. Technologie ist jedenfalls der Schlüssel, um dieses scheinbare Dilemma zu lösen und die aktuellen industriellen Herausforderungen zu bewältigen.

www.phoenixcontact.com

Thomas Lutzky
Geschäftsführer Phoenix Contact Österreich

„Im Rahmen unserer Initiative „Digital Factory Now" bieten wir Betreibern fertige Plug & Play-Lösungen inklusive Software an, mit denen sofort Verbesserungen erzielt werden, ohne die bestehende CE-Zertifizierung der Maschine zu verletzen."

© Tonodiaz | Freepik

FÜNF LEITPLANKEN FÜR DIE WAHL DER RICHTIGEN DATENBANK

Parallel zu modernen IT-Infrastrukturen steigen die Anforderungen an Datenbanken. **Couchbase** skizziert ihr Anforderungsprofil in fünf Punkten. Erstens geht es um Automatisierung. IT- und Datenbank-Administratoren müssen von Routinetätigkeiten entlastet werden. Zweitens müssen die in Datenbanken gespeicherten Informationen mittels Analytics besser genutzt werden. Drittens sprechen Faktoren wie Kosten, Flexibilität und Skalierbarkeit eindeutig für die Verlagerung von Datenbank-Funktionen in die Cloud. Viertens sollte bei Edge-Installationen besondere Aufmerksamkeit auf die Edge-Fähigkeit gelegt werden und fünftens sollte die Datenbank auch unabhängig von bestimmten Infrastrukturen oder Plattformen sein. „Datenbanken bilden zusammen mit dem Betriebssystem das Herz jeder IT-Infrastruktur", erklärt Paul Salazar, Senior Director Central Europe bei Couchbase. „Darum prüfe kritisch, wer sich länger bindet, denn ein späterer Umstieg ist nicht nur kosten-, sondern auch zeitaufwendig."

www.couchbase.com

ERWEITERTE ZUSAMMENARBEIT

AvePoint migriert, verwaltet und schützt Daten für eine sichere digitale Zusammenarbeit in der Microsoft Cloud, in SharePoint, Salesforce und Google. Ab sofort können Reseller neben den monatlichen Abonnements auch die Jahreslizenzen des AvePoint-Portfolios über **Ingram Micro** buchen. „Viele Kunden schätzen die Möglichkeit, ihre SaaS-Lösungen jährlich und nicht nur monatlich beziehen zu können", erklärt **Dominic Sabaditsch**, Head of Cloud & Cyber Security bei Ingram Micro Österreich. „Mit den zusätzlichen Jahreslizenzen von AvePoint können wir ab sofort das gesamte Spektrum in den Bereichen Datenmigration, -verwaltung und -sicherung anbieten. Die AvePoint-Lösungen erweitern die Möglichkeiten von cloudbasierten Umgebungen und maximieren damit den Nutzen und die Effizienz für die Kunden bei der digitalen, kollaborativen Zusammenarbeit."

www.ingrammicro.com

Dominic Sabaditsch, Head of Cloud & Cyber Security bei Ingram Micro Österreich

HÖCHSTER PARTNER-STATUS

Bei der Neuordnung des SAP-Partnernetzwerkes hat IT-Dienstleister **adesso** die höchste Statusstufe „Expert" im Bereich SAP Customer Relationship Management erreicht. Partner auf dieser obersten Stufe arbeiten über das gesamte Produktportfolio von **SAP** hinweg, verfügen über besondere Lösungskompetenzen in dem jeweiligen Bereich und haben außergewöhnliche Kundenerfolge vorzuweisen. Ausschlaggebend für die Einstufung von adesso als „Expert" war das durchgängig hohe Skill-Set bei allen wichtigen Indikatoren wie Lösungskompetenz, Praxisnähe, Kundenrelevanz und Servicequalität bis hin zu Vertrieb und Marketing. „Die Auszeichnung bestätigt unsere Erfolge bei der Implementierung von End-to-End-Kundenprozessen mit den Lösungen des SAP-Customer-Experience-Portfolios", erklärt **Markus Blau**, Strategic Business Development SAP CX bei adesso.

Markus Blau, Strategic Business Development SAP CX bei adesso

www.adesso.at

KI UND DER UNIVERSALGELEHRTE

Als Positivspirale bezeichnet Reinhard Birke, General Manager NTT Data DACH AT, die Digitalisierungs- und IT-Prozesse im Unternehmen. Warum er sich keine Sorgen um die Zukunft macht und warum er sich ein anderes Bildungssystem wünscht, erzählt er im Interview.

IoT 4 Industry & Business: Herausforderungen gibt es dieser Tage sehr viele für Unternehmen. Was sind aktuell die größten Herausforderungen?

Reinhard Birke: Ich denke, es hängt alles zusammen. Wir leben in sehr unsicheren Zeiten. Das drückt sich in vielen Bereichen aus. Es gibt politische Unsicherheiten, ökonomische Verwerfungen an den Märkten sowie demografische und strukturelle Herausforderungen. Wir haben eine Diskussion über den Arbeitskräftemangel, ganz aktuell über die 40-Stunden-Woche. Wie wollen wir denn mit der Überalterung der Gesellschaft umgehen? Durch Corona ist das Thema Gesundheit dazu gekommen.

Und damit befinden wir uns gerade in einer Zeit, in der wir nicht genau wissen, wie es weitergeht. Das trifft die Konsumenten, genauso wie die Unternehmen. Die stehen jetzt nicht mehr da und planen Neues mit großen Innovationsbudgets. Es geht eher darum, Margen und die Produktion abzusichern. Ich muss meine IT-Systeme absichern, weil die Bedrohungen massiv zunehmen. Ich muss nachhaltig produzieren und das nicht nur, weil ich will, sondern weil ich muss. In diesem Umfeld geht es nicht darum, die eine Lösung für alles anzubieten, sondern wir müssen zeigen, wie man vernetzt mit diesen Unsicherheiten umgehen kann, um die Geschäftstätigkeit und die Umsätze zu stabilisieren.

IoT: Mit der Digitalisierung und Automatisierung werden Ängste geweckt, dass es den Menschen in gewissen Bereichen nicht mehr braucht. Was tun mit diesen Sorgen?
Birke: Schauen wir doch auf die Alterung der Bevölkerung in Deutschland. Das kann man sicher eins zu eins auf Österreich übertragen. Heute arbeiten dort 59 Millionen Menschen für die Versorgung von 16 Millionen älteren Menschen. Und diese Schere geht weiter zu. In 15 Jahren sind es nur noch 45 Millionen, die für 21 Millionen aufkommen müssen. Wir verlieren pro Generation ein Drittel der Arbeitskraft. Wenn also jemand fragt: Nimmt die KI Arbeitsplätze weg? Dann sage ich: Nein. Ohne KI könnten wir es überhaupt nicht schaffen. Wir müssen uns überlegen, wie wir die Schere zwischen Arbeitskraft und Versorgung für Ältere schließen können. Und dafür haben wir außer Zuwanderung überhaupt noch keine Lösung. Gerade bei den repetitiven Tätigkeiten im Büro, etwa in Excel-Tabellen etwas von A nach B zu kopieren oder Formulare für interne Prozesse auszufüllen, dafür sind doch Programme wie ChatGPT oder Ähnliches prädestiniert. Dadurch wird mehr Zeit frei für Produktivkraft. Mit KI haben wir also überhaupt erst eine Chance, die angesprochene Schere zu schließen. Natürlich ist Technologie nicht die einzige Lösung für das Problem der Demografie. Aber ich denke, dass uns Technologie die Chance gibt, jene Menschen, die im erwerbsfähigen Alter stecken, so produktiv wie möglich einzusetzen.

IoT: Wenn jetzt einfache Tätigkeiten automatisiert werden, gehen Jobs für Menschen mit geringer Bildung verloren.
Birke: Es geht nicht nur um die Arbeitsplätze für Menschen mit geringerem Bildungsniveau, sondern KI unterstützt vor allem in Berufen, die sehr viel mit wiederholenden Tätigkeiten und vor allem Wissens- und Informationsabruf zu tun haben. Denken Sie an medizinische Diagnostiker oder Anwälte und Richter. Das sind Berufsbilder mit hohem Bildungsniveau. In ihren Bereichen helfen automatisierte Systeme schon heute dabei Vorschläge zu erarbeiten, aus denen die Experten dann wählen können. Wir müssen uns daher vielmehr die Frage stellen: Sind wir bildungstechnisch auf eine Post-Wissensgesellschaft vorbereitet? Wenn die KI etwas viel schneller, präziser und verknüpfter findet, als wir es überhaupt parat hätten, geht es um die Frage, welche Arten von Bildung brauchen wir? Vielleicht müssen wir in viel kreativere Berufszweige gehen. Wir müssen beginnen, anstatt nach Antworten zu suchen, zu lernen, wie man die richtigen Fragen stellt. Das wird unseren Blick auf die Wissensgesellschaft, wie wir sie kannten, ändern. Das wird wahrscheinlich allen Generationen so gegangen sein, aber ich denke, heute ist die Disruption einfach am größten.

IoT: Wenn man das jetzt weiterdenkt, bleibt am Ende ein sehr einfacher Mensch zurück, wenn die KI sämtliches Wissen übernimmt. Als Mensch werden wir vom Wissen der KI abhängig sein, weil wir unser Wissen verloren haben. Das klingt etwas dystopisch.
Birke: Wir müssen unser Bildungssystem komplett neu überdenken. Wir haben Lehrpläne, die über 100 Jahre alt sind und wir lehren den Kindern genau dasselbe, was wir ihnen schon vor 500 Jahren beigebracht haben. Das ist eine Katastrophe, weil sich die Welt komplett verändert hat. Daher sehe ich es überhaupt nicht dystopisch, sondern extrem positiv. Ich denke, dass unsere Wissenszukunft im Humboldtschen Sinne stattfinden muss. Es gibt nicht nur einen Wissenskorridor, sondern eine Landkarte von Möglichkeiten, auf der man für sich selbst herausfinden kann, was einen interessiert. Wir gehen heute in Richtung Wissensindustrie, die uns immer stärker spezialisiert. Dadurch verlieren wir die Möglichkeit der Vernetzung über unterschiedliche Gebiete hinweg. Wenn Sie an die früheren Universalgelehrten, wie Leibniz, Newton oder andere denken, die sind durch eine ganz andere Art »

Reinhard Birke
General Manager NTT Data DACH AT

„Ich denke, dass uns Technologie die Chance gibt, jene Menschen, die im erwerbsfähigen Alter stecken, so produktiv wie möglich einzusetzen."

In der Medizin und der Justiz können automatisierte Systeme Vorschläge erarbeiten, auf deren Basis die Experten letztendlich entscheiden.

von Bildung entstanden. Die Spezialisierung verhindert sehr viel Kreativität. Was uns von KI oder Automatisierungssystemen unterscheidet: Menschen sind kreativ und entlang ihrer Interessensgebiete Suchende und Forschende in der Welt des Wissens. Wenn uns KI dabei unterstützt, aus dieser Spezialisierung wegzukommen, wenn sie uns vom Auswendiglernen hin zu einer interessensbasierten Gesellschaft führt, dann ist das für mich keine Dystopie, sondern ein wunderbares Zukunftsbild.

IoT: Die Pandemie hat digital viel Mögliches und Unmögliches zu Tage gefördert. Dinge, die man sich vorher vorgestellt hat, haben nicht funktioniert. Anderes, über das man vorher nie nachgedacht hat, war plötzlich möglich. Was hat Sie am meisten überrascht?

Birke: Für mich gab es zwei große Überraschungen. Das eine war, wie schnell wir den Umstieg ins digitale Arbeiten geschafft haben. Die zweite Überraschung passiert gerade jetzt. Für Menschen in der Mitte der Alterspyramide ist es etwas ganz Tolles und Neues von zu Hause aus arbeiten zu können. Unter den jüngeren Menschen ist das überhaupt nicht der Fall. Die haben in der Pandemie so viele Einschränkungen im sozialen Kontext erlebt, die wollen ins Büro kommen. Gleichzeitig ist es für die Jüngeren aber völlig logisch, dass Homeoffice möglich ist, wohingegen die Älteren das als Errungenschaft betrachten. Das finde ich eine extrem spannende Entwicklung, die ich so nicht gesehen habe.

IoT: Sie bezeichnen IT als Multifunktionswerkzeug. Was meinen Sie damit?

Birke: IT passt in sehr viele Schlösser. IT hilft uns in der Nachhaltigkeit genauso wie in der Sicherheit und in der Prozessoptimierung. Wenn Sie etwa ein Security-Projekt einführen, müssen Sie zuerst alle Rollen bereinigen, alle Prozesse anschauen und verschlanken. Dann werden Sie erkennen, dass Sie dadurch auch extrem viele Kosten sparen können und die Prozesse viel nachhaltiger werden. Das heißt: Durch ein IT-Security-Projekt kommen Sie zu resilienteren Prozessen. Und durch diese Prozesse kommen Sie, ganz im Sinne des ökologischen Fußabdrucks, zu nachhaltigeren Systemen. Das heißt, investiere ich in einen der drei Bereiche, bin ich automatisch Nutznießer der Verbesserung der anderen. Denn das passiert automatisch. Sobald ich meine Prozesse resilienter, also weniger anfällig machen möchte, dann muss ich sie robuster machen. Das bedeutet: Ich muss schauen, wo die Schwachstellen sind, über die Energie entweicht. Deswegen finde ich, dass gerade jetzt Investitionen in Smart Operations, IoT, aber vor allem auch in IT-Security so wichtig sind.

IoT: Wenn wir zum Thema Sicherheit kommen: Die Angriffe steigen. Sehr vielen Unternehmen ist das bewusst, dennoch hapert es bei der Umsetzung. Wie kann man diese Lücke weiter schließen?

Birke: Es braucht eine Enttabuisierung des Themas. Viele Unternehmen haben Angst vor dem Reputationsschaden und sind bereit, den Angreifern das geforderte Lösegeld zu zahlen. Das ist eine wahnsinnig schlechte Idee, weil die Angreifer dann die Informationen über die Angriffsvektoren ins Netz stellen und der nächste Angriff praktisch bevorsteht. Gleichzeitig geben wir nur sieben Prozent unserer IT-Budgets für Security aus. Dem steht in Deutschland ein Schaden von 403 Milliarden im Jahr gegenüber. Anders ausgedrückt: Wir geben den Angreifern mehr Geld, als wir den Verteidigern geben. Und das machen wir, weil wir Angst haben, dass unsere Marken beschädigt werden. Hier muss es eine Enttabuisierung geben. Es muss möglich sein zu sagen: Ja, wir hatten hier ein Problem – unsere IT war nicht sicher – aber jetzt haben wir alles im Griff. 84 Prozent der Unternehmen sind von Angriffen betroffen, die Dunkelziffer ist sogar um neun Prozent höher. Das bedeutet: Alle sind betroffen! Man hört aber nur von wenigen.

IoT: Sie haben schon Resilienz erwähnt. Die ist zu einem neuen Buzzword geworden. Wie sehen Sie das?

Birke: Ich würde es unter dem Aspekt subsumieren, wie widerstandsfähig wir gegen disruptive Veränderungen sind und wie wir reagieren können. Das geht ja dann auch ins Persönliche. Wie kann ich meine eigene Widerstandsfähigkeit stärken. Vielleicht indem ich mich selbst und meine Stärken stärke? Ich würde mir in Österreich, aber auch in Deutschland, weniger Sorgen machen, als wir das derzeit medial erleben. In den letzten paar 100 Jahren sind wir aus den verschiedensten Krisen immer wieder gestärkt hervorgegangen. Eine Krise wird immer auch das Potenzial der Erneuerung haben. Das haben viele österreichische Unternehmen genützt und Krisen hervorragend gemeistert. Besser als andere europäische oder amerikanische Unternehmen. Österreich hat durch seine kleinere und wendigere Ökonomie einen Vorteil. Wir können rascher als andere reagieren, haben uns angepasst und immer wieder Nischen gefunden.

https://at.nttdata.com

TECHNOLOGIE-NEWS

PROTOKOLLKONVERTIERUNG FÜR BIS ZU 200 SPS-TREIBER

Industrielles Kommunikationsgateway für die Übertragung von IoT-Daten

Das Zeitalter des Internet of Things (IoT) hat die industrielle Kommunikation quasi neu erfunden. Um die mit der rasanten industriellen Digitalisierung einhergehenden Möglichkeiten der Prozessoptimierung nutzen zu können, müssen Geräte, Anlagen und Maschinen verbunden und miteinander kommunizierfähig gemacht werden. Das ECU-1251 von Advantech wurde für modernes Edge Computing im industriellen Umfeld entwickelt und überzeugt durch seine umfassenden Protokollkonvertierungs-Funktionen.

IoT-Gateway mit leistungsfähigem Prozessor

Das IoT-Gateway mit integrierter WISE-EdgeLink-System-Architektur bietet 2x LAN-, 4x COM-Ports und 1x Micro-PCIe für 4G/3G/WiFi/GPRS-Module. Die intelligente Kommunikations- und Datenerfassungslösung ermöglicht es, kritische Anlagen zu überwachen, die Leistung der Geräte zu verfolgen, Alarmmeldungen zu erhalten oder auch die Systemverwaltung und -konfiguration durchzuführen. So können Wartungsarbeiten und Serviceeinsätze vor Ort minimiert, die Kosten erheblich gesenkt und eine bessere Überwachung und Kontrolle der Geräte und Anlagen vor Ort gewährleistet werden. Das IoT-Gateway arbeitet mit einem leistungsstarken Cortex-A8-Prozessor in einem Betriebstemperaturbereich von -40 °C bis 70 °C. Es unterstützt bis zu 200 SPS-Protokolle und einen Web-Service für Online-Überwachung zu jeder Zeit und von jedem Ort.

Integrierte Protokollkonvertierungssoftware

Zur Implementierung von IoT ist die Datenerfassung und Digitalisierung von Anlagen der erste wichtige Schritt. Der Hersteller Advantech hat, um den Programmieraufwand zu reduzieren, die Software WISE-EdgeLink entwickelt und z.B. in das IoT-Gateway ECU-1251 integriert. Diese Protokollkonvertierungssoftware unterstützt mehr als 200 Kommunikationsprotokolle (z.B. Modbus, DNP3, OPC-UA, MQTT, BACnet und IEC-60870-5-104) und macht es somit möglich, auch Altgeräte in IoT-Anwendungen einzubinden. „Alles spricht von Cloud-fähigen Lösungen und Edge-Device-Management. Mit diesem Gateway wird die Verwaltung und der reibungslose Betrieb von Feldgeräten optimiert und die Realisierung einer industriellen IoT-Infrastruktur ermöglicht", ist auch Christoph Gattinger, einer der IoT-Experten aus dem Hause BellEquip, dem niederösterreichischen Systemanbieter infrastruktureller Lösungen für den effizienten und sicheren Betrieb elektronischer Anwendungen, begeistert.

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
- USV, Energieverteilung und Energiemessung
- 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 & IoT
christoph.gattinger@bellequip.at

SO WIE BERG UND PROPHET

Top-Service, schnellere Reaktion, innovative Angebote – das alles zeichnet Unternehmen aus, die eventgetrieben arbeiten. Der revolutionäre Weg dorthin führt über bewegte Daten, automatisierte Prozesse und das Denken in Ereignissen. Daher müssen die Daten zu den Mitarbeitern kommen und nicht umgekehrt.

Jeden Tag treffen Mitarbeiter in Unternehmen aufgrund von hereinkommenden Ereignissen eine Vielzahl von Entscheidungen. Auch wenn es für jeden Einzelnen nur kleine Entscheidungen sind, für das Unternehmen summieren sie sich zu einem Berg an Events. Jede Entscheidung beeinflusst die Kundenzufriedenheit, das Wachstum oder Wettbewerbsvorteile. Daher sollten die Mitarbeiter die benötigten Informationen aktuell und automatisch bekommen.

Gerald Tretter
Senior Manager bei BearingPoint

„Es passiert immer irgendwo etwas. Der Alltag in jeder Branche ist von geplanten, genauso wie von unvorhersehbaren Ereignissen geprägt, auf die schnell und richtig reagiert werden muss, damit die Kunden zufrieden sind."

Das wird jetzt möglich: Eventgetriebene Systeme melden, dass etwas passiert, unterstützen Entscheidungen in Echtzeit und revolutionieren damit Geschäftsprozesse. „Bis jetzt wurden Prozessdaten erfasst, archiviert, periodisch ausgewertet und darauf basierend Entscheidungen getroffen. Aber dann ist es oft zu spät: Weil wenn ich im Nachhinein erfahre, dass zehn Prozent meiner Lieferungen verspätet beim Kunden eingelangt sind, kann ich nichts mehr ändern. Eventgetriebene Prozesse haben den Vorteil, dass sie auf die Realität aufmerksam machen. Wenn ein Lieferwagen jetzt im Stau steht, kann ich entweder die Route ändern oder den Kunden informieren und zwar genau dann, wenn es dringend ist. Dieses Entscheiden und Handeln in Echtzeit ist das Revolutionäre am Realtime Enterprise“, erklärt Björn Grosser, Partner und Geschäftsführer von BearingPoint Österreich.

Björn Grosser
Partner und Geschäftsführer von BearingPoint Österreich

„Wenn die Daten zu den Mitarbeitern kommen, dann ändert sich das grundsätzliche Verhalten im Unternehmen.“

Ein Alltag voller Ereignisse. Die Prozesse in jedem Unternehmen bestehen aus einem Strom von Ereignissen. Das können die einzelnen Stufen einer Logistikkette sein, von der Abholung der Ware über den Transport mit verschiedenen Verkehrsmitteln bis zur Zustellung. Für kritische Infrastrukturen geht es ums Monitoring, Checken von Grenzwerten und schnelles Reagieren. Bei Versicherungen oder Banken betrifft es Verträge, die geprüft, geändert oder verlängert werden müssen. Im Handel ist es die Customer Journey, vom ersten Interesse an einem Produkt über Informationen oder Angebote einholen bis zur Kaufentscheidung. „Es passiert immer irgendwo etwas. Der Alltag in jeder Branche ist von geplanten, genauso wie von unvorhersehbaren Ereignissen geprägt, auf die schnell und richtig reagiert werden muss, damit die Kunden zufrieden sind. Daher unterstützen wir Unternehmen, wie sie beginnen können, eventgetrieben zu denken und ein Realtime Enterprise zu werden. Gemeinsam suchen wir einen Business Case, der sich rechnet und evaluieren dazu Fragen, zum Beispiel: Wie kann ich mehr Umsatz machen, wenn ich Arbeit verlagere oder anders mache“, beschreibt Gerald Tretter, Senior Manager bei BearingPoint, die ersten Schritte. Denn eventgetriebenes Denken stellt für Unternehmen einen Paradigmenwechsel dar.

Prozesse und IT sollen ereignisgetrieben funktionieren. Geschäftsprozesse werden derzeit in Unternehmen so abgebildet, wie es die dahinterstehende Technologie ermöglicht. Datensätze sind in riesigen Datenbanken archiviert und wenn man eine Information benötigt, so wird diese dort gesucht. Moderne eventbasierte Systeme arbeiten mit bewegten Daten, d.h. sie können zu jedem Zeitpunkt anzeigen, wo sich beispielsweise eine Lieferung gerade befindet. So kann ein Logistiker vorab festlegen, dass ein automatischer Alarm erfolgt, wenn sich ein Fahrzeug längere Zeit nicht oder nur langsam bewegt – weil dann anzunehmen ist, dass es im Stau steht. Diese Information wird über die GPS-Daten des Fahrzeugs an das System übermittelt und mit der berechneten Ankunftszeit verglichen. Sollte sich eine Verzögerung ergeben, so kann entweder in einfachen Fällen der wartende Kunde automatisch vom System verständigt werden oder bei komplexeren Lieferungen bekommt der Mitarbeiter im Kontrollzentrum automatisch einen Hinweis in Echtzeit, dass er eingreifen muss.

Besserer Service und mehr Zeit für Kunden. Der Vorteil ergibt sich aus dem Ansatz, erstmals mit bewegten Daten arbeiten zu können. Dazu Tretter: „Eventgetriebene Systeme vergleichen Echtzeitdaten mit Erfahrungswerten und lösen eine Aktion oder einen Alarm aus. Das heißt, die Daten kommen zum Mitarbeiter. Das macht den entscheidenden Unterschied zu herkömmlichen Systemen aus, denn früher musste ein Mitarbeiter zu den Daten kommen: Er musste auf eine Liste oder ein Kontrollboard klicken und nachschauen, wo etwas zu tun ist. Eventgetriebenes Arbeiten spart mühselige Kontrollaufgaben und damit Zeit und es verbessert den Kundenservice.“ Die beste Entscheidung können Mitarbeiter dann treffen, wenn sie alle relevanten Informationen aktuell zur Verfügung haben. Gleichzeitig unterstützt sie das System mit Vorschlägen, denn frühere Entscheidungen sind gespeichert und werden mit dem aktuell zu entscheidenden Ereignis verknüpft – so kann die geeignete Aktion vorgeschlagen werden. Natürlich haben Mitarbeiter viel eigene Erfahrung. Mit herkömmlichen Systemen müssen sie jedoch – mangels aktueller Daten – oft nach Bauchgefühl entscheiden. Jeder Mensch ist dabei anders und hat unterschiedliche Risikoszenarien. Zusätzlich steht ein großer demographischer Wechsel bevor, erfahrene Fachkräfte gehen in Pension und Nachfolger werden händeringend gesucht. Unternehmen müssen daher über Alternativen nachdenken und da bietet die Automatisierung von Routinetätigkeiten eine große Chance.

Transformation braucht Begleitung. Um mit bewegten Daten als Realtime Enterprise zu arbeiten, ist ein Paradigmenwechsel nötig, betont Grosser: „Wenn die Daten zu den Mitarbeitern kommen, dann ändert sich das grundsätzliche Verhalten im Unternehmen. Das erfordert eine große Transformation, die Menschen, Prozesse und Systeme betrifft. Hier können wir unsere umfassenden Erfahrungen von Organisation bis Technologie einbringen, um Unternehmen auf dem Weg zur eventgetriebenen Organisation zu begleiten. Sie sollen Daten nicht mehr brach liegenlassen, sondern in Echtzeit nützen können, um damit Geld zu verdienen.“

www.bearingpoint.com

DIE ZWEI SEITEN VON ChatGPT

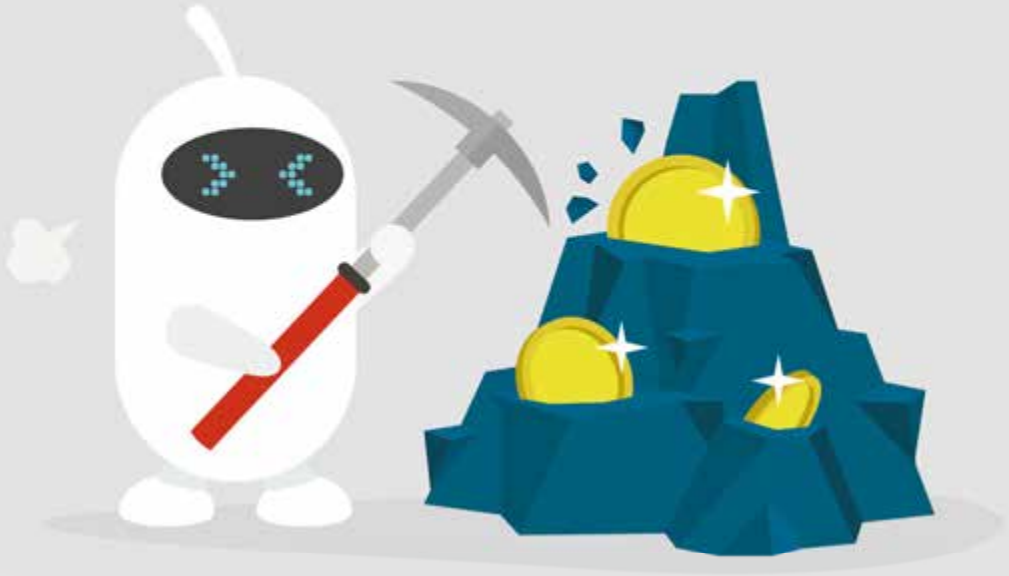
Eine Technologie kann noch so nützlich und „gut" sein, dass sie nicht auch zur missbräuchlichen Verwendung aufruft. So passiert das aktuell mit dem KI-Chatbot ChatGPT, der sich als Einfallstor für Hacker und Scammer erweisen kann. Kaspersky-Experten haben eine laufende Malware-Kampagne entdeckt, die sich den Hype rund um ChatGPT zunutze macht. Dazu verbreiten Cyberkriminelle den Trojaner „Fobo", indem sie Gruppen in Facebook erstellen, die den offiziellen OpenAI-Konten zum Verwechseln ähnlich sehen, oder sich als Communities von ChatGPT-Begeisterten ausgeben. Diese betrügerischen Gruppen hosten scheinbar offizielle Beiträge mit Neuigkeiten über den Dienst und werben für ein Programm, das sich als Desktop-Client für ChatGPT ausgibt. Sobald die Nutzer auf den Link eines Beitrags klicken, werden sie auf eine gut gefälschte Webseite geleitet, die fast genauso aussieht wie die offizielle ChatGPT-Webseite. Die Seite fordert den Nutzer auf, eine angebliche ChatGPT-Version für Windows herunterzuladen. In Wirklichkeit ist das ein Archiv mit einer ausführbaren Datei. Nachdem der Installationsvorgang beginnt, bricht er abrupt mit einer Fehlermeldung ab, laut der das Programm nicht installiert werden konnte. Die Betroffenen denken dann wohl, dass das Programm einfach nicht installiert werden konnte und vergessen es. Tatsächlich setzt sich jedoch die Installation des Stealer-Trojaners, Trojan-PSW.Win64.Fobo, fort, ohne dass das Opfer etwas davon bemerkt. Dieser Trojaner zielt darauf ab, Informationen über gespeicherte Konten von verschiedenen Browsern zu stehlen, darunter Chrome, Edge, Firefox oder Brave. Die Angreifer sind speziell an den Cookies und Anmeldeinformationen von Facebook-, TikTok- und Google-Konten interessiert. Darya Ivanova, Sicherheitsexpertin bei Kaspersky, kommentiert die Malware-Kampagne wie folgt: „Diese Kampagne ist ein hervorragendes Beispiel dafür, wie Angreifer Social-Engineering-Techniken nutzen, um das Vertrauen auszunutzen, das Nutzer beliebten Marken und Diensten entgegenbringen. Nutzer müssen sich bewusst darüber sein, dass ein legitim aussehender Dienst nicht immer bedeutet, dass er es auch ist. Sie sollten sich stets über aktuelle Techniken und Taktiken von Cyberkriminellen informieren und wachsam sein, um sich vor Angriffen dieser Art zu schützen." Daher an dieser Stelle ein wichtiger Hinweis: ChatGPT ist ein reines Online-Tool und nur unter „chat.openai.com" verfügbar. Es gibt derzeit keine mobilen oder Desktop-Apps für irgendein Betriebssystem.

Fast perfekte Täuschung. Hacker nutzen ChatGPT auch gerne selbst um Phishing-Texte und einfache Schadprogramme schneller und besser automatisiert erstellen zu können. „Wirklich ausgefeilte neue Malware wird man damit dagegen vorerst nicht erstel-

ChatGPT ist in aller Munde, auch in denen von Hackern und Betrügern. Etwa um Täuschungen glaubwürdiger zu machen oder einfach die Anfangsbegeisterung auszunützen. Neben klaren Warnungen, gibt es aber auch Beruhigung von Seiten der Experten.

len können. Und auch die Bedrohungslandschaft wird sich nicht wesentlich verändern, abgesehen von der erhöhten Häufigkeit", erklärt Stanislav Protassov, Acronis Executive Board Member und Mitbegründer. „KI-Lösungen wie ChatGPT werden manchmal auch als ‚stochastische Papageien' bezeichnet, weil sie als Sprachmodelle mit enormen Textmengen trainiert wurden und sie gut darin sind, schnell viele Texte zu generieren. Allerdings spielen Textinhalte bei Phishing-Angriffen eher selten allein die entscheidende Rolle. Während die Betrüger mit ChatGPT auch leichter Texte in anderen Sprachen generieren können, ist es nicht ausgemacht, dass diese damit auch besser bzw. überzeugender werden", so Protassov. Seiner Meinung nach gibt es noch weitere Möglichkeiten, wie ChatGPT von Cyberkriminellen eingesetzt werden könnte. Unerfahrene Angreifer könnten die KI zur Analyse von Quellcodes und dem Finden von Schwachstellen einsetzen. Das wäre grundsätzlich nichts Neues, es wäre nur schneller. Ebenso schneller könnte die Code-Automatisierung funktionieren. Auch wenn die ChatGPT-Richtlinien das Schreiben von Malware blockieren, sind einfachere Makros trotzdem möglich. Und letztendlich spielt es den Chatbots für Social-Engineering-Angriffe in die Hände. Kompromittierung von Geschäfts-E-Mails, Liebesschwindeleien oder betrügerische Job-Portal-Anbahnungen, die mehrere Interaktionsrunden mit den Opfern erfordern, könnten leichter automatisiert und skaliert werden, weil sich diese Interaktionen für die Opfer wie echte Gespräche anfühlen, während die Kriminellen kaum noch persönlich eingebunden sind. Unternehmen und speziell Einzelpersonen können sich dennoch vor solchen Betrügereien schützen. Es gilt weiterhin auf die üblichen Täuschungsindikatoren – wie etwa verdächtige Dringlichkeitsbehauptungen. Genauso wie bestimmte Schlüsselbegriffe wie „dringend", „Überweisung", „sofort handeln", „Passwort eingeben" etc., zu achten. Mit ChatGPT wird es auch nicht auf neue, magische Weise möglich, den Anschein zu erwecken, dass eine E-Mail von einer Bank kommt. Die Betrüger werden weiterhin auf ihre altbewährten Methoden wie leicht verwechselbare E-Mail-Adressen und Domain-Namen zurückgreifen müssen. „Manchmal kann man scheinbar vernünftige Unterhaltungen führen. Aber es gibt dann ein einfaches Mittel, um zu erkennen, dass man nicht mit einem Menschen redet: Geben Sie unsinnige Aufforderungen ein! ChatGPT wird hier anders reagieren als ein Mensch und versuchen, den Prozess trotzdem zu verarbeiten und darauf – meist unsinnig – antworten", erklärt Stanislav Protassov.

www.acronis.com
www.kaspersky.com



KÜNSTLICHE INTELLIGENZ HEBT DATENSCHÄTZE

Wie kann man Instandhaltung, Engineering und Produktivität mit PID-Daten verbessern? Heubach nutzt dafür die Künstliche Intelligenz Festo AX und zieht damit den maximalen Wert aus den Daten von Maschinen und Anlagen.

Täglich sammeln Sensoren in Produktionsanlagen riesige Datenmengen. Unternehmen erkennen dabei aber selten, wie wertvoll die richtige Auswertung großer Datenmengen ist. So entstehen Datengräber, deren Potenziale unentdeckt bleiben. Ähnlich ging es der Heubach-Gruppe. Der Hersteller von Pigmenten, Pigmentpräparationen, Farbstoffen und Spezialmaterialien sammelte bisher Daten von PID-Reglern in einer zentralen PIMS-Datenbank (Produktions-Informations-Management-System). Laut Brancheninsidern häufen viele Chemie- und Pharmahersteller solche Daten an, die dann aber meist ungenutzt auf Servern liegen bleiben. Oft werden die Produktionsdaten in verdichteter Form abgelegt – im Falle der PID-Regler mit Abtastraten von zwei Sekunden. Dank der Künstlichen Intelligenz von Festo AX wurde nachgewiesen, dass aus zentralen PID-Daten Nutzen für Instandhaltung, Engineering und Produktivität erzielt werden kann.

Michael Pelz
Automation & Digitization Manager bei Heubach

„Die Ergebnisse waren schon nach dem ersten Schritt der KI-Analyse erstaunlich gut."

Standorte weltweit optimieren. Die PIMS-Datenbanken haben einen unschätzbaren Vorteil: Sie enthalten die Daten aller Regler aus unterschiedlichen Systemen, unterschiedlicher Hersteller und von allen angebundenen Produktionsstandorten. Michael Pelz, Automation & Digitization Manager bei Heubach, dazu: „Unser Ziel wäre ein zentrales Controller-Monitoring-System. Um das zu erreichen, müsste es gelingen, die Daten im Kontext sinnvoll auszuwerten und nutzbar zu machen und somit ein einheitliches Instrument zu schaffen, mit dem wir die Regler aller angebundenen Standorte weltweit analysieren können." Anhand der daraus gewonnenen Ergebnisse könnten dann Regler gezielt analysiert und optimiert werden, beispielsweise mit einer Optimierungs-Software im eingesetzten Scada-System und mit Experten vor Ort. Als Teil der Lösung zeichnete sich für Heubach ab, die Software Festo Automation Experience (Festo AX) zu nutzen. „Sie hilft unseren Kunden, Entscheidungen auf Basis von Fakten zu treffen", betont Digitalisierungsexperte Eberhard Klotz von Festo. Festo AX ist eine flexible und einfach zu bedienende Lösung, die es Anwendern ermöglicht, durch Künstliche Intelligenz (KI) und Maschinelles Lernen den maximalen Wert aus den Daten von Maschinen und Anlagen zu ziehen.

© Festo SE & Co. KG

Eberhard Klotz
Digitalisierungsexperte bei Festo

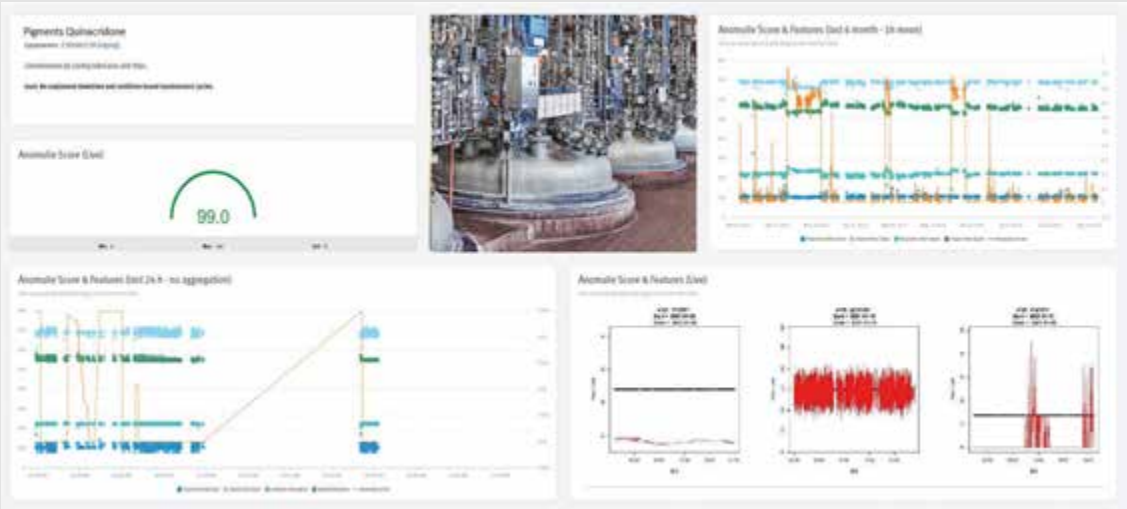
„Festo Automation Experience (Festo AX) hilft unseren Kunden, Entscheidungen auf Basis von Fakten zu treffen."

KI bewertet Ausgangsdaten. Im ersten Schritt bewertete die KI von Festo AX – als pragmatischer Ansatz – die Ausgangsdaten von mehreren Monaten und bereinigte diese falls erforderlich. Experten aus den Bereichen Instandhaltung, Prozess-Engineering (Qualität) und Operations Improvement Management von Heubach begleiteten diesen Schritt und bewerteten die ersten Ergebnisse aus den historischen Offline-Daten. Im zweiten Schritt meldeten die Fachabteilungen bezüglich der variablen Batch-Prozesse zurück, welche Sensitivität für die Regler, abhängig von deren physikalischen Funktionen, möglich sein sollte. Zum Beispiel wurde bewertet, ob der Faktor Temperatur weniger kritisch als der Faktor Durchfluss oder der Faktor Druck ist. Im Anschluss wurde festgelegt wie die unterschiedlichen Fehlerabweichungen zu priorisieren sind. Eine zusätzliche Trendlinie der Anomalie-Scores sollte den Fachabteilungen zusätzlich helfen, exakt, früh und vor allem einfach die Abweichungen pro Batch zu erkennen. Damit sollten Algorithmen und Fehler-Scores innerhalb der KI-Auswertung unter Einbeziehung der Erfahrungen von Experten und Gegebenheiten vor Ort anpassbar sein. Wichtig war auch, eine einfache Visualisierung der Ergebnisse umzusetzen, mit dem Ziel, in Zukunft aggregierte Dashboards nutzen zu können. Im dritten Schritt sollte das Projekt portierbar (on premise) sein und in eine Online-Abfrage inklusive Visualisierung innerhalb bestehender Systeme münden können, was die Implementierung aus Data-Security-Sicht sehr vereinfacht.

Optimale Anpassung des Algorithmus. „Die Ergebnisse waren schon nach dem ersten Schritt der KI-Analyse erstaunlich gut: Man sah sehr gut, welche Regler beispielsweise eine starke Stellgrößenschwankung aufwiesen und dadurch die Stellglieder schneller verschleißen lassen", erklärt Digitalisierungsexperte Pelz. Neben vielen gut eingestellten und unauffälligen Reglern fand die KI auch Regler die konstant die Sollwerte nicht erreichten, stark überschwangen, oszillierten oder bei denen manuell eingegriffen wurde. Bei manchen Reglern waren durch die unterschiedlichen Einsatzgebiete die Ergebnisse aber nicht immer sofort nachvollziehbar. „In einem engen Austausch zwischen Regler- und Data-Science-Experten konnte der KI-Algorithmus auf weitere Besonderheiten in der (Batch)-Produktion angepasst werden. Zum pragmatischen und schnellen Austausch der Ergebnisse waren in dieser Phase tatsächlich nur klassische Office-Tools ausreichend", ergänzt Pelz.
Da unterschiedliche Prozessleitsysteme im Einsatz waren, war eine Regleranalyse bisher immer nur auf Betriebsebene und mit unterschiedlichen Tools möglich. „Doch mit dieser Lösung haben wir gleich zwei herausragende Vorteile: Erstens ist sie herstellerübergreifend und auf einem zentralen System global nutzbar, so dass wir den Algorithmus für alle Systeme und Regler einsetzen können. Zweitens ist die Festo-Lösung IT-seitig so flexibel, dass vom pragmatischen Offline-Pilotprojekt über eine On-premise-Lösung innerhalb eigener IT-Systeme bis zu einer cloudbasierten Implementierung eine Nutzung und Weiterentwicklung möglich ist", freut sich der Automation & Digitization Manager von Heubach.

Dank KI aktuelle und zukünftige Herausforderungen effektiver meistern. „Gerade in den aktuellen Zeiten ist es wichtig, die Produktionsprozesse in Bezug auf Energieverbrauch, Menge und Qualität möglichst effektiv optimieren und langfristig überwachen zu können. Dabei kann in Zukunft das zentrale Controller-Monitoring-System ein wichtiger Baustein sein, gerade auch im Rahmen der voranschreitenden Optimierung des CO_2-Fußabdrucks in der Produktion", so Digitalisierungsexperte Pelz.

www.festo.com



Festo AX ist eine flexible und einfach zu bedienende Lösung, die es Anwendern ermöglicht, durch Künstliche Intelligenz (KI) und Maschinelles Lernen den maximalen Wert aus den Daten von Maschinen und Anlagen zu ziehen.

KI-UNIVERSITÄT EHRT IHRE ERSTEN ABSOLVENTEN

Ende Jänner beging die **Mohamed bin Zayed University of Artificial Intelligence** (MBZUAI) in Abu Dhabi ihre erste akademische Abschlussfeier mit 52 Studenten aus 24 Ländern, die jetzt ihre Hochschulabschlüsse in den KI-Schlüsselbereichen Computer Vision und Maschinelles Lernen in der Tasche haben. „Als Fundament für die technologische Wettbewerbsfähigkeit in der Künstlichen Intelligenz hat sich MBZUAI der Durchführung transformativer Forschung, der Entwicklung modernster Technologien und der Ausbildung kreativer und hart arbeitender Talente verschrieben", sagte Eric Xing, Präsident und Universitätsprofessor der MBZUAI.

www.mbzuai.ac.ae

UNFÄLLE AUTONOMER AUTOS SMART SIMULIERT

Die Entwicklung realistischer Crash-Szenarien und Simulationen zukünftiger Verkehrssituationen,

an denen autonome Fahrzeuge beteiligt sind, steht im Mittelpunkt eines aktuellen Projekts der IMC Fachhochschule Krems. Im ersten Schritt des Projekts werden Verkehrsszenarien aus öffentlich zugänglichen Datenbanken in spezielle Simulationen eingespeist. Anschließend werden in einem Optimierungsprozess basierend auf modernsten Suchalgorithmen neue Verkehrsszenarien mit steigender Gefährlichkeit und Schwere erstellt. Das Projekt ist Teil eines großen, von der EU finanzierten internationalen Forschungsprojekts, das darauf abzielt, Sicherheitsmechanismen für autonome Fahrzeuge zu entwickeln, die die Unfallfolgen durch den Einsatz fortschrittlicher Fertigungstechnologien verringern.

www.fh-krems.ac.at

ERFORSCHUNG DES KLIMAWANDELS

IBM und das Marshall Space Flight Center der **Nasa** wollen im Rahmen einer Zusammenarbeit neue Einblicke in die immense Sammlung von Geodaten der Nasa gewinnen. Dabei wird die als Basismodell bekannte KI-Technologie erstmals auf die Beobachtungsdaten der Nasa-Satelliten für Erdbeobachtung angewendet. Durch die Analyse von Satellitendaten in der Größenordnung von Petabyte sollen Veränderungen im geografischen Fußabdruck von Phänomenen wie Naturkatastrophen, zyklischen Ernteerträgen und in den Lebensräumen der Wildtiere identifiziert werden. Die Basismodelltechnologie wird die Forscher dabei unterstützen, Analysen über kritische Umweltsysteme auf unserem Planeten bereitzustellen. „Basismodelle haben sich bei der Verarbeitung natürlicher Sprache bewährt und es ist an der Zeit, dies auf neue Bereiche und Modalitäten auszuweiten, die für Unternehmen und Gesellschaft von Bedeutung sind", sagt Raghu Ganti, leitender Forscher bei IBM.

www.ibm.com

© kjpargeter | Freepik

SMARTE AMPELN

Auf Basis Künstlicher Intelligenz sollen smarte Fußgängerampeln den Verkehrsfluss mittels flexibler Ampelschaltungen verbessern, die Wartezeiten verringern und vor allem die Sicherheit aller Verkehrsteilnehmer:innen erhöhen. Die Testphase startet in der deutschen Stadt Füssen.

Für den einen ist sie zu kurz, für den anderen zu lang und für den Rest nicht koordiniert. Scheinbar machen Ampeln, was sie wollen. Mit Hilfe von Künstlicher Intelligenz sollen sie künftig ihre Grünphasen an die Bedürfnisse unterschiedlicher Personengruppen anpassen können. Seit dem Frühjahr 2022 ist die Bernard Gruppe gemeinsam mit der net digital AG – beziehungsweise deren Tochtergesellschaft irisnet – und dem Institut für Straßenwesen der RWTH Aachen an der Entwicklung einer neuartigen Lichtsignalanlage beteiligt. Die „Smarte Fußgängerampel“ erkennt in Echtzeit, ob ältere beziehungsweise vulnerable Personen oder Kinder die Straße queren möchten und kann aufgrund dessen eine längere Grünphase initiieren. „Unser Team ist für das Kamerasystem in Form unseres selbst entwickelten Bernard Mobility Analyser sowie für dessen Installation zuständig. Damit werden die Verkehrsteilnehmerinnen und -teilnehmer anonym erfasst. Die erhaltenen Daten werden direkt in das Steuergerät der Ampeln eingebunden und so programmiert, dass die Informationen der Kamera im Ampelsystem umgesetzt werden können“, erklärt Stefan Schwarz, CTO der Bernard Gruppe.

Start der Testphase. „Der Sicherheitsfaktor steht hier im Zentrum. Überall, wo mit erhöhtem Fußgängeraufkommen zu rechnen ist, machen ‚smarte Ampeln‘ Sinn: Zebrastreifen, Kreuzungen vor Schulen, Krankenhäusern oder Altenheimen, Übergänge in Fußgängerzonen, aber auch vor Event-Locations oder Fußballstadien“, sagt Schwarz. Aktuell geht das Projekt in die erste Testphase in der deutschen Stadt Füssen. Hier wird an zwei Standorten mit erhöhtem Personenaufkommen getestet, um verschiedene Szenarien abdecken zu können: Bei einer Kreuzung vor einem Krankenhaus sowie direkt beim Übergang in eine Fußgängerzone. Dabei wird der eingesetzte Bernard Mobility Analyser laufend um KI-Algorithmen für mögliche Anwendungsfälle erweitert. „In der Testphase zeichnet der Algorithmus auf, wie er in einer jeweiligen Situation reagieren beziehungsweise die Lichtsignalanlage schalten würde. Dies wird im Anschluss validiert, um die Zuverlässigkeit zu prüfen. Die Kamera wird also bereits gesteuert, aber die Steuerung noch nicht im Straßenverkehr umgesetzt“, erklärt Stefan Schwarz.

Erhöhte Verkehrssicherheit. Durch die flexiblen Ampelschaltungen wird der Verkehrsfluss verbessert, die Wartezeiten an Lichtsignalanalgen verringert und vor allem die Sicherheit der Verkehrsteilnehmer:innen erhöht. Dabei wird die aktuelle Verkehrslage immer mitberücksichtigt: Grünphasen für Fußgänger:innen werden nur initiiert, wenn tatsächlich Personen queren möchten. Die Ampel erkennt den Kreuzungswunsch und reagiert zeitnah, um lange Wartezeiten zu vermeiden. Auch auf unerwartete Ereignisse, wie etwa stürzende Personen, kann die Ampel spontan reagieren, was maßgeblich zum Schutz des Personenverkehrs beiträgt.

www.bernard-gruppe.com
www.rwth-aachen.de
www.irisnet.de

CLOUD & SECURITY

Cloud-Angebote bieten maximale Flexibilität und Produktivität. So ist es kein Wunder, dass die Nachfrage nach Cloud-Services kontinuierlich steigt. Bei allen Vorteilen dürfen IT-Reseller und Cloud Service Provider die Security nicht aus dem Blick verlieren, weiß Hermann Ramacher, Geschäftsführer ADN Distribution GmbH.

Hermann Ramacher, Geschäftsführer ADN Distribution GmbH

Die Vorteile des Modells Cloud haben auch in Deutschland zu einer nahezu flächendeckenden Verbreitung geführt. Laut dem KMPG-Cloud-Monitor 2022 lehnen nur noch drei Prozent der deutschen Unternehmen Cloud Computing komplett ab, fast 50 Prozent verfolgen eine Cloud-Only- oder Cloud-First-Strategie. Die zunehmende Cloud-Nutzung ist auch bei den Cyberkriminellen nicht unbemerkt geblieben. Dem Sicherheitsspezialisten Check Point zufolge ist die Zahl der Angriffe gegen Cloud-basierte Netzwerke 2022 gegenüber dem Vorjahr um 48 Prozent gestiegen. Die Veränderungen in der Arbeitswelt erhöhen das Risiko von Identitätsdiebstahl und Cloud-Account-Übernahmen zusätzlich.

Starker Schutz von Zugangsdaten. Cloud-Anbieter bieten eine ganze Reihe von Tools, mit denen IT-Reseller und Cloud Service Provider (CSP) ihre Cloud-Umgebungen sicherer machen und gegen Cyberangriffe schützen können. Zu den wichtigsten gehört das Thema Authentifizierung allein mit Nutzername und Passwort. Das ist allerdings gefährlich und nicht mehr zeitgemäß. Wie die Microsoft-Sicherheitsexperten Lee Makler und Alexander Weinert auf der RSA-Konferenz 2020 zeigten, waren mehr als 99 Prozent aller kompromittierten Konten nur durch ein Passwort gesichert.

Schutz sensibler Daten. Kunden fragen oft, ob Public-Cloud-Dienste überhaupt im Einklang mit der Datenschutzgrundverordnung zu nutzen sind. Diese Frage lässt sich auf jeden Fall bejahen, denn Public-Cloud-Anbieter haben umfangreiche Vorkehrungen getroffen, um den Schutz und die Vertraulichkeit von Kundendaten sicherzustellen. So werden beispielsweise alle Informationen während der Übertragung und Speicherung mehrfach verschlüsselt. IT-Reseller und CSPs müssen sich jedoch klar darüber sein, dass Datenschutz nicht allein in der Verantwortung des Cloud-Providers liegen kann. Sowohl IT-Dienstleister als auch Kunde müssen entsprechende Compliance-Regeln aufstellen sowie die notwendigen technischen und organisatorischen Maßnahmen ergreifen, um die Datenschutz-Konformität sicherzustellen.

Schutz vor Cyberbedrohungen. Cloud-Instanzen, aber auch Server im eigenen Rechenzentrum sind einem ständigen Strom von Hacker-Angriffen ausgesetzt. IT-Reseller und CSPs müssen daher Bedrohungen schnell erkennen und einschätzen können. Mit Defender for Cloud und Defender for Servers bietet Microsoft Lösungen, die nicht nur Instanzen in der Azure-Cloud schützen, sondern auch Hybrid- und Multi-Cloud-Umgebungen absichern. Ein weiterer wesentlicher Baustein in jeder Sicherheitsstrategie ist der Schutz von Endgeräten – schließlich sind Notebooks, Tablets und Smartphones häufig genutzte Einfallstore für Trojaner und andere Malware.
IT-Reseller und CSPs müssen Cloud-Umgebungen effizient absichern, potenzielle Bedrohungen schnell erkennen und Daten vor fremden Zugriffen schützen. Nur so können sie die Risiken von Cyberangriffen und Datenschutzverstößen für sich und ihre Kunden minimieren.

www.adn.de

Im „grünen" Billa in Altenmarkt an der Triesting werden alle Daten egal ob Wärme-, Wasser-, Gas- oder Strom-Verbraucher zentral erfasst und über eine europäische Cloud-Lösung von Microsoft verwaltet.

© Wexplore Productions GmbH

SUPERMARKT DER ZUKUNFT

Ein neues Billa-Pilotprojekt zeigt, wie Digitalisierung und datenbasiertes Energiemanagement den Betrieb von Handelsfilialen Kosteneinsparungen von bis zu 25 Prozent und eine bessere Handelsspanne ermöglichen. Der IT-Dienstleister Tietoevry Austria unterstützt Rewe International dabei sein Filialnetz nachhaltiger zu betreiben.

Rewe International ist einer der größten Energieverbraucher des Landes, allein die Handelsmarke Billa Österreich betreibt mehr als 1.200 Supermärkte. Dort sind viele unterschiedliche Gewerke im Einsatz: von der Heizung bis zur Klimatisierung, von der Beleuchtung bis zur Lüftung, von Backöfen bis hin zu Kühlregalen und Gefriertruhen. Das Problem: Die einzelnen Steuerungen der Gewerke waren bislang nicht vernetzt und erzeugten voneinander abgeschottete „Datensilos", die eine zentrale Überwachung aller Anlagen und transparente Energieeffizienz-Entscheidungen verhinderten. „Angesichts steigender Energiekosten wird ein energieeffizientes Facility Management wirtschaftlich immer relevanter. Denn die hohen Energiekosten knabbern an der Handelsspanne", sagt Georg Schaider, Head of Electrical Engineering & Energy-Management bei der Rewe International AG.

IoT-Lösung für Supermarkt der Zukunft. Zur Lösung der Herausforderungen hat der Digitalisierungs-Spezialist Tietoevry Austria gemeinsam mit den Partnern Microsoft und Beckhoff Automation eine IoT-Lösung entwickelt: Im Supermarkt in Altenmarkt an der Triesting werden alle Daten der Gewerke – egal, ob Wärme-, Wasser-, Gas- oder Strom-Verbraucher – zentral erfasst und über eine europäische Cloud-Lösung von Microsoft verwaltet. Eine Benutzeroberfläche stellt in der Filialleitung alle wichtigen Statusinformationen der Gewerke übersichtlich dar. „Das Personal kann nun vor Ort transparent überwachen, ob alle technischen Systeme des Marktes optimal funktionieren, ob eine Abweichung bzw. Störung selbst behoben werden kann oder ob ein:e Instandhaltungstechniker:in gebraucht wird. Bei Auffälligkeiten wird das Personal alarmiert und kann datenbasiert sofort die richtigen Energiemanagement-Entscheidungen treffen", erklärt Lukas Keller, Head of Advisory bei Tietoevry Austria, die Vorteile. Und Jutta Grabenhofer, Sustainability Lead bei Microsoft Österreich, ergänzt: „Mit der Cloud for Sustainability helfen wir Organisationen bei der Ermittlung, Berichterstattung und Reduktion ihres ökologischen Fußabdrucks. Die Klimawende kann uns aber nur gelingen, wenn wir alle Transparenz über unsere Emissionen sicherstellen und diese mit unseren Partnern teilen, um gemeinsam das Reduktionsziel zu erreichen. Cloudbasierte Lösungen bringen nicht nur einen technologischen Mehrwert, sondern ermöglichen auch einen ökologischen Vorteil aufgrund des drastisch reduzierten Fußabdruckes der Cloud. Die Erfolgsgeschichte von Rewe und Tietoevry zeigt, dass Partnerschaften und die Nutzung von cloudbasierter Technologie der richtige Weg sind, um unser ambitioniertes Ziel einer negativen CO_2-Bilanz bis 2023 zu erreichen – nämlich mit unseren Lösungen mehr CO_2 aus der Atmosphäre zu entfernen, als wir selbst als Technologieanbieter verursachen." Für Rewe International macht sich das smartere Energie- und Instandhaltungsmanagement jedenfalls rasch bezahlt. „Wer die richtigen Effizienz- und Sparmaßnahmen konsequent umsetzt, kann je nach Größe und Beschaffenheit eines Marktes ein Einsparungspotenzial von bis zu 25 Prozent realisieren", kalkuliert Georg Schaider abschließend.

www.tietoevry.com/at

MEHR KONTROLLE

Führungskräfte aus 1.000 Organisationen aus zehn Ländern, darunter Deutschland, Frankreich, Italien, die USA, Großbritannien, Indien und Australien wurden für die Studie „The journey to cloud sovereignty: Assessing cloud potential to drive transformation and build trust" des Capgemini Research Institute befragt. Der Studie zufolge haben Organisationen Bedenken, eine Public Cloud als Basis ihrer digitalen Transformation zu nutzen: 69 Prozent der Befragten befürchten, in einer solchen Cloud-Umgebung möglicherweise extraterritorialen Gesetzen zu unterliegen, beispielsweise wenn die Daten außerhalb der EU gespeichert werden. 68 Prozent sind besorgt über fehlende Transparenz und Kontrolle darüber, was mit ihren Daten in der Cloud geschieht. Darüber hinaus befürchten 67 Prozent eine Abhängigkeit von bestimmten Cloud-Anbietern, deren Unternehmenssitz außerhalb der eigenen Gerichtsbarkeit liegt. Die Mehrheit der Unternehmen und Behörden weltweit will vor allem auf souveräne Cloud-Plattformen setzen, um Compliance mit Regularien sicherzustellen (71 Prozent) oder, um mehr Kontrolle und Transparenz über ihre Daten zu haben (67 Prozent). Extraterritoriale Datenzugriffe zu verhindern ist für 65 Prozent ein weiterer Grund.

„Die Souveränität der eigenen Lieferkette und IT ist zu einer

Souveräne Cloud-Plattformen werden zunehmend wichtiger für Unternehmen und Behörden. Die größten Treiber für Cloud-Souveränität sind gesetzliche Regulierungen sowie der Wunsch von Organisationen nach mehr Kontrolle über ihre Daten. Das zeigt eine Studie des Capgemini Research Institute.

strategischen Frage geworden. Für Organisationen, die derzeit noch zögern, die Vorteile der Cloud zu nutzen, ist Cloud-Souveränität ein Weg dorthin. Souveräne Clouds, in denen sie ihre Daten noch besser kontrollieren und schützen können, gewinnen damit branchen- und grenzübergreifend an Bedeutung. Gerade für den öffentlichen Sektor sind Vertrauen, Transparenz, Wahlmöglichkeiten sowie die Portabilität von Daten die wichtigsten Prioritäten. Es ist daher nicht überraschend, dass gerade Behörden und Regierungsstellen souveräne Clouds einsetzen möchten oder es zumindest in Erwägung ziehen“, erklärt Arun Philip Varghese, Head of Custom & Cloud Solution bei Capgemini in Österreich. „Bei der Entwicklung ihrer Cloud-Strategien sollten sich Organisationen – besonders im öffentlichen Sektor – nicht auf Compliance-Anforderungen beschränken, sondern eine ganzheitliche Sicht auf ihre Daten entwickeln. So können sie das Potenzial der souveränen Cloud – wie Vertrauen, Kooperation und Innovationsbereitschaft – auch für sensible Datenfelder abrufen und einen besseren Service für Bürgerinnen und Bürger schaffen oder Wettbewerbsvorteile schaffen“, so Varghese.

Rechtliche Lage am Speicherort. Fast die Hälfte der Organisationen (43 Prozent) definiert souveräne Cloud-Lösungen als die Speicherung ihrer Daten innerhalb ihrer bevorzugten Gerichtsbarkeit – unabhängig von der ursprünglichen Herkunft des Cloud-Anbieters. Nur 14 Prozent definieren die souveräne Cloud so, dass ausschließlich Cloud-Anbieter mit Gerichtsstand im eigenen Land genutzt werden dürfen.
Bei der Auswahl eines Anbieters konzentrieren sich Unternehmen und Behörden in erster Linie auf vier Schlüsselfaktoren: Identitäts- und Zugriffsmanagement sowie Verschlüsselung (82 Prozent), den Schutz sensibler Daten durch eine isolierte Cloud-Umgebung (81 Prozent), wettbewerbsfähige Kosten (69 Prozent) sowie die Verfügbarkeit von lokalen oder regionalen Rechenzentren (66 Prozent).

Neue Erwartungen an Souveränität. Auf die Frage, welche Cloud-Umgebung sie in den nächsten ein bis drei Jahren nutzen werden, nannte mehr als ein Drittel (38 Prozent) der Organisationen eine Public- oder Hybrid-Cloud mit lokalen Rechenzentren. 30 Prozent erwarten, dass sie eine technisch und betrieblich separierte Cloud-Version oder eine lokale rechtliche Einheit eines Hyperscalers nutzen werden. Nur elf Prozent planen, ausschließlich mit Cloud-Anbietern zu arbeiten, die ihren Sitz im Geltungsbereich derselben Gerichtsbarkeit haben wie die Organisation selbst. Im öffentlichen Sektor berücksichtigt fast die Hälfte (48 Prozent) der Befragten eine souveräne Cloud entweder bereits als Teil ihrer Cloud-Strategie oder plant, sie in den nächsten 12 Monaten einzubeziehen.
Sowohl für den öffentliche Sektor als auch die Privatwirtschaft stehen die Einhaltung rechtlicher Vorschriften sowie der Schutz vor extraterritorialem Datenzugriff im Vordergrund; der öffentliche Sektor räumt diesen jeweils eine noch etwas höhere Bedeutung ein (76 Prozent gegenüber 70 Prozent bei privaten Unternehmen bzw. 69 Prozent gegenüber 64 Prozent). Insgesamt erwartet sich die öffentliche Verwaltung mehr datenbezogene Vorteile von einer souveränen Cloud als private Unternehmen.

Zusammenarbeit fördern. Mit Cloud-Souveränität möchten Organisationen nicht nur den strengsten regulatorischen Anliegen gerecht werden und Datensicherheitsanforderungen erfüllen, sondern auch weitere Vorteile für sich erschließen: 60 Prozent glauben, dass eine souveräne Cloud die gemeinsame Datennutzung und den Datenaustausch mit vertrauenswürdigen Partnern in einem Ökosystem erleichtern würde. 42 Prozent der Befragten sind der Meinung, dass ein vertrauenswürdiger, interoperabler Cloud-Service ihnen bei der Skalierung neuer Technologien wie 5G, Künstliche Intelligenz und dem Internet der Dinge helfen könnte.

www.capgemini.com

VORSCHAU

IoT4 NR. 2-2023 | Erscheinungstermin: 29. Juni 2023

DER WEG ZUM IoT

Mit Hilfe von LoRaWAN-Sensoren kann auf einfache, schnelle und kostengünstige Weise ein Monitoring der prozessrelevanten Umgebungsparameter in industriellen Produktionsstätten umgesetzt werden. Einer der sich damit besonders gut auskennt ist **Christoph Gattinger**, Vertrieb & technische Beratung beim Systemhaus BellEquip. Wir sprechen mit ihm über Umgebungsmonitoring, Sensorik & IoT und natürlich über den Einsatz von LoRaWAN.

ENERGIEWENDE IN SICHT?

Die Energiewelt ist auf fast allen Ebenen ihrer technischen und kommerziellen Architektur mit Unbeständigkeit konfrontiert. Ganz gleich, ob man ein Produktionsunternehmen, ein Energielieferant oder ein Netzbetreiber ist, die anhaltende Marktdynamik setzt die Anlagen, die Rentabilität und die Geschäftsmodelle unter Druck. Technologiestrategen und Systemintegratoren sind gleichermaßen gefordert, Lösungen zu finden, um hier Stabilität und Selbstbestimmung zu erlangen. Wie die Lösungen aussehen können, erklärt **Johannes Petrowisch**, Geschäftsführer von Copa-Data CEE/ME im Gespräch.

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

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

Geschäftsführer: Thomas Lunacek

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

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

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

Impressum

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

Chefredaktion:
Mag. Barbara Sawka
+43 699/1911 26 96
b.sawka@technik-medien.at

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

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

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.

7. Jahrgang
©2023 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.

JETZT NEU:

1-MINUTEN-VIDEO

Mit dem 1-Minuten-Video bringen Sie es auf den Punkt. In einer Minute ist das Wesentliche erklärt. Sie haben eine Weltneuheit und wollen dessen USP ganz gezielt hervorstreichen? Sie positionieren sich in einem neuen Markt oder wollen eine Botschaft vermitteln – niederschwellig und ohne großen Zeitaufwand?

Wir setzen es für Sie in Szene.

RUFEN SIE UNS AN! WIR ERKLÄREN ES IHNEN. IN EINER MINUTE.

Thomas Lunacek
+43 676 848 205 13 oder
Gudrun Lunacek
+43 676 848 205 12

Ab sofort auf: YouTube https://www.youtube.com/@technikmedien

MM MASCHINENMARKT | IoT4 INDUSTRY&BUSINESS

T&M TECHNIK & MEDIEN VERLAGSGMBH

Technik & Medien Verlagsges.m.b.H.
Traviatagasse 21-29/8/2, A-1230 Wien
+43 1/876 83 79-0, office@technik-medien.at
www.technik-medien.at
www.maschinenmarkt.at

Open for business

OPC UA und OPC UA FX

Automatisierungspyramide

Industrial IoT

Digitales Business basiert auf Konnektivität. Produktion in Losgröße 1, software-gesteuerte Anpassung, Ferndiagnose, und End-to-End-Integration der Wertschöpfungs-kette – all das erfordert nahtlose Kommunikation zwischen Maschinen und Systemen. Mit B&R steht die digitale Zukunft weit offen: Von einer Generation FX-fähiger Bus-Controller und Steuerungen bis hin zum TSN-Switch und der integrierten Entwicklungsunterstützung in Automation Studio.
Erfahren Sie mehr unter **br-automation.com**