IoT4 INDUSTRY & BUSINESS
Das Magazin für IoT, Big Data und Security

www.iot4industry.at

Erscheinungstermin: 22. November 2022 3 | 2022

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

3 x jährlich

Bei Aucotec heißt es:

MEHR WERT SCHÖPFEN MIT DIGITAL TWIN

Im Fokus
VON DER KÜR ZUR PFLICHT

Im Gespräch
DIGITAL TWIN UND SMART FACTORY

Im Gespräch
ANGRIFFE UND LÖSUNGEN

TECHNIK & MEDIEN VERLAGSGMBH

H-Save Ausgabeautomat

Wege sparen durch dezentrale Versorgung

HABERKORN

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

haberkorn.com

Liebe Leserin, lieber Leser,

Ich bin ein Mensch der Worte. Ich mag Worte und interessante Sätze. In dem nun langsam zu Ende gehenden Jahr habe ich viele neue Worte in meinen Wortschatz aufgenommen. Ich möchte sie Ihnen an dieser Stelle nicht vorenthalten: Machine Learning, Cyber-Resilienz, Pen-Test, Predictive Maintenance, Cloud Computing, Künstliche Intelligenz, Virtual Reality, Backup, Hacker, Ransomware, SaaS, Data Breach Costs, Data Loss Protection, Gaia X, OT, IIoT, Cyber Security, CISO, Information Gathering, Disaster Recovery, On-Premise, Log4j, Open Source, Digitalisierung, Big Data, IoT usw. Die Liste ließe sich leicht verlängern und wird auch kommendes Jahr länger werden, denn dann geht es für mich in die zweite Runde in der Verantwortung für dieses Magazin. Und auf die freue ich mich schon sehr.

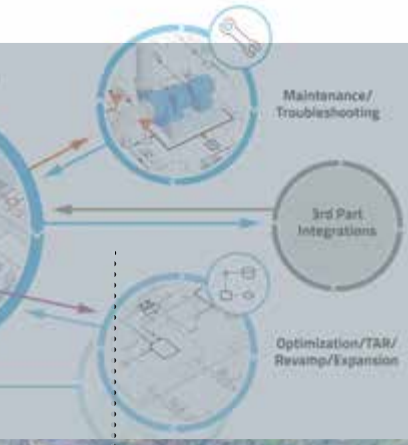
Und ich freue mich auch auf ein paar Änderungen, die wir vornehmen werden. Wir werden auf das EINE Fokusthema verzichten und stattdessen in jeder Ausgabe die großen Trendthemen im Allgemeinen und in den Details behandeln. Damit wollen wir den permanent wichtigen Themen mehr Raum geben und nicht mehr warten, bis sie endlich laut Mediaplan dran sind. Was ganz sicher bleibt, sind unsere Gespräche mit Expert:innen und Branchenkenner:innen. Denn sie sind das Kernstück dieses Magazins. Und mein absoluter Favorit, schon aus völlig eigennützigen Gründen. Ich habe dadurch die Gelegenheit mit interessanten Menschen über spannende Themen zu sprechen und meine persönliche Neugierde an den großen Themen des Heftes zu stillen. Ich hoffe, dass ich Ihnen damit auch ein paar Antworten auf Ihre Fragen mitbringen kann.

Auch in diesem Heft habe ich wieder viel Neues erfahren. Etwa dass es Hacker mit Herz gibt, dass die Kosten eines Cyber-Angriffs in die Millionen gehen und dass wir es mittlerweile mit einer richtigen Industrie zu tun haben, „die wahrscheinlich mehr DevSecOp wie normale Unternehmen macht“ (Zitat Ziggy Schauer, IBM ab Seite 16). Ich habe auch verstanden, dass die IT-Abteilung und die Security-Abteilung zwei Paar Schuhe sind. Ich habe aber auch von den besseren Seiten der modernen Welt erfahren, nämlich dass man dank Künstlicher Intelligenz eventuell weniger Lebensmittel verschwendet und den gezielten Einsatz von Dünger und Pestiziden im Weinberg steuern könnte.
Sollten Sie sich bestimmte Themen wünschen, Interviews mit besonderen Expert:innen oder den Blick auf noch unbekannte „Welten“, dann schreiben Sie mir – ich werde der Sache gerne nachgehen.

Ich wünsche Ihnen viel Spaß beim Lesen dieser Ausgabe, einen schönen Winter und Jahreswechsel! Wir lesen einander wieder am 23. März 2023 an dieser Stelle. Vorher finden Sie uns natürlich im Internet und auf LinkedIn.

Alles Liebe
Barbara Sawka

INHALT
NOVEMBER 2022



Coverstory

Wie kann man den Mehrwert von Dokumentationen nutzen? Bei der Aucotec AG heißt es dazu: Daten statt Dokumente. Dafür hat der Software-Anbieter eine Kooperationsplattform entwickelt, die mit ihrem universellen Datenmodell alle Kerndisziplinen des Engineerings in einer SSoT vereint.

www.aucotec.at

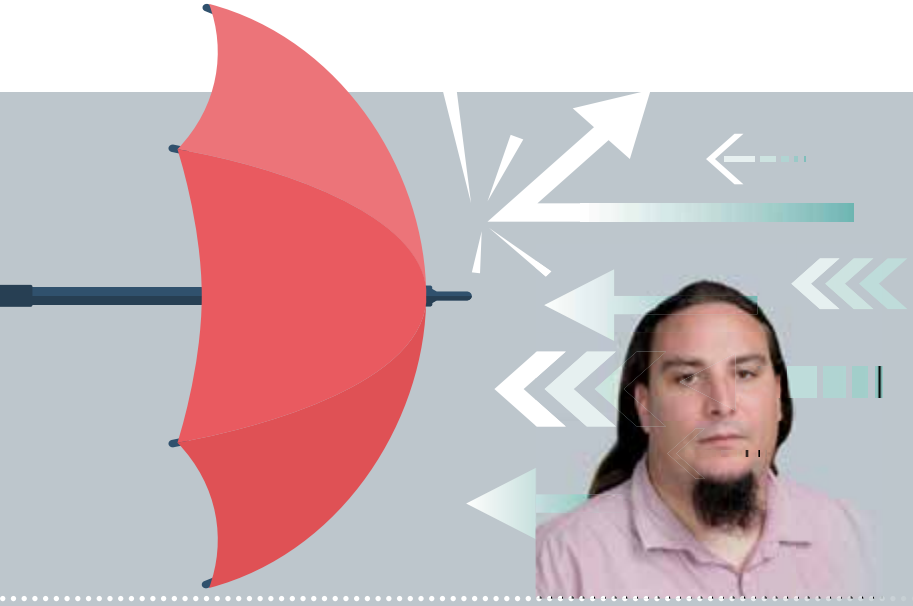
Lesen Sie mehr ab Seite 6!

IM FOKUS

IM GESPRÄCH

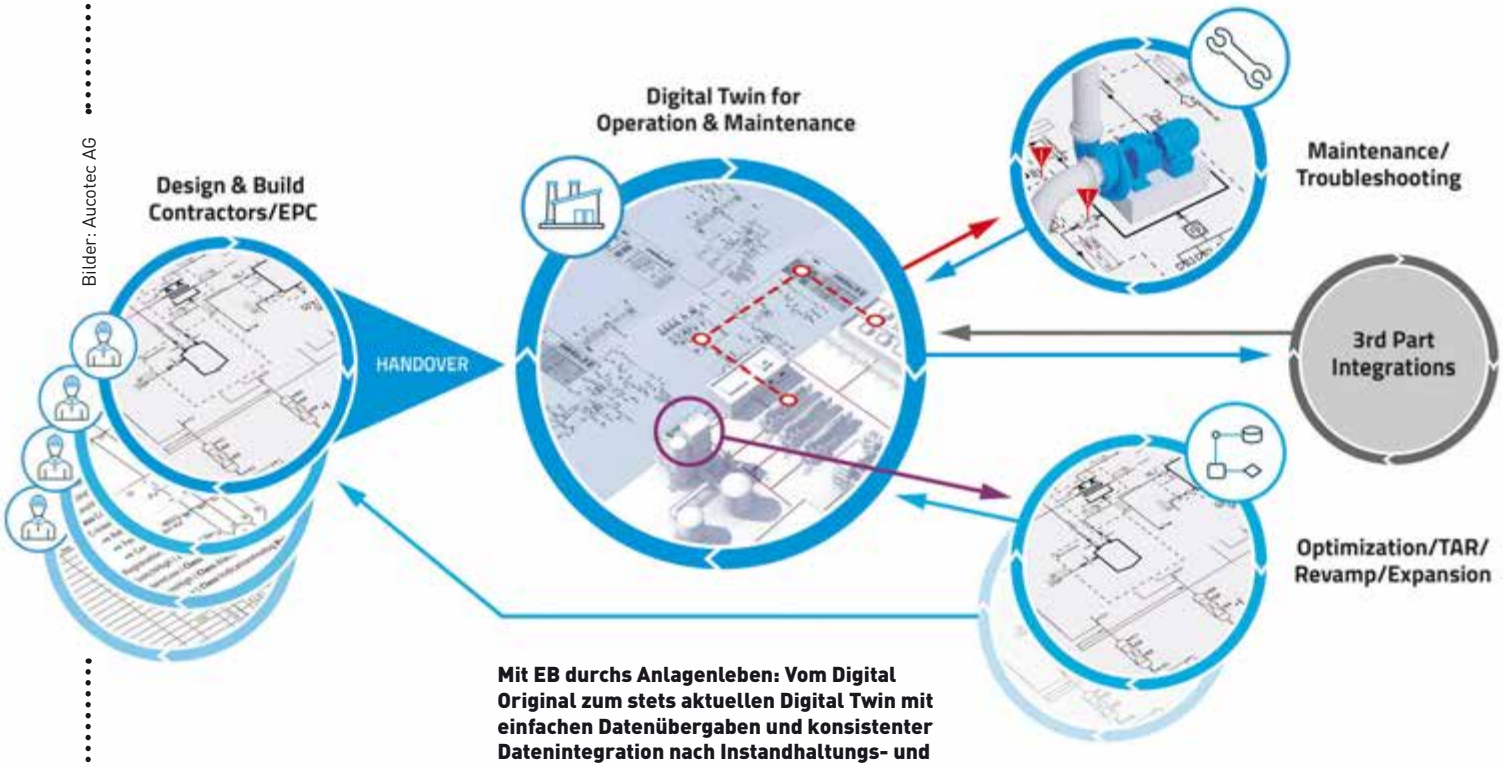
SECURITY | BIG DATA | CLOUD COMPUTING | KI

STÄNDIGE RUBRIKEN



MEHR WERT SCHÖPFEN MIT DIGITAL TWIN

Bilder: Aucotec AG



Mit EB durchs Anlagenleben: Vom Digital Original zum stets aktuellen Digital Twin mit einfachen Datenübergaben und konsistenter Datenintegration nach Instandhaltungs- und Umbaumaßnahmen.

Coverstory

Wie kann man den Mehrwert von Dokumentationen nutzen? Bei der Aucotec AG heißt es dazu: Daten statt Dokumente. Dafür hat der Software-Anbieter eine Kooperationsplattform entwickelt, die mit ihrem universellen Datenmodell alle Kerndisziplinen des Engineerings in einer SSoT vereint.

Von der Feed-Phase über P&IDs, Detail-Engineering bis Automation wächst der Digitale Zwilling in EB's zentralem Datenmodell zusammen.

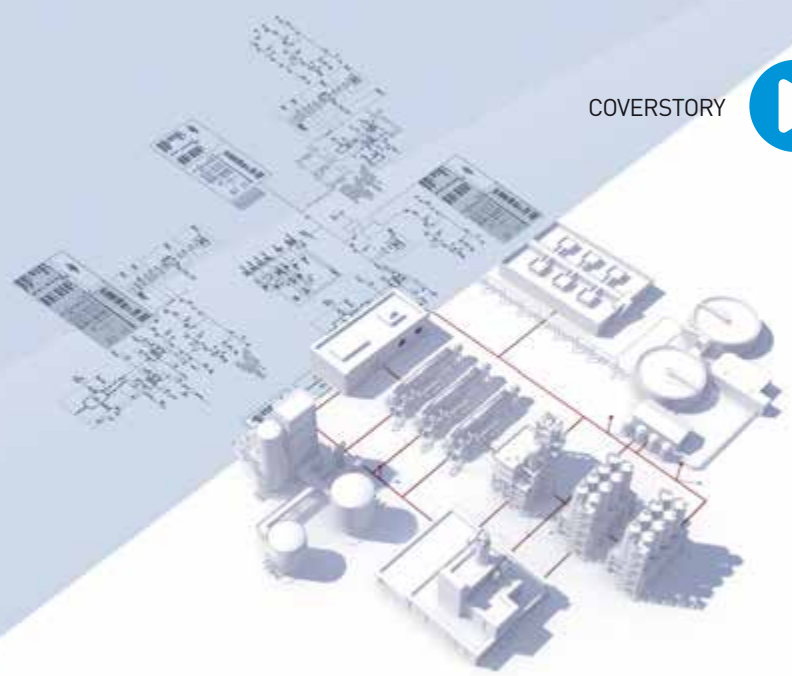
Im Anlagen-Engineering werden Millionen Daten generiert, geändert, aktualisiert und dokumentiert. Über Jahre. Das kostet viel Geld, Zeit und Know-how. Und dann? Die Anlage ist geliefert und in Betrieb, die Dokumentation jedoch schlummert in diversen Dateien oder gar in irgendwelchen Ordnern. „So verliert sie an Wert, umso mehr, wenn nicht jede Reparatur oder Anlagen-Optimierung nachgetragen wird. Dabei eröffnen aktuelle Anlagendaten jede Menge Möglichkeiten zur Wertschöpfung", sagt Reinhard Knapp, Leiter Global Strategies beim Software-Anbieter Aucotec. Wichtigste Voraussetzung, diese Möglichkeiten nutzen zu können, ist laut Knapp das Prinzip „Daten statt Dokumente". Das erfordert eine Single Source of Truth (SSoT), in der in einem universellen Modell alle Daten von Basic- über Process- und Detail-Engineering bis zur Leitsystem-Konfiguration vereint sind – nur so wird eine Dokumentation zum umfassenden Digitalen Zwilling. „Er bildet nicht nur disziplinübergreifend die gesamte Anlagen-Realität mit allen Logiken und Verknüpfungen ab, sondern kann im Lifecycle der Anlage mit all ihren physischen Änderungen konsistent mitwachsen", sagt Knapp. Jede Eingabe, also auch jede Änderung, ist für alle Beteiligten sofort sichtbar, ohne manuelles Übertragen oder Schnittstellen. „Ein Digitaler Zwilling, der nur eine statische Momentaufnahme ist, würde dem Wert der Daten so wenig gerecht wie ihre Haltung in disziplinorientierten Containern", betont er.

Halbe Wirklichkeit – doppelte Arbeit. Noch immer weit verbreitet sind Ketten aus Spezialtools, die disziplinspezifisch z.B. nur P&IDs mit Behältern, Rohren und Flanschen oder nur das Elektrikmodell samt Verkabelung darstellen können. Ein Tank mit Sensor und Pumpe, aber ohne dazugehörigen Loop und ohne das Wissen, ab und bis zu welchem Wert die Pumpe arbeiten soll, zeigt nur die halbe Wirklichkeit. Und die macht doppelt so viel Arbeit beim Planen wie im Betrieb. Denn in einer Toolkette muss jedes Fachsystem einzeln „gefüttert" werden, auch mit den unvermeidlichen Änderungen. Zusammenhänge sind nicht erkennbar, ganz zu schweigen von einer durchgängigen Daten-Navigation. Das Wartungspersonal muss später die relevanten Informationen aus mehreren Quellen zusammenklauben.

Toolketten sind auch der Grund, warum die unvermeidlichen Anlagenänderungen, etwa durch Reparaturen, oft nicht oder nur unzulänglich bei der Dokumentation ankommen. Das kon- >>

Reinhard Knapp
Leiter Global Strategies, Aucotec

„Die Dokumentation verliert an Wert, umso mehr, wenn nicht jede Reparatur oder Anlagen-Optimierung nachgetragenen wird. Dabei eröffnen aktuelle Anlagendaten jede Menge Möglichkeiten zur Wertschöpfung."



Ein Digitaler Zwilling, der nur eine statische Momentaufnahme ist, wird dem Wert der Daten nicht gerecht.

sistente Nachtragen in diversen Spezialtools ist sehr zeitaufwendig und fehleranfällig. Liegen nur Papier-Dokumentationen oder „tote“ PDFs vor, die schon mit den Roteinträgen vorangegangener Änderungen überfrachtet sind, ist der aktuelle Stand kaum nachvollziehbar. Das ist im Störfall besonders fatal, aber auch, wenn ein Umbau ansteht oder nach einer Stillstandsphase eine neue Betriebsgenehmigung fällig wird.

Mit Engineering Base wächst zusammen, was zusammengehört. Deshalb hat die Aucotec AG eine Kooperationsplattform entwickelt, die mit ihrem universellen Datenmodell alle Kerndisziplinen des Engineerings in einer SSoT vereint. Jedes Objekt gibt es nur einmal in der Datenbank von Engineering Base (EB) und jede Fachrichtung kann es jederzeit aus ihrer Sicht spezifizieren. Gleichzeitig sieht jeder, was die anderen Disziplinen bereits erarbeitet haben und baut direkt darauf auf. Ob bei Antrieb, Flowstream oder Verkabelung: Änderungen zeigt die Plattform in allen Konsequenzen automatisch auf, weil sie die Zusammenhänge kennt. „So wächst der Digital Twin mit all seinen Aspekten von der Feed-Phase bis zur Inbetriebnahme konsistent zu einer Einheit zusammen, die den enormen Schatz an Anlagenwissen durchgängig offenlegt“, erklärt Knapp.

Zwilling statt älterer Schwester. Diese Einheit in EB‘s Datenmodell macht es auch deutlich einfacher, die As-built-Dokumentation als Digitalen Zwilling lebendig und aktuell zu halten. Techniker:innen können mit EB Mobile View, einer webservicebasierten App, im Nu alle relevanten Daten jedes Anlagenbereichs auf ein mobiles Gerät ziehen, statt sie mühselig zusammenzusuchen. Zudem erlaubt die App, per Redlining Änderungsinformationen direkt an den Objekten einzugeben und sie an das Engineering zurückzuspielen, „damit der Zwilling nicht zur älteren Schwester der Anlage mit nur leidlicher Ähnlichkeit wird, sondern seinen Namen verdient“, betont der Aucotec-Stratege. Sind OPC-UA-fähige Geräte in der Anlage verbaut, können sie sogar direkt mit EB kommunizieren und damit ihre Existenz oder Modifizierung dem Digital Twin melden. So ist der Service immer up to date. Und vor Umbauten muss nicht erst ein Team den Ist-Zustand in der Anlage scannen und dann nachtragen.

DIE FÜNF WICHTIGSTEN „ZUTATEN“ ZUM ENGINEERING EINES LEBENDIGEN DIGITAL TWIN

1. Quelle

Anlagen bestehen aus vielen miteinander verbundenen Teilen. Ihr Digitaler Zwilling muss diese Verbindungen kennen und darstellen. Damit die Fachabteilungen ihr Wissen effizient verknüpfen können, ohne aufeinander warten zu müssen, brauchen sie ein zentrales Datenmodell, die Single Source of Truth (SSoT) für alle Kerndisziplinen des Engineerings. Nur so sind Dateneingaben automatisch für alle Beteiligten sichtbar – ohne Übertragungen und Schnittstellen wie bei Ketten aus disziplinspezifischen Tools.

2. Unabhängigkeit

In der zentralen Quelle existiert jedes Objekt nur einmal. Jede Disziplin bearbeitet ihre Sicht darauf. Früher brauchte ein Objekt, um verwaltbar zu sein, ein Normkennzeichen, im Stromlaufplan waren Symbolplatz und Betriebsmittelkennzeichen notwendig. Sind Objekte unabhängig von ihrer Verwendung darstellbar, reicht ein Symbol. Eine Pumpe erbt dann z.B. mit der Leistungsdefinition automatisch den passenden Satz Attribute. Ändert sich die Leistung, passen sich die Darstellungen an.

3. Parallelität

Engineeringprozesse immer stärker zu parallelisieren, ist längst erzwungene Realität. Viel Zeit und Datenqualität gehen verloren, wenn die Parallelisierung mit ungeeigneten Toolketten versucht wird. Der Zeitdruck macht es jedoch unmöglich, vermeintlich vorgelagerte Projektschritte abzuwarten. Mit der SSoT ist eine starre Bearbeitungsfolge passé, die Fachbereiche können schneller loslegen, parallel arbeiten und agil kooperieren.

4. Änderungsmanagement

Änderungen sind mühsam, unendlich, unausweichlich. Ketten aus spezialisierten Einzeltools führen zu einem aufwendigen Reigen fehleranfälliger Änderungsübertragungen. In einem zentralen Datenmodell dagegen verbreiten sich Änderungen unmittelbar automatisch in alle Gewerke. Konsistenz ist „System-immanent“. Zusätzlich ermöglicht die SSoT u.a. transparentes Data Tracking, Versionshistorien und rollenbasierte Rechtevergaben für den gesamten Zwilling.

5. Datenpflege

Sie ist das A und O, um den Digital Twin lebendig zu halten. Aktualität ist sein Lebenszweck, sobald die Anlage in Betrieb geht. Ob Störfall, Wartung oder Umbauten, immer ist Zeit viel Geld. Mit Webservices und dank SSoT werden physische Änderungen in der Anlage schnell ans Engineering kommuniziert, auch direkt von der Anlage zu ihrem Zwilling via OPC UA. So sind Umbauten zuverlässig planbar und Störfälle schnell behoben.

Damit dieses Vorgehen auch Betreibern älterer Anlagen mit entsprechenden Dokumentationen offensteht, hat Aucotec zu EB ein Migrationskonzept entwickelt, das Bestandsdaten während ihrer Übernahme prüft, zum Teil ergänzt bzw. zusammenführt und so auf ein Digital-Twin-Level anhebt. Den Wert des Datenbestands für eine Chemieanlage bezifferte ein Aucotec-Kunde einmal auf rund fünf Millionen Euro. Sein Erhalt war ein wichtiger Grund, auf EB umzusteigen.

Vom Daten- zum Geschäftsmodell. Doch es ist nicht nur unnötig, den Wertverlust von Dokumentationen hinzunehmen, sondern auch, den Mehrwert nicht zu nutzen, den aktuelle, leicht zugängliche und verwertbare Bestandsdaten bieten. Mit dem Datenmodell in EB können z.B. aus Herstellern Full-Service-Anbieter werden. Wer kennt ein Produkt besser als sein „Erzeuger"? Und wo, wenn nicht in dem System, mit dem eine Anlage entwickelt wurde, sind die Daten dazu am präzisesten und umfassendsten? Ein Kompressoren-Hersteller etwa verkauft nicht mehr die Anlage, sondern die Druckluft. Er betreibt die Teilanlage selbst, sein Know-how, im Datenmodell manifestiert, ist Garant für Qualität und Verlässlichkeit. Der Gesamtanlagen-Betreiber wird deutlich entlastet und setzt mit höherer Wahrscheinlichkeit auch künftig auf diesen Lieferanten.

Aucotecs Entwickler:innen haben zudem EB mit einer Webservice-Technologie ausgestattet, die es erlaubt, das System mit browserbasierten Frontend-Produkten für individuelle Spezialaufgaben zu ergänzen, also Apps, die Möglichkeiten für weitere Geschäftsmodelle eröffnen. Hier kommt wieder die SSoT, das zentrale Datenmodell zum Tragen, das die Objekte direkt nutzbar macht, auch für Analysen und KI-Einsatz.
So lassen sich per App Wartungsvorgänge unterstützen oder Ist-Zustände in der Anlage aufnehmen und daraus Optimierungsangebote für den Betreiber entwickeln. Auch Monitoring für bestimmte Zielgruppen ist möglich oder die Unterstützung von Predictive Maintenance. Dazu ist EB in der Lage, weil das System auch abstrakte Objekte, sogenannte Interpretationen, die in herkömmlichen Dokumenten gar nicht auftauchen, verwaltet. Etwa Messtypen zur funktionalen Beschreibung eines Sensors. Damit lässt sich ein Predictive-Maintenance-System automatisiert in die Lage versetzen, Zustandsdaten aus der laufenden Anlage richtig zu interpretieren. Bei zigtausenden Signalen ein enormer Zeitgewinn. „Sofern der Digital Twin ein lebendiges Abbild bleibt, also mit ‚seiner' Anlage mitwächst, lässt sich daraus eine Menge Mehrwert schöpfen, statt dass sich der Wert in der Dokumentation erschöpft", so das Fazit von Reinhard Knapp.

www.aucotec.at

Aucotec-Österreich-Geschäftsführer Ing. Heinz Rechberger erklärt, warum das Anlagen-Engineering in Industrie 4.0 so wichtig ist.

„Industrie 4.0 heißt Digitalisierung. Für das Anlagen-Engineering bedeutet das, ein virtuelles Abbild der Anlage, ihren „Digital Twin" bereitzustellen. Dazu müssen mehrere Voraussetzungen erfüllt sein:
Zunächst braucht so ein Anlagenmodell Struktur. Da bietet sich die IEC 81346 an, deren drei hierarchische Strukturen zu Funktion, Produkt und Ortsaspekt auf Objektebene intelligent verknüpft sind. Ein Anlagenmodell muss außerdem detailliert genug sein, um später in der Wartung beispielsweise den Signalverlauf einer Messung verfolgen zu können. Dazu muss nicht nur der Sensor enthalten sein, sondern auch Informationen wie Anschlüsse, Kabel, Klemmen oder Kanal der Leitsystem-Karte. Darüber hinaus ist zentrale Verfügbarkeit essenziell. All diese Informationen müssen in einem Modell liegen statt in etlichen – und damit potenziell inkonsistenten – Teilmodellen.

Viele Engineering-Werkzeuge sind recht weit von diesen Anforderungen entfernt. Meist sind das historisch gewachsene „Engineering Suites", also Sammlungen von Spezial-Tools. Ihr Zusammenwirken wird über Schnittstellen geregelt, die jedoch kein zentrales Modell ergeben. Da eine Suite naturgemäß viele Datenquellen enthält, kann sie nie die für Industrie 4.0 erforderliche „Single Source of Truth" sein.

Aucotecs Plattform Engineering Base dagegen bietet heute bereits mit ihrer mehrschichtigen Serverarchitektur genau diese disziplinübergreifende, zentrale Datenquelle für die Abbildung eines kompletten digitalen Anlagenzwillings."

AUS DEM HINTERHALT

Kein Tag ohne Cyberangriff. Egal ob Ransomware, Supply-Chain-Angriffe oder Deep Fakes – die Gefahren sind vielfältig und vor allem kann es jeden treffen. Und die Angriffe werden als gefährlicher als der Mitbewerb eingestuft. Aufgeben ist dennoch keine Option.

2022 war eines der stärksten Jahre, was die Verbreitung von Cyberangriffen auf digitale Infrastrukturen von öffentlichen Versorgungsunternehmen, Unternehmen, Regierungsbehörden und Usern betrifft. Diese Angriffe wurden von einer Vielzahl von Angreifern und Kriminellen durchgeführt, die zunehmend dreister und effektiver vorgehen. Durch diese Angriffe und Datenschutzverletzungen verlieren Unternehmen weltweit jährlich Millionen an Dollar/Euro. Die Schäden reichen dabei weit über die finanziellen Kosten hinaus. In den letzten drei Jahren zählten der Abgang von Kund:innen (27 %), der Verlust von Kundendaten (25 %) und die Schädigung des Rufs oder der Marke (23 %) zu den negativen Folgen – das zeigt die aktuelle „Global Digital Trust Insights Survey“ von PwC. Aus der Befragung von 3.522 Führungskräften in 65 Ländern, darunter 30 in Österreich, geht klar hervor: Das Thema Cybersicherheit rückt rund um den Globus zunehmend in den Fokus der Unternehmen. Auch in Österreich. Gefragt

Georg Beham
Partner und Cybersecurity & Privacy Leader bei PwC Österreich

„Das Thema Cybersicherheit hat oberste Priorität und muss von der Geschäftsleitung und den Aufsichtsräten in das Unternehmen direkt zu allen Mitarbeitenden getragen werden.“

Markus Sageder
Cybersecurity-Experte bei Cisco Österreich

„Hybrides Arbeiten verlangt nach einer soliden Strategie seitens der Unternehmen und einer Investition in Geräte, Protokolle und Anwendungen als entscheidende Maßnahmen für IT-Security."

nach den größten digitalen Risiken für ihre Geschäfte für das kommende Jahr geben 77 % der heimischen Unternehmen Gefahren durch Cyberkriminelle und 67 % durch Hacker:innen bzw. Hacktivist:innen als größte Bedrohung an. Deutlich weniger gefährdet fühlen sich die heimischen Führungskräfte etwa durch die Konkurrenz (33 %). „Die Tricks der Cyberkriminellen werden immer raffinierter. Wo sie durch bestens entwickelte Software-Systeme, Firewalls und Virenscanner nicht weiterkommen, versuchen sie, Anwender:innen durch Täuschung zur Installation von Schadsoftware oder Herausgabe sensibler Daten zu bewegen. Deswegen hat das Thema Cybersicherheit oberste Priorität und muss von der Geschäftsleitung und den Aufsichtsräten in das Unternehmen direkt zu allen Mitarbeitenden getragen werden", erläutert Georg Beham, Partner und Cybersecurity & Privacy Leader bei PwC Österreich. Wie die Studie zeigt, hat sich hier in den letzten Jahren viel bewegt und das Thema ist mittlerweile auch auf der Führungsebene angekommen. „Trotz aller Fortschritte, die die heimischen Organisationen bei der Verbesserung ihrer Cybersicherheit gemacht haben, zeigt unsere Umfrage, dass noch viel zu tun ist. Es gibt meiner Erfahrung nach drei Dinge, die eingeführt werden müssen, um mit der digitalen Transformation Schritt zu halten: Eine Kontinuitäts- und Notfallplanung mit klaren Playbooks, ein Überwachungsmodus, der Angriffe zuverlässig meldet und stoppt, sowie das rasche Schließen von neuen Schwachstellen", so Georg Beham.

Schwachstelle Homeoffice. Remotearbeit ist mittlerweile zum Standard geworden. Was für den einen zu einer neuen Qualität der Arbeit geworden ist, ist für die Security-Verantwortlichen zu einer neuen Herausforderung gewachsen. Dazu hat Cisco die europaweite „EMEA Consumer Security"-Studie erstellt, um die Einstellung zur Cybersicherheit im privaten Bereich zu beleuchten. Die Ergebnisse zeigen, dass viele Arbeitnehmer:innen ihr privates Gerät häufig für berufliche Aufgaben wie das Versenden von E-Mails, berufliche Anrufe und die gemeinsame Bearbeitung von Dokumenten nutzen. Das zeigt, dass die Absicherung privater Devices von Seiten der IT- oder Security-Teams »

Priorität haben muss. 63 % der Befragten setzen Multifaktor-Authentifizierung (MFA) und biometrische Daten ein, um ihre privaten Geräte vor unerlaubten Systemzugriffen zu schützen. Unternehmen haben die Möglichkeit, diese Technologie einzusetzen, um die Einführung einer starken MFA am Arbeitsplatz voranzutreiben. Dem Wissen über die Bedeutung der eigenen vernetzten Geräte steht jedoch eine gewisse Untätigkeit gegenüber, wenn es beispielsweise um den Schutz des heimischen Internetzugangs geht. Ein Sechstel der Befragten hat sein Passwort noch nie geändert und bei weiteren 20 % ist dies schon mehr als ein Jahr her.

Ebenfalls kritisch ist die Nutzung von öffentlichen WiFi-Netzen. 76 % gaben an, bereits öffentliche Netze genutzt zu haben, um beispielsweise E-Mails abzurufen. 70 % erledigten außerdem komplexere Aufgaben. „Hybrides Arbeiten verlangt nach einer soliden Strategie seitens der Unternehmen und einer Investition in Geräte, Protokolle und Anwendungen als entscheidende Maßnahmen für IT-Security. Die Wahrscheinlichkeit unbefugter Zugriffe kann dadurch deutlich minimiert werden. Zugriffe auf Anwendungen in der Cloud sollten ebenfalls nach individuellem Bedarf und Kontext abgestimmt werden“, empfiehlt Markus Sageder, Cybersecurity-Experte bei Cisco Österreich.

Die gefährlichsten Cybercrime-Trends. Emotet, Trickbot, Clop, Agent Tesla, Apache Log4j – die Zahl der kursierenden Schadprogramme wächst jeden Tag um mehr als 400.000 neue Varianten. Mit ein Grund dafür, dass Cybervorfälle mittlerweile weltweit auf Platz eins der größten Business-Risiken gerutscht sind. Ransomware-Attacken erleben dabei ein besonders starkes Wachstum. Ein weiterer Trend sind groß angelegte Supply-Chain-Angriffe, die auf schwache Glieder einer Lieferkette abzielen und über sie ganze Versorgungssysteme lahmlegen. Das Gefährliche an Supply-Chain-Angriffen ist, dass sie nicht erkannt werden, da sie bewusst auf Anbieter und Lieferanten abzielen, anstelle direkt auf das betroffene Unternehmen. Dadurch lassen sie sich schwieriger erkennen und verhindern. Auch der

Dariush Ansari
Geschäftsführer des IT-Sicherheitsspezialisten Network Box Deutschland GmbH

„Wenn Mitarbeitenden die Relevanz von Informationssicherheit und Awareness-Maßnahmen bewusst ist, wird sich auch ihr Umgang mit Cybergefahren verbessern.“

Ausbau von KI verleitet Cyberkriminelle zu tückischen neuen Angriffstechniken: Mit sogenannten Deepfakes gaukeln sie durch Bilder, Audio- und Videofälschungen täuschend echte Inhalte vor. Hinzu kommen Taktiken wie das Voice-Cloning, welche bewirken, dass Computer wie echte Menschen klingen. Dabei imitieren die Angreifenden beispielsweise die Stimme eines Vorgesetzten künstlich und bringen Mitarbeitende über einen Anruf dazu, sensible Informationen preiszugeben oder Überweisungen zu tätigen. „Bei allen neuen Trends lässt sich eines klar sagen: Phishing und Social Engineering bleiben die Dauerbrenner unter den Angriffsmethoden“, so Dariush Ansari, Geschäftsführer des IT-Sicherheitsspezialisten Network Box Deutschland GmbH. Die Cyberkriminellen feilen ihre Methoden immer weiter aus und greifen aktuelle Themen und Entwicklungen für zielgenaue Angriffe auf. Dabei geht der Trend von herkömmlichen Phishing-Attacken, bei denen Zielpersonen nach Zufall in das Raster des Angreifers fallen, zu Spear-Phishing-Angriffen, bei denen das Opfer zum Teil über Wochen und Monate gezielt ausspioniert wird. In diesem Zeitraum werden Gewohnheiten und Präferenzen in Erfahrung gebracht, um dann maßgeschneiderte, personenbezogene E-Mail- bzw. Phishing-Angriffe zu realisieren. Fazit: Die Schnittstelle zwischen Mensch und Maschine bleibt weiterhin Einstiegstor Nummer eins. „Umgekehrt bedeutet das aber auch, dass der Mensch der wichtigste Faktor für die Cyberresilienz von Organisationen ist“, so Ansari. „Wenn Mitarbeitenden die Relevanz von Informationssicherheit und Awareness-Maßnahmen bewusst ist, wird sich auch ihr Umgang mit Cybergefahren verbessern.“ Um sich auf die Flut an neuen Angriffsformen vorzubereiten, sollten Unternehmen also auf die Schulung ihrer Mitarbeitenden setzen und sie zusätzlich mit Tools ausrüsten, die ihnen bei der Erkennung von schädlichen Inhalten helfen.

www.pwc.at
www.cisco.com
www.network-box.eu

EUROPAMEISTER DER NACHWUCHSHACKER GEKÜRT

„Stress war im wahrsten Sinne des Wortes vorprogrammiert", fasst CSA-Vorstand und Mitorganisator Joe Pichlmayr mit einem Augenzwinkern das spannende Finale der diesjährigen **8. European Cyber Security Challenge** (ECSC2022) zusammen. Zwei Tage lang ging es am 14. und 15. September zwischen 330 höchst talentierten und motivierten Cyber-Security-Talenten um Netzwerk- und Systemkenntnisse, Cryptographie und Steganographie, Reverse Engineering und Exploitation-Know-how, Hardware-Hacking sowie Web-, Mobile- und Wireless-Security. Beim Attack&Defense-Szenario, der Königsdisziplin, mussten die Finalist:innen zeitgleich ihre eigenen Netzwerke absichern und die der anderen Teams hacken.

Die Sieger-Teams. Als Sieger der ECSC2022 ging schließlich das Team Dänemark hervor, das sowohl bei den Aufgaben im Jeopardy-Format als auch im Attack&Defense-Szenario die beste Wertung erzielte. Das Team Deutschland erreichte mit Stärken im Attack&Defense-Szenario den ausgezeichneten 2. Platz, während das Team Frankreich vor allem bei den Aufgaben im Jeopardy-Format punktete und es in der Gesamtwertung auf den 3. Platz schaffte. Das Team Austria als diesjähriges Gastgeberland schaffte es auf den 10. Platz und damit unter die Top 10 der insgesamt 33 angetretenen Teams.
Neben 29 europäischen Nationen nahmen auch vier Gast-Teams an der ECSC2022 teil. Team Canada erreichte den Platz 13, das Team USA schaffte es auf Platz 15 und die Teams Israel und Vereinigte Arabische Emirate landeten nacheinander auf Platz 29 und 30. „Verlierer gibt es bei der ECSC ohnehin nicht", so Joe Pichlmayr: „Mit der Qualifikation aus über 18.000 Schüler:innen und Student:innen haben die Teilnehmer:innen bereits eindeutig ihr Talent und ihr Fachwissen bewiesen." Die Teilnahme an der Qualifikation sei auch ein toller Einstieg in eine mögliche Cyber-Security-Laufbahn: „Wer sich hier behaupten kann und es sogar ins Finale schafft, hat sehr gute Karten – auch auf dem Job-Markt, wo sich unsere Finalist:innen ihren Traumjob im wahrsten Sinn des Wortes aussuchen können."

www.ecsc2022.eu

CYBERATTACKEN VERSCHÄRFEN ANGESPANNTE LAGE IM STROMSEKTOR

Im Zuge der Energiewende – und der damit verbundenen Digitalisierung der Netze – stellt das zunehmende Risiko von Cyberattacken die Energieversorger vor Herausforderungen. Verstärkt haben sich diese im Zuge der Covid-19-Pandemie und seit dem Beginn des Krieges in der Ukraine. Gerhard Christiner, technischer Vorstand des Übertragungsnetzbetreibers **Austrian Power Grid** (APG) stellte im Rahmen von Österreichs Energie Kongress 2022 Ende September klar, dass Cybersicherheit als „Top-Thema" zu den bestehenden Herausforderungen hinzukomme. Die APG habe diesbezüglich umfassende Vorkehrungen getroffen. Laut Christiner bleiben Bedrohungen aus dem Cyberraum „ein abstraktes Risiko. Man hat nie das Gefühl, man ist sicher".

www.apg.at

Gerhard Christiner, technischer Vorstand des Übertragungsnetzbetreibers APG


Ingrid Kriegl, Inhaberin von Sphinx IT Consulting

DIE „PILLE DANACH“

Hacker finden immer wieder Wege sogar die besten IT-Systeme zu knacken und zu verschlüsseln. Der Betrieb steht – oft müssen Bitcoins fließen. Danach bekommen Betroffene zwar mit großer Wahrscheinlichkeit das Entschlüsselungspasswort, doch muss die IT alle Systeme wieder zum Laufen bringen. Welche Hintertüren sich die Angreifer offengelassen haben, bleibt ungewiss. Das Wiener IT-Beratungsunternehmen **Sphinx IT Consulting** entwickelt die „Pille danach“ gegen Cybercrime. Damit soll die IT von KMUs nach einem Cyberangriff nach wenigen Minuten wieder genauso wie vor dem Angriff funktionieren. Lösegeld-Forderungen seien somit vom Tisch. Mit der Lösung namens Blueboxx werden Daten unverzüglich, vollständig, in sich konsistent und ohne Ausfallzeit wiederhergestellt. Was wie ein Wunder klingt, ist in Wirklichkeit recht einfach: Blueboxx ist eine geschickte Kombination aus bewährten Open-Source-Komponenten. Der Betrieb wird wiederhergestellt, indem die gesamte IT auf den Stand vor dem Angriff zurückgesetzt wird – so als würde man einen Film zurückspulen. Ingrid Kriegl, Inhaberin von Sphinx IT Consulting und Misssi Eis: „Als Inhaberin zweier Mittelstands-Unternehmen blutet mir das Herz, regelmäßig über erfolgreiche Hackerangriffe zu lesen, obwohl es eine zu 100 Prozent zuverlässige Schutzmaßnahme gibt. Jedes Unternehmen, das Lösegeld zahlen muss, ist eines zu viel.“

www.sphinx.at

DEUTLICHE LÜCKEN IN CYBERSICHERHEIT

Cybersicherheit wird noch immer in Silos gedacht – zu dem Schluss kommt eine Studie des Spezialisten für IoT-Security **Onekey**. „Vielfach denken Unternehmen und Unternehmer noch immer in klassischen Silos, was die IT-Sicherheit angeht. Dabei wird das unmittelbar gewachsene Risiko vieler unterschiedlicher Firmware-Versionen in IoT-Anlagen oft übersehen“, warnt Jan Wendenburg, Geschäftsführer von Onekey. Zu den Bereichen mit höchster Gefährdung gehören IoT-Geräte und Anlagen in der Medizin (47 Prozent), der kritischen Infrastruktur (45 Prozent) und der Fertigung (39 Prozent). Befragt wurden für den „IoT-Sicherheitsreport 2022“ über 300 Unternehmensvertreter aus der Führungsebene. „Alle Bereiche der Industrie sind verwundbar – denn Hacker nutzen konsequent jeden Schwachpunkt und nicht nur die, die von Industrievertretern gewünscht werden“, sagt Wendenburg. Das besondere Risiko im IoT-Sektor sei dabei, dass jedes Gerät und jede Anlage eine eigene Firmware habe – also eine Software, die das Gerät oder die Anlage selber steuert. Da hier kaum Leitlinien noch verbindliche Vorgaben bestünden, legten viele Hersteller bisher nur wenig Wert auf lückenlose Sicherheit gegen Attacken.

Haftung der Leitungsebene. Der Onekey-Chef weist auch auf die zunehmende Haftung von Unternehmensführern hin: „Es ist absehbar, dass in sehr naher Zukunft für Versäumnisse in der IT-Sicherheit unmittelbar die Geschäftsleitung in die Haftung genommen wird“, so Wendenburg. Diese Forderung wurde auch während der Hannover Messe 2022 durch den VDE – Verband der Elektrotechnik Elektronik Informationstechnik e. V. – laut gestellt. Daher müsse jeder Bestandteil einer IT-Anlage – allem voran die Software – lückenlos überprüfbar und rückführbar sein, so Wendenburg. Einig sind sich die befragten Unternehmensvertreter zumindest bei der herstellerseitig gegebenen Sicherheit von IoT-Anlagen: Nur 12 Prozent halten die Maßnahmen zum Hackerschutz für ausreichend, 54 Prozent sehen sie als teilweise ausreichend an, 24 Prozent


Jan Wendenburg, Geschäftsführer von Onekey

als nicht ausreichend und fünf Prozent sogar als mangelhaft. „Der Schlüssel zu mehr Sicherheit liegt darin, schon frühzeitig in der Entwicklung von neuen intelligenten Geräten, Anlagen und Maschinen, automatische Sicherheits- und Compliance-Prüfungen zu nutzen. Dabei können auch gleichzeitig automatisiert Software-Stücklisten, sogenannte „Software Bill of Materials“, erzeugt werden. So wird mit wenig Aufwand viel Sicherheit und Transparenz erreicht“, erklärt Jan Wendenburg.

www.onekey.com

ZWISCHEN LEISEN LÖSUNGEN

„Lernen Sie eine Bitcoin-Wallet anzulegen", rät Siegfried „Ziggy" Schauer, Associate Partner Security IBM Österreich, all jenen, die sich nicht um ihre Security-Strategie kümmern wollen. Was er sonst noch über Cyber-Angriffe und die Möglichkeiten ihnen entgegenzuwirken weiß, verrät er im Gespräch.

IoT 4 Industry & Business: Vielen Unternehmen sind die Gefahren und vor allem die Kosten eines Cyber-Angriffs nicht bewusst. Was kostet so ein Angriff im Schnitt?

Siegfried Schauer: Nach dem kürzlich veröffentlichten IBM „Cost of a Data Breach"-Report beläuft sich die Schadenssumme eines klassischen Cyber-Angriffs auf 4,35 Mio. US-Dollar. Unternehmen könnten sich wahrscheinlich drei Millionen davon ersparen, wenn sie ihre IT-Security richtig aufgebaut hätten. Einem CISO muss man nicht erklären, warum er mehr Budget für die Security braucht. Man muss ihn nur dabei unterstützen, das seiner Geschäftsführung beizubringen. Denn der Geschäftsführer haftet per se, sobald es durch Security Incidents mangels ausreichender „State of the Art"-Sicherheitsmaßnahmen zu Schäden kommt. Im Grunde haben CEOs drei Möglichkeiten dem vorzubeugen: 1. Sie hören auf ihren CISO und unterstützen ihn. 2. Sie hören nicht, dann sollten sie lernen, ein Bitcoin-Wallet anzulegen. Sie werden es brauchen, denn die Frage, ob man einem Angriff ausgesetzt werden könnte ist längst beantwortet (und „Lösegeld" bzw. Erpressersummen werden meist in Krypto bezahlt). Die dritte Möglichkeit wäre, sich aus dem Geschäft zurückzuziehen – auf eine einsame Insel ohne Netzanbindung zum Beispiel. Letztendlich geht es nicht um das, „Ob" man angegriffen wird, sondern um das „Wann" und „Wie".

IoT: Warum fühlen sich so viele Unternehmen dennoch nicht persönlich gefährdet?

Schauer: Ich glaube, das hängt mit der Grundeinstellung zur Digitalisierung im Unternehmen zusammen. Wenn man versucht, dem alteingesessenen Geschäftsführer, der zwei Jahre vor der Pension steht, zu erklären, dass er jetzt etwas gegen Ransomware machen muss, wird die Antwort klassisch nach „Das haben wir bis jetzt auch nicht gebraucht" klingen. Allerdings steigt das Interesse sehr deutlich, wenn in den Medien ein großes Unternehmen auftaucht, das gehackt wurde oder wenn eines aus einer ähnlichen Branche oder der näheren Umgebung angegriffen wurde. Dann mehren sich die Anrufe bei uns.

UND LAUTEN ANGRIFFEN

IoT: Also ist ein Hackerangriff die beste Werbung?
Schauer: Leider ja. Und warum funktionieren diese Angriffe so gut? Einfach weil es die Unternehmen oft nicht schaffen, banale Angriffe abzuwehren. Dabei verlaufen diese häufig nach dem gleichen Muster. Als Beispiel: Das Ziel eines Ransomware-Angriffes ist es, Geld zu machen. Diese Hacker haben zwar Interesse daran sich im Unternehmen einzunisten und Daten zu sammeln, aber in erster Linie wollen sie zeigen, dass sie da sind, indem sie die Rechner verschlüsseln und Geld fordern. Aber wir haben in der Vergangenheit auch schon Angreifer gesehen, die den Key gratis zur Verfügung gestellt haben, weil sie eine Einrichtung trafen, welche sie eigentlich nicht angreifen wollten. Es gibt also manchmal auch Hacker mit einem Mindestmaß an Ethik, wenngleich das eine vermutlich im Promillebereich liegende Ausnahme darstellt. Und darauf kann man sich natürlich nicht verlassen.

IoT: Warum werden solche Organisationen überhaupt angegriffen?
Schauer: Die Hacker, die nach der beliebten „Make Money fast"-Methode vorgehen, greifen nicht zielgerichtet an, jeder ist ein „Potential Target". Diese Hackergruppen und deren TTPs – also tactics, techniques and procedures – unterscheiden sich auf den ersten Blick kaum von jenen Gruppen, die zielgerichtete Angriffe planen. Die einen wollen lange unentdeckt bleiben und die anderen wollen alles verschlüsseln und schnell Geld machen. Sobald sie merken, dass ein größeres Environment und nicht nur ein PC und ein Smart-TV dahinterstecken, beginnen sie mit dem Information Gathering – damit ist das Sammeln von Informationen gemeint – und schauen, mit welchen Unternehmen sie es zu tun haben und wie groß es ist. In der Regel suchen sie unter anderem die Geschäftsberichte, da diese ganz genau aussagen, wie viel Umsatz das Unternehmen macht und wie hoch der Ransom (das Lösegeld) sein könnte. Und der liegt in den meisten Fällen irgendwo zwischen zehn und 20 Prozent. Als Verantwortlicher können Sie sich also überlegen zu bezahlen oder die Firma zuzusperren, wenn die Security-Aufgaben nicht nach „State of the Art"-Methodik erfolgte. Wobei sich meine Haltung in den letzten 20 Jahren dazu nicht geändert hat. Ich würde niemandem empfehlen zu bezahlen, weil man damit deren Industrie weiter nährt. Und deren Industrie ist groß, stark am Wachsen und unserer nicht so unähnlich, wie man aus manchen prominenten Leaks sehen konnte. Die haben Reporting Lines, Sales Teams mit Zielvorgaben, Developmentabteilungen, die wahrscheinlich mehr DevSecOps[1] wie normale Unternehmen machen, IT-Support, ein Management, und sie schulen gezielt ihre Mitarbeiter im Umgang mit den Tools, die zum Einsatz kommen.

IoT: Aber wenn das zu so einer Industrie geworden ist, wird man dem überhaupt noch Herr?
Schauer: Am ehesten ist es vielleicht mit der Pharmaindustrie zu vergleichen. Man braucht eine neue Krankheit wie z.B. Corona und dann finden schlaue Köpfe in einem Labor ein Gegenmittel. So ähnlich ist es auch in unserer Industrie. Aber man kann sich schon sehr gezielt schützen, wenngleich es 100 Prozent nicht gibt, aber Ransomware ist verglichen mit zielgerichteten Angriffen, die auf z.B. eine spezielle Industrie abzielen oder ähnlich Triviales. Oft würde schon die meistens nicht vorhandene EDR(Endpoint Detection & Response)-Lösung helfen, einen Schaden zu verhindern oder zu minimieren – damit sind die Endgeräte geschützt und natürlich sollte man auch auf sein Netzwerk nicht vergessen, denn auch dort kommunizieren die Angreifer. Moderne – oder besser gesagt „State of the Art"-Lösungen sind im Gegensatz zu einfachen Virenscannern mit AI und Machine-Learning-Algorithmen bestückt, sie bringen mehr Intelligenz mit in der Erkennung von noch unbekannten Bedrohungen, etwa auf Basis von Anomalien, aber auch weil sie mit Threat-Intelligence-Informationen angereichert werden. Das heißt: Sie erkennen z.B. ob ein PDF beim Öffnen eine URL ausführt und diese wiederum im Hintergrund einen Browser aufruft, welcher dann Schadcodes nachlädt. Oder wenn eine .exe-Datei ausgeführt wird, die nicht ausgeführt werden sollte. Auch ermöglichen diese Systeme, Rechner noch bevor eine »

[1] DevSecOps steht für Development (Entwicklung), Security (Sicherheit) und Operations (Abläufe).

Siegfried „Ziggy" Schauer
Associate Partner Security IBM Österreich

„Wir müssen mehr Bewusstsein dafür schaffen, dass jeder ein Opfer werden kann und sich die Leute wirklich um ihre Security kümmern müssen."

Infektion stattfindet, komplett vom Netz zu trennen. Der Unterschied im Betrieb im Vergleich zum klassischen AV ist zwar ein wenig aufwendiger, da man auf Prozessebene verstehen muss, wie das Betriebssystem funktioniert und warum die Solution hier einen potenziellen Schadcode entdeckt hat, aber die Sicherheit wird dadurch markant erhöht.

IoT: Der Mensch wird häufig als die größte Schwachstelle in Sachen Security bezeichnet. Was meinen Sie dazu?
Schauer: Der Faktor Mensch spielt definitiv eine sehr wichtige Rolle. Ein gutes Beispiel ist die HR-Abteilung. Die Mitarbeitenden der HR haben die Aufgabe, die Lebensläufe von Bewerbern anzuschauen. Es ist also Teil ihrer Arbeit, Dateien aufzumachen. Hier muss es Systeme geben, die diese Anhänge vorher überprüfen. Denn von Personalverantwortlichen kann man nicht erwarten, dass sie ein Phishing- oder ein infiziertes Mail erkennen. Vor allem wenn man schon als Experte zwei, dreimal hinschauen muss, wenn es gut präparierte E-Mails sind. Aber man kann die Leute gezielt schulen, dass sie sich den Absender genau ansehen oder ob das E-Mail komisch wirkt. Im Zweifel lieber einmal öfter bei der Security-Abteilung nachfragen. Und dann bleibt auch bei jenen, die sich normalerweise mit diesen Themen gar nicht beschäftigen, soviel hängen, dass sie bei einem Verdacht richtig handeln.

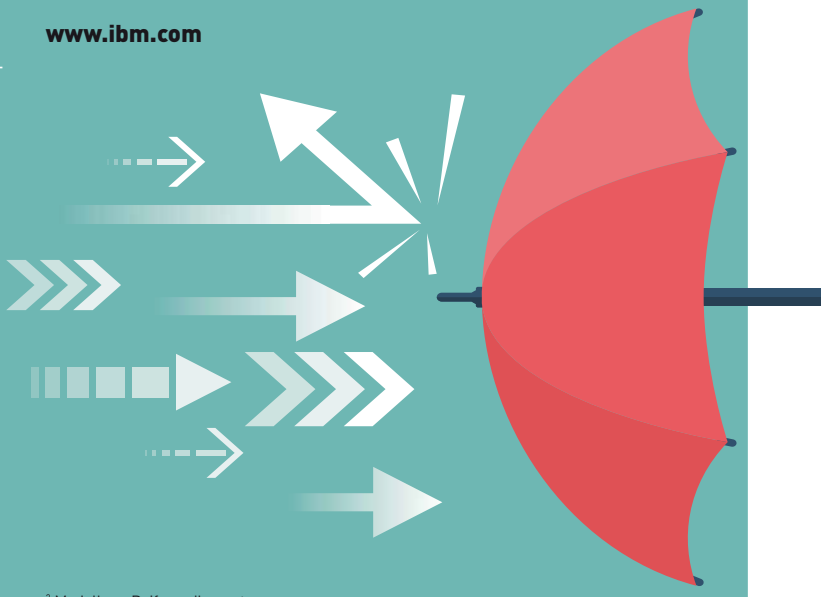
IoT: Bislang war man der Meinung, dass nur die IT-Abteilung Daten produziert und für diese zuständig ist. Mittlerweile produziert jeder Mitarbeitende Daten, das Gefühl für die Verantwortung und Sicherheit dafür schiebt man gerne weiter der IT-Abteilung zu.
Schauer: Natürlich, aber man muss hier eines klar unterscheiden: Die IT-Abteilung ist nicht gleich Security-Abteilung. Das wird leider oft miteinander vermischt. Die IT ist die klassische Systemadministration, die sich darum kümmert, dass die ERP-Systeme laufen, dass jeder einen Laptop hat, auf dem er arbeiten kann, dass alle Programme funktionieren oder dass die Patches für Windows und andere Software ausgerollt werden. Die IT-Security sollte hingegen nicht im IT-Betrieb, sondern eher im Riskmanagement oder der Finanzabteilung angesiedelt sein. Kurzgefasst: Die IT kümmert sich um den Betrieb der Firewall, die Security um die Policies, wie die Firewall zu betreiben ist.

IoT: Wie helfen Sie Ihren Kunden?
Schauer: Wenn wir mit Unternehmen arbeiten, dann machen wir zuerst einmal ein Review, ein sogenanntes Maturity Assessment[2]. Dafür verwenden wir als Basis das Cybersecurity Framework der NIST[3] und auch ISO 27001. Darauf basierend machen wir eine technische Simulation und eine Gap-Analyse und schauen, was bereits alles im Unternehmen umgesetzt ist. Und zwar nicht nur technisch, sondern auch organisatorisch. Das fügen wir dann in einer Risikomatrix zusammen. Schließlich muss der Geschäftsführer bzw. der Verantwortliche entscheiden, ob er mit dem möglichen Risiko leben kann oder nicht. Mein Rat: Man sollte seine Security-Maßnahmen tunlichst von einem Dritten überprüfen lassen. Wenn man sich selbst auditiert, neigt man meist dazu, die Realität zu schönen.

IoT: Die einen propagieren das Backup, die anderen die Cloud, um ihre Sicherheit zu verbessern. Wozu tendieren Sie?
Schauer: Ein Backup ist unabkömmlich, aber eine Cloud ist kein Backup. Man muss seine Backups regelmäßig machen, überprüfen und sie vor allem nicht am Firmenstandort aufbewahren. Letzteres ist Bestandteil jeder Security-Strategie. Bei der Cloud verlassen sich die Kunden meiner Meinung nach noch zu viel auf den Cloudprovider. Der ist im Grunde nur für die Infrastruktur, nicht aber für die Plattform und die darauf laufenden Applikationen verantwortlich. Die Verantwortung dafür trägt das Unternehmen, welches die Plattform und die Applikationen betreibt. Natürlich wird ein Cloudprovider seine Infrastruktur besser schützen können, als jemand, der sich selbst eine Cloud aufbaut, denn das ist ein immenser Aufwand, personell wie monetär. Damit ist nicht eine kleine betriebene Cloudinstanz gemeint, die auf einem NAS[4] laufen kann, sondern Systeme die mehrere Rechenzentren füllen.

IoT: Müssen wir mit den Gefahren und Angriffen zu leben lernen?
Schauer: „Ja" ist da vielleicht eine zu kurze Antwort. Aber ich glaube, wir müssen mehr Bewusstsein dafür schaffen, dass jeder ein Opfer werden kann und sich die Leute wirklich um ihre Security kümmern müssen. Aber man hört auch immer nur die Storys von den Breaches, nie von den bahnbrechenden Technologien, die Sicherheitsforscher entdeckt haben. Und das ist eines der grundlegenden Probleme. Security wird grundsätzlich immer als Kostentreiber gesehen, für eine Sache, die man nicht sieht. Und wenn man etwas sieht, ist das meist schlecht, weil es ja ein Angriff sein könnte, der trotz Invest in die Security stattfand. Leider setzt sich dann aber niemand hin und zeigt auf was noch weiter passieren hätte können, wenn man diesen Invest in die Systeme und das Knowledge der Leute nicht getätigt hätte. Dabei ist Security der Business Enabler, der es Unternehmen ermöglicht, auch trotz eines Angriffs weiter arbeiten und produzieren zu können. Das ist die Krux an der Sache.

www.ibm.com



[2] Modell zur Reifegradbewertung
[3] National Institute of Standards and Technology
[4] NAS, englisch für netzgebundener Speicher

© DilokaStudio | Freepik

ES WIRD TEUER

Die IBM-„Cost of a Data Breach"-Studie 2022 zeigt, dass die Kosten für Datenschutzverletzungen mit 4,35 Millionen US-Dollar ein Allzeithoch erreicht haben. Diese Kosten steigen sogar noch, wenn man auf Zero-Trust-Strategien verzichtet.

Zu den wichtigsten Ergebnissen der IBM-„Cost of a Data Breach"-Studie 2022 gehören:

- **Rückstände bei Zero Trust in kritischer Infrastruktur:** Fast 80 % der Unternehmen mit kritischer Infrastruktur setzen keine Zero-Trust-Strategien ein, wodurch die durchschnittlichen Kosten einer Datenschutzverletzung auf 5,4 Millionen US-Dollar steigen. Wobei es sich bei 28 % der Datenschutzverletzungen bei diesen Unternehmen um Ransomware- oder zerstörerische Angriffe handelte.
- **Bezahlen, zahlt sich nicht aus:** Ransomware-Opfer, die den Lösegeldforderungen von Erpressern nachkamen, hatten durchschnittlich nur 610.000 US-Dollar niedrigere Kosten für eine Datenschutzverletzung im Vergleich zu denen, die nicht zahlten – ohne dass der bezahlte Lösegeldbetrag berücksichtigt wird.
- **Sicherheitslücken in Clouds:** 43 % der untersuchten Unternehmen befinden sich in einem frühen Stadium der Umsetzung von Sicherheitsmaßnahmen in ihren Cloudumgebungen oder haben noch gar nicht damit begonnen. Dies resultiert in durchschnittlich mehr als 660.000 US-Dollar höheren Kosten einer Datenschutzverletzung als bei untersuchten Unternehmen mit ausgereifter Sicherheit in ihren Cloudumgebungen.
- **KI und Automatisierung bei Security bringen Kosteneinsparungen von mehreren Millionen US-Dollar:** Untersuchte Unternehmen, die KI und Automatisierung für Security nutzen, verzeichneten durchschnittlich 3,05 Millionen US-Dollar weniger Kosten bei Datenschutzverletzungen im Vergleich zu Unternehmen, die die Technologie nicht einsetzen – dies ist die größte Kosteneinsparung, die in der Studie beobachtet wurde.

Die Studie basiert auf einer umfassenden Analyse zwischen März 2021 und März 2022 von realen Datenschutzverletzungen bei 550 Unternehmen weltweit.

www.ibm.com

DATA LOSS PROTECTION MUSS CHEFSACHE WERDEN

Backups sind die letzte Verteidigungslinie gegen Datenverlust. Wenn diese Mauer fällt, dann sind Daten im Fall von erfolgreichen Cyberattacken oder Serverschäden nicht mehr wiederherzustellen. Unternehmen sollten daher den Überblick über ihre Backup-Infrastruktur behalten.

Die Verfügbarkeit von Daten ist für jedes Unternehmen betriebsentscheidend. Lange Zeit arbeiteten Produktionssysteme abgekoppelt von ihrer Umwelt. Im Zuge der Digitalisierung und damit zusammenhängender Entwicklungen wie Industrie 4.0 und Internet of Things fließen immer größere Datenströme zwischen Maschinen, OT und den damit zusammenhängenden IT-Infrastrukturen.

Ohne Backup keine Produktionssicherheit. Intelligent vernetzte Industrieanlagen funktionieren nur noch, wenn sie entsprechend konfiguriert sind und mit den richtigen Daten gefüttert werden. Stehen bestimmte Konfigurations- oder Maschinendaten fehlerhaft, unvollständig oder überhaupt nicht bereit, kann dies die Produktionsprozesse stark beeinträchtigen. Bei einem erfolgreichen Cyberangriff werden z.B. Daten verschlüsselt oder gehen für immer verloren – wenn sie nicht separat gesichert wurden. Server und Devices, auf denen essenzielle Daten gespeichert sind, können aber genauso gut auch durch (Natur-)Katastrophen oder Hardwarefehler beschädigt werden. Ein Datenverlust ohne die Möglichkeit der Wiederherstellung führt zu monatelangen Produktionsausfällen, die sich Unternehmen nicht leisten können. Datensicherheit bedeutet, dass die Produktion auch in Notfällen aufrechterhalten bzw. innerhalb kurzer Zeit wiederhergestellt werden kann. Ein Backup muss deshalb als wesentlicher Teil jeder Sicherheitsstrategie betrachtet werden.

Schwieriger Überblick, mangelhafte Reports, fehlerhafte Backups. Sicherungskopien werden auf unterschiedlichen Servern abgelegt. Häufig werden verschiedene Backups mithilfe unterschiedlicher Tools erstellt, weil ein einziges Tool in vielen Fällen nur einen Teil der Backup-Infrastruktur abdeckt. Präzise Konfigurationsdaten für jedes einzelne Backup sind nur unvollständig verfügbar. Um Fehler zu beheben, müssen sich Teams die benötigten Informationen mühsam aus vielen Quellen selbst zusammensuchen. Bestimmte logische Fehler werden im Backup-Programm gar nicht erst angezeigt. Andere, sogenannte „False Positives“ werden nicht automatisch als solche erkannt. All das bedeutet erhöhten Arbeits- und Zeitaufwand und ein hohes Risiko, dass Fehler im Backup unerkannt durchrutschen.
Zudem mangelt es an Reporting-Funktionen, die die Bedürfnisse der Backup-Verantwortlichen erfüllen. Berichte werden nicht selten durch Skripte erstellt, die Administratoren mühevoll selbst gebaut und das Unternehmen unter Umständen längst verlassen haben. Ihre Nachfolger vertrauen beim routinemäßigen Reporting darauf, wissen aber nicht, wie es genau funktioniert. Möglicherweise deckt das Skript bestimmte Bestandteile der sich verändernden Backupumgebung oder neue Funktionen der Backup-Software gar nicht mehr ab.

Monitoring und Reporting automatisieren. Ein hochautomatisiertes Monitoring- und Reporting-Tool wie z.B. Backup Eagle überwacht lückenlos die gesamte Backupumgebung über unterschiedliche Software und Devices hinweg. Der unabhängige Blick von außen ist notwendig. Nur so werden „blinde Flecken“ oder bestimmte Fehler im Backup erfasst, die innerhalb der Logik der Backup-Software häufig unentdeckt bleiben. Im Notfall führen diese unbemerkten Lücken im Backup zu Datenverlust. Administratoren brauchen zudem eine Übersicht, die ihnen die Kontrolle zurückgibt und ihnen innerhalb kürzester Zeit die Informationen zusammenstellt, die sie brauchen – für sich selbst oder für Audit-Prüfer. Der Schutz vor Produktionsausfällen beginnt dort, wo für Datensicherheit gesorgt wird.

www.schmitz-rz-consult.de

Der Autor
Stefan Schröder
... ist CTO bei der Schmitz RZ Consult GmbH.


© Paul Kufec

„CYBERBEREICH IST ESSENZIELL FÜR ÖSTERREICH“

Im Rahmen der 10. IKT-Sicherheitskonferenz in Wien wurde über die aktuellen Bedrohungsszenarien diskutiert und auch der Cyber-Security-Europameister 2022 gekürt.

Mitte September trafen sich rund 4.000 nationale und internationale Teilnehmer bei der IKT-Sicherheitskonferenz 2022 in Wien. Mit 80 Vorträgen nationaler und internationaler Cyber-Security-Experten und einer Ausstellung von über 80 Cyber-Security-Unternehmen war es die bisher größte IKT-Sicherheitskonferenz. „Die Entwicklung des Cyberbereichs ist essenziell für Österreich. Denn Cyberattacken gehören neben Pandemien und Terrorangriffen und regionalen Konflikten zu den wahrscheinlichsten Einsatzszenarien unserer Zeit. Mit der IKT-Sicherheitskonferenz versammeln wir die europäische Elite auf diesem Gebiet und bieten so Raum, um noch mehr Synergien zu schaffen. Auch das Bundesheer sucht laufend Talente in diesem Fach. Die Cyber-Grundwehrdiener des Bundesheeres leisten jetzt schon einen wichtigen Beitrag für Österreich. Darüber hinaus starten wir heuer mit dem Fachhochschul-Bachelor-Studiengang für ‚militärische informations- und kommunikationstechnologische Führung‘, für den sich zukünftige IKT-Offiziere bewerben können“, so Verteidigungsministerin Klaudia Tanner bei der Eröffnungs-Pressekonferenz.

Cyber-Security-Europameister 2022 gekürt. Im Zuge der Konferenz wurde mit einem Live-Hacking gezeigt, wie einfach es ist, sich in unterschiedliche Systeme einzuschleusen. Einen weiteren Schwerpunkt bildete die Analyse vergangener Vorfälle sowie von Bedrohungsszenarien. Passend dazu präsentierten Experten Lösungsansätze und Vorbeugungsmaßnahmen. Unter anderem waren auch Themen wie High-End-Abhörtechnik, Spionageabwehr und Drohnen Teil der Vortragsreihe.
Ein besonderes Highlight der IKT-Sicherheitskonferenz war die dort stattfindende European Cyber Security Challenge 2022. Dieser, von der Europäischen Union veranstaltete, Wettbewerb brachte über 300 IT-Nachwuchstalente aus 34 europäischen aber auch anderen internationalen Ländern nach Wien, um sich um den Titel „European Champion in Cyber Security“ zu messen. Als Sieger der ECSC2022 ging schließlich das Team Dänemark hervor, das sowohl bei den Aufgaben im Jeopardy-Format als auch im Attack&Defense-Szenario die beste Wertung erzielte. Das Team Deutschland erreichte mit Stärken im Attack&Defense-Szenario den 2. Platz, während das Team Frankreich vor allem bei den Aufgaben im Jeopardy-Format punktete und es in der Gesamtwertung auf den 3. Platz schaffte. Das Team Austria als Gastgeberland schaffte es auf Platz 10.

Über eine Million potenzieller Schwachstellen. Im Rahmen der Sicherheitskonferenz präsentierte das Schweizer Cybersecurity-Unternehmen Dreamlab Technologies AG einen wissenschaftlichen Scan der österreichischen Cyberdimension, also aller ans öffentliche Internet angeschlossener Geräte wie Firewalls, Infrastrukturen und Server. Über eine Million potenzieller Schwachstellen wurden dabei identifiziert. Diese Schwachstellen beinhalten unter anderem nicht mehr unterstützte Betriebssysteme mit dokumentierten Sicherheitslücken, nicht aktualisierte Firewalls, ungeschützte Datenbanken, angreifbare Webseiten (auf welchen z.B. die Passwörter von Benutzern gestohlen werden können), angeschlossene industrielle Geräte (mit Schwachstellen und in vielen Fällen ohne vorgeschaltete Firewalls), FTP-Server sowie Webcams. Ein separater CyObs-Scan der von der Verwaltung genutzten Domains zeigte auch, dass die behördlichen Internetinfrastrukturen viele potenzielle Schwachstellen aufweisen. Die 873 untersuchten und aktiven .gv.at-Domains zeigten über 5.500 potenzielle Schwachstellen auf.

www.bundesheer.at
www.cyobs.com

HOME OF SECURITY

Es ist eines der drängendsten Themen unserer Zeit und an Aktualität kaum zu überbieten: Der Ruf nach mehr IT-Sicherheit wird immer lauter, gerade mit Blick auf die Sicherheit kritischer Infrastrukturen. Ende Oktober tauschten sich internationale Fachleute auf der it-sa Expo&Congress in Nürnberg dazu aus.

„Daten und IT-Infrastrukturen zu schützen ist eine Aufgabe, der sich IT-Sicherheitsverantwortliche auf allen Ebenen gemeinsam stellen. Die it-sa bietet ihnen dafür seit 2009 in Nürnberg den Rahmen – und war noch nie so relevant wie dieses Jahr“ erklärt Frank Venjakob, Executive Director it-sa, NürnbergMesse. Wie wichtig gerade jetzt der Schulterschluss in der IT-Sicherheitsgemeinschaft ist, zeigten die internationalen Gemeinschaftsstände aus Österreich, der Tschechischen Republik und Südkorea. „Die Resonanz in der Branche war überragend, bereits im September waren alle in diesem Jahr verfügbaren Flächen vergeben“, freut sich Venjakob. Zur diesjährigen it-sa Expo&Congress reisten die ausstellenden Unternehmen aus 29 Ländern an. Die Zahl der Messebeteiligungen aus dem Ausland war, verglichen mit der bisher größten Ausgabe der it-sa 2019, weiter gestiegen, ebenso die von internationalen Ausstellern belegte Fläche. Auch der Blick auf die gesamte Ausstellungsfläche zeigt, dass die it-sa ihren Wachstumskurs nach einer Unterbrechung im letzten Jahr konsequent fortsetzt: In den Hallen 6, 7 und 7A belegten die rund 700 Aussteller mehr Fläche denn je zuvor. 15.229 Besucher:innen informierten sich.

Viel Raum für Start-ups. Das enorme Innovationspotenzial, über das gerade junge IT-Sicherheitsfirmen verfügen, belegte die Sonderfläche Startups@it-sa und der Athene Startup Award UP22@it-sa, der zum fünften Mal auf der Messe verliehen wurde. Gewonnen hat TrustCerts für das beste Cybersecurity-Startup der DACH-Region.

Die Initiative „Deutschlands bester Hacker“ und die Vortragsreihe „Women in Cybersecurity“ zeigten Ansätze, mehr Fachkräfte für Aufgaben in der IT-Sicherheit zu begeistern und die rund 350 Forenbeiträge brachten Fachwissen auf den Punkt. Hervorzuheben sind dabei die „it-sa insights“, produktneutrale Vorträge und Panels sowie die Special Keynote der Avast-CISO Jaya Baloo zur Herausforderung der Quanten-Kryptografie. Post Quantum Cryptography, so Baloo, mache große Fortschritte. Die Industrie sieht sie vor enormen Herausforderungen, die sie in ihrem Vortrag „Our Secure Quantum Future“ beleuchtete.

Begleitet wurde die Fachmesse vom Congress@it-sa und mit der Jahrestagung der IT-Sicherheitsbeauftragten der Länder und Kommunen als erneut wichtige Anlaufstelle für Verantwortliche in der öffentlichen Verwaltung. Hybride Elemente auf der Messe und die Abbildung ausgewählter Messe-Highlights auf der Online-Dialogplattform it-sa 365 komplettierten das umfassende Informationsangebot.

www.itsa365.de

Frank Venjakob
Executive Director it-sa

„Daten und IT-Infrastrukturen zu schützen ist eine Aufgabe, der sich IT-Sicherheitsverantwortliche auf allen Ebenen gemeinsam stellen.“

SO GELINGT DIE **CYBER-SICHERHEITSSTRATEGIE** IN DER PRODUKTION

Der nächste Cyberangriff ist nur eine Frage der Zeit. Bedrohungen wie die im DACH-Raum grassierende Ransomware GandCrab zeigen dies deutlich. Um Angriffe auf kritische Systeme des produzierenden Gewerbes zu vermindern, benötigen diese eine ganzheitliche Sicherheitsstrategie und Cyberresilienz.

Produktionsanlagen sind heute stark mit den IT-Systemen vernetzt. Es reicht deshalb bereits die Infektion eines Systems innerhalb einer hybriden Cloud-Infrastruktur aus, damit sich Eindringlinge auf das gesamte Netzwerk ausbreiten und massiven Schaden anrichten können – etwa durch das Lahmlegen von Maschinen oder Steueranlagen. Angriffe dieser Art sind mittlerweile zur alltäglichen Bedrohung geworden. Das gilt nicht nur für große Firmen. Im Jahr 2021 waren laut OECD 60 % der kleinen und mittelständischen Unternehmen betroffen. Zwei Jahre zuvor lag die Zahl nur bei 11,7 %. Laut dem Threat Report von Eset trifft Organisationen im DACH-Raum zurzeit besonders die Ransomware GandCrab. Diese war bei fast einem Viertel aller erkannten Attacken beteiligt.

Um solche Angriffe abzuwehren oder im Schadensfall die vollständige Wiederherstellung zu garantieren, braucht es neben präventiven Maßnahmen, eine ganzheitliche Security- und Backup-Strategie. Wenn Unternehmen ihre Cyberresilienz steigern wollen, ist es jedoch mit rein technischen Lösungen nicht getan. Die erste Verteidigungslinie jeder Organisation sind ihre Mitarbeiter:innen.

Vom traditionellen zum ganzheitlichen Sicherheitskonzept. Die Methoden der Cyber-Kriminellen werden nicht nur im technischen Bereich immer raffinierter. Phishing-Mails und Social-Engineering-Methoden zielen stattdessen auf die größte Schwachstelle im Unternehmen ab: die Mitarbeiter:innen. Ist dieser erste Schutzwall überwunden, ist es für den Kriminellen in der Regel ein Leichtes, sich im Firmennetzwerk zu verbreiten und Schaden anzurichten. Deshalb gilt es für Unternehmen, einen ganzheitlichen Ansatz zu verfolgen. Regelmäßige Mitarbeiterschulungen sensibilisieren die Belegschaft für aktuelle Bedrohungen und helfen bei der Prävention.

Der Eindringling muss schnellstmöglich entdeckt werden, um den Zugriff auf sensible Unternehmensdaten so gering wie möglich zu halten. Dabei hilft etwa ein kontinuierliches Daten-Monitoring. Dieses erkennt ein erhöhtes Datenaufkommen, das durch die Verschlüsselungsprozesse generiert wird. Ein KI-gestütztes Zero-Trust-Konzept ist ebenfalls ein guter Ansatz, um unbefugten Zugriff präventiv den Riegel vorzuschieben. Ist die Malware erst einmal aufgespürt, sollten Unternehmen in Zusammenarbeit mit IT-Forensikern die Systeme bereinigen und die aufgespürten Sicherheitslücken schließen.

Die richtige Backup-Strategie. Damit das Unternehmen nach einem Ransomware-Befall so schnell wie möglich sein Geschäft wieder aufnehmen kann, ist eine Backup-Strategie mittels Snapshots notwendig. Diese stellen eine Momentaufnahme der Daten zum Zeitpunkt der Speicherung dar und sollten idealerweise mehrere Monate zurückreichen. Mit einem Snapshot ist es ein Leichtes, den Zustand vor dem Angriff in kürzester Zeit wiederherzustellen. Um dennoch kein Risiko einzugehen, sollten Unternehmen mindestens eine Kopie getrennt vom Netzwerk aufbewahren.

Mit der rasant zunehmenden Cyberbedrohung ist also für das produzierende Gewerbe eine ganzheitliche Sicherheitsstrategie unerlässlich. Diese umfasst neben technischen Abwehr-Mechanismen auch ein effizientes Datenmanagement und Backup-Funktionen. Dabei sollten Unternehmen das Fundament ihres Schutzwalles nie vergessen: den geschulten Mitarbeiter.

www.netapp.com

Der Autor
Peter Hermann
... ist Country Manager Österreich beim globalen Cloud- und Daten-orientierten Softwareanbieter NetApp.

Über 150 Teilnehmer:innen folgten der Einladung zur kostenlosen Veranstaltungsreihe „Safety&Security Network Conference 2022“ in Wien, Linz und Graz.

VON DER **KÜR** ZUR **PFLICHT**

Pilz hat die bevorstehende Anpassung der Maschinen-Produkte-Verordnung zum Anlass genommen um in einer aktuellen Umfrage die Veränderung der Wahrnehmung der Kunden im Zusammenspiel von Safety&Security zu betrachten. Die Wissenslücken wurden bei der „Safety&Security Network Conference“ geschlossen.

Bereits zum zweiten Mal hat der Automatisierer Pilz im Rahmen der Safety&Security-Umfrage den aktuellen Wissensstand und das Verständnis für das Thema Cybersecurity innerhalb der OT erhoben.

Die erste Befragung im Jahr 2020 zeigte deutlich, dass das Thema der Maschinensicherheit auf dem Markt vollkommen angekommen und adäquat umgesetzt ist. Immerhin hatten die Unternehmen nach der Formulierung der Maschinensicherheitsrichtlinie bereits 25 Jahre Zeit die rechtlichen Anforderungen entsprechend umzusetzen. Nun steht die Überarbeitung der Richtlinie 2006/42/EG bevor. Neue Themen wurden in die Agenden der zukünftigen Maschinen-Produkte-Verordnung mitaufgenommen, um die neuen Risiken, die sich aus den aufstrebenden digitalen Technologien ergeben, ausdrücklich zu regeln. Auch sind bereits Normen zu diesen Themen entstanden. Die Normenrichtlinie EN IEC 62443 beispielsweise, schreibt die IT-Sicherheitsanforderungen an Automatisierungssysteme vor und weist dem betrachteten System ein Security-Level (SL) zu. Systemintegratoren, Produktlieferanten, Betreiber und Dienstleister werden mit Hilfe dieser Normenreihe bewerten, in wie weit ihre Maschinen, Produkte und Dienstleistungen die funktionalen IT-Sicherheitsfähigkeiten erbringen können. Wo diese Betrachtungen heute noch weitgehend auf „freiwilliger“ Basis beruhen, werden diese, mit der Integration des Themas Cybersecurity in der zukünftigen Maschinen-Produkte-Verordnung, zur Pflicht.

Erkennbare Unsicherheiten. Auch die Befragung aus dem heurigen Jahr zeigt deutlich, dass die Unternehmen noch starken Aufholbedarf beim Thema der OT-Security haben. Das betrifft die Verantwortlichkeiten ebenso wie das Verständnis über Gefahrenquellen. Die Erhebung ergab, dass bereits über 20 Prozent der befragten Unternehmen wissentlich angegriffen wurden. Der wirtschaftliche Schaden des eigenen Unternehmens durch Ransomware-Angriffe stellt die größte Sorge dar, gefolgt vom Diebstahl von Betriebsgeheimnissen oder Rezepturen. Trotz der steigenden Tendenz an Angriffen haben nur sieben Prozent der befragten Unternehmen einen eigenen OT-Security-Verantwortlichen. In den meisten Fällen wird die Verantwortlichkeit noch der IT zugeschrieben. Die Praxis zeigt allerdings, dass man dort keine bzw. nur wenig Verantwortung für die OT-Security übernimmt. Nicht aus Unwillen heraus, sondern vielmehr weil die Vulnerabilität nicht bewusst ist. Die im Zuge der aktuellen Safety&Security-Umfrage klar erkennbare Unsicherheit hat gezeigt, dass eine frühzeitige und konkrete Information essenziell ist. Obwohl es noch einige Zeit brauchen wird, bis die neue Maschinenverordnung in Kraft treten wird, hat sich Pilz dazu entschlossen, diese Themen aufzunehmen und den Kunden näherzubringen. Immerhin entwickelt sich das Thema der OT-Security von der Kür zur Pflicht.

Erfolgreiche Veranstaltung. Pilz hat daher im Herbst zur kostenlosen Veranstaltungsreihe „Safety&Security Network Conference

2022“ geladen. Hier erhielten über 150 Teilnehmer:innen in drei Sessions in Wien, Graz und Linz einen Ausblick auf die Maschinen-Produkte-Verordnung sowie auf die in Aussicht gestellten neuen Aufgaben an die IT und OT – entsprechend den gesetzlichen Anforderungen für die Industrial Security. Wie weit der Einsatz Künstlicher Intelligenz in der Industrie, aber auch im Alltag bereits fortgeschritten ist, war ebenso Thema, wie die Gestaltung des sicheren Weges zur Maschine der Zukunft. Im Zuge der Netzwerkgespräche hat sich gezeigt, dass sich die Kunden sehr wohl der generellen Verantwortung für die neuen Themen der Maschinenverordnung, Künstliche Intelligenz und Cybersecurity, bewusst sind. Allen voran wurden die Security-Anforderungen, wie beispielsweise Kommunikationsschnittstellen, Benutzer-Authentifizierung und geplante Aufzeichnungspflichten – auch auf Maschinenebene – mit größtem Interesse aufgenommen und als klare Herausforderung für die Zukunft gesehen. Aber auch die parallel erwarteten Regulierungen zu Security (NIS 2) und die geplante KI-Verordnung, die unabhängig von der Maschinenverordnung für Unternehmen zu berücksichtigen sein werden, wurden aufgezeigt. Vielen Teilnehmer:innen war ihre zukünftige Führungsverantwortung für ein Umsetzen eines Cybersicherheitsmanagements nach NIS 2 noch gar nicht bewusst. Die hohe Zahl der Anmeldungen, das positive Feedback, die angeregten und anregenden Gespräche, sind ein Beleg für das Interesse der Branche und damit auch ein Beweis für die Aktualität des Themas, das im kommenden Jahr viel Aufwind erfahren wird. Die erfolgreiche Informationsveranstaltung wird daher auch im kommenden Jahr weiter bestehen.

www.pilz.at

Für mehr Details zur Safety&Security Network Conference:

Der Autor
David Machanek
ist Geschäftsführer des Automatisierers Pilz Österreich

MULTIVIEW SWITCH FÜR ULTIMATIVE BENUTZERKONTROLLE IN 4K UHD

Per Mauszeiger automatisch und in Echtzeit zwischen bis zu 4 Rechnern umschalten

Der neue Mutliview Switch AdderView CCS-MV 4224 von Adder liefert bis zu vier verschiedene Video-, Audio- und USB-Signale an einen einzelnen Arbeitsplatz. Ein vom Benutzer auf einem oder zwei Monitoren anpassbares Layout bietet größte Flexibilität in anspruchsvollsten Arbeitsumgebungen und vor allem ultimative Kontrolle über/bei kritischen Prozessen. Dabei kann ohne Tastendruck, automatisch und in Echtzeit zwischen Computern umgeschaltet werden.

Kontrollraumumgebungen „aufräumen" und verbessern

Mit zunehmender Anzahl von Computern und immer größeren Bildschirmen stoßen Kontrollraumumgebungen oftmals an ihre Grenzen. Der neue Multiviewer wurde als vollständige Kontrollraumlösung für bis zu zwei Monitore konzipiert, die den „Schreibtisch aufräumt" und sensible Informationen oder kritische Abläufe so darstellt, wie der Benutzer sie braucht. Er gibt Benutzern die volle Kontrolle über die Ressourcen, auf die sie zugreifen müssen und das in 4K UHD-Auflösung. Das Ergebnis sind größtmögliche Usability und Benutzerakzeptanz, die z.B. auch über vollständig konfigurierbare, farbcodierte Fensteranzeigen auf den Bildschirmen erreicht wird.

Key-Features des neuen Mutiview Switches:

- Einzelne Arbeitsplätze können direkt mit vier Video-, Audio- und USB-Quellen verbunden werden.
- In Kombination mit einer AdderLink Infinity IP KVM-Matrix kann auf beliebige Quellen in einem Netzwerk zugegriffen werden.
- Nahtlose Cursor-Interaktion zwischen den Quellen.
- Farbcodierte Bildschirmkonfigurationen gewährleisten eine schnelle Kanalidentifizierung, Echtzeit-Datenvisualisierung und verbesserte Entscheidungsfindung.
- Optimierte Arbeitsplatzergonomie und verbessertes Situationsbewusstsein für kritische Abläufe.

Die Adder-Produktentwicklung fasst die Stärken wie folgt zusammen: „Der AdderView CCS-MV 4224 ist die ideale Lösung für Bediener, die in komplexen, unternehmenskritischen Kontrollräumen arbeiten. Die erheblich verbesserte Desktop-Ergonomie gewährleistet, dass der Benutzer situationsbewusst und schnell zwischen den Quellen wechseln kann, ohne die Konzentration zu verlieren.

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 -messung
- Umgebungsmonitoring, Sensorik & IoT
- Industrielle Netzwerktechnik & WLAN
- Technik, Service, Support & RMA

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

Weitere Informationen:
Ing. Franz Weber
Vertrieb & technische Beratung
KVM & A/V Signalverteilung
franz.weber@bellequip.at

SECURE REMOTE MAINTENANCE

Weltweit. Einfach. Sicher.

www.br-automation.com/remote-maintenance

Weltweit zugreifen
Fernwartung vom Büro aus oder von unterwegs

Einfach implementieren
Integrierte Lösung aus einer Hand

Sicher verbinden
Jede Art Daten sicher übertragen

PERFECTION IN AUTOMATION
A MEMBER OF THE ABB GROUP

100 % DATEN UND 100 % COMMITMENT

Unternehmen müssen ihren Datenschatz hegen und pflegen, sagt Michaela Mader, Geschäftsführerin von dataspot., einer Data-Excellence-Beratung mit eigener Metadatenmanagement-Software mit Sitz in Wien und Linz. Für Mader geht es nicht nur um das Sammeln, Strukturieren und Analysieren von Daten, sondern vor allem um die Verantwortlichkeit beim Datamanagement.

IoT 4 Industry & Business: Daten werden gerne als das Öl bzw. das Gold des 21. Jahrhunderts gesehen. Was sagen Sie dazu?
Michaela Mader: Mir gefällt die Variante mit dem Gold besser als mit dem Öl, da das nicht sehr nachhaltig ist. Ich glaube, dass viele Unternehmen erkannt haben, dass sie ihren Datenschatz im Griff haben müssen. Mittlerweile stehen die unterschiedlichsten Ideen und Initiativen zum Thema Digitalisierung im Raum, was immer man darunter auch versteht. Aber eines ist fix: Man braucht Daten dafür. Das Bewusstsein ist in den letzten Jahren gewachsen, dass man sich um seine Daten kümmern und sie hegen und pflegen und als Wert im Unternehmen ansehen muss. Bei dataspot. sind wir sehr grundlagenorientiert. Das bedeutet: Es geht um die Veränderung hin zu einem datengetriebenen Unternehmen inklusive dem nötigen Commitment.

IoT: Sehen Sie einen Unterschied zwischen Datendurchgängigkeit und Datengetriebenheit?
Mader: Uns geht es darum, dass unsere Kunden das Thema von der Businessseite her sehen und erkennen, dass alles was eine Organisation an Aufgaben hat, zu 100 % in den Daten abgebildet ist. Und diese entstehen, weil Geschäftsprozesse durchgeführt werden. Egal ob die Daten bewusst ins System kommen oder automatisch über Sensoren generiert werden. Früher war man der Meinung, Daten entstehen nur in der IT-Abteilung. Dadurch haben sich die Fachbereichsmitarbeiter:innen nicht verantwortlich gefühlt. Jetzt kommt es zu einem Paradigmenwechsel. Daten entstehen überall im Unternehmen. Deswegen sind uns Definitionen, Regeln und die Abbildung von Prozessen etc. so wichtig.

IoT: Daten entstehen auch in der Produktion und sollen bei Wartung und Betrieb helfen.
Mader: Das stimmt, aber diese Sensordaten kommen sehr unstrukturiert in einem String, der z.B. EA00234 heißt. Diese Daten kann man leider nicht eins zu eins in eine Datenbank übertragen, bevor nicht ganz viele Programmierer damit befasst waren. Das

liegt daran, dass die Sensor-Hersteller keine Metadaten zur Verfügung stellen und wenn, dann sind sie nicht automatisierbar zu verarbeiten. Dabei geht es doch darum, aus den Daten zu lernen, etwa um den Business-Prozess zu verbessern oder die Produktionskosten zu senken. Das heißt, ich muss die Daten verstehen und interpretieren können. Also brauchen wir zuerst eine fachliche Übersetzung, die auch ein Normalsterblicher lesen kann und er weiß, dass das Feld EA00234 eine Temperatur von 23,4 Grad bedeutet. Häufig werden Systeme installiert und parametrisiert, aber nirgends werden die Parameter festgehalten. Es ist nicht so leicht wie versprochen.

IoT: Bei der Datenanalyse gibt es zwei Ansätze: alles sammeln oder nur jene Daten, aus denen man konkret Nutzen zieht. Wie sieht Ihr Zugang zu diesem Thema aus?

Mader: Mir ist der Zugang Top-down persönlich lieber, dann hat man immer einen konkreten Use Case dahinter. Sprich: Ich will eine Auswertung machen, ein Modell rechnen, ein Produkt entwickeln oder auf eine fachliche Fragestellung reagieren können. Das ist zweckgebunden und ganz im Sinne der Datensparsamkeit. Ich finde es wichtig, dass man nur die Daten, die einen Zweck haben, speichert und zu 100 % pflegt. Etwa Kundendaten, die der gemeinsame Datennenner im Unternehmen sind. Die sind meist nicht nur einmal, sondern 3, 4, 5 Mal in verschiedenen Systemen hinterlegt. Da muss man eine Harmonisierung durchführen und eine „Golden Source" definieren, also eine führende Quelle, von der sämtliche Daten stammen sollen. Da sind Definitionsarbeiten und Governance-Fragen vorzunehmen, die wir im Rahmen unserer Data Excellence klären.

IoT: Wie bringt man Unternehmen zu der angesprochenen Datengetriebenheit?

Mader: In erster Linie erzeugt man das, indem man nach den Kernprozessen und den ureigensten Tätigkeiten im Unternehmen fragt und sie dann zu Papier bringt. Wir machen das in Form eines Datenmodells, in dem man die Beziehungen zueinander sieht. Und wir haben auch die Erfahrung gemacht, sobald die Daten unter Governance sind und die Leute wissen, dass ihre Daten gut behandelt werden, dann sind sie auch viel eher bereit, sie zu teilen. Etwa mit einem Data Scientist, um ein Analytics-Modell zu rechnen. Das ist ein Prozess, den man anstoßen muss. Und dann kommt es automatisch zu einer Änderung des Mindsets. Außerdem schneiden wir die Use Cases klein zu. Zum einen wollen wir nicht, dass den Beteiligten bei solchen Vorhaben die Luft ausgeht und zum anderen gibt es bei diesen Projekten keinen Big Bang Approach. Die Leute brauchen aber auch einen Quick Win.

IoT: Sie sprechen sehr viel von Data Excellence. Was verstehen Sie darunter?

Mader: Diesen Begriff haben wir selbst vor sechs Jahren erfunden und die Themenführerschaft dafür im DACH-Raum übernommen. Der Ausgangspunkt war der bereits etablierte Begriff der Data Governance, der stark über die Regulatorik kommt. Bei Data Excellence geht es auch – aber nicht nur – darum zu wissen, wie die Verantwortlichkeiten und Rollen geregelt sind, welche Prozesse und Berichtspflichten es gibt und welche Workflows dahinter liegen. Es bezeichnet den gesamten Rahmen hinsichtlich Fachlichkeit, technischer Umsetzungen, Datenmanagement, organisatorischer und inhaltlicher Themen, damit man tatsächlich mit den Daten arbeiten kann. Und da kommen wir zum Thema Metadaten, der Information *über* die Daten. Also: Von welchen Daten sprechen wir überhaupt? Wie sehen die Verantwortlichkeiten aus? Dies bedingt sich gegenseitig und man muss all diese Themen adressieren, damit man die Daten in den Griff kriegt. Und dafür haben wir den Überbegriff Data Excellence geschaffen.

IoT: Wie weit beschäftigt sich dataspot. mit dem Thema Security?

Mader: Security ist die IT-technische Umsetzung von Sicherheitsmaßnahmen. Aber zu definieren, welche Sicherheitsmaßnahmen man braucht, das ist eine fachliche Angelegenheit. Das haben wir auch bei der Umsetzung von Datenschutzanforderungen. Löschmechanismen oder Speicherfristen zu implementieren ist technisch. Aber zu fragen, wie lang muss ich Daten aufbewahren, wann darf ich sie löschen, wo werden die Daten gespeichert – das sind fachliche Definitionsfragen, die wir im Zuge unserer Modellierungen erledigen. Dazu zählen auch abgestufte Benutzungs- und Berechtigungskonzepte. Wer darf auf welche Daten zugreifen? Wer darf welche Auswertungen sehen, wer darf welche Datenausschnitte sehen? Und um das kümmern wir uns.

www.dataspot.at

Michaela Mader
Geschäftsführerin von dataspot.

„Es geht um die Veränderung hin zu einem datengetriebenen Unternehmen inklusive dem nötigen Commitment."

© Zoe Goldstein

FESTIVAL DER DIGITALISIERUNG

Neues erfahren, sich zwei Tage über die dringendsten Fragen zu Digitalisierung und Nachhaltigkeit austauschen, in Technologien und virtuelle Welten hineinschnuppern und herausfinden, was sie für Gesellschaft und Wirtschaft bedeuten – das war die Digital X Mitte September in Köln.

5G, IoT, Autonomes Fahren, Metaverse oder Robotik: Wie werden wir in der Zukunft leben und arbeiten? Konkrete Antworten darauf erhielten die 70.000 Besucher:innen auf der Digital X am 13. und 14. September 2022 in Köln. Dazu tauchte die Telekom Deutschland die ganze Stadt in ihre Unternehmensfarbe und zeigte mit mehr als 300 Partnern, in über 200 sogenannten Brandhouses und mit rund 60 Start-ups ihre Innovationen, Lösungen und Praxisbeispiele aus der Welt. In diesem Jahr war die Messe zum ersten Mal auch für private Besucher geöffnet, um neue Formen des Wissensaustausches und neue Impulse direkt zu den Anwender:innen zu bringen.
Hinter dem jährlichen Event steht die Deutsche Telekom als Initiator zusammen mit ihren internationalen Partner-Unternehmen – darunter Microsoft, Samsung, Zoom, Cisco, Jabra oder auch der Mittelstandsverband BMVW. Ihr gemeinsames Ziel: Gesellschaft und öffentliches Leben durch neue Technologien vereinfachen und bereichern. Und das „X" in „Digital X" steht für das Vielfache. Das Vielfache an Möglichkeiten, die die Digitalisierung mit sich bringt. „In den beiden Tagen haben wir gezeigt, welche enorme Kraft in Partnerschaften steckt. Die Digital X bringt Deutschland in Sachen Digitalisierung einen entscheidenden Schritt nach vorne", sagte Hagen Rickmann, Geschäftsführer Geschäftskunden der Telekom Deutschland und Schirmherr der Digital X.

Eine Stadt als Zukunftsmesse. Die Digital X erstreckte sich, thematisch gegliedert, über mehrere Stadtteile Kölns. Vom Mediapark im Norden bis zum Belgischen Viertel im Süden zeigte die Telekom gemeinsam mit ihren Partnern die neuesten Entwicklungen in der Digitalisierung. Es gab keine Stände wie auf herkömmlichen Messen. Dafür beherbergten örtliche Restaurants und Lokale das Informationsangebot. In den zahlreichen Pop-Up-Shops wollte die „Weltausstellung der Digitalisierung" die Megatrends rund um Mobilität, Sicherheit, Zukunft der Arbeit, Urbanisierung oder Nachhaltigkeit live erlebbar machen: Ein ferngesteuerter Tattoo-Roboter von Kuka zeigte, wie Roboter und Mensch einmal über Ländergrenzen hinweg miteinander arbeiten können. Wem der Magen knurrte, der konnte sich an einem Food-Truck mit veganem Essen aus dem 3D-Drucker versorgen. ByondXR präsentierte in mehreren Stationen, wie aus einem Online-Shop mit eingeblendeten 3D-Produkten, Avataren und erweiterter Realität (XR) ein virtuelles Shop-Erlebnis wird. Interessant für Einrichtungen der Pflege und des Gesundheitswesens ist der vernetzte Trinkbecher von Laqa, der an eine ausreichende Flüssigkeitsaufnahme erinnert. 5G schafft die Voraussetzung für autonomes Fahren. Mira zeigte, wie Fahrer ihre Fahrzeuge aus der Ferne steuern.

5G, IoT, Autonomes Fahren, Metaverse oder Robotik: Die Digital X 2022 zeigte, wie wir leben und arbeiten werden.

Mittler zwischen Start-ups und Kunden. Das Future Quartier der Digital X stand ganz im Zeichen von Innovationen. Über 60 Start-ups präsentierten hier ihre Lösungen aus den Bereichen Nachhaltigkeit, Gesundheit, Individualisierung, Zukunft der Arbeit und Wissenskultur/Bildung. Besucher:innen erlebten digitale Zwillinge per 3D-Scanner, Kundensupport aus der Ferne mit Augmented Reality, digitale Kleidung auf dem Smartphone oder Hautbildanalysen direkt am Messestand. Erstmals wurden die Digital X Awards in Kooperation mit dem Bundesverband mittelständische Wirtschaft (BVMW) verliehen. Prämiert wurden Nölle + Nordhorn, Rauschenberger, Select, Emons und German Volunteers. Einen Sonderpreis erhielt die #WeAreAllUkrainians gemeinnützige GmbH eine Initiative von Wladimir Klitschko.

Die Auswahl der Gewinner erfolgte durch eine unabhängige Jury, die von den wissenschaftlichen Partnern Universität St. Gallen und Eidgenössische Technische Hochschule Lausanne beraten wurde. „Digitalisierung ist keine Frage mehr des Ob, es geht nur noch um das Wie. Wer digitalisiert, brilliert. Wer nicht digitalisiert, der verliert. In der Corona-Pandemie haben sich Unternehmen mit einem hohen Digitalisierungsgrad als deutlich resilienter erwiesen“, sagt Markus Jerger, Vorsitzender der Bundesgeschäftsführung des BVMW. Digitale Lösungen trügen dazu bei, die eigene Wettbewerbsfähigkeit zu stärken. Und Jurymitglied sowie Initiator der Digital X Hagen Rickmann ergänzt: „Es braucht nach wie vor digitale Vorreiter und anschauliche Beispiele für die Transformation. Die Award-Gewinner haben neue Technologien und Trends bereits in die Realität und für den Mittelstand übersetzt. Sie sind genau diese Vorbilder, von denen viel zu lernen ist.“

www.digital-x.eu

REPORT ZEIGT: CYBERANGRIFFE FORDERN RASCHES HANDELN

FORTINET

Cybersecurity in der Industrie muss sowohl OT als auch IT umfassen. Und gehandelt werden muss laut 2022 State of Operational Technology and Cybersecurity Report von Fortinet sofort.


Bild: Getty Images

Cyberangriffe nehmen zu. Das bestätigt der 2022 State of Operational Technology and Cybersecurity Report von Fortinet. So erlebten 93 % der befragten OT-Unternehmen 2021 einen Angriff, bei 78 % von diesen waren es mehr als drei. Ein falscher Klick, und Unternehmen stehen handlungsunfähig da. „Jetzt ist die Zeit zu handeln“, appelliert deshalb **Mirco Kloss**, Team Lead Business Development | Operational Technology D-A-CH bei Fortinet.

Früher war das kein Thema, denn die Produktion war isoliert. Heute werden industrielle Prozesse digitalisiert, OT und IT wachsen zusammen. IIoT verspricht nichts weniger als höhere Produktivität, Effizienz, Reaktionsfähigkeit und Rentabilität. All das, nachdem ein Industrieunternehmen strebt.

Fortinet Security Fabric schützt OT

Leider steigt eben die Anfälligkeit für Cyberangriffe. Unternehmen, so der Report, sollten deshalb vor allem Transparenz in den Netzwerken herstellen und die Geräte-Komplexität verringern.

Da effektive Cybersecurity sowohl IT- als auch OT-Netzwerke umfassen muss, braucht es eine ganzheitliche Sichtweise. Ein Mesh-Plattform-Ansatz wie die


Bild: Fortinet

Fortinet Security Fabric mit zentralisierter Verwaltung und einer Sicherheitsrichtlinie, die volle Transparenz und granulare Kontrolle bietet, ist unerlässlich. Damit IIoT nicht zum Geschäftsrisiko, sondern zum Erfolgsfaktor wird.

www.fortinet.com/de

Advertorial

Die Teilnehmenden des Gaia-X-Hub-Austria-Workshops in Alpbach (vlnr): Mario Drobics (AIT), Tobias Höllwarth (EuroCloud), Roland Fadrany (Gaia-X AISBL), Thomas Hahn (Siemens AG), Staatssekretär Florian Tursky (BMF), Sektionschefin Henriette Spyra (BMK), Jochen Borenich (K-Businesscom), Roland Sommer (Industrie Platform 4.0), Christian Tauber (K-Businesscom), Helmut Leopold (AIT)

AUF DEM WEG ZUR EUROPÄISCHEN DATENSOUVERÄNITÄT

Der Gaia-X Hub Austria diskutierte Ende August in Alpbach mit Vertreter:innen aus Industrie und Verwaltung die notwendige Positionierung Österreichs in einem zukünftigen souveränen, digitalen Europa.

Die steigende Herausforderung für Unternehmen, mit der Digitalisierung in allen Wirtschaftsbereichen Schritt zu halten und damit auch im globalen Maßstab wettbewerbsfähig zu bleiben, bildet den Ausgangspunkt der europäischen Gaia-X-Leitinitiative. Mit der rasanten Entwicklung von Cloud- und Edge-Computing zum vorherrschenden, weil kosteneffektiven IT-Bereitstellungsmodell, geriet die europäische Wirtschaft im letzten Jahrzehnt zunehmend in die Abhängigkeit großer internationaler Cloud-Anbieter. Keines der großen globalen Internet- oder Datenunternehmen kommt aus Europa. Zusätzlich wird der Wohlstand zukünftiger Generationen zunehmend von datenbasierten Geschäftsmodellen beeinflusst. Europa muss seine wirtschaftliche und technologische Stärke sowie sein politisches Gewicht in den digitalen Raum übertragen. Neue Regulierungsstrategien und Gesetze für den Umgang mit Daten sowie neue am Markt angebotene Fähigkeiten und IT-Dienste müssen bestehende Monopolstrukturen aufbrechen, um Fortschritt in und für Europa zu ermöglichen. Mit der Gaia-X-Initiative ist Europa angetreten, größtmögliche Datensouveränität für künftige datengetriebene Märkte sicherzustellen. Vertraulichkeit, Datenschutz, Cybersicherheit, Technologieneutralität und Interoperabilität sind dabei europäische Kernwerte. Gaia-X stellt Regelwerke für einen souveränen organisationsübergreifenden Datenaustausch, als auch entsprechende Software-Komponenten nach dem Open-Source-Prinzip zur Verfügung. Zur Umsetzung der Gaia-X-Vision wurde im Jänner 2021 in Brüssel die Non-Profit-Organisation Gaia-X European Association for Data and Cloud AISBL gegründet.

Alpbach-Workshop als Auftakt zur Gaia-X-Hub-Austria-Kommunikationsoffensive. Ende März 2022 wurde der österreichische Gaia-X Hub auf Initiative des Bundesministeriums für Finanzen, des Staatssekretariats für Digitalisierung und des Bundesministeriums für Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie ins Leben gerufen. Der Gaia-X Hub Austria zielt darauf ab, die Wettbewerbsfähigkeit österreichischer Unternehmen zu stärken, die Souveränität in der modernen Datenwirtschaft zu steigern und wichtige Akzente zur grünen Transformation zu setzen. Als Start einer geplanten Kommunikationsoffensive zur europäischen Gaia-X-Initiative wurde Ende August im Rahmen des Europäischen Forum Alpbach ein Workshop organisiert, in dem namhafte Expert:innen und Stakeholder aus Politik, Wirtschaft und Industrie sowie Forschung die gesellschaftlichen und wirtschaftlichen Aspekte der datengetriebenen Wertschöpfung und der europäischen Initiative Gaia-X diskutierten.

Resümee der Diskussion: Es ist jetzt entscheidend, europaweite Kollaboration zu forcieren und das Gaia-X-Regelwerk als Ausgangspunkt für den Aufbau von Daten-Ökosystemen zu nutzen, um nachhaltige, ressourcenschonende Produktionsprozesse und Kreislaufwirtschaften, modernes Umweltmanagement, CO_2-Reduktion, erneuerbare Energiesysteme, effiziente Gesundheitssysteme, etc. zu bauen.

www.gaia-x.at

GREEN IT ALS SCHLÜSSEL ZUR WETTBEWERBSFÄHIGKEIT

Betrachtet man die Auswirkungen der Klimakrise wird der Faktor Nachhaltigkeit zum entscheidenden Thema der Gesellschaft. Im Fokus muss auch die IT stehen, denn gerade Rechenzentren tragen zum steigenden Energieverbrauch bei.

Während die Digitalisierung von Prozessen in einzelnen Unternehmen Ressourcen einspart, so führt die globale digitale Transformation zu einer weltweiten exponentiellen Ressourcennutzung. Durch steigende virtuelle Arbeitsabläufe entstehen immer größere Mengen an Daten, die in Rechenzentren gespeichert werden – die je nach Größe und Konstitution mehr oder weniger CO_2-Emissionen produzieren. Studien zeigen, dass aktuell bereits zwei Prozent der weltweiten Energie auf den Rechenzentrumsbetrieb entfallen. Umso tragischer ist es, wenn Daten abgelegt, jedoch weder analysiert noch für den Unternehmenserfolg genutzt werden. Die Wahl des Speicherorts für Daten, die Form der Daten und die richtige Datenplattform sind also ein entscheidender Schritt sowohl für den Unternehmenserfolg als auch für die Erhaltung der Umwelt. Dies verleiht Green IT eine immense Bedeutung.

Initiativen, Maßnahmen und Zertifizierungen. Durch Maßnahmen wie der Green-IT-Initiative oder der Europäischen Ökodesign-Richtlinie ist es gelungen, den Stromverbrauch durch IT in Deutschland seit 2017 zumindest relativ konstant zu halten – rund zwei Prozent des Landesstromverbrauchs. Aber Blockchain-Technologie oder Künstliche Intelligenz treiben den Energiebedarf von Rechenzentren in die Höhe. Laut einer Studie von The Shift Project von 2019 könnten die Emissionen der Digitalwirtschaft in den kommenden fünf Jahren jedoch bereits acht Prozent des gesamten CO_2-Ausstoßes betragen.

Welche Rolle spielt Green IT in Unternehmen. Laut einer Studie von Capgemini spielt Green IT in den meisten Unternehmen derzeit nur eine geringe Rolle – nur jedes fünfte Unternehmen mit einer Nachhaltigkeitsstrategie berücksichtigt den Klimabeitrag der IT. Das liegt unter anderem an fehlendem Fachwissen, geben insgesamt 53 Prozent der Befragten an. Und nur 43 Prozent der Führungskräfte kennen den Betrag an CO_2-Emissionen, den ihre IT verursacht. Eine umfassende Strategie mit Zeitvorgaben und konkret definierten Zielen haben nur 18 Prozent; nur sechs Prozent setzen eine nachhaltige IT bereits um. Und dies ändert sich auch in den nächsten Jahren nicht: Lediglich 22 Prozent der Unternehmen planen, ihren CO_2-Fußabdruck durch eine nachhaltige IT um mehr als ein Viertel zu reduzieren. Dabei haben Unternehmen die Relevanz von nachhaltigen Geschäftsentscheidungen auf Datenbasis durchaus erkannt. Laut einer Studie von Cloudera stellen bereits heute mehr als ein Fünftel (21 Prozent) der Entscheidungsträger in deutschen Unternehmen höhere Investitionen in Umwelt, Soziales und Unternehmensführung vor die Entwicklung neuer Produkte und Dienstleistungen (18 Prozent) oder die Aufrechterhaltung oder Steigerung ihrer Gewinne (19 Prozent). Dies ist jedoch nicht ganz uneigennützig, denn neben der ökologischen Notwendigkeit sind auch die wirtschaftlichen Vorteile nachhaltiger IT nicht von der Hand zu weisen – sowohl hinsichtlich des Geschäftsergebnisses als auch durch gesellschaftliche Reputation, Markenimage und Kundenbindung. Am Interessantesten ist aber, dass 27 Prozent der Entscheidungsträger glauben, dass Mitarbeiter:innen das Unternehmen verlassen – in Zeiten von Fachkräftemangel ein entscheidendes Kriterium.

https://de.cloudera.com

Siniša Mitrović
Regional Director Eastern Europe and Austria bei Cloudera

„Studien zeigen, dass aktuell bereits zwei Prozent der weltweiten Energie auf den Rechenzentrumsbetrieb entfallen."

DIGITALE ZWILLINGE FÜR

Die smarte Fabrik wird real. Worauf man sich auf dem Weg dorthin einlässt, wie das geht und welchen Sinn das überhaupt macht, erklären Uwe Scharf, Chief Business Unit Officer bei Rittal, und Steffen Rattke, Leiter Presales bei German Edge Cloud, im Gespräch.

IoT 4 Industry & Business: Digitalisierung ist längst in den modernen Fabriken angekommen. Wie können diese nun optimal damit umgehen?

Uwe Scharf: Ja, für die Fertigungs-Unternehmen ist das Thema Digitalisierung in der Produktion immer greifbarer. Die Ziele sind klar: mehr Transparenz, Wissen, Geschwindigkeit und Nachhaltigkeit. Die Frage für viele Unternehmen lautet: Mit welchen Schritten kommen sie am besten voran? Die Datenqualität ist der entscheidende Faktor. Dabei sollte der Blick auf das Umfeld der Fertigung erweitert werden. Für eine „Smart Production" gilt es gleich drei Ökosysteme mit ihren jeweiligen Digitalen Zwillingen klug zu verbinden: Anlagen, Produkte und Fertigungsprozesse.

IoT: Woher kommen die Daten der Zwillinge?

Scharf: Die Daten entstehen in Ökosystemen, die heute oft noch lückenhaft vernetzt sind. Wenn es gelingt, für Anlagen, Produkte und Fertigungsprozesse je einen vollständigen Digitalen Zwilling zu erzeugen und diese intelligent zu verbinden, ist das ein sehr relevanter Schritt auf dem Weg zur Smart Production. Beim Digitalen Zwilling der Anlagen können wir unsere Kunden schon sehr weitgehend unterstützen. Eplan und Rittal treiben gemeinsam mit den Steuerungs-, Schaltanlagen- und Maschinenbauern die durchgängige Digitalisierung voran, mit Software von Eplan schon ab dem ersten Klick beim Engineering sowie mit Systemtechnik, Software und Automation von Rittal. Werden diese Daten beispielsweise über die digitale Schaltplantasche Rittal ePocket aktuell gehalten, profitieren die Anlagenbetreiber auch im Betrieb von einem Zwilling ihrer Anlagen als „Single Source of Truth" in der Cloud.

IoT: Sie sprachen von drei Zwillingen: Anlagen, Fertigungsprozesse und Produkte.

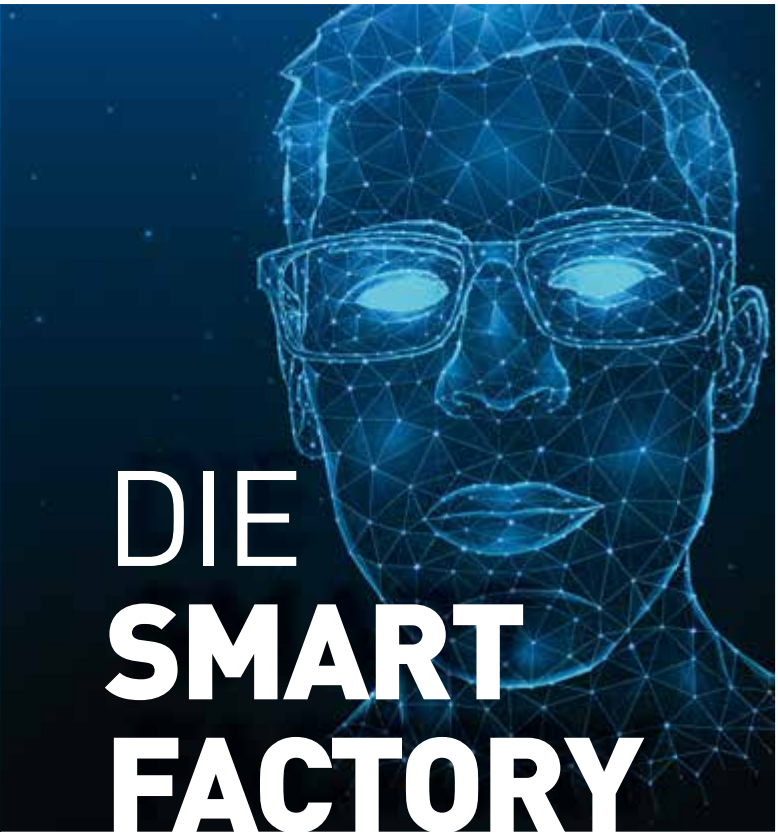
Scharf: Auch rund um die anderen Zwillinge können wir die Erfahrungen unserer Schwesterunternehmen einbringen. Bei den Fertigungsprozessen kommt German Edge Cloud (GEC) ins Spiel. GEC nutzt die Informationen der Anlagendaten zur schnelleren Vernetzung und zur Visualisierung der Prozesse als Digitaler Fertigungszwilling. IIoT-gestütztes Produktionsmanagement mit dem Oncite Digital Production System erhöht dann die Effizienz und Flexibilität der Fertigung. Dafür sind auch vollständige Datensätze für jedes einzelne Werkstück erforderlich – gewissermaßen ein Digitaler Produktzwilling. Hier steigert Cideon die Datendurchgängigkeit mit Erfahrung in CAD/CAM, PDM/PLM und Produktkonfiguration.

IoT: Wo genau setzt GEC an?

Steffen Rattke: Zuerst müssen die Maschinen vernetzt und die Daten in Kontext gesetzt werden. Das braucht viel Domänenwissen über Automatisierung und Fertigungsprozesse. Sie müssen erkennen, welcher Sensor welche Daten an welcher Maschine misst und welche Rückschlüsse daraus zum Fertigungsprozess gezogen werden können. Mit Maschinen- und Anlagendaten von Eplan kommen wir dabei schneller voran. Wir kontextualisieren alle Produktions- und Prozess-Daten und legen diese für wertige

Steffen Rattke
Leiter Presales bei German Edge Cloud

„Die Oncite DPS ist Plattform- und Applikationsfunktionalität in einer integrierten Lösung mit moderner, flexibler Architektur."



DIE SMART FACTORY

Analysen sinnhaft übereinander. Die gute Nachricht: Wer das geschafft hat, kann schnell neues Wissen und damit Nutzen aus den Daten ziehen, beispielsweise durch einen vollständigen virtuellen Überblick über alle Fertigungsprozesse in nahezu Echtzeit. Auf dieser Basis können Sie Fehler finden und die Prozesse optimieren. In unserer Unternehmensgruppe haben wir das mit Rittal im Werk Haiger umgesetzt.

IoT: Die Lösung von GEC nennt sich Oncite. Jetzt gibt es Oncite DPS. Was ist neu?
Rattke: Wir haben unsere Cloud-nativen industriellen Anwendungen zum vollwertigen Gesamtsystem Oncite Digital Production System (DPS) erweitert. Das Ergebnis verbindet ehemals getrennte Kernkomponenten einer digitalen Produktion in einem integrierten System: intelligentes Fertigungsmanagement mit MES- und MOM-Funktionen, Industrial IoT für die Datenanalyse, einen Digitalen 3D-Zwilling für die Realtime-Sicht auf die Produktion sowie Low-Code Development für einfache Anwendungsentwicklung und Digitalisierung der Datenströme. Hinzu kommt Edge und Cloud Computing für die skalierbare und souveräne Datenverarbeitung. Die Oncite DPS ist Plattform- und Applikationsfunktionalität in einer integrierten Lösung mit moderner, flexibler Architektur. Ganz neu ist die strategische Partnerschaft mit den Prozessintegrations-Spezialisten von Scheer. Scheer PAS ist jetzt als Low-Code & Integration Platform Teil des Systems.

IoT: Wo liegen die Vorteile von Low-Code?
Rattke: Wir sprechen von Wandlungsfähigkeit und Flexibilität. Mit Low-Code lassen sich Anwendungen und Anpassungen schnell und ohne umfassende IT-Kenntnisse umsetzen. Das Prinzip: Die Anwendungen werden auf einer grafischen Oberfläche modelliert, sogar einfach mit Drag & Drop. Die Umsetzung in Programm-Code erfolgt automatisch. Das Ergebnis: Das Domänenwissen rund um den Inhalt der Anwendung in der Fertigung mündet ohne den Umweg über aufwendige Programmierung direkt in Digitalisierung. So geht es für die Fertigungs-Unternehmen noch einfacher und schneller voran. Dazu braucht es eine agile Plattform, die Microservices ermöglicht. Die Idee der Composable Enterprise von Scheer PAS passt also ideal zum DPS.

IoT: Wie sieht die Zukunft der Fertigungsindustrie in Sachen Smart Factory aus?
Rattke: Grundsätzlich kommt es darauf an, die digitale Transformation schnell in die Breite zu bringen, insbesondere bei mittelständischen Zulieferern als Rückgrat für die Lieferketten der Automobilindustrie. Das ist unser Antrieb als Gründungsmitglied und Beirat beim offenen Automotive-Datenökosystem Catena-X. Innerhalb der Fabrik steht jetzt für viele Unternehmen, die schon weiter fortgeschritten sind, die nächste Phase Richtung „Smart" an: Der Übergang von der eher starren „Execution" ihrer Prozesse hin zu mehr Agilität und IIoT-gestützter Regelungsfunktion – also Manufacturing Operations Management in nahezu Echtzeit. Ein Hindernis ist häufig der Mangel an Flexibilität vieler bestehender MES/PCS/Scada-Anwendungen durch ihre monolithische Software-Architektur. Software, die mit modernen Microservices das Industrial IoT nutzt, führt dank ihrer Flexibilität schneller und günstiger zum Ziel. Hier setzen wir mit dem DPS an. Natürlich müssen die in vielen Fabriken bereits eingesetzten Systeme berücksichtigt werden. Oncite DPS bietet daher flexible Möglichkeiten zur schrittweisen Migration und harmonisiert und modernisiert die IT-Architektur.

www.rittal.at
www.gec.io

Uwe Scharf
Chief Business Unit Officer bei Rittal

„Für die Fertigungs-Unternehmen ist das Thema Digitalisierung in der Produktion immer greifbarer. Die Ziele sind klar: mehr Transparenz, Wissen, Geschwindigkeit und Nachhaltigkeit."

DIGITALISIERUNG UND AUTOMATISIERUNG **BRINGEN MEHR**

Digitalisierung ist in der Breite angekommen sagt Thomas Lutz, Leiter E-Business & Logistik-Lösungen beim Technischen Händler Haberkorn. Dazu bietet das Unternehmen spannende Tools zu Beschaffung und Management von technischen Produkten wie Schläuchen, Maschinenelementen, Hydraulik und Arbeitsschutz.

IoT 4 Industry & Business: Digitalisierung ist in aller Munde und hat sich in den letzten beiden Jahren weiter verstärkt. Merken Sie das auch bei neuen Kundenanfragen, dass diese ihre Beschaffungsprozesse digitalisieren wollen?

Thomas Lutz: Digitalisierung ist natürlich ein Dauerbrenner bei vielen unserer Kunden. Und man sieht auch, dass dieses Thema nicht nur auf der Managementebene stattfindet, sondern dass es in der Breite angekommen und zu einem strategischen Ziel geworden ist. Unsere Ansprechpartner sind auch sehr aktiv in der Umsetzung. Sie erkennen, dass Digitalisierung nicht heißt, Dinge einfach nur digital zu machen, sondern dass mit ihr auch die Möglichkeit verbunden ist, Prozesse zu optimieren, zu automatisieren und letztlich auch die Effizienz und Transparenz zu steigern.

IoT: Sie bezeichnen Standardisierung und Automatisierung als Geheimwaffe. Welche Lösungen gibt es aus dem Hause Haberkorn diesbezüglich?

Lutz: Das ist einerseits der unternehmensübergreifende elektronische Datenaustausch und andererseits geht es um integrierte Systeme wie beispielsweise unsere Automaten. Das sind die Tools, die wir einsetzen. Darüber hinaus geht es um jene Prozesse, die alles miteinander verbinden. Das sind dann sehr kundenspezifische Lösungen. Die beginnen damit, dass wir über verschiedene Dienste den Bestand des Kunden in die Prozesse unsererseits integrieren können und damit entsprechend berücksichtigen, was der Kunde bereits lagernd hat, im Verhältnis zu dem, was er bestellen will.

IoT: Wie sieht es aus, wenn ein Kunde mit anderen Lieferanten arbeitet? Bleiben das Silos oder können Sie diese Systeme für den Kunden miteinander verbinden?

Lutz: Den Begriff Silo würde ich jetzt nicht teilen. Wenn wir mit unseren Kunden an einer Problemstellung arbeiten, betrachten wir auch die Prozesse dahinter ganzheitlich. Daher stimmen sich unsere verschiedenen Tools mit dem Bestand des Kunden ab, damit er nicht daran vorbeizukaufen kann, nur weil es für ihn im Moment nicht transparent ist. Etwa soll er keine Produkte über den Online-Shop kaufen können, die er schon vorrätig hat. Ein weiteres Beispiel könnte sein, dass der Kunde Produkte im Bereich Arbeitsschutz standardisiert hat und in einem unserer Automaten bereitstellt. Dann soll es ausgeschlossen sein, einen Bypass aufmachen zu können, um weitere Produkte zu bestellen, die schon in den Automaten verfügbar sind. Dafür braucht es ganzheitliche Lösungen, die in sich auch konsistent sind. Damit das wirklich großen Nutzen stiften kann, ist es sinnvoll nur mit einem Partner zusammenzuarbeiten, da die Abstimmung einfacher zu bewältigen ist. Sollte es weitere Lieferanten geben, die Produkte für einen definierten Cluster liefern und dem Kunden wichtig sind, dann integrieren wir diese Lieferanten als Partner in unser System, damit für den Kunden sichergestellt ist, dass der Prozess funktioniert.

IoT: Die Beschaffung hat sicher einen größeren Anteil an der Wertschöpfung des Unternehmens, als man glaubt. Stichwort C-Teile etwa, die in Summe große Positionen ausmachen. Was meinen Sie dazu?

Lutz: Grundsätzlich ist der Ertrag umso besser, je niedriger die Kosten sind. Bei den C-Teilen sind die Prozesse sehr, sehr aufwendig und der Wert der Produkte ist im Verhältnis gering. Das heißt: Preisverhandlungen bei C-Teilen bringen meistens viel weniger, als die Prozesse durch Digitalisierung und Automatisierung zu optimieren. Daher übernehmen wir die Disposition, füllen die Automaten nach und stellen sie dezentral auf, sodass die Mitarbeiter kurze Wege haben. Die einzige operative Tätigkeit beim Kunden ist dann nur mehr der Verbrauch der Produkte und Bezahlung der Rechnung.

IoT: Lieferketten-Probleme sind allgegenwärtig. Kann Haberkorn mit seinen Lösungen dabei helfen die Prozesse und die Verfügbarkeit zu optimieren?

Lutz: Gerade in der Zusammenarbeit mit unseren Kunden, speziell wenn wir ganzheitliche Lösungen managen, haben wir einen sehr guten Einblick in die Abläufe unserer Kunden. Wir stimmen uns mit ihm genau zu seinen Prognosen beim Verbrauch ab, damit wir unsere Bevorratung entsprechend steuern, falls aus irgendeinem Grund die Beschaffungssituation kritisch wird. Hier prüfen wir mit dem Kunden auch rechtzeitig alternative Produkte. Das heißt, wir nehmen da eine sehr aktive Rolle ein, um zu garantieren, dass die Versorgung für den Kunden gesichert wird. Das machen wir auf der einen Seite mittels Bevorratung und auf der anderen mittels aktiven Managements. Gleichzeitig monitoren wir auch die Supply Chain, um zu sehen wo es kritisch werden könnte und machen dann mitunter eine größere Eindeckung oder probieren auch Alternativen aus.

IoT: Kann in Zukunft Künstliche Intelligenz dabei helfen die Lieferketten weltweit zu beobachten, um sie besser zu managen?

Lutz: Aktuell haben wir nichts in dieser Richtung im Einsatz. Wir beobachten diese Entwicklung aber natürlich und sind sehr neugierig, was sich an dieser Stelle tut. In unserer Strategie geht es um eine Kombination zwischen digitalen Lösungen und persönlichen Gespräche mit den Kunden und Lieferanten. Das ist für uns der richtige Weg. Wenn es um Effizienz sowie die Verarbeitung großer Datenmengen geht: das können digitale Tools richtig gut lösen. Es geht aber auch darum, zu schauen, wer die richtigen Partner sind und ob sie die richtige Einstellung haben und bemüht sind auch von ihrer Seite die richtigen Maßnahmen umzusetzen. Das sind Themen, die aus meiner Sicht digitale Systeme nur begrenzt lösen können.

IoT: Zum Abschluss würde ich noch gern über das Thema Sicherheit sprechen. Könnten Ihre Tools, wie etwa die Automaten, ein Einfallstor für Attacken sein oder sind das gekapselte Systeme?

Lutz: Die Daten von unserem Kunden sind auf jeden Fall geschützt, weil – wenn überhaupt notwendig – die Daten im Haberkorn-Rechenzentrum liegen. Allerdings stellt sich die Frage, ob wir wirklich Daten hinsichtlich der DSGVO brauchen. Oft ist das gar nicht notwendig und wir verarbeiten ja auch keine kritischen Informationen. Daher kann ich mir nur schwer vorstellen, dass die Automaten ein großes Einfallstor sein könnten. Das Schlimmste wäre, dass man das Gerät außer Betrieb nimmt. Aber dafür haben wir im Hintergrund Prozesse, die diese Systeme überwachen und feststellen, ob sie arbeiten. Selbst am Sonntagnachmittag, wenn im Normalfall niemand arbeitet, melden sich die Systeme, sollten sie noch aktiv sein. Wenn ein Gerät also etwas macht, was wir nicht erwarten, dann können wir rechtzeitig darauf reagieren.

www.haberkorn.com

OHNE WÄRE ALLES NICHTS

Ohne Hardware gäbe es keine Digitalisierung ist Michael Smetana, Managing Director von HP Österreich, überzeugt. Denn gerade die Drucker und PCs leisten einen ungeahnten Beitrag zu verschiedenen Innovationen. Sie sind aber auch ein Einfallstor für Hacker. Mit HP Wolf Security wurde diesen der Kampf angesagt.

IoT 4 Industry & Business: Alle sprechen von Digitalisierung. Kaum jemand denkt dabei an die dafür nötige Hardware. Was meinen Sie dazu?

Michael Smetana: Eine leistungsfähige Hardware ist die Grundvoraussetzung für die Digitalisierung. Das gilt für eine Vielzahl von Anwendungsbereichen: Im klassischen Büroumfeld sind es modernste Drucker mit leistungsstarken Scan-Einheiten, die über ein entsprechendes Workflow-Management bei der Digitalisierung von Unterlagen einen wesentlichen Beitrag leisten.
Im industriellen Umfeld haben HP-Innovationen beispielsweise wesentlich zur Digitalisierung der Druckindustrie beigetragen, die voll automatisierte Druckabläufe in kleinen bis mittleren Stückzahlen oder personalisierte Druckprodukte zu erschwinglichen Preisen ermöglichen. Digitale Druckmaschinen werden mit Software- und Cloud-Lösungen zur vollautomatischen „Web-to-Print"-Lösung. Das bedeutet, der Kunde bestellt im Internet ein Druckprodukt. In der Druckerei entsteht vollautomatisiert das fertige Produkt. Ein Anwendungsbeispiel: 80 Prozent der in Europa so hergestellten Fotobücher werden auf Druckmaschinen von HP produziert.
Aktuell ein wichtiger Trend: die Digitalisierung der Produktionsindustrie. 3D-Drucker ermöglichen es, durch eine lokale Produktion Wertschöpfung in Länder wie Österreich zurückzuholen, dabei gleichzeitig Lieferketten zu sichern und einen Beitrag zu einer nachhaltigeren Produktion zu leisten.
Ein konkretes Beispiel: View Point System GmbH, ein Unternehmen aus Wien, hat mit Hilfe unserer 3D-Drucker eine Augmented-Reality-Brille bis zur Serienreife entwickelt. Tagsüber arbeiteten die Entwickler an der Verbesserung des Prototyps, der nachts per 3D-Drucker gedruckt wurde. Am nächsten Tag wurde dieser Prototyp begutachtet, optimiert und über Nacht erneut gedruckt. Ein Prozess, der die Produktentwicklung deutlich beschleunigt hat. Mittlerweile druckt das Unternehmen das Serienprodukt ebenfalls hier in Wien und vermeidet damit lange Lieferketten.
Spricht man über Digitalisierung geht es auch immer um massive Mengen an Daten. Das Thema ist Edge Computing. Wir sind hier seit 50 Jahren sehr erfolgreich unterwegs, mit einem deutlichen Marktanteil. Gemeint sind leistungsstarke Computer – sogenannte Workstations. Man spricht von Geräten am „Edge of the Network", also dort wo sich die großen Datenmengen befinden und man sich bei einem Datentransfer schwertun würde, diese in der Cloud zu managen. Das macht man mit sehr performanten Geräten. Sie sehen, eine Vielzahl an Hardware, die an unterschiedlichen Stellen einen wichtigen Beitrag zur Digitalisierung leistet.

IoT: Auf Ihrer Website habe ich einen interessanten Begriff gefunden: gerechte Digitalisierung. Was bedeutet das?

Smetana: Digitalisierung muss für jede und jeden zugänglich bleiben. Wir dürfen die Gesellschaft nicht teilen. In diejenigen, die Zugang zu digitalen Dienstleistungen haben und sich auskennen und diejenigen, die es sich nicht leisten können. Das gilt lokal ebenso wie geopolitisch. Das Thema hat gerade

in der Pandemie auch in Österreich im Bildungsbereich eine besondere Aufmerksamkeit bekommen. Uns ist es wichtig, dass bei der Digitalisierung jeder mitgenommen wird und die Chancen, die sich draus ergeben auch nutzen kann. Deshalb bieten wir kostenlose Bildungsprogramme über HP Life an. Sie sind bereits in viele Sprachen übersetzt, gerade für Länder in Afrika, Lateinamerika, aber auch für Osteuropa und den arabischen Raum. Also dort, wo Menschen oftmals sehr schwer Zugang zu Bildung haben. Gemeinsam mit der UNO helfen wir Schulen auszustatten, damit Menschen Zugang zu Digitalisierung bekommen und lernen können. Das ist eine gesamtgesellschaftliche Verantwortung. Dafür braucht es einen Schulterschluss von vielen, die das unterstützen, fördern und finanzieren.

IoT: Security ist in aller Munde. HP hat unter dem Namen HP Wolf Security diverse Lösungen im Programm. Wie sehen diese aus?

Smetana: Ein Großteil der Cyberattacken – fast dreiviertel – finden über das klassische Endgerät statt. Wichtig – dazu zählen nicht nur PCs und Notebooks sondern auch Drucker. Moderne Drucker sind mittlerweile kleine PCs mit einem Motherboard, einer Festplatte und einem Betriebssystem. Sie sind im Firmennetz integriert und zumeist ungeschützt. Somit sind sie ein hervorragendes Ziel für einen Cyberangriff. Deshalb schützen wir die Endgeräte besonders. HP-Drucker für Unternehmenskunden, ebenso wie Notebooks und PCs, haben beispielsweise einen speziellen Security-Chip eingebaut, mit dem das Bios – quasi das Stammhirn des Druckers – bei jedem Laden verifiziert wird. Denn das Problem beginnt bereits bevor das Betriebssystem geladen wurde. Viele Hacker modifizieren auf Bios-Level. Wenn unsere Geräte Unregelmäßigkeiten beim Booten merken, dann warnt Sie die Software und kopiert eine versteckte „Golden Copy" zurück ins Betriebssystem.

IoT: KI hilft auch bei Security-Lösungen. Welche Ansätze verfolgt HP?

Smetana: Klassische Virenscanner haben ein großes Problem: Sie funktionieren nur dann gut, wenn sie ein Virus bereits kennen. Hier haben wir zwei Lösungen unter der Marke HP Wolf Security vereint. Einmal nutzen wir das Prinzip der Mikro-Virtualisierung. Jeder E-Mail-Anhang wird beim Öffnen zur Vorsicht in einer virtuellen, geschützten Umgebung geladen. Ist die Datei oder der Link infiziert, reicht es, das Fenster zu schließen und die Bedrohung ist eliminiert. Die Technologie bieten wir vor allem Firmenkunden an.
Ich habe Rechenzentrumsleiter in Österreich oft gefragt, ob sie in diesen Zeiten – mit der Vielzahl an Angriffen und unterschiedlichen Angriffsszenarien – noch gut schlafen. Die allermeisten waren sich einig, dass es keine hundertprozentige Sicherheit geben kann. Aber es gilt, alle technischen Möglichkeiten auszunutzen, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu minimieren. Es ist ein Wettlauf. Aber das Gute ist, mittels modernster Sicherheitskonzepte in Netzwerk und, mehr denn je wichtig, direkt im Endgerät kann die Bedrohungslage deutlich reduziert werden. Ein wesentlicher Erfolgsfaktor bei Sicherheitskonzepten ist übrigens auch die Sensibilisierung der Mitarbeitenden. Wir müssen uns von dem Glauben verabschieden, dass es absolute Sicherheit gibt. Aber wir können es den Angreifern deutlich schwerer machen.

www.hp.com

Michael Smetana
Managing Director HP Österreich

„Eine leistungsfähige Hardware ist die Grundvoraussetzung für die Digitalisierung. Das gilt für eine Vielzahl von Anwendungsbereichen."

Auf einem oberösterreichischen Weingut sorgen Drohnen und 5G für das Monitoring großer Ackerflächen und die gezielte Anwendung von Düngemitteln. Das soll helfen in den Lebensmittelversorgungsketten nachhaltiger zu werden.

BESSERER WEIN DURCH SMART FARMING?

Das Projekt von Huawei und Dronetech mit Drohneneinsatz im Spargel- und Weinbau ist das erste in Österreich und will mit einer Echtzeit-Bilderkennung den Pflanzenwuchs analysieren.

Die Zukunft der Landwirtschaft ist smart. Das zeigt ein Pilotprojekt auf dem oberösterreichischen Nussböckgut. Dort fliegen Drohnen ein und aus, beobachten die Rebstöcke und erkennen dank Künstlicher Intelligenz, wann und wo der Einsatz von Wasser oder Pestiziden notwendig ist. Mittels 5G übermitteln die Drohnen ihre Erkenntnisse in Echtzeit an die Winzer:innen. Die können dann gezielt reagieren – ein absoluter Mehrwert für Mensch und Natur. Nun erreicht das Projekt seine zweite Phase: Die Drohnen können selbst auf Ergebnisse reagieren – das reduziert den Einsatz von Pestiziden und Chemikalien drastisch. „Das Projekt von Huawei und Dronetech mit Drohneneinsatz im Spargel- und Weinbau ist das erste in Österreich und hier wollen wir mit einer Echtzeit-Bilderkennung den Pflanzenwuchs analysieren und damit die Ernte, den Output und die Qualität der Produkte verbessern“, erklärt Mag. Andreas Reichhardt, Leiter der Sektion IV - Telekommunikation, Post & Bergbau des Bundesministeriums für Finanzen.

Smarte Technologien für Reduktion von Pestiziden. „In der heutigen Zeit sind wir in der Landwirtschaft mit vielen Herausforderungen konfrontiert. Die Landwirtschaft ist sehr arbeitsintensiv, Fachpersonal ist schwer zu bekommen und es ist wichtig, die Pflanzen so umweltfreundlich wie möglich zu behandeln“, erklärt

Sobald die Drohnentechnologie am Nussböckgut gemeinsam mit Huawei etabliert wird, soll in einer zweiten Phase ein Shared-Drone-Service enstehen.

Beatrix Velechovsky, Weinbäuerin des Nussböckguts in Leonding. David Hopf, CEO von Dronetech Austria beschreibt: „KI-gestützte Drohnen sind ein wichtiger Schritt auf dem Weg in eine nachhaltige Landwirtschaft. Gemeinsam mit Huawei haben wir eine Lösung entwickelt, die nicht nur den Einsatz von Pestiziden und Düngemitteln massiv reduzieren, sondern auch die Effizienz der Landwirtschaft steigern und die Arbeitskosten senken kann. Das hilft dabei in unseren Lebensmittelversorgungsketten nachhaltiger zu werden."
Drohnen für die Landwirtschaft der Zukunft sind mit speziellen Sensoren ausgestattet: Mit hochauflösenden RBG-Sensoren kann der Gesamtzustand des Feldes, sowie Löcher in der Bepflanzung beurteilt und ein „Green Leaf Index" erstellt werden. Ein „Multispektralsensor" hilft bei der Erstellung des „Normalised Difference Vegetation Index", welcher Rückschlüsse darauf zulässt, wie gesund eine Pflanze ist. Doch das ist nicht das einzige Anwendungsfeld, bei der eine Drohne zum Einsatz kommen kann.

5G und Künstliche Intelligenz für verschiedenste Anwendungsfelder. In der zweiten Phase, „Digital Sky", steht die Entwicklung eines Shared-Economy-Konzepts für Drohnendienste im Fokus. „Nachdem sich die Drohnentechnologie am Nussböckgut gemeinsam mit Huawei etabliert hat, entwickeln wir nun in Phase II einen Shared-Drone-Service", erklärt Felix Müller, COO von Dronetech Austria. „Dabei können Landwirte, Gemeinden, Firmen oder Privatpersonen über ein Webportal Drohnen, und die smarte Technologie dahinter, für verschiedenste Anwendungsfelder mieten. Die Drohne fliegt, macht Aufnahmen und übermittelt diese in Echtzeit an die Auftraggeber." Beispielsweise für die Inspektion von Solarpanelen, das Verkehrsmanagement oder die Abnutzungserkennung von Stromleitungen. Erich Manzer, Deputy CEO von Huawei Österreich sieht darin enormes Potenzial: „5G wurde für drei wesentliche Anwendungsfelder entwickelt: Für hohe Bandbreite, geringe Latenzzeiten und um Millionen von Devices zu verbinden. Mit dem Einsatz von Drohnen in Kombination mit KI und 5G können viele ressourcenintensive Vorgänge wie Wartungen oder Instandhaltungen effizienter gelöst werden." Die größte Herausforderung für 5G-Drohnen ist aktuell noch die Netzversorgung. Momentan sind 5G-Netze primär für den Endnutzer ausgelegt, der sich am Boden oder in Gebäuden befindet. Die Versorgung für die Drohnen, die teilweise in 50 Meter Höhe über den Feldern fliegen, muss noch optimiert werden. Mag. Andreas Reichhardt, aus dem Bundesministerium für Finanzen meint dazu: „Wir wollen die Chancen der digitalen Transformation nutzen, dazu braucht es eine optimale Infrastruktur, hier ist der Schwerpunkt im Bereich 5G."

www.huawei.com

DEEP LEARNING IN DER FENSTERPRODUKTION

Um seine Fertigungs- und Montageprozesse effizienter zu gestalten, setzt Fensterhersteller Velux auf Bildverarbeitungstechnologien und erfährt durch Künstliche Intelligenz und Deep-Learning-Lösungen von Sick einen Effizienzschub.

Lasse Hedeby ist leitender Automatisierungsprogrammierer bei Velux A/S und führt das Team für die Entwicklung von Lösungen für die industrielle Bildverarbeitung.

In den letzten Jahren ist Deep Learning als Teilbereich der KI viel benutzerfreundlicher geworden. Heute können Deep-Learning-Lösungen auf kompakten Industriesteuerungen ausgeführt werden. Das macht sich auch die Firma Velux zu Nutze. Als Lasse Hedeby, leitender Automatisierungsprogrammierer bei Velux A/S in Dänemark, von den Deep-Learning-Lösungen von Sick erfuhr, sah er eine Möglichkeit, die Effizienz in der Produktion zu steigern und die Mitarbeiter:innen effektiver einzusetzen, indem er ihnen monotone Arbeitsaufgaben abnimmt.

Einsparung auf 20 Personenstunden. In der Vergangenheit hat Velux die Produktqualität durch manuelle Prüfungen der Teilkomponenten seiner Fenster sichergestellt. Obwohl dieses System immer gut funktioniert hat, gab es Einschränkungen. Je nachdem, wie erfahren die Mitarbeiter:innen waren, kam es zu Abweichungen bei der Bewertung der Komponenten. Durch die monotone Arbeit kam es schon mal zu Betriebsblindheit. Um das auszuschließen, beschloss Lasse Hedeby die Bediener bei dieser manuellen Arbeit mit einer Kamerainspektion zu unterstützen. Für den Programmierer Hedeby bedeutete das allerdings enorme zusätzliche Arbeit, denn bei Velux fallen viele Teilprozesse an. Für jeden dieser Prozesse muss eine neue Software für neue industrielle Bildverarbeitungssysteme entwickelt werden. Die Erstellung einer regelbasierten Software für alle Prozesse kann leicht bis zu 200 Personenstunden in Anspruch nehmen. Durch den Einsatz der Deep-Learning-Lösung, die auf Sick AppSpace basiert, konnte Hedeby die Entwicklungsdauer für die neue Software auf 20 Stunden und damit einen Bruchteil der Zeit reduzieren.

Problemlösung durch enge Kooperation. In einem der jüngsten Projekte wurden Lösungen von Sick eingesetzt, um zu prüfen, ob Aluminiumprofile einer Jalousie ausreichend mit Polyethylenschaum gefüllt sind. Das Training der Software zur Erkennung exakt gefüllter Profile ging schnell und lieferte gute Ergebnisse, aber der Prozess verlief nicht perfekt. Die Profile sind lang und dünn, so dass bei der Überprüfung der Profile durch die Kameras die für die Bewertung relevanten Informationen nur einen sehr kleinen Teil des Bildes ausmachen. Die Lösung erforderte die Anpassung einer Standard-SensorApp, die das Bild des Bildverarbeitungssensors von Sick in drei separate Bilder aufteilt, um den Deep-Learning-Algorithmus effizienter zu machen. Die Softwareingenieure von Velux A/S und Sick halfen sich gegenseitig bei der Entwicklung der Lösung, und beide Teams profitierten von dieser Zusammenarbeit. Lasse Hedeby sagt, er habe „noch nie einen Lieferanten erlebt, der so flexibel ist und einen so guten Support bietet wie Sick“.

Der Weg in die Zukunft. Lasse Hedeby arbeitet bereits an der nächsten Aufgabe. Mit Hilfe von KI soll sichergestellt werden, dass Schrauben in einer Haltevorrichtung montiert und festgezogen werden. Die Aufgabe ist mit einem gewöhnlichen regelbasierten industriellen Bildverarbeitungssystem nur schwer zu bewältigen, da sowohl Metall als auch Schrauben eine sehr unterschiedliche Oberfläche mit vielen Lichtreflexionen haben können. Die ersten Versuche sind vielversprechend. Die Fähigkeit der Deep-Learning-Lösung von Sick, eine solche Vielfalt komplexer Probleme problemlos zu bewältigen, zeigt deutlich, dass dies der Weg in die Zukunft der kamerabasierten Inspektion und industriellen Automation ist.

www.sick.at

GEFAHR GEBANNT

Die dataFeed OPC Suite Extended von Softing bietet mit OPC UA Reverse Connect zusätzliche Sicherheit bei der Datenintegration.

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. Der heute aktuelle OPC-UA(Unified Architecture)-Standard ist plattformunabhängig und nutzt moderne Sicherheits- und Datenmodellierungstechnologien für die Implementierung zukunftssicherer, skalierbarer und erweiterbarer Lösungen. Mit Hilfe von Begleitnormen wird die Nutzung von OPC UA für den Endanwender nochmals vereinfacht. Jetzt ermöglicht Softing die sichere Kommunikation zwischen OPC-UA-Komponenten in OT und IT, die durch Firewalls oder DMZs getrennt sind mit der Integration von OPC UA Reverse Connect in seine dataFeed OPC Suite Extended V5.22. Die dataFeed OPC Suite Extended ist 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 OPC-UA-Reverse-Connect-Funktionalität gewährleistet die Suite eine sichere Kommunikation zwischen OPC-UA-Komponenten, die durch Firewalls oder DMZs getrennt sind.

Sicherer Verbindungsaufbau. OPC UA Reverse Connect vermeidet traditionelle Client-Server-Verbindungen, bei welchen der Client den Verbindungsaufbau zum Server vornimmt. Stattdessen verbindet sich der Server aktiv mit dem Client. Das ist für Netzwerke wichtig, in denen sich der Server in einer geschützten Umgebung befindet, wie z.B. im Produktionsnetzwerk einer Fabrik. Es besteht keine Notwendigkeit, die Firewall-Ports vom IT-Netzwerk zum OT-Netzwerk zu öffnen. Die Gefahr eines Angriffs auf das Produktionsnetz ist damit gebannt, da die Firewall geschlossen bleibt.

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 auch 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 außerdem 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.

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.

WENIGER LEBENSMITTEL-VERSCHWENDUNG DURCH KI

Um Waren noch zielgenauer zu bestellen und die Lieferkette entsprechend effizient zu gestalten, hat Spar mit seiner IT-Unit, Microsoft und weiteren Partnern eine KI-Lösung entwickelt, um gezielt Bestellvorschläge und -prognosen für alle Standorte zu ermöglichen.

Mindestens eine Million Tonnen an genießbaren Lebensmitteln landen in Österreich jährlich im Müll. Davon gehen laut dem WWF 79.200 Tonnen auf das Konto des Einzelhandels, 175.000 Tonnen an die Außer-Haus-Verpflegung, wie Betriebskantinen, Restaurants und Caterer. Bei der Produktion von Lebensmitteln fallen jährlich 121.800 Tonnen an vermeidbaren Abfällen an. Getoppt wird das alles nur von den österreichischen Haushalten, in denen jährlich 521.000 Tonnen wertvolle Nahrungsmittel im Müll landen. Seinen Anteil an der Verschwendung möchte die Handelskette Spar dank Künstlicher Intelligenz reduzieren. Mittels neuer IT-Lösung von Spar ICS Daten werden Verkaufsmengen, Wetterbedingungen, Sonderangebote, Marketingaktionen, Saisonalität und andere Faktoren analysiert und eine präzise Vorhersage der optimalen Menge pro Filiale erstellt. Schon seit Jahrzehnten gibt es automatische und ausgeklügelte Warenbestellung. Die adap-

Markus Kaser
Spar-Vorstand für IT, Einkauf, Marketing und CSR

„In diesem Projekt nutzt Spar die Potenziale der Technologien und Künstlichen Intelligenz, um die Bedürfnisse unserer Kund:innen zu erfüllen und dabei gleichzeitig Ressourcen zu sparen."

tierte Version wird jetzt im Bereich Obst und Gemüse eingesetzt. „Die Vorteile sind vielfältig – nicht nur für das Unternehmen, die Lieferant:innen, die Kund:innen und die Mitarbeiter:innen – sondern auch und vor allem für die Umwelt. Für die großen Herausforderungen unserer Zeit, wie auch den Klimawandel, bieten uns neue Technologie sowie die richtigen digitalen Tools Lösungsansätze. In diesem Projekt nutzt Spar die Potenziale der Technologien und Künstlichen Intelligenz, um die Bedürfnisse unserer Kund:innen zu erfüllen und dabei gleichzeitig Ressourcen zu sparen“, erläutert Markus Kaser, Spar-Vorstand für IT, Einkauf, Marketing und CSR, das Projekt. Das Ergebnis ist eine Genauigkeit der Vorhersage von über 90 Prozent. All das soll dazu führen, dass in der richtigen Filiale exakt die benötigte Menge zur richtigen Zeit verfügbar ist und dadurch die Lebensmittelverschwendung noch stärker reduziert wird. Das nun in Österreich abgeschlossene Projekt war Teil der Microsoft Initiative „Mach heute morgen möglich“.

Cloud-Lösungen als Basis. Umgesetzt wurde das Projekt von der Spar-eigenen IT-Unit, der Spar ICS, mit den Partnern Microsoft und Paiqo. Aufgrund der großen Datenmengen und dem variablen Bedarf an Rechenleistung fiel die Wahl auf die Microsoft Cloud. Die Advanced-Analytics-Werkzeuge von Microsoft Azure greifen auf diese cloudbasierten Daten zu und machen damit eine intelligente Lieferkette überhaupt erst möglich. Diese Lösungen bieten die notwendigen Voraussetzungen, um mit der Datenmenge sowohl horizontal als auch je nach Workload zu skalieren. „Gerade im Bereich von Künstlicher Intelligenz benötigen wir hin und wieder enorme Rechenleistung, aber oft nur für begrenzte Zeit. Diese Anforderung lässt sich speziell über eine hochskalierbare Cloud kosteneffizient abdecken“, erklärt Spar-ICS-Geschäftsführer Andreas Kranabitl die Notwendigkeit der Cloud für dieses Projekt.

Effiziente Lieferketten durch KI. Spar-Kund:innen profitieren schon länger von effizienten Lieferketten und Vorhersagen beim Bestellprozess. Seit einiger Zeit werden die benötigten Mengen an Obst und Gemüse vorhergesagt, erst danach bestellt und extra für Spar reif geerntet. Da frische Zutaten ohne unnötige Lagerzeiten sofort und genussreif im Regal verfügbar sind und gleich auf dem Teller oder im Kochtopf landen, wird weniger entsorgt: sowohl im Handel als auch bei den Kund:innen zu Hause. „Die Vorhersagen sind eine wertvolle Unterstützung für jene Mitarbeiterinnen und Mitarbeiter, die am Bestellprozess beteiligt sind. Künstliche Intelligenz ersetzt dabei nicht die bisherigen Prozesse, sondern ergänzt das Team als wertvolles Mitglied. Die Optimierung der Belieferung von mehr als 1.500 Filialen hat somit positive Auswirkungen auch auf die Arbeit unserer rund 40.000 Mitarbeitenden in den Märkten“, so Hans K. Reisch, stellvertretender Spar-Vorstandsvorsitzender und zuständig für die Filialen.

www.spar.at

© Spar | Johannes Brunnbauer

Spar hat mit seiner unternehmenseigenen IT-Unit, Microsoft und Paiqo eine Lösung entwickelt, um mit Hilfe von Daten und Künstlicher Intelligenz gezielte Bestellvorschläge und -prognosen für alle Spar-Standorte zu ermöglichen.

VON LENOVO AUSGEWÄHLT

Veeam Software hat sich mit **Lenovo** für die neue Lösung Lenovo TruScale Backup-as-a-Service (BaaS) zusammengeschlossen. Als erste Datensicherungslösung, die zu TruScale hinzugefügt wird, bietet Veeam allen Lenovo-Benutzern nun BaaS nach dem Pay-as-you-go-Prinzip über die Infrastructure-as-a-Service-Plattform von Lenovo. Die einheitliche Lösung wurde entwickelt, um die Datensicherungsstrategie von Unternehmen zu modernisieren, die Verwaltung von riesigen Datenmengen zu unterstützen und die steigenden Anforderungen an die Leistung und Multi-Workload-Verfügbarkeit zu erfüllen und gleichzeitig die Gesamtbetriebskosten mit einem flexiblen Kostenmodell zu senken. „Von Ressourcen-Knappheit bis hin zu Ransomware-Angriffen sind IT-Organisationen mit dem ständigen Risiko von Ausfallzeiten und Datenverlusten konfrontiert“, erklärt **John Jester**, Chief Revenue Officer bei Veeam, „und als führender Anbieter von moderner Datensicherung sind wir stolz darauf, Teil von Lenovo TruScale zu sein, um von Experten entwickelte und verwaltete BaaS und Disaster-Recovery-as-a-Service anzubieten. Diese neue Lösung von Veeam und Lenovo hilft allen Unternehmen, die Komplexität der Modernisierung ihrer Datensicherungsstrategie zu reduzieren und das Vertrauen in den Schutz ihrer Daten zu gewährleisten.“

www.veeam.com/de

VERÄNDERUNG IM VORSTAND

Daniela Bünger folgt dem scheidenden Finanzvorstand Dr. Matthias Heiden mit Anfang des kommenden Jahres in den Vorstand der **Software AG**. Zuvor war sie CFO of Global Financial Services and Insurance bei Atos und davor CFO der Region Benelux und Nordics von Atos. Eine weitere Station ihrer Laufbahn war das Beratungsunternehmen Accenture, bei dem sie neun Jahre tätig war. Bünger verfügt über profunde Erfahrungen in der Verbesserung und Straffung betrieblicher Prozesse, der Stärkung wiederkehrender Umsatzströme sowie der Eingliederung übernommener Unternehmen. Sie tritt ihr Amt zu Beginn der Beschleunigungsphase der Helix-Transformation an. „Ich finde es großartig, dass ich in dieser wichtigen Phase ihrer strategischen Entwicklung zur Software AG komme. Das Unternehmen ist dank der Helix-Strategie gut vorangekommen, und jetzt ist der Zeitpunkt, um das nachhaltige, profitable Unternehmenswachstum weiter voranzutreiben. Ich bin zuversichtlich, dass ich dem Unternehmen helfen kann, die Entwicklung des wiederkehrenden Konzernumsatzes, des Cashflows und der Marge zu beschleunigen. Ich freue mich darauf, gemeinsam mit dem Team das große Potenzial des Unternehmens auszuschöpfen und ab Januar mit aller Kraft durchzustarten“, so Daniela Bünger.

www.softwareag.com

NASUNI ERWEITERT EUROPÄISCHE PRÄSENZ

Steigende Kundennachfrage nach modernen File-Data-Services befeuert die strategische Investition der **Nasuni Corporation**, die nun weitere Investitionen im DACH-Markt angekündigt hat. Nasuni ermöglicht es Unternehmen, von überall aus auf Dateien zuzugreifen und sie zu schützen. Dies geschieht über hochmoderne Dateidienste, die auf dem einzigartigen Cloud-nativen globalen Dateisystem von Nasuni aufsetzen. Die Cloud-Lösung ersetzt herkömmliche Network Attached Storage und Datensicherungstechnologien. Dabei konsolidiert sie Dateidaten in einem leicht erweiterbaren Cloud-Objektspeicher zu einem Bruchteil der Kosten. „Hybrides Arbeiten, Ransomware-Angriffe und die Geschwindigkeit der heutigen globalen Geschäftswelt beschleunigen den Wandel weg von traditioneller hardwarebasierter Speicherung hin zu einem softwaredefinierten Dateidienstleistungsmodell. Nasuni hat vor fast einem Jahrzehnt Pionierarbeit bei cloudbasierten Dateidatendiensten geleistet, und die jüngsten Investitionen in Verbindung mit unserem anhaltenden, schnellen Wachstum bestätigen unsere Vision. Wir gehen davon aus, dass wir das DACH-Team in den nächsten zwei Jahren weiter ausbauen werden, da wir kontinuierlich Wachstumsraten verzeichnen“, ergänzt **David Grant**, Präsident von Nasuni.

www.nasuni.com

KI-SPEZIALIST 7LYTIX ERHÄLT FINANZIERUNG

© Hermann Wakolbinger

Franziskos Kyriakopoulos und das Investoren-Team hinter dem Data-Science- und Prognose-Spezialisten 7Lytix.

V.l.n.r.
Georg Kirchmayr (Element),
Peter Paminger (Raiffeisen Invest),
Franziskos Kyriakopoulos (7Lytix),
Daniel Haider (Raiffeisen Invest),
Christian Matzinger (HTF),
Eugen Sorg (CFP),
Christoph Niemöller (Mediaprint) und
Thomas Meneder (HTF)

Der **OÖ HightechFonds** und die **Element Beteiligungs GmbH** unterstützen den Produktlaunch des Linzer Start-ups 7Lytix auf den internationalen Märkten. Die vielseitig einsetzbare Software analysiert in Unternehmen vorhandene Datenpools, um daraus treffsichere wirtschaftliche Prognosen zu erstellen. Dazu nützt die Software KI. Unter Einbeziehung großer Datenmengen erstellt sie Prognosen, aus denen wiederum Handlungs- und Verbesserungsoptionen abgeleitet werden können. „Das reicht vom Bestellmanagement über voraussichtliches Kundenverhalten bis hin zu Wartungszyklen und noch viel weiter", erklärt Gründer und CEO Franziskos Kyriakopoulos. „Konkret bedeutet das: Unsere Software kann z.B. voraussagen, wie viele Semmeln in welcher Lebensmittelfiliale in welcher Woche voraussichtlich gekauft werden oder wann der richtige Zeitpunkt ist, Maschinen oder Anlagen zu warten, bevor sie kaputt gehen und Stehzeiten entstehen." Auch der regionale Venture Capital Fonds ist dem Start-up schon seit mehreren Jahren verbunden und steht dem Gründer und seinem Team auch als Sparringspartner zur Seite. Gemeinsam mit der Elements GmbH stellt der OÖ HightechFonds auch zusätzliches Kapital zur Erschließung internationaler Märkte.

www.7lytix.com

IT-AUTOMATISIERUNGS-TREIBER

Red Hat und **IBM Research** haben das erste Community-Projekt zur Schaffung intelligenter NLP-Fähigkeiten für Ansible und die IT-Automatisierungsindustrie angekündigt. Das „Project Wisdom" nutzt ein KI-Modell und zielt darauf ab, die Produktivität von Entwicklern im Bereich IT-Automatisierung zu steigern und sie für IT-Fachkräfte mit unterschiedlichen Fähigkeiten und Hintergründen leichter erreichbar und verständlich zu machen. Project Wisdom basiert auf KI-Grundlagenmodellen, die von IBM's AI for Code abgeleitet sind, und erlaubt es Nutzern, Befehle in Form eines einfachen englischen Satzes einzugeben. Anschließend analysiert es den Satz und erstellt den gewünschten Automatisierungsworkflow, der als Ansible Playbook bereitgestellt wird und für die Automatisierung einer beliebigen Zahl von IT-Aufgaben verwendet werden kann. Im Unterschied zu anderen KI-gesteuerten Coding-Tools fokussiert sich Project Wisdom nicht auf die Anwendungsentwicklung, sondern adressiert die steigende Komplexität der Unternehmens-IT, die mit der zunehmenden Einführung hybrider Clouds einhergeht. **Chris Wright**, CTO and SVP of Global Engineering, Red Hat, erklärt dazu: „Dieses Projekt zeigt beispielhaft, mit welcher Kraft Künstliche Intelligenz die Art und Weise, mit der Unternehmen Innovationen vorantreiben, fundamental verändern kann. Es macht Fähigkeiten, die typischerweise in den Betriebsteams angesiedelt sind, anderen Unternehmensbereichen zugänglich. Mit intelligenten Lösungen können Unternehmen Einstiegshürden senken, entstehende Qualifikationslücken schließen und organisationsweite Silos aufbrechen, um die Arbeit in der Unternehmenswelt neu zu gestalten."

www.redhat.com

VERANSTALTUNGSKALENDER

DEZEMBER 2022

CyberSec4Europe Summit
1.-2.12.2022 | Brüssel

IoT Tech Expo
1.-2.12.2022 | London, hybrid

Digital Transformation Week
1.-2.12.2022 | London, hybrid

AI & Big Data Expo
1.-2.12.2022 | London, hybrid

Cyber Security & Cloud Expo
1.-2.12.2022 | London, hybrid

Edge Computing Expo
1.-2.12.2022 | London, hybrid

DevOpsCon – Conference for Continous Delivery, Microservices, Containers, Cloud and Lean Business
5.-8.12.2022 | München, hybrid

ScaleUp 360° Enterprise Cloud Governance
6.-7.12.2022 | virtuell

Applying AI & Machine Learning to Finance & Technology
7.12.2022 | New York, hybrid

The AI Summit New York
7.-8.12.2022 | New York

IT-Tage 2022 Remote
12.-15.12.2022 | virtuell

SANS Frankfurt December 2022 – Cyber Security Training
12.-17.12.2022 | Frankfurt/Main, hybrid

Conf42: Web 3.0
15.12.2022 | virtuell

JÄNNER 2023

Int. Conference on Internet Technologies and Society (ICITS)
2.-3.1.2023 | Berlin

Int. Conference on Artificial Intelligence, Soft Computing and Applications (AISCA)
2.-3.1.2023 | Zürich

Int. Conference on Computer Science and Machine Learning (CSML)
2.-3.1.2023 | Zürich

Int. Conference on Internet Technologies and Society (ICITS)
4.-5.1.2023 | Frankfurt/Main

Int. Conference on Artificial Intelligence and Soft Computing (ICAISC)
4.-5.1.2023 | Hamburg

Int. Conference on Power Control and Embedded System (ICPCES)
13.-14.1.2023 | Brüssel

Int. Conference on Artificial Intelligence and Soft Computing (ICAISC)
25.-26.1.2023 | Wien

Conf42: DevOps
26.1.2023 | virtuell

Int. Conference on Advanced Computing (ADCOM)
28.-29.1.2023 | Kopenhagen

IoT Solutions World Congress
31.1.-2.2.2023 | Barcelona

FEBRUAR

ScaleUp 360° IT & Cloud Security
1.-2.2.2023 | virtuell

Int. Conference on Robotics and Smart Manufacturing (ICROSMA)
2.-3.2.2023 | Berlin

ICAFMEC – Int. Conference on Advances in Fog and Mobile Edge Computing
6.-7.2.2023 | virtuell

ICRAFMEC – Int. Conference on Recent Advances in Fog and Mobile Edge Computing
6.-7.2.2023 | virtuell

Data Science Salon: AI & Machine Learning in the Enterprise
8.-9.2.2023 | Austin, hybrid

The Smart City Event
14.-17.2.2023 | Ft. Lauderdale

Intelligente Edge Expo
14.-17.2.2023 | Ft. Lauderdale

IoT Evolution Expo
14.-17.2.2023 | Ft. Lauderdale

Industrial IoT Conference
14.-17.2.2023 | Ft. Lauderdale

5G Expo
14.-17.2.2023 | Ft. Lauderdale

Int. Conference on Artificial Intelligence and Soft Computing (ICAISC)
16.-17.2.2023 | Zürich

MÄRZ

Int. Conference on Artificial Intelligence and Soft Computing (ICAISC)
2.-3.3.2023 | Berlin

ACM/IEEE Int. Conference on Human-Robot Interaction
13.-16.3.2023 | Stockholm

embedded world
14.-16.3.2023 | Nürnberg

The European Chatbot & Conversational AI Summit
15.-16.3.2023 | Edinburgh, hybrid

CloudFest
21.-23.3.2023 | Rust, Europa-Park

ScaleUp 360° Big Data
29.-30.3.2023 | virtuell

Conf42: Cloud Native
30.3.2023 | virtuell

APRIL

ICCCKD – Int. Conference on Cloud Computing and Knowledge Discovery
3.-4.4.2023 | virtuell

ScaleUp 360° Smart Manufacturing
12.-13.4.2023 | virtuell

MAI

Int. Conference on Artificial Intelligence and Soft Computing (ICAISC)
3.-5.5.2023 | Hamburg

Digital Future Congress
4.5.2023 | Graz

Rise of AI
9.-10.5.2023 | Berlin, hybrid

ScaleUp 360° Software Testing & Automation
9.-10.5.2023 | virtuell

EIC – European Identity and Cloud Conference
9.-12.5.2023 | Berlin, hybrid

Big Data & AI World Frankfurt
10.-11.5.2023 | Frankfurt/Main

ScaleUp 360° AI in Business Summit
10.-11.5.2023 | virtuell

Conf42: Machine Learning
18.5.2023 | virtuell

World Conference on Cyber Security and Ethical Hacking (WCCSEH)
23.-24.5.2023 | Berlin

Int. Conference on Electrical and Electronics Engineering (ICEEE)
25.-26.4.2023 | Wien

JUNI

ScaleUp 360° Data Governance
21.-22.6.2023 | virtuell

ICMAEC – Int. Conference on Multi-Access Edge Computing
22.-23.6.2023 | virtuell

Big Data & Analytics Summit Canada
22.-23.6.2023 | Toronto

Data Science Week: World Conference on Data Science & Statistics
26.-28.6.2023 | Frankfurt/Main

automatica
27.-30.6.2023 | München

SEPTEMBER

ICMECT – Int. Conference on Mobile Edge Computing Technologies
16.-17.9.2023 | Rom

OKTOBER

Cybertech Europe
3.-4.10.2023 | Rom

it-sa
10.-12.10.2023 | Nürnberg

NOVEMBER

SPS
14.-16.11.2023 | Nürnberg

productronica
14.-17.11.2023 | München

Conf42: DevSecOps
30.11.2023 | virtuell

DEZEMBER

Conf42: Internet of Things (IoT)
14.12.2023 | virtuell

VORSCHAU

IoT4 NR. 1-2023 | Erscheinungstermin: **23. März 2023**

OT MAG MAN EBEN

IT-Sicherheit und OT-Sicherheit sind definitiv zwei Paar Schuhe. Im Gegensatz zu fast allen anderen Anbietern hat sich Otorio vom ersten Tag an rein auf den Schutz von Produktionsumgebungen und kritischen Infrastrukturen fokussiert. Kraftwerke, Produktionsstraßen, Roboter und Schweißmaschinen, ... dort und in vielen ähnlichen Bereichen hört IT-Sicherheit auf und fängt OT-Sicherheit an. **Kay Ernst**, Regional Sales Director DACH, hat hier (fast) einzigartige Geschichten zu erzählen.

RANDERSCHEINUNG

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

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.

6. Jahrgang

Auflage: 13.000 Exemplare

IoT4 INDUSTRY&BUSINESS

Das Magazin für IoT, Big Data und Security

Zum kostenlosen Abo

Das nächste Heft erscheint am
23. MÄRZ 2023
Anzeigen-/Redaktionsschluss:
6. März 2023

T&M TECHNIK & MEDIEN VERLAGSGMBH

www.iot4industry.info

Zukunft ist jetzt.

IO-Link

Sensoren und Systeme
mit IO-Link

Mehr Informationen unter
pepperl-fuchs.com/tr-io-link

Datenaustausch vom Sensor in die Steuerung und darüber hinaus – standardisiert und transparent.

Your automation, our passion.

PEPPERL+FUCHS