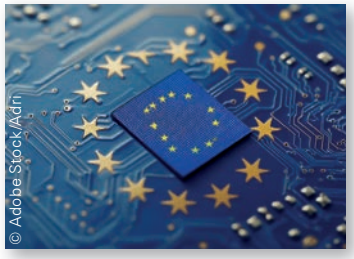
JOURNAL FÜR INNOVATION, TECHNIK UND INDUSTRIE

NEW BUSINESS

INNOVATIONS


© Freepik/a_tor


© Adobe Stock/Adri

- **Voller Datendrang:** Der richtige Umgang mit digitalen Ressourcen
- **Eigene „Sinne" für das Netz:** Warten auf die nächste Mobilfunkgeneration
- **Neues Sicherheitsprogramm:** Microsoft verteidigt Europas Cybersicherheit

NEW BUSINESS INNOVATIONS IST EIN PRODUKT DER NEW BUSINESS VERLAG GMBH

AUSGABE 7–8 | JULI/AUGUST 2025 • WWW.NEWBUSINESS.AT

LIEBE LESERINNEN UND LESER!

Nach 5G kommt 6G. Aber bis es so weit ist, verkürzt erst einmal 5.5G die Wartezeit auf die nächste Mobilfunkgeneration, und die hat viele neue Möglichkeiten im Gepäck. Welche das sein könnten, lesen Sie ab Seite 4.
Mit dem neuen IT- und Data Center stärkt die Linz AG Telekom die digitale Infrastruktur der Stadt. Was es alles zu bieten hat, erfahren Sie ab Seite 8.
Unternehmen erlauben Externen häufig den Zugriff auf ihr IT-Netzwerk. Das ist zwar praktisch, aber auch riskant für die Sicherheit von Systemen und Daten. Warum, das finden Sie ab Seite 22.
KI bietet viele Chancen, birgt aber auch Risiken. Daher setzt die Regierung jetzt mit einem Chatbot der KI-Servicestelle auf Informationsvermittlung, Verständlichkeit und Zugänglichkeit. Ab Seite 32 gibt es die Details.
Microsoft hat ein neues europäisches Sicherheitsprogramm ins Leben gerufen, um die Cybersicherheit in Europa zu stärken. Die Details haben wir ab Seite 38.
Die Europäische Cybersicherheitsbehörde ENISA hat Software-Supply-Chain-Angriffe zur größten Bedrohung erklärt. Damit besteht akuter Handlungsbedarf auch für industrielle IT- und OT-Systeme. Wie der aussieht, schreiben wir ab Seite 45.
Die TU Graz gründet die erste universitäre Business GmbH zur Softwareverwertung in Österreich. Welche Ziele das neue Unternehmen verfolgt, erzählen wir auf Seite 52.
Mit dem ersten Umweltzeichen für ein Rechenzentrum setzt Wien ein Zeichen für eine klimafitte Digitalisierung. Auf Seite 58 lesen Sie, was es damit auf sich hat.

Wir wünschen Ihnen mit dieser Auswahl sowie den vielen weiteren interessanten Geschichte viel Vergnügen.

AWARD FÜR START-UPS

Aufruf an junge Cybersecurity-Talente: UP25@it-sa sucht die besten Start-ups.

Innovative Ideen im Bereich IT-Sicherheit und Datenschutz sind gefragter denn je – nicht zuletzt vor dem Hintergrund zunehmender Bedrohungen durch Cyberkriminalität und wachsender regulatorischer Anforderungen. Genau hier setzt der Athene Startup Award UP25@it-sa an: Der renommierte Wettbewerb zeichnet jährlich besonders vielversprechende Neugründungen und junge Unternehmen aus Deutschland, Österreich und der Schweiz aus, die zukunftsweisende Lösungen im Bereich IT-Sicherheit und Datenschutz entwickeln.
Gesucht werden nicht nur technologische Innovationen, sondern auch tragfähige und skalierbare Geschäftsmodelle, die den IT-Sicherheitsmarkt nachhaltig bereichern können. Noch bis 31. Juli 2025 können sich Start-ups mit einem klaren Fokus auf IT-Security oder Privacy-Themen online bewerben.

15.000 EURO PREISGELD

Der Award wird von den Sponsoren Deutsche Telekom Security, Kaspersky und Infinigate unterstützt, die ein Gesamtpreisgeld von 15.000 Euro zur Verfügung stellen. Eine unabhängige Fachjury wählt anhand der Bewerbungsunterlagen fünf Finalisten aus. Bewertet werden unter anderem die technische Qualität der Lösung, das Geschäftsmodell, die Marktfähigkeit und die unternehmerische Vision.
Das große Finale findet am 8. Oktober 2025 im Rahmen der it-sa Expo&Congress in Nürnberg statt – Europas führender Fachmesse für IT-Sicherheit. Dort präsentieren die fünf ausgewählten Start-ups ihre Konzepte im Rahmen eines Live-Pitchs, aus dem die Jury den Preisträger kürt. BS

Foto: NürnbergMesse GmbH

IMPRESSUM

Medieneigentümer, Herausgeber- und Redaktionsadresse: NEW BUSINESS Verlag GmbH, 1180 Wien, Kutschkergasse 42, Tel.: +43 1 235 13 66-0 • **Geschäftsführer:** Lorin Polak • **Sekretariat:** Sylvia Polak • **Chefredaktion:** Victoria E. Morgan, Bettina Ostermann • **Redaktion:** Rudolf N. Felser, Barbara Sawka, Albert Sachs • **Art-Direktion:** Gabriele Sonnberger • **Lektorat:** Caroline Klima • **Herstellung:** MAßGEDRUCKT® • **Coverfoto:** Adobe Stock/RealPeopleStudio • Unsere Verlagsprodukte entsprechen den Anforderungen der EU-Verordnung über die allgemeine Produktsicherheit (GPSR).

ITDESIGN: 25 JAHRE INNOVATION

Die ITdesign Software Projects & Consulting GmbH feiert 2025 ihr 25-jähriges Bestehen. Seit der Gründung im Jahr 2000 hat sich das Unternehmen als führender Anbieter von IT-Lösungen in Österreich etabliert und setzt kontinuierlich neue Maßstäbe in den Bereichen Digitalisierung, Security und IT-Management.

Gegründet von 18 Gesellschaftern mit einer gemeinsamen Vision, verfolgt ITdesign seit einem Vierteljahrhundert einen klaren Kurs: Unternehmen durch maßgeschneiderte IT-Lösungen erfolgreicher zu machen. Heute beschäftigt ITdesign über 70 Mitarbeiter:innen und erzielte im Jahr 2024 einen Umsatz von 11,9 Millionen Euro.

Das IT-Software-Unternehmen steht für Qualität, Innovationskraft und partnerschaftliche Zusammenarbeit. Durch eine transparente Organisationsstruktur und eine konsequente Kundenorientierung hat sich ITdesign einen festen Platz in der IT-Branche gesichert.

Mit einer starken Fokussierung auf die Themen Sicherheit und Effizienz entwickelt ITdesign Lösungen, die nicht nur aktuelle IT-Herausforderungen bewältigen, sondern auch langfristig den Geschäftserfolg ihrer Kunden sichern. Große Kunden wie Asfinag, Porr, Grazer Wechselseitige Versicherung, Felbermayr, Palfinger und Lenzing AG vertrauten schon auf das Know-how von ITdesign.

Die Geschäftsführung (v. l.): Darius König, Alexander Chvojka, Florian Müllner

TECHNOLOGIE MIT ZUKUNFT

ITdesign bietet ein umfassendes Portfolio an IT-Dienstleistungen, darunter:

- Digitalisierung & Identity-Management: Sichere und effiziente Lösungen für modernes Arbeiten.
- IT-Infrastruktur & Security: Schutz vor Cyberbedrohungen und hochverfügbare IT-Systeme.
- IT-Betrieb & Managed Services: Maßgeschneiderte Betreuung und zuverlässige IT-Landschaften.
- Organisationsentwicklung: Strategische Beratung für zukunftsfähige Unternehmen.

MEILENSTEINE AUS 25 JAHREN ITDESIGN

2000: Gründung der ITdesign Software Projects & Consulting GmbH

2007: Einführung einer innovativen, transparenten Organisationsstruktur

2012: Das bisher größte Projekt würde man heute „modern Client" nennen, mit mehr als 10 Mio. Dienstleistung mit 6 Partnern für im Endausbau 50.000 User

2025: Über 70 Mitarbeitende, 11,9 Millionen Euro Umsatz

MASSGEBLICHER MITGESTALTER DER IT-WELT VON HEUTE UND MORGEN

„Man soll sich ja nicht selbst auf die Schulter klopfen, aber wir sind sehr stolz, seit 25 Jahren die IT-Welt maßgeblich mitzugestalten. Dafür geben wir alles, jeden Tag. Unser Erfolg basiert dabei auf der kontinuierlichen Entwicklung innovativer IT-Lösungen und einer Unternehmenskultur, die auf Vertrauen und Zusammenarbeit setzt", erklärt Alexander Chvojka, Geschäftsführer von ITdesign.

„Wir stehen an der Schwelle zu einer neuen Ära der IT. Unternehmen, die heute auf KI, Automatisierung und Security setzen, sichern sich morgen den Marktvorsprung. ITdesign ist der Partner, der sie dabei begleitet – mit Know-how, Innovation und einem tiefen Verständnis für ihre individuellen Anforderungen", sind sich die drei Geschäftsführer, Alexander Chvojka, Darius König und Florian Müllner, einig.

RÜCKFRAGEN & KONTAKT

ITdesign Software Projects & Consulting GmbH
Anton-Freunschlag-Gasse 49, 1230 Wien
Tel.: +43 1 699 33 99-0
office@itdesign.at
www.itdesign.at


1

EIGENE „SINNE“ FÜR DAS NETZ

Nach 5G kommt 6G. Aber bis es so weit ist, verkürzt erst einmal 5.5G die Wartezeit auf die nächste Mobilfunkgeneration – und hat viele neue Möglichkeiten im Gepäck. Doch dafür muss die Basis stimmen.

5G ist nicht gleich 5G und in vielen 5G-Netzen steckt unter der Oberfläche noch 4G. Das klingt nicht nur kompliziert, sondern ist es auch. Aber der Reihe nach. Um Mobilfunkbetreibern den Umstieg von 4G bzw. LTE (Long Term Evolution) auf den nächsten Evolutionsschritt möglichst leicht zu machen, wurde 5G Non-Standalone (5G NSA) entwickelt. Dieser Standard ist sozusagen ein Hybrid zwischen 4G und 5G. Ein Teil des Netzes, das Kernnetzwerk (oder Core Network), basiert dabei noch auf dem 4G-Standard, den die Netzbetreiber bereits implementiert hatten. Das ist, grob gesagt, der Teil, in dem die Verwaltung sowie Steuerung des Netzes und der Teilnehmer vonstattengeht. Der andere Teil, alles was sich ab den Mobilfunkmasten und bis zu den Endgeräten bzw. Nutzer:innen abspielt, wurde bei 5G Non-Standalone aufgerüstet. Dieses „Upgrade“ löste einige der Versprechen von 5G ein, aber nicht alle. Denn das Core Network, auf dem alles basiert, war schlicht nicht dazu in der Lage.


2

IT-BASIERENDER ANSATZ

»Ein 5G Core ist moderner, ein mehr IT-basierender Ansatz bei der Architektur. Mit so einem sehr softwarebasierenden Modell ist es leichter, Innovationen umzusetzen.«

Ian Fogg, Analyst CCS Insight

EIN EIGENES STÜCK VOM NETZWERK-KUCHEN

Um in den vollen Genuss der vielfältigen Möglichkeiten von 5G zu kommen, unter anderem geringere Latenzen, höhere Geschwindigkeiten und gänzlich

neue Möglichkeiten wie etwa Network Slicing (quasi private Netze mit garantierter Performance innerhalb des Gesamt-Mobilnetzes) braucht es auch die entsprechenden Grundlagen. Die schafft 5G Standalone (5G SA), für das es aber ein neues Kernnetzwerk braucht. Erst dann ist man komplett in die 5G-Welt eingetaucht. Die globale Einführung von 5G SA verläuft regional unterschiedlich. Während der asiatische Raum hier oft eine Vorreiterrolle einnimmt, sind europäische Betreiber zögerlicher. In Österreich hat bislang beispielsweise nur der Anbieter Drei bereits umgestellt.

SYMBIOSE VON NETZ UND KI

Was aufbauend auf der Basis von 5G SA alles möglich wird, zeigte etwa der Technologiekonzern Huawei auf dem vergangenen Mobile World Congress (MWC) in Barcelona. Eine besondere Rolle kommt dabei künstlicher Intelligenz zu. Beim nächsten Schritt, dem Standard 5.5G – auch unter 5G Advanced bzw. 5G A bekannt – gehen die Mobilfunknetze sozusagen eine Symbiose mit KI-Technologien ein. Dadurch ergeben sich auf der einen Seite viele Möglichkeiten, Einsparungen und Vereinfachungen auf der Verwaltungsebene, also im Betrieb der Netze, andererseits sollen so aber auch neue Anwendungsfälle und Geschäftsmodelle für die Nutzer:innen entstehen. Li Peng, Corporate Senior Vice President und President of ICT Sales & Service von Huawei, betonte in seiner Keynote am MWC nicht nur, wie Netzbetreiber mittels künstlicher Intelligenz das volle Potenzial ihrer Netzwerke ausschöpfen können, sondern auch, dass sich die immer stärkere Verbreitung der KI-Nutzung ebenso auf die Anforderungen an die Netze auswirkt: „Wir sind auf dem Weg in eine gänzlich intelligente Welt. Intelligente Anwendungen wachsen stark und stellen neue Anforderungen an die Netze."

Ian Fogg, Analyst von CCS Insight, ging im Gespräch mit NEW BUSINESS am Rande des MWC etwas mehr ins Detail: „Ein 5G Core ist moderner, ein mehr IT-basierender Ansatz bei der Architektur. Mit so einem sehr softwarebasierenden Modell ist es leichter, Innovationen umzusetzen." Zu diesen Innovationen zählt Fogg beispielsweise die deutlich leichtere und schnellere Umsetzung der bereits erwähnten Network Slices, die sich durch KI-Unterstützung in der Provisionierung etwa auch für temporäre Events leicht umsetzen ließen. Mit diesen vom restlichen Netzwerk abgegrenzten Bereichen lässt sich beispielsweise die Servicequalität für gewisse Anwendungen garantieren. Das wird teilweise schon heute gemacht, wie Fogg berichtete: So wurde etwa beim Glastonbury Festival in Großbritannien ein eigener „Slice" für die Bezahlterminals reserviert, um zu gewährleisten, dass Bezahlvorgänge selbst beim größten Datenaufkommen immer zuverlässig funktionieren. Mittels KI soll sich der Aufwand dafür drastisch reduzieren lassen.

Eine weitere Anwendung, die der Analyst nannte, ist IoT. Dafür ist 5G RedCap (kurz für: Reduced Capability) vorgesehen. Der Fokus liegt dabei nicht auf hohen Datenraten oder ultrakurzen Latenzzeiten, sondern vor allem auf möglichst langen Batterielaufzeiten. Er beerbt damit Standards wie Narrowband-IoT (NB-IoT), die heute für solche Zwecke eingesetzt werden, ist aber zukunftssicherer. Denn mit der weiteren Verbreitung von 5G Standalone werden irgendwann auch die dann alten 4G-Infrastrukturen abgeschaltet, so wie es jetzt bei 3G der Fall ist. Es ist auf Dauer nicht wirtschaftlich, diese Strukturen parallel zu betreiben. Außerdem zeigt sich unter anderem beim 2G-Standard die potenzielle Gefahr überholter Technologien, die aus verschiedenen Gründen „am Leben erhalten" werden müssen – die bei 2G eingesetzten Verschlüsselungsverfahren sind längst geknackt und unsicher.

6G FRÜHESTENS AB 2030

Der nächste Schritt wird dann 6G sein. Laut Ian Fogg ist damit „in freier Wildbahn" aber allerfrühestens ab dem Jahr 2030 zu rechnen. Was der nächste Standard im Detail alles an Innovationen enthalten und ermöglichen wird, ist zum derzeitigen Zeitpunkt mehr oder weniger Spekulation. Die Arbeiten daran laufen. Es ist aber davon auszugehen oder zumindest zu hoffen, dass der Umstieg von der moderneren 5G-SA-Architektur durch seine flexiblere, softwarebasierende Natur mit geringerem Aufwand möglich sein wird als bei früheren Entwicklungsschritten.

Fogg stellte in Aussicht, dass dann das Mobilfunknetz möglicherweise eigene „Sinne" bekommt und seine Umgebung wahrnehmen können wird, um sich, unterstützt von künstlicher Intelligenz, beispielsweise selbst an die unterschiedlichen Umweltbedingungen im Wechsel der Jahreszeiten anzupassen, an Muster im Verkehrsaufkommen oder auch an Bewegungsmuster von Personengruppen bzw. einzelnen Personen. Besonders in den höheren Frequenzbereichen, die man für schnellere Datenübertragungen braucht, macht es etwa einen Unterschied, ob ein Baum gerade dicht belaubt ist, er seine Blätter verloren hat oder ob Schnee liegt. Das 6G-Netz der Zukunft könnte das selbst erkennen und sich dementsprechend optimieren, um den Nutzer:innen immer die bestmögliche Performance zu bieten. RNF

3

Li Peng, Corporate Senior Vice President und President of ICT Sales & Service von Huawei, auf dem diesjährigen MWC

Fotos: Freepik/a to z (1), RNF (2), Huawei (3)

GAIA-X WIRKT

Beim International Digital Security Forum 2025 diskutierten internationale Expert:innen über die Zukunft souveräner Datenräume. Im Fokus: Gaia-X als Basis für resiliente, wettbewerbsfähige digitale Ökosysteme.

Im Rahmen des diesjährigen International Digital Security Forums (IDSF) Anfang Juni fand unter dem Titel „The Next Generation of Trusted Data Sharing (Gaia-X)" eine international besetzte Diskussion statt, die sich ganz der Zukunft souveräner digitaler Ökosysteme widmete. Unter der Leitung von Roland Fadrany, Chief Operating Officer der Gaia-X-Initiative, diskutierten Senadin Alisic (Strategy Advisor, Combitech AB, Schweden), Detlef Eckert (Gründer von Deep Digital Consulting B.V., Autor von „40 Years of European Digital Policies", Belgien) und Insuk Kim (Präsidentin der Korean-German Association of Economics and Management (KDGW), CEO des HANDA-Forums, Südkorea) über die entscheidende Rolle souveräner Datenräume für eine resiliente und wettbewerbsfähige digitale Wirtschaft. „Gaia-X ermöglicht Unternehmen durch ein globales, standardisiertes und transparentes Trust Framework, Daten vertrauensvoll und souverän zu nutzen. Weil Daten zum zentralen Asset für digitale Ökosysteme und KI-Strategien geworden sind, ist dieses Trust Framework das Fundament für die Wettbewerbsfähigkeit in globalen Wertschöpfungsketten. Damit die Teilnehmenden ihre digitale Souveränität wahren können, hat Gaia-X eine Reihe föderierter Vertrauensdienste implementiert, die von unabhängigen Gala-X Digital Clearinghouses betrieben werden. Dadurch entfällt die Notwendigkeit zentraler Plattformbetreiber", erklärt Fadrany

V.l.n.r.: Detlef Eckert, Roland Fadrany, Senadin Alisic, Insuk Kim

SOUVERÄNE DATENRÄUME SIND BASIS

Insuk Kim strich die besondere Bedeutung von Gaia-X für die wirtschaftliche Zusammenarbeit zwischen Korea und Europa heraus. Sie arbeitet derzeit an Anwendungen und Lösungen zwischen europäischen und koreanischen Unternehmen in den Bereichen Smart Cities, Produktion, Gesundheit und Energie. Digitale Ökosysteme bilden die Grundlage für eine wettbewerbsfähige und selbstbestimmte digitale Wirtschaft. Standardkonforme, souveräne Datenräume bilden die Basis, um sich im Wettbewerb globaler Wertschöpfungsketten behaupten zu können. Diese Session hat gezeigt, wie Gaia-X Unternehmen durch die Nutzung des Gaia-X Trust Frameworks dabei unterstützen kann, Daten vertrauensvoll, souverän und über Unternehmens- und Landesgrenzen hinaus zu nutzen.

Vor dem Hintergrund geopolitischer Spannungen und zunehmender Plattformabhängigkeit unterstrichen die Diskussionsteilnehmer:innen die Dringlichkeit: Souveräne Dateninfrastrukturen sind kein „Nice-to-have", sondern essenziell für wirtschaftliche Zukunftsfähigkeit, Innovationskraft und digitale Resilienz. Mit Gaia-X entwickelt sich ein wachsendes Netzwerk, das technologische Lösungen, regulatorische Prinzipien und internationale Zusammenarbeit vereint. Die Session bei der #IDSF25 machte klar: Datensouveränität ist keine abstrakte Vision, sondern ein globales Gemeinschaftsprojekt und Gaia-X ist ein aktiver Treiber dieses Wandels. BS

Foto: Katharina Schiffl

T-SYSTEMS AUSTRIA GESMBH

Die öffentliche Verwaltung steht vor einem doppelten Umbruch: Digitalisierung und Pensionierungswelle fordern neue Lösungen. T-Systems bietet mit ihren souveränen Cloud-Diensten eine sichere, zukunftsfähige Antwort.

Souveräne Cloud für den digitalen Staat

Gemeinden, Landesverwaltungen und Bundesbehörden stehen gleich vor zwei Herausforderungen: Sie müssen einerseits die digitale Modernisierung ihrer Verwaltungsprozesse vorantreiben und sich gleichzeitig auf den bevorstehenden demografischen Wandel – die vielen Pensionierungen – vorbereiten. Zwar gilt der öffentliche Sektor noch immer eher als Nachzügler in Sachen Digitalisierung, hat er doch in den letzten Jahren einige wichtige Digitalisierungsprojekte umgesetzt. Ein erfolgreiches Beispiel ist hierbei das Portal FinanzOnline, über das Anträge wie die Arbeitnehmerveranlagung direkt an das Finanzamt übermittelt werden können. Das soll jedoch erst der Anfang sein. Weitere Schritte in Richtung Digitalisierung sind geplant, um den Abbau von Bürokratie voranzutreiben sowie Bürger:innen effiziente und sichere digitale Dienstleistungen anzubieten.

Parallel zeichnet sich bis 2034 eine erhebliche Pensionierungswelle ab, bei der viel Fachwissen verloren gehen könnte. Gleichzeitig fehlt es oft an Ressourcen, um neues Personal schnell einzuarbeiten. Angesichts von Kostendruck und Personalmangel sollen moderne Technologien wie künstliche Intelligenz (KI) und automatisierte Abläufe gezielt entlasten: durch die Digitalisierung von Fachwissen, beschleunigte Prozesse und mehr Zeit für den direkten Kontakt mit den Bürger:innen. Aber was braucht es aus technischer Sicht für dieses Zukunftsszenario?

Eduard Kowarsch, Head of Cloud Services T-Systems Austria

Cloud ist nicht gleich Cloud

Mit der zunehmenden Digitalisierung wächst die Komplexität der Aufgaben erheblich, denn öffentliche Einrichtungen verarbeiten immer größere Mengen sensibler Daten – von personenbezogenen Informationen bis hin zu sicherheitsrelevanten Dokumenten. Dies bringt eine entsprechende Verantwortung mit sich, der nur mit den höchsten Standards in puncto Datenschutz und Sicherheit entsprochen werden kann. Es braucht einen Ort, an dem diese Daten gespeichert und verwaltet werden können: eine Cloud. Aber nicht irgendeine, denn herkömmliche Public-Cloud-Lösungen stoßen bei den speziellen Anforderungen des öffentlichen Sektors oft an ihre Grenzen. Ein wesentlicher Kritikpunkt liegt in der Tatsache, dass viele dieser Dienste über internationale Rechenzentren betrieben werden, wodurch die Gefahr besteht, dass wir die Kontrolle über unsere Daten und auch über den Zugriff verlieren.

Durch den Einsatz von Sovereign-Cloud-Lösungen von T-Systems wird hingegen sichergestellt, dass sensible Daten nicht in Drittländer abfließen und dass vor allem europäische Datenschutzbestimmungen DSGVO-konform eingehalten werden. Dieser Aspekt ist für die öffentliche Hand von großer Bedeutung, weshalb T-Systems eine Cloud-Lösung entwickelt hat, die speziell auf den öffentlichen Sektor zugeschnitten ist. Sie liefert höchste Anforderungen an Datensouveränität, Sicherheit und Rechtskonformität.

Beratung, Migration und Betrieb aus einer Hand

T-Systems liefert nicht nur die Infrastruktur, sondern begleitet Institutionen des öffentlichen Sektors entlang des gesamten Prozesses – von der strategischen Beratung über die technische Umsetzung bis hin zum sicheren Betrieb. Seit vielen Jahren bietet T-Systems souveräne IT-Services an, die sich auch kontinuierlich weiterentwickeln. Das Portfolio ist weit gefächert: von verschlüsselten Public-Cloud-Lösungen bis hin zu voll souveränen Lösungen, basierend auf Open Source. Je nach Lösungsansatz können alle drei Dimensionen digitaler Souveränität – Datenhoheit, Betriebskontrolle und technologische Unabhängigkeit – abgedeckt werden. Eine souveräne Cloud bedeutet dabei vor allem eines: die vollständige Kontrolle über digitale Prozesse zu besitzen, frei von Abhängigkeiten gegenüber Drittstaaten. Mit dem Rückhalt der technologischen Infrastruktur von T-Systems gibt es bei Digitalisierungsthemen im öffentlichen Sektor demnach nur eine Richtung: vorwärts.

RÜCKFRAGEN & KONTAKT
T-Systems Austria GesmbH
Rennweg 97–99, 1030 Wien
Tel.: +43 570 57-0
kommunikationAT@t-systems.com
www.t-systems.at

Das Rechenzentrum bietet im Endausbau Platz für 204 Serverracks bzw. für ca. 9.000 Server.

DIGITALES HERZSTÜCK FÜR LINZ

Mit dem neuen IT- und Data Center stärkt die Linz AG Telekom die digitale Infrastruktur der Stadt. Das energieeffiziente Rechenzentrum punktet mit modernster Technik, höchster Sicherheit und nachhaltiger Kühlung durch Fernkälte.

Der Bedarf bei Unternehmen an hochqualitativen Möglichkeiten für die Verwaltung ihrer Daten steigt laufend. Als verantwortungsvoller IT- und Telekommunikationsdienstleister hat sich die Linz AG Telekom deshalb rechtzeitig für den Bau eines weiteren, hocheffizienten Rechenzentrums entschieden. Am 27. Mai wurde das neue IT- und Data Center feierlich eröffnet. Am 2. Juni 2025 folgt die Inbetriebnahme. Das neue IT- und Data Center verfügt über zukunftsweisende Technik, zertifiziert nach den neuesten Normen, und ist für höchste Ansprüche an Innovation, Sicherheit und Leistung gerüstet. Es verfügt über rund 600 m^2 Serverfläche. Damit bietet das Rechenzentrum im Endausbau Platz für 204 Serverracks auf zwei Ebenen bzw. für ca. 9.000 Server. Die beiden Serverräume bzw. -ebenen verfügen jeweils über 102 Server- bzw. IT-Racks.

Mit der Integration des neuen IT- und Data Centers ins multifunktionale Netzgebäude der Linz AG-Tochter Linz Netz GmbH wurde auch in puncto nachhaltiger Standortwahl ein neuer Maßstab gesetzt. Beispielsweise wird für die Kühlung des neuen Rechencenters Fernkälte aus der ebenfalls im Netzgebäude befindlichen Fernkältezentrale eingesetzt. Die Abwärme aus dem IT- und Data Center wiederum wird künftig das Netzgebäude beheizen. Die bepflanzte Grünfassade ist ein sichtbares weiteres Beispiel für Nachhaltigkeit. Die Linz AG investiert hier insgesamt rund 14 Millionen Euro.

MODERNE INFRASTRUKTUR TRIFFT AUF HÖCHSTE SICHERHEITSSTANDARDS

Bürgermeister Dietmar Prammer, Aufsichtsratsvorsitzender der Linz AG begrüßt die Eröffnung: „Mit dem neuen IT- und Data Center setzen wir einen weiteren Meilenstein für die digitale Zukunft unserer Stadt. Auf rund 600 m² Serverstellfläche entsteht Raum für bis zu 9.000 Server – betrieben mit Energieeffizienz und modernster Sicherheitsarchitektur.

Mit der bepflanzten Fassade will die Linz AG ein sichtbares Zeichen für Nachhaltigkeit setzen.

Besonders freut mich, dass dieses Rechenzentrum höchste technologische Maßstäbe setzt sowie ein Vorzeigeprojekt für Nachhaltigkeit ist: Die Fernkälteversorgung sowie die Nutzung der Abwärme zur Gebäudebeheizung zeigen eindrucksvoll, wie Innovation und Klimaschutz Hand in Hand gehen können. Ich gratuliere der Linz AG Telekom und allen Projektbeteiligten zur zukunftsweisenden Investition in den Standort Linz."

HÖCHSTE VERSORGUNGSSICHERHEIT DER LINZ AG GILT AUCH FÜR DATEN

Linz-AG-Generaldirektor Erich Haider sagte bei der Eröffnung: „Die rasche und sichere Verfügbarkeit von Daten zählt längst zu den Grundbedürfnissen unserer Zeit und ist ein wichtiger Standortfaktor. Daher freut es mich, dass die Linz AG auch auf diesem Gebiet Maßstäbe setzt. Mit unserem Geschäftsbereich Linz AG Telekom haben wir ein breites Angebot für Unternehmen. Ein Segment ist die sichere Verwaltung von Daten in modernen Rechenzentren. Ab sofort verfügt die Linz AG Telekom über zwei IT- und Data Center. Das erhöht unser Angebot an hochqualitativen Serverstellplätzen. Zudem können Unternehmen nun ihre Daten auf zwei Standorte aufteilen und somit die Sicherheit noch einmal erhöhen. Das neue Netzgebäude unterstreicht durch das Rechenzentrum seine informelle Bezeichnung ‚digitales Herz der Stadt Linz'."

V. l. n. r.: Markus Past, Leiter Linz AG Telekom, Jutta Rinner, Vorstandsdirektorin Linz AG, Erich Haider, Generaldirektor Linz AG, Dietmar Prammer, Bürgermeister Linz, Josef Siligan, Vorstandsdirektor Linz AG

Fotos: Linz AG/Fotokerschi

SYNERGIEN WERDEN FÜR DAS KLIMAKONZEPT DES RECHENZENTRUMS GENUTZT

Linz AG-Vorstandsdirektor Josef Siligan ergänzt: „Ein Alleinstellungsmerkmal des neuen IT- und Data Centers ist die Integration ins Multifunktionsgebäude der Linz Netz GmbH. Der vielleicht größte Vorteil liegt in der optimalen Synergienutzung, die insgesamt zu den Stärken der Linz AG zählt. Wir können hier die ebenfalls im Gebäude integrierte Fernkältezentrale für die wichtige Kühlung des Rechenzentrums nutzen. Gleichzeitig wird das IT- und Data Center künftig mit seiner Abwärme das neue Netzgebäude beheizen. Mit dem ebenfalls im Netzgebäude befindlichen neuen Umspannwerk stärken wir nicht nur die Stromversorgung in Linz, sondern sichern auch die redundante Stromversorgung unseres Rechenzentrums ab. Ein weiteres Synergieplus für die Businesskunden ergibt sich durch die bereits vorhandenen Tiefgaragenplätze im neuen Netzgebäude." BS

ETC – ENTERPRISE TRAINING CENTER

Über 900 IT-Fachleute und Wirtschaftsentscheider:innen informierten sich bei der techConference 25 über praxisnahe KI-Lösungen zur Automatisierung von Prozessen sowie aktuellste Sicherheitsstrategien.

Die größte IT-Konferenz Österreichs

Mehr als 70 Sessions und Workshops vermittelten den Teilnehmenden wertvolles Know-how.

■ Schon seit 2015 wächst die Community der techConference kontinuierlich – jedes Jahr mit faszinierenden Einblicken in die neuesten Microsoft- und Tech-Trends, wertvollen Netzwerkmöglichkeiten und frischen Perspektiven von und mit internationalen Top-Expert:innen, Branchenpionier:innen und Vordenker:innen. Zu der größten IT-Konferenz Österreichs versammelten sich in diesem Jahr am 3. und 4. Juni in der Messe Wien mehr als 900 IT-Fachleute und Wirtschaftsentscheider:innen, um sich von den Speaker:innen frische Insights aus den Themengebieten „AI, Data & Apps", „Business Applications", „Power Platform & Developer", „Security", „Infrastructure" sowie „HR, Skilling & Recruiting" zu holen.

Zusätzlich zu den inspirierenden Keynotes der Expert:innen auf den insgesamt drei Bühnen gab es auch exklusive Workshops in mehreren Räumen, um vor Ort praktische Skills zu erwerben.

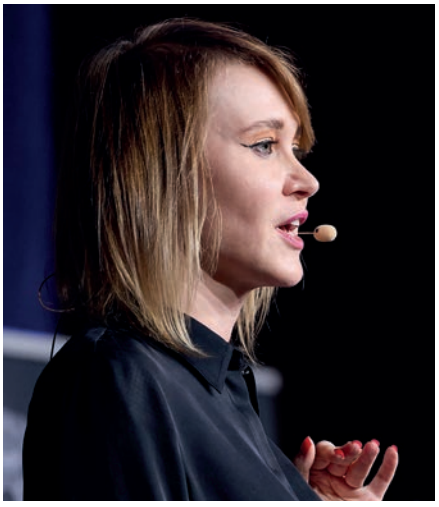
Know-how für den gezielten KI-Einsatz

Besonderes Augenmerk wurde bei der Planung der techConference 25 auf das Thema künstliche Intelligenz gelegt, um den Teilnehmenden den Einstieg in das KI-Zeitalter zu erleichtern. Denn während 35 Prozent der Unternehmen aus der Finanzbranche und 31 Prozent der Industrieunternehmen bereits strategisch auf künstliche Intelligenz setzen, haben laut dem EY KI Readiness Check bisher nur zwölf Prozent aller österreichischen Unternehmen KI fest in ihr Geschäftsmodell integriert.

„Diese Zahlen verdeutlichen die große KI-Kluft in den heimischen Unternehmen. Trotz verfügbarer Technologie fehlt vielen Unternehmen das Know-how für den gezielten KI-Einsatz", sagte Christoph Becker, Organisator der techConference und Geschäftsführer des ETC (Enterprise Training Center). Deswegen zielte die Konferenz mit über 70 praxisorientierten Sessions und Workshops darauf ab, diese Lücke zu schließen und das notwendige Know-how für den Einstieg ins KI-Zeitalter zu vermitteln. Hunderte IT-Fachleute nutzten die Gelegenheit, bei der größten IT-Konferenz Österreichs in der Messe Wien die neuesten KI-Fortschritte live zu erleben.

Neue Microsoft-Rechenzentren als Fundament für die digitale Transformation

Zugleich markierte die techConference 25 ein weiteres Highlight im Rahmen der Launchphase von Microsofts Cloudregion Österreich und bot den perfekten Rahmen für die „Microsoft Data Center Lounge", in der sich die Teilnehmer:innen von den anwesenden Expert:innen Firsthand-Einblicke holen sowie über die Angebote und Lösungen der Launchpartner zum Start der Cloudregion informieren konnten.


V.l.n.r.: Christoph Becker, Geschäftsführer ETC, die Security-Expert:innen Paula Januszkiewicz und Sami Laiho.

Zum Auftakt der Konferenz betonte Florian Slezak, Cloud Region Lead bei Microsoft Österreich, die transformative Kraft der neuen Microsoft-Rechenzentrumsregion in Ostösterreich: „Mit diesen Rechenzentren können österreichische Unternehmen Digitalisierung mit lokaler Datenhaltung und -verarbeitung sowie kürzester Latenz realisieren." Der Betrieb mit 100 Prozent erneuerbarer Energie aus Österreich unterstreiche zudem das Nachhaltigkeitsengagement. Diese Infrastrukturinvestition wurde als wichtiger Katalysator für die digitale Souveränität und Wettbewerbsfähigkeit des Standorts gewertet.

KI-Agenten werden massentauglich

Eines der zentralen inhaltlichen Highlights der Konferenz war das Thema KI-Agenten – autonome Systeme, die komplexe Aufgaben selbstständig erledigen können. Martina Grom und Co-Referent Toni Pohl zeigten beispielsweise im Workshop „Build Your Own Agents: From No-Code to Pro-Code", wie Teilnehmende ohne tiefgreifende Programmierkenntnisse eigene KI-Assistenten entwickeln und in bestehende Microsoft-365-Umgebungen integrieren können. Andreas Aschauer, Senior Technology Specialist bei Microsoft, und Helmut Wimmer, Cloud Solution Architect, präsentierten im Talk „(Autonomous) Agents mit Copilot Studio", wie Low-Code-Plattformen die schnelle und effiziente Entwicklung von autonomen KI-Agenten ermöglichen.

Cybersicherheit: Lernen von den Besten

Mit den Chancen der KI wachsen zugleich auch die Risiken. Die polnische Harvard-Absolventin Paula Januszkiewicz, renommierte Enterprise-Security-Spezialistin, präsentierte in „Lessons from the Field" beeindruckende Fallbeispiele – von kompromittierten Domänenadministratoren bis hin zu komplexen Ransomware-Attacken – und zeigte, wie sich Incident-Response-Prozesse optimieren lassen.

Der Finne Sami Laiho, einer der weltweit führenden Cybersecurity-Experten für Windows-Systeme und bekannt als „Windows-Guru", skizzierte in „Cybersecurity 2025/2026" die künftigen Bedrohungsszenarien und enthüllte in „11 Wege, Windows 11 zu hacken – und wie man es verhindert" gefährliche Lücken sowie wirksame Gegenmaßnahmen. Die von Paula Januszkiewicz und Sami Laiho gewonnenen – und mit den Teilnehmer:innen geteilten – Erkenntnisse machen deutlich: Ohne ein durchdachtes Sicherheitskonzept öffnet die KI-Integration neue Angriffsvektoren. Österreichische Unternehmen sind deshalb gefordert, ihre Sicherheitsarchitekturen parallel zur Einführung von KI-Anwendungen grundlegend zu überarbeiten.

Breite KI-Nutzung nur durch kontinuierlichen Wissensaufbau

Bei der techConference 25 wurde klar: Künstliche Intelligenz bietet großes Potenzial, doch in vielen österreichischen Firmen gibt es noch Schwierigkeiten bei der Implementierung. Zwar sind die nötigen Technologien und Infrastrukturen inzwischen vorhanden, aber es fehlt an Fachwissen und angepassten Geschäftsmodellen. Wenn Österreich diese Probleme nicht systematisch angeht, läuft das Land Gefahr, nur KI-Lösungen aus dem Ausland zu nutzen. Das würde die Wettbewerbsfähigkeit und digitale Unabhängigkeit schwächen. Deshalb sind mehr Bildungsangebote und praktische Trainings nötig, um die Lücke zwischen Technik und Unternehmenspraxis zu schließen.

Die Planungen für die nächste techConference laufen bereits. Der Termin steht noch nicht endgültig fest, aber streichen Sie sich schon jetzt im Kalender den Juni 2026 rot an. Denn dann versammelt sich die Tech-Community wieder in Wien zur größten IT-Konferenz Österreichs, um tief in aktuelle Themen einzutauchen und die einzigartigen Networking-Möglichkeiten zu nutzen.
https://techconference.at/

ETC

RÜCKFRAGEN & KONTAKT
ETC – Enterprise Training Center
Modecenterstraße 22/Office 4/5. Stock
1030 Wien
Tel.: +43 1 533 17 77-0
info@etc.at, **www.etc.at**

Anzeige • Fotos: ETC/APA-Fotoservice/Schedl

1

KEINE KOMPROMISSE

Ein ERP-System ist das Rückgrat effizienter Unternehmensprozesse. Daher lohnt es sich, bei Auswahl und Einführung keine Kompromisse einzugehen und einige Bereiche besonders sorgfältig zu planen.

Unternehmen sollten bei ERP-Systemen keine Kompromisse eingehen“, empfiehlt Christian Biebl, Geschäftsführer des Stuttgarter ERP-Herstellers Planat. In einer Ära, in der der produzierende Mittelstand mit Lieferkettenproblemen, Fachkräftemangel und dynamischen Märkten kämpft, ist eine maßgeschneiderte ERP-Software essenziell, die exakt den Anforderungen genügt.
In der heutigen Geschäftswelt sind Systeme für Enterprise Resource Planning unverzichtbar. Sie sind das zentrale Steuerungsinstrument, das alle wesentlichen Unternehmensbereiche – von Vertrieb und Einkauf über Produktion und Logistik bis hin zu Finanzen und Personal – miteinander verbindet und integriert. Ein leistungsfähiges ERP-System ermöglicht effizientere Abläufe, fundiertere Entscheidungen und verschafft Unternehmen einen klaren Wettbewerbsvorteil. Angesichts dieser fundamentalen Bedeutung ist es entscheidend, bei der Einführung und Nutzung eines ERP-Systems einen konsequenten Kurs zu verfolgen und kritische Bereiche nicht durch unüberlegte Kompromisse zu schwächen.

DIE FALLE DER KURZFRISTIGEN KOMPROMISSE

Die Implementierung eines ERP-Systems ist ein Großprojekt, das erhebliche interne Ressourcen bindet. Es ist nur menschlich, dass im Projektverlauf der Wunsch entsteht, den Prozess

Egal ob im Lager, im Büro oder in der Produktion: ERP-Systeme funktionieren nur, wenn man bei der Implementierung und im Betrieb keine Kompromisse eingeht.

zu beschleunigen oder Kosten zu senken, indem man von den ursprünglichen Plänen abweicht. Dafür geht man gerne einige Kompromisse ein.

Um sicherzustellen, dass ein ERP-System sein volles Potenzial entfaltet und eine solide Grundlage für das Unternehmen bildet, gilt es, in einigen Schlüsselbereichen kompromisslos zu agieren. Ein ERP-System kann sein volles Potenzial nur dann entfalten, wenn es auf einer klaren strategischen Basis aufbaut. Dazu gehört zunächst eine fundierte Anforderungserhebung mit präziser Analyse bestehender Prozesse und einer definierten Zielstruktur – unter Einbindung aller relevanten Stakeholder. Auf dieser Grundlage erfolgt die Auswahl eines passenden Systems und eines zuverlässigen Implementierungspartners, wobei neben Funktionalität auch Architektur, Integrationsfähigkeit, Skalierbarkeit und langfristige Kosten berücksichtigt werden müssen. Von zentraler Bedeutung ist zudem die Datenqualität: Nur bereinigte, verlässliche Daten und ein professionelles Stammdatenmanagement sichern langfristig den Systemnutzen. Eine konsequente Teststrategie mit realitätsnahen Szenarien hilft dabei, Fehler frühzeitig zu erkennen. Gleichzeitig ist die Akzeptanz der Nutzer:innen entscheidend: Change-Management-Maßnahmen, zielgerichtete Schulungen und fortlaufender Support sorgen für eine hohe Nutzerzufriedenheit. Abgerundet wird ein erfolgreicher ERP-Rollout durch strenge Sicherheits- und Compliance-Vorgaben sowie die nahtlose Integration in die bestehende Systemlandschaft – nur so entstehen durchgängige Prozesse und eine konsistente Datenbasis im gesamten Unternehmen.

STRATEGISCHE INVESTITION IN DIE ZUKUNFT

Das Eingehen von Kompromissen führt typischerweise zu signifikanten negativen Auswirkungen. Dazu gehören erhöhte Betriebskosten durch manuelle Nacharbeit und Fehlerkorrekturen oder eine mangelnde Verlässlichkeit der Datenbasis, was zu suboptimalen oder falschen Geschäftsentscheidungen führen kann. Weitere mögliche Folgen sind eine geringe Anwenderakzeptanz und ineffiziente Systemnutzung, zusätzliche Kosten und Verzögerungen, potenzielle Compliance-Verstöße sowie eine limitierte Skalierbarkeit und Zukunftsfähigkeit des Systems. Christian Biebl erklärt: „Die Implementierung eines ERP-Systems ist eine strategische Investition, die die Leistungsfähigkeit und die Agilität eines Unternehmens auf lange Sicht prägt. Angesichts dieser Tragweite ist ein disziplinierter, sorgfältiger und in seinen Kernaspekten kompromissloser Ansatz nicht nur wünschenswert, sondern eine Notwendigkeit."

Organisationen, die bereit sind, in eine gründliche Planung, die Auswahl der optimal passenden Lösung, eine methodische Implementierung, die Sicherung der Datenqualität, umfassendes Testen, die Befähigung ihrer Mitarbeiter:innen sowie die Integration und Sicherheit des Systems zu investieren, schaffen eine robuste und zukunftsfähige Grundlage. Sie positionieren sich für operationelle Exzellenz, fundierte, datengestützte Entscheidungen und die notwendige Flexibilität, um in einem sich ständig wandelnden Marktumfeld erfolgreich zu agieren. BS

STRATEGISCHE INVESTITION

»Die Implementierung eines ERP-Systems ist eine strategische Investition, die die Leistungsfähigkeit und die Agilität eines Unternehmens auf lange Sicht prägt.«

Christian Biebl, Geschäftsführer Planat GmbH

Fotos: Frolopiaton Palm/Freepik (1+3), tsyhun/Freepik (2), Planat GmbH (4)

AUS DEM ORBIT NACH ÖSTERREICH

Andreas J. Wagner, Geschäftsführer von SAP Österreich, im Interview über seine neue Aufgabe, den digitalen Entwicklungsstand heimischer Unternehmen und seine Ziele für den heimischen Markt.

Der gebürtige Steirer Andreas J. Wagner, seit Jahresanfang Geschäftsführer von SAP Österreich, ist seit rund 18 Jahren für das europäische Softwareunternehmen tätig. Zuletzt zeichnete er global für digitalisierte Lieferketten verantwortlich. Für seine neue Aufgabe hat er sich einige Dinge vorgenommen. Im Gespräch mit NEW BUSINESS spricht Wagner über seine Ziele, wie er den digitalen Entwicklungsstand in Österreich einschätzt und welche Potenziale künstliche Intelligenz und Cloud den heimischen Unternehmen bieten.

HERR WAGNER, WIE WAR ES, ALS GLOBALER CHIEF BUSINESS OFFICER FÜR DIGITALISIERTE LIEFERKETTEN WIEDER IN EINE LOKALE ROLLE ZU SCHLÜPFEN?

In der globalen Rolle fühlt man sich wie ein Satellit, der im Orbit kreist. Man hat diesen Gesamtüberblick und einen starken strategischen Fokus. Ich war auch global in einer kundenspezifischen Rolle und habe viele Kundenbesuche in vielen Ländern gemacht. So lernt man andere Kulturen, andere Märkte kennen und sieht auch das Potenzial in diesen Märkten. Das ist eine sehr spannende Rolle.

Das Interessante in der Geschäftsführungsrolle ist auf der anderen Seite, dass ich nun End-to-End-Verantwortung für einen Markt und einen starken persönlichen Impact auf ein Land habe. Somit baut man eine ganz andere Beziehung zu den Kunden auf. Das ist sehr motivierend. Vor meiner Rückkehr nach Österreich hat ein Kollege zu mir gesagt: „Andreas, there is one thing I can tell you. There is nothing more rewarding than being the managing director of your own home country.“ Er hatte recht. Das ist etwas, was Spaß macht.

ALS „SATELLIT" HATTEN SIE EINEN GUTEN ÜBERBLICK. WIE WÜRDEN SIE DEN DIGITALEN ENTWICKLUNGSSTAND DER ÖSTERREICHISCHEN UNTERNEHMEN EINSCHÄTZEN – ETWA IN SACHEN KI?

Was mir an den Amerikanern gefällt, ist ihre positive Grundeinstellung. Die fehlt manchmal hier in Österreich. In den Medien liest man viel Negatives, obwohl es viele positive Dinge zu berichten gibt. Aber ja, ich glaube im Bereich der Digitalisierung – gerade, was KI betrifft – hat Österreich noch Nachholbedarf. Einer Studie zufolge nutzen nur 8 Prozent der Unternehmen in Österreich generative KI, in Europa sind es im Durchschnitt schon 13,5 Prozent.

Es wäre wichtig, bei der digitalen Bildung mehr zu machen. Die Schere zwischen dem Zugang zu neuen Technologien und der Weiterentwicklung der digitalen Bildung geht immer weiter auf. So entstehen dieser soziale Schmerz und die Angst vor neuen Technologien, was dann dazu führt, dass zum Teil überreguliert wird. Das spürt man in Europa und in Österreich stark.

AN WELCHEN PUNKTEN SOLLTE MAN ANSETZEN, UM DIESE SITUATION ZU VERBESSERN?

Neben der Bildung wäre es auch wichtig, den Standort für Unternehmen und Entwickler, die sich mit dem Thema KI beschäftigen, attraktiver zu machen – mehr Netzwerke, mehr Cluster, mehr Förderung. Natürlich fehlt es auch ein bisschen an Risikokapital, gerade für Start-ups.

IN DEN VERGANGENEN MONATEN IST VIEL BEWEGUNG IN DAS THEMA EUROPÄISCHE IT-SOUVERÄNITÄT GEKOMMEN. IN WELCHER ROLLE SIEHT SICH DIE SAP, ALS EINES DER GRÖSSTEN EUROPÄISCHEN IT-UNTERNEHMEN?

Unser Vorstand hat klar seine Absicht erklärt, in eine europäische Cloud zu investieren. Wir sind bereit, beim Aufbau einer europäischen Cloud eine Führungsrolle einzunehmen. Dazu steht SAP als Unternehmen. Wir bauen zum Beispiel in Deutschland die Delos Cloud für den Verwaltungsbereich auf. Momentan fließt sehr viel Entwicklung in den Bereich der Sovereign Cloud.

EUROPA WIRD SICH NICHT VON HEUTE AUF MORGEN VON ANBIETERN AUS ANDEREN REGIONEN DER WELT UNABHÄNGIG MACHEN KÖNNEN. VON WELCHEN ZEITRÄUMEN SPRECHEN WIR IHRER MEINUNG NACH?

Es müssen ja nicht gleich alle Prozesse in die Sovereign Cloud. Aber ich kann mir durchaus vorstellen, dass in den nächsten fünf Jahren einiges passieren könnte und dass kritische Kernprozesse in eine Sovereign Cloud wandern können.

VON DER CLOUD ZURÜCK ZUR KI. WOBEI KANN KI AUS SICHT VON SAP DIE ANWENDERUNTERNEHMEN AM MEISTEN UNTERSTÜTZEN?

KI kann in allen Bereichen Kosten reduzieren und Effizienz erhöhen. Ein ganz wichtiger Bereich sind entscheidungsrelevante Informationen. Mit unserer neuen SAP Business Data Cloud geben wir Unternehmen die Möglichkeit, sowohl externe als auch interne, strukturierte und unstrukturierte Daten zu standardisieren. Für den Einsatz von KI braucht es auf der einen Seite vertrauensvolle Daten, aber auch starke Prozesse. SAP kann extrem viel dazu beitragen, dass die richtigen Daten zur schnellen und besseren Entscheidungsfindung zur Verfügung stehen. Das könnte zu einem KI-Meilenstein werden.

Generell lässt sich aber auch vieles automatisieren, Prozesse lassen sich papierlos machen, Bürokratie in unterschiedlichen Bereichen kann reduziert werden, Reports – denken Sie nur an ESG-Reports – lassen sich automatisch generieren. Es gibt vielfältige Anwendungsfälle.

Man muss aber immer zwischen genereller künstlicher Intelligenz und generativer künstlicher Intelligenz unterscheiden. Heute wird viel als KI bezeichnet, das es schon länger gibt und was man früher auch anders genannt hat. Unser KI-Agent Joule zum Beispiel ist eine agentische KI, die über alle unsere Prozesse hinweg unterstützt.

ENTSCHEIDUNGSRELEVANTE INFORMATIONEN

»KI kann in allen Bereichen Kosten reduzieren und Effizienz erhöhen. Ein ganz wichtiger Bereich sind entscheidungsrelevante Informationen.«

Andreas J. Wagner, Geschäftsführer SAP Österreich

SAP SITZT AN EINER ZENTRALEN SCHLÜSSELSTELLE ZWISCHEN DATEN UND KI, UM DARAUS EINEN MEHRWERT ZU GENERIEREN.

Genau. Dieses Zusammenspiel zwischen Prozessen, Daten und KI empfinden wir als extrem wichtig. In unseren Systemen laufen viele Daten zusammen – auch Daten, die nicht aus SAP-Systemen kommen. KI-Systeme brauchen diese Daten, und mit der SAP Business Data Cloud versuchen wir, das Ganze zu standardisieren.

DIE KRUX SIND IMMER DIE DATEN, BESONDERS IM ZUSAMMENHANG MIT KI. HAT SICH DIE DATENQUALITÄT IN DEN FIRMEN – ODER SAGEN WIR DATENDISZIPLIN – IN DEN LETZTEN JAHREN VERBESSERT?

Eher im Gegenteil. Es werden immer mehr Daten produziert und immer mehr davon sind unstrukturierte Daten, die ebenfalls einbezogen werden müssen. Es geht darum, diese Daten aufzubereiten, zu standardisieren, auszulesen und in den Business-Kontext zu setzen.

Fotos: RNF

DA KOMMT AUCH WIEDER KI INS SPIEL?
Absolut. Da kann KI eine sehr, sehr große Rolle spielen.

WIE IST ES BEI DEN UNTERNEHMEN, MIT DENEN SIE SPRECHEN, UM DAS VERSTÄNDNIS DAFÜR, WAS KI WIRKLICH KANN UND IST, BESTELLT?
Es gibt einen großen Hype um das Thema. Da wird der Begriff manchmal vielleicht auch etwas erweitert oder größer gemacht, als er tatsächlich ist. Nichtsdestotrotz bietet KI eine unheimliche Chance. Wir lernen jeden Tag dazu, was man mit KI machen kann. In einer Woche wird die Situation wieder eine neue sein. Das ist ein extrem spannender Bereich. KI ist ein ganz wichtiger Bestandteil der digitalen Transformation. Wir werden immense Einsparungen und Effizienzsteigerungen sehen, die wir auch in vielen Bereichen brauchen werden, weil wir auch aufgrund der demografischen Situation gar nicht die Ressourcen und das Personal haben, die anstehenden Herausforderungen zu stemmen.

WAS HABEN SIE SICH IN IHRER POSITION ALS ÖSTERREICH-GESCHÄFTSFÜHRER VORGENOMMEN?
Bei uns intern habe ich für 2025 und darüber hinaus das Motto „Collective Power" ausgerufen. Ich möchte alle Bereiche zusammenbringen, weil ich glaube, nur dann, wenn man gemeinsam arbeitet, kann man erfolgreich sein. Collective Power ist für mich der Zusammenschluss aus Vertrieb, der Beratung, der Supporteinheit, aber auch unseren Partnern, unserem Ökosystem. Wir haben Collective Power Awards ausgeschrieben, für die Mitarbeiterinnen und Mitarbeiter Projekte und Erfolge einreichen können. Die Zusammenarbeit als ein großes Ganzes wird damit stärker in den Vordergrund gerückt.
Was mir auch wichtig ist, ist, den Standort Österreich zu stärken. Das heißt, mehr SAP-Experten in Wien zu verankern, sowohl bei uns als auch bei den Kunden und Partnern, und weiter auf einen Wachstumskurs zu setzen – was Umsatz, aber auch was Mitarbeiterinnen und Mitarbeiter betrifft. Wir wollen in diesem Jahr auf über 700 Mitarbeitende wachsen.
Wir setzen auch stark auf den Ausbau unseres Partner-Ökosystems. Aktuell haben wir rund 100 Softwarepartner, die in Österreich tätig sind, mit mehr als 3.000 Mitarbeiterinnen und Mitarbeitern. Dieses Ökosystem ist wichtig, um die Reichweite zu erhöhen, gerade wenn man verstärkt in den Mittelstand geht, aber auch, um Innovationen zu treiben, etwa zum Thema KI. Darüber hinaus haben wir heuer ein eigenes Neukundenteam gegründet und wollen die Zusammenarbeit mit der DSAG *(Anm.: der Verband „Deutschsprachige SAP Anwendergruppe")* und auch die Partnerschaften mit unseren Kunden weiter verstärken.
Die Unterstützung von Unternehmen bei ihrer Transformation in die Cloud ist ein weiteres großes Ziel von mir. Gerade dem Mittelstand kann Cloud sehr viel bringen, weil es oft schwer ist, die notwendigen IT-Ressourcen am Markt zu finden. Insofern ergeben sich dadurch große Chance für den Mittelstand, an Innovationen zu partizipieren und dadurch die eigene digitale Transformation voranzutreiben. RNF

INFO-BOX

SAP NOW AI Tour Vienna
Am 25. September findet in der Marx Halle in Wien die „SAP NOW AI Tour Vienna" statt. Sie bietet den passenden Rahmen, um sich mit Branchenkolleg:innen und SAP-Expert:innen zu aktuellen Themen auszutauschen und herauszufinden, wie KI, Daten und Anwendungen auf innovative Weise kombiniert werden können.
www.sap.com/austria/events/sapnowvienna.html

Fotos: RNF

TRENDS FÜR VERWALTUNGS-IT

Von künstlicher Intelligenz bis hin zum digitalen Humanismus: Das BRZ untersucht im aktuellen Technologieradar 48 Technologien. KI spielt dabei eine immer größere Rolle bei der Entwicklung von IT-Anwendungen.

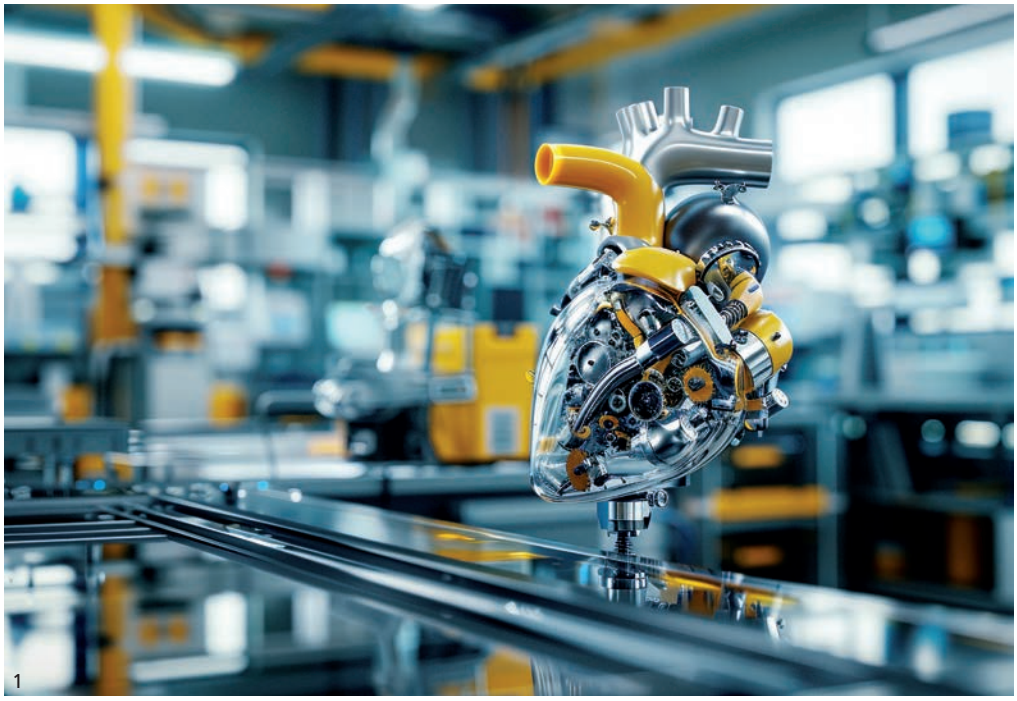
Foto: BRZ

Das vom BRZ (Bundesrechenzentrum) entwickelte Technologieradar berichtet jährlich über IT-Perspektiven und -Trends für den Public Sector. „Mit dem Technologieradar haben wir ein Instrument in der Hand, um Überblick zu schaffen und eine genaue Einordnung der unterschiedlichen IT-Trends und Technologien vorzunehmen. Künstliche Intelligenz hat für die Verwaltung großes Potenzial und kann sehr nutzbringend eingesetzt werden, um Herausforderungen wie etwa die Pensionierungswellen abzufedern. Wir sehen auch einen großen Beitrag zur nachhaltigen Einsparung und zur Unterstützung des Konsolidierungspfades durch den gezielten Einsatz von KI und der Digitalisierung im Allgemeinen. KI entwickelt sich rasend schnell weiter, deshalb müssen wir technisch genau hinschauen, wenn es beispielsweise darum geht, ethische Standards einzuhalten“, erklärt BRZ-Geschäftsführer Roland Ledinger.

SECHS TOP-TRENDS

Das BRZ hat im Technologieradar sechs Top-Trends identifiziert, die die Verwaltungs-IT in den nächsten Jahren prägen werden: Agentic AI, IT for Green, Nutzung synthetischer Daten, Total Experience, Digitaler Humanismus und Digitale Souveränität. Bei Agentic AI geht es um den nächsten Schritt in der Funktionalität von KI-Tools: Sind die bisherigen Chatbots als Content-Erzeuger bekannt, werden die KI-Agenten Aktionen ausführen und Entscheidungen treffen können. „Green IT“ zielt darauf ab, die Informationstechnologie selbst umweltfreundlicher zu gestalten. Bei „IT for Green“ liegt der Fokus darauf, wie IT eingesetzt wird, um allgemeine ökologische Ziele zu erreichen. Insgesamt verfolgt die Branche das Ziel, den CO_2-Fußabdruck der IT-Infrastruktur zu verringern und den Energieverbrauch von Hardware, Software und Rechenzentren zu senken. Im Mittelpunkt des Digitalen Humanismus steht die menschenzentrierte Gestaltung technologischer Entwicklungen. Verantwortungsvolle bzw. vertrauenswürdige KI bezieht sich auf die Entwicklung und den Einsatz künstlicher Intelligenz unter Berücksichtigung ethischer, sozialer und rechtlicher Standards. Ziel ist es, sicherzustellen, dass KI-Systeme transparent, fair, sicher und im Einklang mit Werten und Gesetzen eingesetzt werden. Synthetische Daten sind Daten, die künstlich generiert werden. Sie werden als Ersatz für reale Daten in einer Vielzahl von Anwendungsfällen genutzt, darunter Datenanonymisierung, Entwicklung von KI und maschinellem Lernen, datenschutzgerechte Weitergabe von Daten usw. Die zeitaufwendige und teure Aufgabe der Erstellung von Testdaten kann durch synthetische Daten umgangen werden. Total Experience („Gesamterlebnis“) ist ein Ansatz, der mehrere Disziplinen, etwa User oder Employee Experience miteinander kombiniert. Eine „Total Experience“-Strategie verbindet digitale und nichtdigitale Technologien, um das Vertrauen und die Zufriedenheit der Bürger:innen sowie der Mitarbeiter:innen in die öffentlichen Dienste zu erhöhen und Dienste besser zu personalisieren. Eine solche erhöhte Personalisierung soll eine maßgeschneiderte direkte Ansprache ermöglichen, die auf individuelle Bedürfnisse und Anforderungen von Kunden eingeht.

Durch die zunehmende Digitalisierung der Verwaltung und deren Services ist besonderes Augenmerk darauf zu legen, dass die eingesetzten IT-Produkte und -Dienstleister die digitale Souveränität nicht schwächen oder gar sukzessive abbauen. Digitale Souveränität ist auch ein wesentlicher, gesamteuropäisch zu betrachtender Aspekt bei der Verwendung von Cloud-Services für die öffentliche Verwaltung und beim Einsatz von Open-Source-Software. BS



1

AM PULS DES WANDELS

2025 dürfte ein abermals anspruchsvolles Jahr für die Automobilwirtschaft werden. Steigen die Anforderungen an die Automobilzulieferer, müssen sich ihre Prozesse verändern. Dazu braucht es die IT.

Die aktuelle Krise in der Automobilindustrie stellt Zulieferer vor massive Herausforderungen: Eine schwache Auftragslage und der Wechsel zur Elektromobilität, gepaart mit steigenden Kosten, einem starken Preisdruck durch OEMs sowie der Anspruch, hohe Qualitätsstandards einzuhalten, verzögert eine rasche Erholung der Branche. Die IT schafft die Basis für alle Veränderungen, Innovationen und die nahtlose Zusammenarbeit mit Partnern auf der ganzen Welt. Thomas Forst, Principal Industry Manager Series Production (Schwerpunkt Automotive) bei der All for One Group, beleuchtet die wachsende Bedeutung aktueller IT-Trends und die Chancen, die sie für Automobilzulieferer eröffnen.

ELEKTROMOBILITÄT SORGT FÜR GROSSE UMBRÜCHE

Auch Zulieferer müssen im Zuge dieses Wandels ihr Portfolio anpassen und neu ausrichten. Sie müssen bestehende Komponenten für die E-Mobilität optimieren oder neue Produkte entwickeln. Dabei müssen sie kreativ und innovativ sein und eng mit ihren Geschäftspartnern zusammenarbeiten. Auch Unternehmensstrukturen ändern sich: Geschäftsbereiche werden aufgegeben oder neu hinzugefügt. All das erfordert eine IT-Landschaft, die kontinuierliche Veränderungen zulässt, Kollaboration fördert, neue Technologien bereitstellt und schnelle Innovationszyklen abbilden kann. „Um diese Transformation effizient zu meistern, braucht es ein modernes ERP-System, das maximale Flexibilität bietet und dabei neue und zukünftige Technologien zur Verfügung stellt, um Prozesse zu optimieren. Vor diesem Hintergrund ist der Wechsel auf SAP S/4HANA nicht nur technologische Pflicht, sondern strategische Notwendigkeit“, erklärt Thomas Forst.

AUTOMATISIERUNG UND VERNETZUNG MACHEN DIE PRODUKTION ZUKUNFTSFÄHIG

Smart Factories mit IoT und vernetzten Systemen ermöglichen flexiblere und effizientere Produktionsprozesse. Condition


2


3

Monitoring und Predictive Maintenance helfen dabei, Verschleiß frühzeitig zu prognostizieren, Ausfälle zu vermeiden und Kosten zu senken. Zudem verbindet IoT die Produktion mit dem ERP, sodass Prozesse Ende-zu-Ende automatisiert werden können. Daten aus der Produktion fließen beispielsweise in die Lieferplanung oder werden in einem digitalen Zwilling visualisiert, der den Maschinenpark exakt virtuell abbildet. „Mit einem modernen ERP wie SAP S/4HANA in Kombination mit IoT schaffen Zulieferer somit eine Plattform, die Produktion und Geschäftsprozesse nahtlos verbindet. Das verbessert Planbarkeit und Reaktionsfähigkeit in der Lieferkette und steigert so Flexibilität, Stabilität und Wettbewerbsfähigkeit“, erläutert Thomas Forst.

KI WIRD 2025 WEITERHIN EINE SCHLÜSSELROLLE IN DER AUTOMOBILPRODUKTION SPIELEN

KI-basierte Anwendungen steigern die Effizienz, indem sie Prozesse wie die optische Inspektion, Verfügbarkeitsprüfungen und Predictive Maintenance automatisieren. Um jedoch den größtmöglichen Mehrwert zu erzielen, ist es entscheidend, die individuellen Bedürfnisse und Prozesse jedes Unternehmens zu analysieren und die KI-Nutzung passgenau darauf abzustimmen. Nur so kann KI die Wettbewerbsfähigkeit von Automobilzulieferern langfristig steigern und ihre Produktion nachhaltig optimieren.

VERÄNDERUNGEN DER GLOBALEN MARKTANTEILE UND EDI-STANDARDS

Die Elektromobilität verändert den globalen Automobilmarkt grundlegend. Während China als Leitmarkt für E-Fahrzeuge dominiert, verlagern deutsche Unternehmen ihre Produktion zunehmend ins Ausland, um Kosten zu senken. Die Marktverschiebung zwingt deutsche Zulieferer, ihren Fokus stärker auf internationale Hersteller und Kunden auszurichten. „Ohne Echtzeit-Datenaustausch mittels EDI- und Cloud-Technologien sind die Anforderungen an globale Lieferketten nicht zu bewältigen. Sie sorgen für eine reibungslose Kommunikation und sind unverzichtbar für komplexe Just-in-Time- und Just-in-Sequence-Anlieferungen“, erklärt Thomas Forst.

STRENGERE ESG-VORGABEN ERFORDERN NACHHALTIGE UND RESILIENTE LIEFERKETTEN

Nachhaltige und resiliente Lieferketten werden immer wichtiger, da ab 2025 strengere ESG-Vorgaben für zahlreiche Unternehmen gelten. Die Automobilbranche muss ihre CO_2-Bilanz verbessern und gleichzeitig ihre Lieferketten widerstandsfähiger gegen globale Krisen machen. Resilienz geht dabei Hand in Hand mit neuen Compliance-Regulatorien wie der EU-CSR-Direktive oder dem deutschen Lieferkettensorgfaltspflichtengesetz (LkSG). Die Basis für stabile und nachhaltige Lieferketten ist eine vollständige Transparenz über die gesamten Lieferantenbeziehungen. „Das ist nur mit einer konsequenten Digitalisierung machbar! Der digitale Kern im S/4HANA und der digitale Datenaustausch über EDI, Services oder Business Networks sind die Grundlage. Auch Speziallösungen wie SAP IBP, Ariba und Supply Chain Control Tower helfen, Transparenz in komplexen Liefernetzwerken zu schaffen, Risiken frühzeitig zu erkennen und alternative Lieferanten effizient zu integrieren“, so Thomas Forst. BO

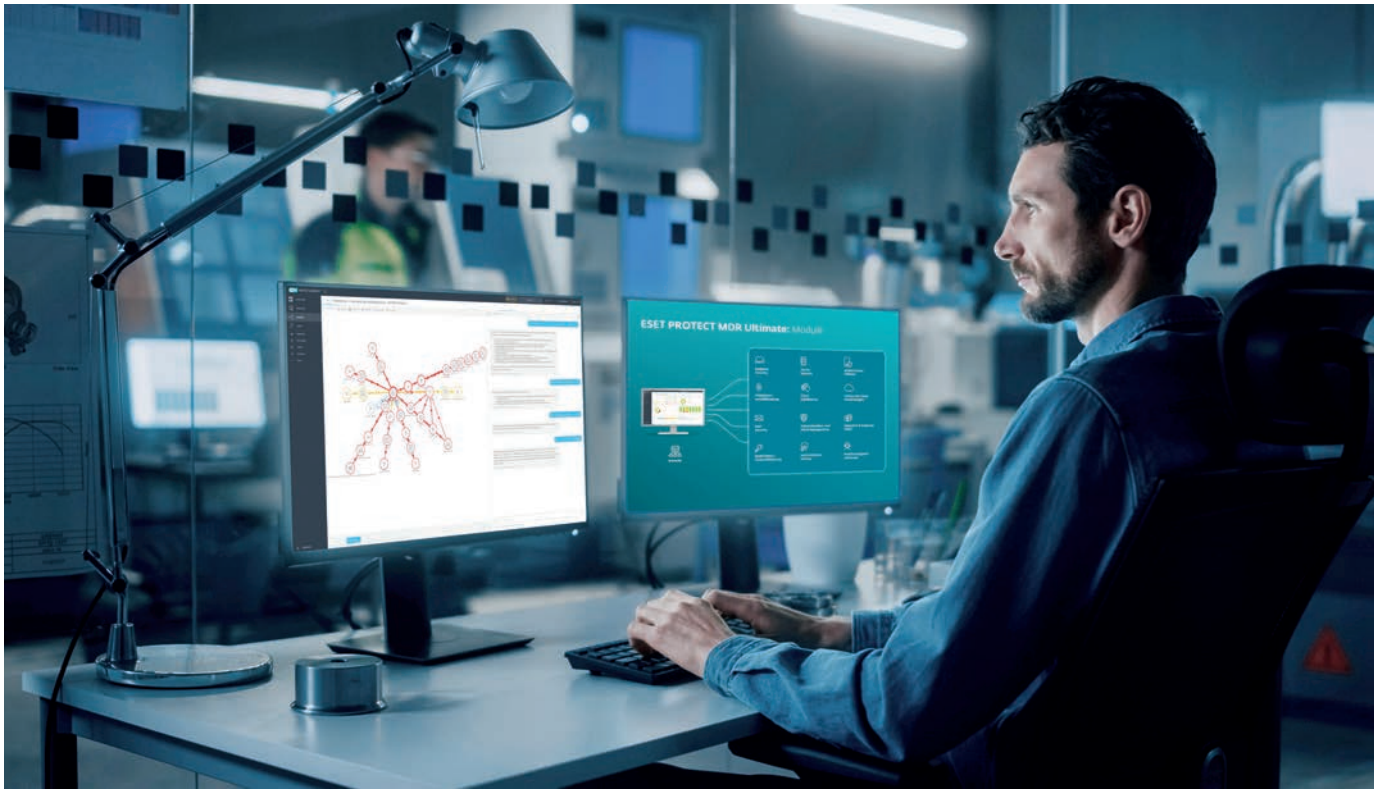
www.all-for-one.com/de

Fotos: Freepik (1), usertrmk/Freepik (2), anumahmadlove786/Freepik (3)

ESET

ESET Threat Intelligence: So profitieren Unternehmen von Bedrohungsinformationen in Echtzeit plus künstlicher Intelligenz.

Klassische Gefahrenabwehr reicht nicht



ESET Threat Intelligence verbindet automatisierte Erkennung mit Expertenanalysen.

■ Die Bedrohungslandschaft im Cyberraum verändert sich täglich: Neue Angriffsvektoren, raffiniertere Malware und ausgefeilte Taktiken von Cyberkriminellen stellen Unternehmen vor immense Herausforderungen. In dieser dynamischen Umgebung reicht es nicht mehr, sich allein auf reaktive Sicherheitsmaßnahmen zu verlassen. Unternehmen benötigen Threat Intelligence (TI), um Bedrohungen frühzeitig erkennen, analysieren und proaktiv darauf reagieren zu können.

Threat Intelligence basiert auf der Erfassung, Analyse und Korrelation sicherheitsrelevanter Daten. Diese Daten stammen aus verschiedenen Quellen, darunter globale Threat Feeds, Malware-Analysen, Darknet-Beobachtungen und forensische Untersuchungen. Wichtig ist dabei nicht nur das Sammeln von Informationen, sondern die richtige Beurteilung/Einordnung und Priorisierung der Daten.

Ein Beispiel verdeutlicht die Problematik: Ein Unternehmen erhält eine Warnung zu verdächtigen IP-Adressen. Doch ohne den richtigen Kontext bleibt unklar, ob es sich um einen echten Angriff oder harmlosen Netzwerkverkehr handelt. Sicherheitsteams verbringen oft Stunden mit der Auswertung von Logs und Threat Feeds, während die Bedrohung möglicherweise schon aktiv ist. ESET Threat Intelligence (ETI) adressiert diese Herausforderungen, indem sie Bedrohungsinformationen hinsichtlich ihrer Relevanz in Echtzeit analysiert und so Unternehmen dabei hilft, fundierte Sicherheitsentscheidungen zu treffen.

Wie funktioniert Threat Intelligence in der Praxis?

Threat Intelligence lässt sich in drei zentrale Kategorien unterteilen:

1. Strategische Threat Intelligence – Hochwertige Analysen über Bedrohungsakteure, deren Motivationen und potenzielle Angriffsziele, die für Management-Entscheidungen relevant sind.
2. Taktische Threat Intelligence – Fokus auf technische Details wie IP-Adressen, Hash-Werte und Malware-Signaturen, die für Sicherheitslösungen nutzbar sind.
3. Operative Threat Intelligence – Informationen über Angriffsvektoren und Methoden, mit denen Angreifer Netzwerke kompromittieren.

ESET Threat Intelligence kombiniert alle drei Ebenen, indem sie automatisierte Erkennung mit Expertenanalysen verbindet. Unternehmen erhalten nicht nur technische Indikatoren zu Bedrohungen, sondern auch eine kontextbasierte Bewertung, die hilft, Sicherheitsprioritäten zu setzen.

ESET AI Advisor: Unterstützung durch KI-gestützte Analyse

Threat Intelligence ist ohne Frage ein leistungsfähiges Werkzeug. Dennoch kann die Flut an Bedrohungsdaten schnell unüberschaubar werden. Genau hier kommt der ESET AI Advisor ins Spiel. Er ergänzt die Threat Intelligence durch KI-gestützte Analysen, die dabei helfen, Bedrohungen schneller zu priorisieren und fundierte Entscheidungen zu treffen.

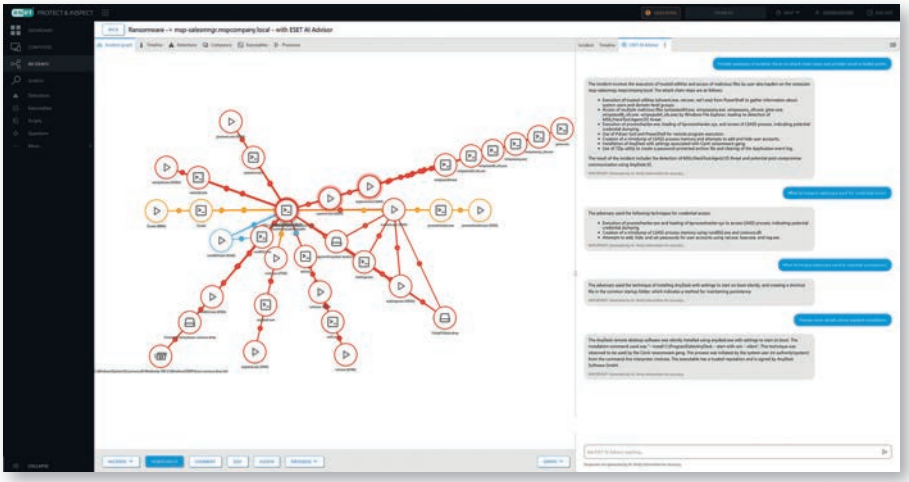
- Echtzeit-Datenanalyse: Die Plattform verarbeitet aktuelle Bedrohungsdaten aus ESET Threat Intelligence Feeds und globalen Sicherheitsquellen.
- Kontextbasierte Risikoanalyse: Statt nur Bedrohungen aufzulisten, liefert die KI eine Bewertung der Gefahr, beispielsweise, ob eine verdächtige IP-Adresse in bekannten APT-Kampagnen genutzt wurde.
- Automatisierte Handlungsempfehlungen: Sicherheitsteams erhalten direkte Vorschläge zur Abwehr, basierend auf einer umfassenden Analyse der Bedrohungslage.

Ein besonderes Merkmal des AI Advisors ist die Nutzung natürlicher Sprachabfragen. IT-Teams können gezielt Fragen stellen, etwa: „Welche neuen APT-Kampagnen sind in den letzten 48 Stunden aktiv geworden?“ Die Plattform liefert daraufhin eine komprimierte, verständliche Antwort mit allen relevanten Informationen. Dies spart wertvolle Zeit und hilft Sicherheitsexperten, Bedrohungen frühzeitig zu identifizieren und angemessen darauf zu reagieren.

Wie ESET Threat Intelligence einen Angriff frühzeitig erkannte

Im Jahr 2023 analysierte ESET eine Welle gezielter Ransomware-Angriffe auf Unternehmensnetzwerke, die durch einen kompromittierten Remote-Zugriffspunkt ermöglicht wurden. Durch den gezielten Einsatz von TI-Feeds konnten Sicherheitsteams in betroffenen Unternehmen frühzeitig erkennen, dass ihre Systeme in Bedrohungslisten auftauchten – noch bevor ein Angriff ausgeführt wurde.

Dieses Beispiel zeigt, wie wichtig kontextbasierte Bedrohungsanalysen und KI-gestützte Sicherheitslösungen sind, um moderne Cyberbedrohungen in Echtzeit zu erkennen und abzuwehren.



Der ESET AI Advisor ergänzt die Threat Intelligence durch KI-gestützte Analysen.

Best Practices: So nutzen Sie Threat Intelligence optimal

Threat Intelligence sollte frühzeitig und strategisch eingesetzt werden – nicht erst im Ernstfall. Wer erst reagiert, wenn sich ein Angriff bereits im System festgesetzt hat, verspielt wertvolle Zeit. Stattdessen sollte Threat Intelligence als fester Bestandteil der Cyberabwehr in die Sicherheitsstrategie eingebunden sein, von der Risikoanalyse bis zur Abwehr verdächtiger Aktivitäten.

KI-gestützte Analysen gehören in den operativen Alltag von Security Operations Centern (SOCs). Die Integration in bestehende SOC-Workflows ermöglicht es, große Datenmengen in Echtzeit zu analysieren, Bedrohungen schneller zu erkennen und Prioritäten klar zu setzen. Moderne Threat-Intelligence-Plattformen arbeiten mit Machine Learning, um Muster zu erkennen, die menschlichen Analysten entgehen würden. Damit liefern sie eine solide Grundlage für Entscheidungen im Incident Response.

Die besten Tools bringen wenig, wenn die Menschen sie nicht richtig nutzen. Daher gehört es mehr als zum guten Ton, Sicherheitsteams im Umgang mit KI-gestützter Threat Intelligence zu schulen. Dazu gehört das Verständnis dafür, wie Modelle trainiert werden, wie man Empfehlungen des Systems bewertet und wo menschliches Urteilsvermögen unerlässlich bleibt. Ziel muss es sein, dass Analysten KI nicht als Black Box begreifen, sondern als Werkzeug, das Transparenz und Effizienz schafft.

Automatisierung ist kein Luxus, sondern Voraussetzung für Skalierbarkeit. Wenn Systeme wie ein AI Advisor konkrete Handlungsempfehlungen geben – etwa zur Netzwerksegmentierung, zur Blockierung verdächtiger IPs oder zur Priorisierung von Schwachstellen – sollten diese automatisiert in Sicherheitsmaßnahmen übersetzt werden. So lassen sich Reaktionszeiten drastisch verkürzen und SOC-Ressourcen auf wirklich kritische Vorgänge konzentrieren.

Fazit: Smarte Threat Intelligence für schnellere & bessere Entscheidungen

ESET Threat Intelligence bietet Unternehmen eine plattformübergreifende Lösung, die Bedrohungsdaten in Echtzeit analysiert, kontextualisiert und automatisch Handlungsempfehlungen liefert. Anstatt sich durch unzählige Threat Feeds und Log-Daten zu kämpfen, können IT-Teams relevante Informationen direkt abrufen – unterstützt durch den ESET AI Advisor, der als intelligenter Assistent für die Bedrohungsanalyse fungiert.

RÜCKFRAGEN & KONTAKT
ESET Deutschland GmbH
Matthias Malcher
Senior Territory Manager Austria
matthias.malcher@eset.at
www.eset.at

Anzeige • Fotos: ESET

1

IT-RISIKO: EXTERNER ZUGRIFF

Unternehmen erlauben Externen häufig den Zugriff auf ihr IT-Netzwerk. Das ist zwar praktisch, aber auch riskant für die Sicherheit von Systemen und Daten.

Um Prozesse im Unternehmen zu verschlanken, werden zum Beispiel Vertriebspartnern, Lieferanten und Subunternehmen Zugänge ins IT-Netzwerk eingeräumt. Werden die Zugriffe auf die Unternehmens-IT richtig verwaltet, ist alles gut. Doch das ist in der Praxis seltener der Fall als gedacht und notwendig. Wo die Schwachstellen im Zugriffsmanagement von Externen liegen, hat eine internationale Studie vom Ponemon-Institut und Imprivata zutage gefördert. Die Studie ist nicht repräsentativ, gibt aber ein gutes Bild des Status quo im Access Management ab. Befragt wurden rund 2.000 IT-Verantwortliche auf drei Kontinenten. Die globalen Ergebnisse unterscheiden sich nicht signifikant von den Ergebnissen in einzelnen Ländern. Merklich unterscheiden sich jedoch die Opferzahlen. In den USA und in Australien waren 42 Prozent der Befragten in den letzten zwölf Monaten von einem Datenleck oder einer Cyberattacke betroffen, die aus der Lieferkette stammte. In Deutschland beispielsweise waren es 9 Prozent mehr, nämlich 51 Prozent.

2

ALARMIEREND

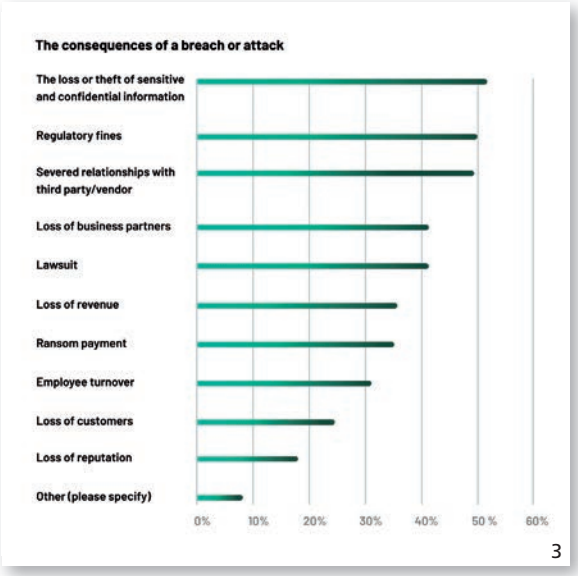
»Mehr als die Hälfte aller Befragten (55 %), gab an, dass ihr Unternehmen die Sicherheits- und Datenschutzpraktiken Externer nicht bewertet, bevor es Zugriffsrechte einräumt.«

Dirk Wahlefeld, Manager Imprivata GmbH

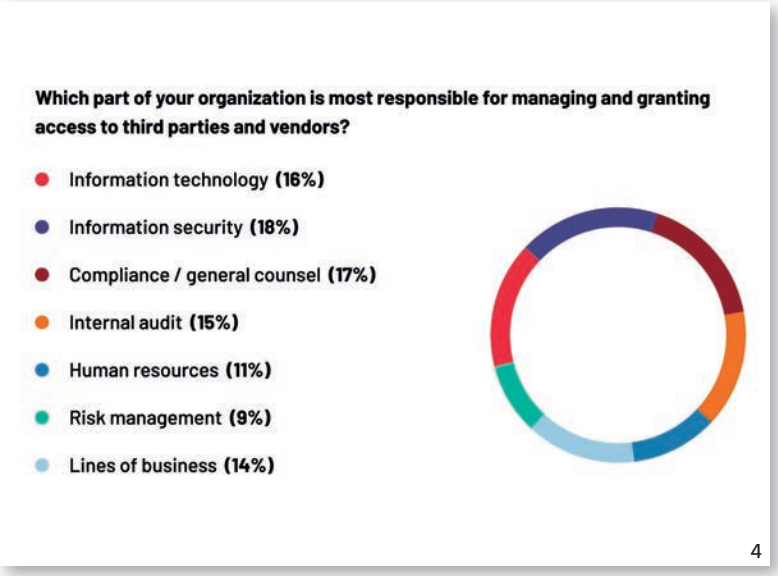
DIE FOLGEN

Die Cyberattacken aus der Lieferkette haben meist gravierende Folgen. Zu den häufigsten zählten:

- der Verlust oder Diebstahl sensibler und vertraulicher Daten (53 %),
- erpresste Strafzahlungen (50 %) und
- belastete Geschäftsbeziehungen (49 %).



3



4

Wie kann man Folgen wie diese verhindern? Dazu liefert die Studie Erkenntnisse für IT-Sicherheitsverantwortliche, wie sie Risiken verringern können. Nachfolgend einige ausgewählte Ergebnisse.

SCHWACHSTELLEN UND IHRE URSACHEN

1. Ein grundlegend einheitliches Verfahren ist erforderlich: 58 Prozent der Befragten gaben an, keine einheitliche Strategie für die Verwaltung von Zugängen und Berechtigungen für Externe zu haben.

2. Dokumentation ist das A und O: In Deutschland haben 50 Prozent der Befragten eine umfassende Dokumentation aller Externen, die auf das Netzwerk zugreifen. Im UK sind es nur 45 Prozent, in den USA 46 Prozent. Folglich weiß etwa jedes zweite Unternehmen nichts über die Zugriffsrechte und -verfahren von Externen. Warum ist das so? Am häufigsten genannte Gründe waren fehlende Ressourcen für die Überwachung von Externen (45 %) und keine zentrale Kontrolle über die Beziehungen zu Externen (37 %). In Deutschland gaben das sogar 42 Prozent an.

3. Zuständigkeiten eindeutig klären: Auf die Frage, wer denn hauptsächlich für die Zugriffe Externer auf das Netzwerk zuständig ist, verteilten sich die Antworten auf sage und schreibe sieben Bereiche: von der IT, IT-Sicherheit über die Compliance- und Rechtsabteilung und Interne Revision bis hin zu Personalabteilung, Risikomanagement und Fachabteilungen. Das war in nahezu jedem Land so.

4. Externe vorab prüfen: Mehr als die Hälfte aller Befragten (55 %) gab an, dass ihr Unternehmen die Sicherheits- und Datenschutzpraktiken Externer nicht bewertet, bevor es Zugriffsrechte einräumt. In Deutschland waren das sogar 62 Prozent. Auf die Frage, warum diese Bewertung nicht stattfindet, antworteten 62 Prozent, dass ihr Unternehmen darauf vertraut, dass der externe Partner wohl integer ist. Gleichzeitig gaben 61 Prozent der Befragten auch in Deutschland zu, dass es an Ressourcen zur Überprüfung und Verifizierung fehlt.

5. Kontrolle fordern: Bei der Frage, warum die IT die Risiken durch den Zugriff Externer nicht in den Griff bekommt, wurden drei Gründe genannt:

- fehlenden Kontrolle oder Steuerung (50 %),
- die Komplexität der Compliance- und gesetzlichen Anforderungen (48 %) und
- der Mangel an Ressourcen oder Budgets (41 %).

Mit zu wenig Ressourcen hatten die Befragten aus Deutschland die wenigsten Probleme (27 %). Ihnen stehen vor allem die komplexen Anforderungen durch Gesetze und Compliance-Regeln im Weg (59 %).

STRATEGIEN UND EINSATZ EFFEKTIVER TOOLS ERFORDERLICH

Die Studie zeigt erstmals auf, wo die Schwachstellen im Zugriffsmanagement liegen. Diese Defizite bestehen, obwohl sich die Mehrheit der Befragten sicher ist, dass der Netzwerkzugriff Externer ein großer Risikofaktor bleiben und sogar zunehmen wird – in Anbetracht steigender Cyberangriffe. Deshalb behandelt die Mehrheit der IT-Verantwortlichen das Thema durchaus mit Priorität. Dennoch spiegelt sich in den Ergebnissen durchaus eine gewisse Hilflosigkeit wider. Die Lösung besteht in Maßnahmen und Tools, die strategisch und konsequent angewandt werden – für alle privilegierten Zugriffsanforderungen – transparent, dokumentiert und effektiv. DW

DER AUTOR

Dirk Wahlefeld ist Manager Unimate Tech Services bei der Imprivata GmbH, einem Anbieter von Lösungen für digitale Identitäten in systemkritischen Branchen.
www.imprivata.com/de

EXIT THE AI DILEMMA

Am Donnerstag, den 5. Juni fand in der ARS Akademie in Wien und online der KI-Event „Powercouple KI & Arbeitswelt“ statt. Im Fokus stand, neben der Technologie selbst, der Appell, jetzt zu handeln und nicht auf eine detaillierte Rechtsprechung zu warten.

Der grundlegende Succus des Tages wurde spätestens beim Experten-Duell klar: Wer sich nicht mit dem Thema KI beschäftigt, wird besonders in der Berufswelt demnächst überholt. Denn die Systeme entwickeln sich derart schnell, dass manche der Vortragenden ihre Inhalte noch wenige Tage vor der Veranstaltung überarbeiten mussten. Die drei Key-Take-aways des Tages sind: handeln, auch wenn die rechtliche Sicherheit noch nicht besteht, schulen und weiterbilden, sich selbst sowie die eigenen Mitarbeiter:innen, und nicht entmutigen lassen von der Revolution, in der wir uns gerade befinden.

NICHT WARTEN, SONDERN HANDELN

Eines wurde an dem Tag deutlich: Wer darauf wartet, dass alles rechtssicher umgesetzt werden kann, der befindet sich noch lange Zeit im Stillstand. Wie Lukas Feiler von Baker McKenzie in seinem Vortrag deutlich machte, kann die Legislative gar nicht schnell genug hinter der rasenden Entwicklung der KI-Systeme hinterherkommen. Demzufolge ist ein gutes Risikomanagement wichtig, um innerbetrieblich genauestens zu überlegen, welche Systeme und welche Strategien die richtigen für das eigene Unternehmen sind. Wer sich auf komplette Rechtssicherheit verlassen will, der riskiert damit die Wettbewerbsfähigkeit des eigenen Unternehmens.

WISSEN ALS MOTOR

Wie Waltraud Jelinek-Krickl in ihrem Vortrag deutlich machte, gibt es aktuell drei Personengruppen: Jene, die KI nutzen und sich damit auskennen; jene, die die Technologie nutzen, sich aber damit nicht auskennen; und jene, welche die KI weder nutzen noch sich damit auskennen. Die für Organisationen „gefährlichsten“ Personen sind hier jene, die die Technologie nutzen, ohne sich damit tatsächlich gut auszukennen. Daher kommt kein Unternehmen, egal ob EPU, KMU oder Konzern, umhin, seine Mitarbeitenden für das Thema zu sensibilisieren. Dabei geht es, so sind sich die Expert:innen einig, nicht darum, eine Reihe an KI-Spezialist:innen im eigenen Unternehmen zu haben. Vielmehr geht es darum, ein einheitliches innerbetriebliches Mindset zu entwickeln, wie man mit dieser Technologie verfahren will. Wie alle Vortragenden auch deutlich betonten: Wir können der Herausforderung KI nicht davonlaufen, sie holt uns sonst irgendwann ein.

NÄCHSTE SCHRITTE

Den Abschluss der Veranstaltung bildete ein inspirierender Vortrag der Philosophin Lisz Hirn. Da durch das Aufkommen der Sprachmodelle und das bald erwartete Auftreten der KI-Agenten die Sorge um die eigene Relevanz bei so machen in den Vordergrund geriet, kam die positive Botschaft ihres Vortrages gerade richtig. Denn wie sie richtig bemerkte, gibt es keine menschenunabhängige Technik – wir sind immer symbiotisch. Jede Technologie hat ein unendliches Potenzial an Veränderungen, die sowohl dystopisch als auch utopisch sein können. Mut, Neugierde und die Bereitschaft zu lernen haben bei solchen Veränderungen auch in der Vergangenheit bereits geholfen und werden es auch bei dieser Revolution tun. BO

INFO-BOX

Über die ARS Akademie

Die ARS Akademie ist Österreichs größter privater Fachseminaranbieter und in allen Bundesländern vertreten. Rund 800 ausgewählte Top-Expert:innen aus Wirtschaft, Praxis und Legistik geben ihr Wissen in rd. 1.200 verschiedenen Veranstaltungen an rd. 18.500 Teilnehmende pro Jahr weiter. Ob topaktuelle gesetzliche Änderungen, neueste Trends oder Basiswissen für den beruflichen Aufstieg – die ARS Akademie bietet mit 15 Fachbereichen ein breites Spektrum an Seminarinhalten und Branchenthemen und deckt so jeden Weiterbildungswunsch ab. Die Seminare können als Präsenzveranstaltung und oftmals auch als Onlineseminar im Virtual Classroom besucht werden. Auf Wunsch können die Weiterbildungen als Inhouse-Seminar gebucht werden.
https://ars.at/

Foto: Freepik

ASSECO SOLUTIONS GMBH

Generative KI kann weit mehr als Texte schreiben. Ihr Potenzial liegt in der aktiven Mitarbeit an Geschäftsprozessen. Die neue ERP-Generation von Asseco schafft mit dem Flow Mode die nötige Basis: digital hinterlegte Abläufe, die KI verstehen und nutzen kann.

Mit Highspeed in die KI-Zukunft

■ Mailings generieren, Recherchen erledigen, Meetings zusammenfassen – schon heute kann GenAI an verschiedensten Stellen im Tagesgeschäft unterstützen. Ihr wahres Potenzial jedoch entfaltet sie bei der Bearbeitung von Kernprozessen. Die dafür notwendige Basis müssen moderne ERP-Lösungen schaffen: ein Schienennetz der Prozessabläufe, das die intelligente Technologie auf Spur hält.

Um Texte zu generieren, braucht KI verlässliche Daten. Um Prozesse auszuführen, verlässliches Prozesswissen. In Zeiten, in denen KI-Agenten Mitarbeitende aktiv in ihrer täglichen Arbeit unterstützen sollen, ist dies relevanter denn je. Doch nur selten sind Prozessabläufe bislang digital im Unternehmen hinterlegt. Das Wissen um die richtigen Abläufe findet sich in den Köpfen der User: Sie wissen, welchen Weg sie sich Schritt für Schritt durch die Masken des ERP-Systems bahnen müssen, welche Schaltflächen es wann zu betätigen gilt, an welchen Stellen welche Daten notwendig sind.

Einmal geschult, ist diese Arbeitsweise für menschliche User in der Regel kein Problem. Anders jedoch für künstliche Intelligenz. Ein KI-Agent benötigt sehr klare Anweisungen, welche Einzelschritte der Reihe nach zur Bearbeitung einer Aufgabe vonnöten sind. Wie ein Hochgeschwindigkeitszug benötigt er Schienen, die ihn durch die richtigen Weichenstellungen effektiv ans Ziel bringen.

Prozessschienen für die KI

Damit ein solches Schienennetz der Prozesse entstehen kann, müssen moderne ERP-Lösungen Möglichkeiten bieten, die spezifischen Abläufe eines Unternehmens digital abzubilden. Idealerweise in einer Sprache, die die KI verstehen kann.

Mit ihrer neuen APplus-Generation bietet die Asseco Solutions ihren Kunden genau das: Der prozessorientierte Nutzungsmodus Flow Mode deckt die zentralen Kernprozesse im Unternehmen ab und führt Anwenderinnen und Anwender Schritt für Schritt durch die Bearbeitung der Aufgabe. Effizient, übersichtlich und benutzerfreundlich.

Damit erhalten Unternehmen gleichzeitig ein Schienennetz ihrer Abläufe. Dieses ermöglicht es wiederum künstlicher Intelligenz in naher Zukunft, auf effiziente Weise mit den Unternehmensprozessen zu interagieren und diese voranzutreiben.

Der Flow Mode liefert die Trassen, über die künstliche Intelligenz – wie auch die menschlichen User – auf direktem Weg zum gewünschten Ziel gelangen kann: ohne Umwege und mit Höchstgeschwindigkeit.

RÜCKFRAGEN & KONTAKT
Asseco Solutions GmbH
Wolfgang-Pauli-Str. 2c/Bauteil 3
4020 Linz
Tel.: +43 732 23 40 14
at.info@assecosol.com
www.applus-erp.com

1

ÖSTERREICH IST VERWUNDBAR

Cyberangriffe werden zunehmend als Werkzeug geopolitischer Auseinandersetzungen eingesetzt. Österreich ist nicht nur betroffen, sondern auch verwundbar. Das zeigt die zehnte Ausgabe der Studie „Cybersecurity in Österreich".

Zum zehnten Mal in Folge veröffentlicht KPMG gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich (KSÖ) die Studie „Cybersecurity in Österreich". Für die Jubiläumsausgabe der Studie wurden 1.391 heimische kleine, mittlere und große Unternehmen aus verschiedenen Branchen befragt. Zahlreiche Interviews mit nationalen und internationalen Expert:innen ergänzen die Publikation.
Die Zahlen sind alarmierend: Angriffe durch staatlich unterstütze Akteure haben sich im Vorjahresvergleich mehr als verdoppelt. Die Angriffe aus Asien und Europa haben sich dramatisch erhöht. Dazu kommt, die Lieferketten der Unternehmen werden gnadenlos erfolgreich angegriffen.

- Jeder 7. Cyberangriff (14 Prozent) in Österreich ist erfolgreich.
- Mehr als jeder 4. Angriff (28 Prozent) ist auf staatlich unterstützte Akteure zurückzuführen.
- Bei jedem 3. Unternehmen (32 Prozent) waren deren Lieferanten oder Dienstleister Opfer von Cyberangriffen, die wesentliche Auswirkungen auf das eigene Unternehmen hatten.
- Jeder zehnte Social-Engineering-Versuch (10 Prozent) nutzt bereits Deepfake-Technologien für Sprach- und Videonachrichten.
- 55 Prozent sagen, dass Österreich nicht gut darauf vorbereitet ist, auf schwerwiegende Cyberangriffe gegen die kritische Infrastruktur zu reagieren.

Fotos: Zhangxiao/Freepik (1), KPMG Austria (2)

GLOBALE KONFLIKTE SIND IM HEIMISCHEN CYBERRAUM ANGEKOMMEN

Cyberangriffe sind das Mittel der Wahl, um politische, wirtschaftliche und gesellschaftliche Ziele zu verfolgen: Von 12 Prozent im Vorjahr auf 28 Prozent heuer haben sich die Angriffe durch staatlich unterstützte Akteure in Österreich mehr als verdoppelt. Angriffe auf Unternehmen haben dabei nicht mehr nur Datendiebstahl oder Erpressung durch Ransomware zum Ziel, vielmehr sollen ganze Geschäftsprozesse manipuliert werden. Kritische Infrastrukturen werden gezielt attackiert, um Unsicherheit zu verbreiten und das gesellschaftliche Zusammenleben zu stören.

Die Verunsicherung ist groß: 55 Prozent halten Österreich für nicht gut vorbereitet, um auf schwerwiegende Angriffe auf die kritische Infrastruktur zu reagieren. Nur 13 Prozent der Befragten sind der Meinung, dass Österreich gut vorbereitet ist. Dazu kommt, die Raffinesse und Fokussierung der Angriffe macht es zunehmend schwieriger, die tatsächlichen Akteur:innen hinter den Angriffen zu identifizieren. Festmachen lässt sich jedoch: Angriffe aus Asien haben sich 2025 mehr als verdoppelt, von 18 auf 41 Prozent, und Angriffe aus Europa sind von 15 auf 29 Prozent gestiegen. Umso dringlicher ist der Appell, eine umfassende nationale Cybersicherheitsstrategie zu implementieren, die internationale Kooperationen stärkt und technologische Investitionen fördert. 88 Prozent der befragten Unternehmen sagen, dass es eine verstärkte EU-weite Zusammenarbeit beim Thema Cybersicherheit benötigt. 69 Prozent wünschen sich, dass heimische Cybersicherheitsunternehmen von der Politik gefördert werden.

DIGITALES GIFT

»Desinformationskampagnen sind wie digitales Gift, das langsam, aber spürbar das Vertrauen in Institutionen, Medien und demokratische Prozesse zersetzt.«

Robert Lamprecht, Studienautor KPMG

DESINFORMATION DURCH SOCIAL ENGINEERING UND DEEPFAKE

Des- und Missinformationen sowie alle anderen Formen der (hybriden) Einflussnahme wirken direkt und ungefiltert auf die Gesellschaft – gerade in Zeiten geopolitischer Spannungen. „Desinformationskampagnen sind wie digitales Gift, das langsam, aber spürbar das Vertrauen in Institutionen, Medien und demokratische Prozesse zersetzt. Die Grenzen zwischen Wahrheit und Manipulation verschwimmen immer mehr", beschreibt KPMG-Partner und Studienautor Robert Lamprecht die aktuelle Entwicklung. Mittel der Wahl für groß angelegte Kampagnen ist heute vor allem Social Engineering: Jeder zehnte Social-Engineering-Versuch nutzt bereits Deepfake-Technologien für Sprach- und Videonachrichten und arbeitet beispielsweise mit der Echtzeit-Imitation von Stimmen.


2

KÜNSTLICHE INTELLIGENZ – CHANCE ODER RISIKO

Von der Verwaltung über die Industrie und kritische Infrastruktur bis hin in den privaten Raum – Digitalisierung und KI durchdringen mittlerweile sämtliche Bereiche. Das ››

» eröffnet eine Vielfalt an neuen Chancen, erhöht aber auch die Angriffsfläche für Bedrohungen drastisch. „KI ist ein starkes Werkzeug in der Cybersicherheit, aber kein Allheilmittel. Ihre Wirksamkeit hängt von der korrekten Einbindung und Anwendung sowie von den eingesetzten Technologien ab. Für eine solide Sicherheitsbasis sollten Unternehmen keinesfalls allein auf KI vertrauen, sondern auch grundlegende Maßnahmen wie Identity-Management, Datenmanagement und Mitarbeiter:innenschulungen priorisieren“, erklärt KPMG-Partner Andreas Tomek.

Es war nie einfacher als heute, Angriffe zielgerichtet vorzubereiten und auszuführen. Dass die Angreifer:innen ihnen dicht auf den Fersen sind, spüren die Unternehmen: 78 Prozent sagen, dass sich mit der Einführung neuer Technologien wie KI die Bedrohungslage verschärft.

DIE LIEFERKETTE ALS ACHILLESFERSE

Unternehmen wissen mittlerweile um die massiven Schäden und Beeinträchtigungen, die Cyberangriffe zur Folge haben können, und haben ihre eigenen Schutzmaßnahmen deutlich verbessert. Die Trendwende haben Cyberkriminelle erkannt und verlagern ihre Angriffe auf ein oftmals schwächeres Glied in der Kette, ihre Lieferanten. Bei jedem dritten Unternehmen (32 Prozent) waren deren Lieferanten oder Dienstleister Opfer von Cyberangriffen, die wesentliche Auswirkungen auf das eigene Unternehmen hatten. „Unzureichende Sicherheitsstandards bei Lieferanten und Dienstleistern öffnen den Cyberkriminellen Tür und Tor. Ein Cyberangriff auf nur ein einziges Glied in der Kette kann verheerende Konsequenzen für das Unternehmen haben und einen Dominoeffekt auslösen“, so Lamprecht.


2

AN EINEM STRANG ZIEHEN

»Behörden, Wirtschaft und Wissenschaft müssen an einem Strang ziehen und gemeinsam eine Sicherheitskultur gestalten, die auf Kooperation, Transparenz und gemeinsames Handeln baut.«

Michael Höllerer, Präsident KSÖ

Hier setzt die europäische Regulatorik an. Richtlinien wie NIS-2 und DORA veranlassen heimische Unternehmen dazu, die Lieferkettensicherheit nicht länger als Randthema zu behandeln, sondern als zentralen Bestandteil der eigenen Cyberresilienz. Noch ist es dahin aber ein weiter Weg: 38 Prozent der befragten Unternehmen geben an, dass ihnen nicht bekannt ist, welche Tätigkeiten zur Gewährleistung der Sicherheit bei ihren Lieferanten oder Dienstleistern durchgeführt werden. Und 47 Prozent haben Sorge, dass Zulieferer nicht dieselben Sicherheitsstandards einhalten und so zum Einfallstor für Cyberangriffe werden.


1

DIGITALE SOUVERÄNITÄT SICHERN

Die Ausgestaltung von Cybersecurity wird unter den aktuellen Vorzeichen und der weiteren Entwicklung zu einer gesellschaftlichen Mammutaufgabe. Innovation und Sicherheit dürfen aber keinen Widerspruch darstellen, sondern sind zwei Seiten derselben Medaille. „Technik allein reicht nicht, den Herausforderungen zu begegnen. Es braucht Menschen, die Verantwortung übernehmen, Risiken verstehen und aktiv an Lösungen mitwirken. Behörden, Wirtschaft und Wissenschaft müssen an einem Strang ziehen und gemeinsam eine Sicherheitskultur gestalten, die auf Kooperation, Transparenz und gemeinsames Handeln baut“, so Michael Höllerer, Präsident des KSÖ.

DIE TOP-ANGRIFFSARTEN 2025

Die positive Nachricht: Die Cybersecurity-Ambitionen der Unternehmen machen sich bezahlt. War im Vorjahresvergleich jede sechste Cyberattacke erfolgreich, ist es in diesem Jahr jede siebte. „Entspannung zeichnet sich aber nicht ab, ganz im Gegenteil: Die Angriffe pendeln sich auf sehr hohem Niveau ein und werden mit jedem Jahr facettenreicher und fokussierter. Wir sind in einer neuen Realität der Cyberangriffe angekommen, die Folgen sind ein teurer Weckruf für unzureichende Cybersicherheitsmaßnahmen“, so Studienautor Robert Lamprecht.

Die Hauptangriffsarten sind neben Phishing-Attacken und Malware (mit jeweils 81 Prozent) Scam-Anrufe (65 Prozent), gefolgt von Business-E-Mail-Compromise mit 59 Prozent und Denial-of-Service-Attacken mit 55 Prozent. BO

Fotos: Absolute Graphic/Freepik (1), Eva Kelety (2)

CRM MADE IN EUROPE

Immer mehr europäische Unternehmen suchen Alternativen zu US-Software und finden sie bei Anbietern wie SuperOffice. Der norwegische CRM-Spezialist punktet mit DSGVO-Konformität und praxisnaher KI.

Immer mehr europäische Unternehmen kehren US-Software aus Sorge um Datenschutz, regulatorische Hürden und mangelnde Kundennähe den Rücken. Der norwegische CRM-Anbieter SuperOffice profitiert spürbar von diesem Wandel. Mit einer umfassenden Transformation, praxisnahen KI-Innovationen und einem klaren Fokus auf Mittelstandskunden verzeichnet das Unternehmen starkes Wachstum und setzt neue Maßstäbe für europäische Softwarelösungen.

Lars Engbork, CEO von SuperOffice, mit seinem Managementteam (2. v. r.)

Foto: SuperOffice

REKORDWACHSTUM IN SICH WANDELNDEM MARKT

SuperOffice wächst derzeit überdurchschnittlich stark, getragen von der steigenden Nachfrage nach CRM-Systemen, die speziell auf europäische Standards ausgerichtet sind. Immer mehr mittelständische Unternehmen suchen nach Softwarelösungen, die nicht nur DSGVO-konform sind, sondern auch langfristige Kundenbeziehungen fördern. „Wir sind nicht hier, um den Status quo zu verwalten, wir sind hier, um neue Maßstäbe zu setzen. Unsere Transformation bedeutet mehr Fokus, schnellere Umsetzung und messbare Ergebnisse für unsere Kunden. Es ist nicht nur eine neue Strategie, es ist eine neue Art zu arbeiten“, sagt Lars Engbork, CEO von SuperOffice.

EUROPA WILL UNABHÄNGIGER WERDEN

Im März unterzeichneten über 100 Organisationen einen offenen Brief an die EU, in dem sie mehr technologische Unabhängigkeit Europas fordern. Seit Jänner verzeichnet die Plattform European Alternatives einen Anstieg des Besucheraufkommens um mehr als 1.200 Prozent – ein deutliches Zeichen für das wachsende Interesse an europäischen Lösungen. Für diesen Wandel sieht sich SuperOffice optimal aufgestellt. Die Plattform wird vollständig in Europa entwickelt, erfüllt alle Anforderungen der DSGVO und bietet einen klar kundenorientierten Ansatz.

KÜNSTLICHE INTELLIGENZ MIT ECHTEM MEHRWERT

Ein zentrales Element der Transformation von SuperOffice ist der Fokus auf KI. Ein engagiertes KI-Team arbeitet daran, Intelligenz direkt in die Plattform zu integrieren. Von der Automatisierung wiederkehrender Aufgaben bis hin zu Echtzeit-Einblicken nutzt SuperOffice KI, um Produktivität zu steigern und Komplexität zu reduzieren. „SuperOffice investiert intensiv in KI – nicht als Modewort, sondern als grundlegende Veränderung, wie CRM Unternehmen stärken kann. KI ist nicht die Zukunft, sie ist das Jetzt. Unsere Investition in KI dient nicht dazu, zu beeindrucken, sondern zu vereinfachen. Unser Ziel ist es, Anwender dabei zu unterstützen, intelligenter zu arbeiten und den Bedürfnissen ihrer Kunden einen Schritt voraus zu sein“, sagt Engbork.

KUNDENBEZIEHUNGEN NEU GEDACHT

Im Zentrum der Produktstrategie von SuperOffice steht der Relationship Loop – ein CRM-Modell, das über den klassischen Vertriebstrichter hinausgeht. Es bildet den gesamten Lebenszyklus von Kundenbeziehungen ab und rückt langfristige Wertschöpfung in den Fokus. „Kundenbeziehungen beginnen und enden nicht mit einem Verkauf. Sie entwickeln sich über die Zeit. Der Relationship Loop spiegelt wider, wie wir CRM verstehen: dynamisch, datengetrieben und auf langfristige Wertschöpfung ausgerichtet. Unsere Produktstrategie unterstützt unsere Kunden dabei, in jeder Phase erfolgreich zu sein“, erklärt Engbork. BS

MEHR PROFITABILITÄT

Hohe Profitabilität ist entscheidend für langfristige finanzielle Stabilität und Wettbewerbsfähigkeit eines Unternehmens. Viele miteinander verwobene Faktoren beeinflussen die Effizienz, mit der Ressourcen genutzt werden, um Einnahmen zu lukrieren.

Für Gerhard Wanek, Geschäftsführer von Cursor Austria, spielen CRM-Systeme durch ihre zentrale Schnittstellenfunktion eine entscheidende Rolle im Zusammenspiel zwischen eingesetzten Ressourcen und lukrierten Einnahmen.

Kundenbeziehungsmanagement ist das Herzstück jedes Unternehmens. Davon ist Gerhard Wanek überzeugt. Der Geschäftsführer von Cursor Austria weiß: „Ein vollständig integriertes CRM-System verbindet sich nahtlos mit anderen wichtigen Systemen und Tools und ermöglicht den abteilungsübergreifenden Austausch von Daten und Informationen. Der umfassende Überblick über Kundeninteraktionen ermöglicht eine effiziente Zusammenarbeit und vermeidet kostenintensive Doppelgleisigkeiten."

ZUFRIEDENE KUND:INNEN SORGEN FÜR GUTE BILANZEN

Abgesehen von der größeren Effizienz, die an sich bereits ein Faktor für die Steigerung der Profitabilität ist, trägt auch die dadurch mögliche nachhaltige Kundenbetreuung wesentlich zur Gewinnmaximierung bei. Denn zufriedene Kund:innen sind in mehrerlei Hinsicht die Basis des Erfolgs. Gerhard Wanek: „Bestehende Kund:innen zu halten, ist billiger, als neue zu gewinnen. Loyale Kund:innen sind weniger preissensibel, da sie den Wert der Produkte oder Dienstleistungen schätzen, und zufriedene Kund:innen empfehlen das Unternehmen weiter und sind auch eher dazu bereit, zusätzliche Produkte oder Dienstleistungen zu kaufen."

NEGATIVES FEEDBACK IN LOYALITÄT VERWANDELN

Oft wird es als Gemeinplatz erachtet, dennoch entspricht es der Realität: Beschwerden und Reklamationen sind ein wichtiger Teil der Kundeninteraktion und dienen zugleich als wertvolle Informationsquelle für strategische Entscheidungen. Ein zentrales System, das den Mitarbeiter:innen immer einen aktuellen 360-Grad-Blick auf die Kund:innen bietet und es ihnen ermöglicht, Anfragen und Beschwerden einfach und schnell aufzunehmen, zu kategorisieren und effizient sofort zur richtigen Stelle zu delegieren, liefert einen wichtigen Beitrag zur Kundenzufriedenheit.

Selbst wenn die Kundenbeziehung stabil erscheint, sollte beachtet werden, dass sich Kundenbedürfnisse im Lauf der Zeit ändern. So bietet zum Beispiel ein auslaufender Vertrag oder eine Tarifanpassung die Chance, mit einer individuellen Gestaltung des neuen Angebots die Kundenbindung zu stärken. Dafür braucht es eine hochqualitative Datengrundlage und Analyse, um durch gezielte Ansprachen sowie Vertriebs- und Marketing-Aktionen das Wechselrisiko minimieren zu können.

„DO IT TOGETHER" STATT „DO IT YOURSELF"

In den vergangenen Jahren hat sich der Trend zu Online-Kundenportalen weiter verstärkt. Der orts- und zeitunabhängige Zugriff der Kund:innen auf ihre Daten und ihre damit gegebene virtuelle Verbindung mit dem Unternehmen bietet diesem die ideale Gelegenheit, anhand der Verknüpfung mit dem CRM ihre Onlineaktivitäten zu analysieren, einzuordnen und entsprechende Maßnahmen einzuleiten. „Dadurch sehen Unternehmen unverzüglich, welche Änderungen der Datensätze und Aktionen ihre Kund:innen im Portal vornehmen. Wenn diese etwa vermehrt Beschwerden absenden, kann dieses Alarmsignal in Maßnahmen zur Kundenbindung umgesetzt werden. Sei es, dass der Vertrieb dann telefonisch Kontakt aufnimmt oder das Marketingteam einen passenden Newsletter versendet und eine Kampagne startet – hier lassen sich Kundenaktionen einfach mit strategischen Maßnahmen zur Verbesserung der Kundenzufriedenheit verbinden", erläutert Gerhard Wanek. BO

Foto: Cursor Austria

HUAWEI

Ohne moderne PV-Lösungen keine Energiewende: Huawei treibt mit intelligenter Technologie, starken Partnern und globaler Innovationskraft den Umstieg auf Solarenergie in Österreich voran.

Huawei: Energiewende durch Innovation

Der Juli ist der sonnenstärkste Monat des Jahres – und damit ein Sinnbild für das ungenutzte Potenzial der Energiewende. Zwar steigen die hierzulande installierten PV-Anlagen und der daraus erzeugte Strom kontinuierlich, dennoch halten sich Vorurteile und Unsicherheiten hartnäckig – befeuert von fehlendem Wissen und haltlosen Theorien, die den Wandel stark ausbremsen. Dabei betont Michael Nowak, Unternehmenssprecher von Huawei Austria: „Erneuerbare Energien und Photovoltaik spielen eine tragende Rolle für die Energiewende. Als führendes Unternehmen können wir die effizientesten sowie sichersten neuen Produkte auch auf dem österreichischen Markt anbieten."

Huawei bietet ein vollständiges, skalierbares PV-Ökosystem – von kompakten Lösungen für Einfamilienhäuser bis hin zu komplexen Systemen für gewerbliche und industrielle Anwendungen. Im Zentrum stehen die vielfach eingesetzten Wechselrichter, ergänzt durch intelligente Energiespeicher, Leistungsoptimierer und smarte Steuerungstechnologien. Die PV-Module selbst stellt Huawei nicht her – dafür liegt der Fokus umso stärker auf der effizienten Nutzung, Speicherung und Verteilung der erzeugten Energie.

Forschung öffnet neue Möglichkeiten

Allein im Jahr 2024 hat Huawei rund 23 Mrd. Euro in Forschung und Entwicklung investiert und konnte dadurch auch viele PV-Technologien auf das nächste Level heben – davon profitieren auch die österreichischen Kunden. „Es ist wie so oft wichtig, über den Tellerrand hinauszublicken und die Potenziale globaler Zusammenarbeit zu erkennen – anstatt die Energiewende auszubremsen, indem man technologisch schwer nachvollziehbare Theorien konstruiert und Misstrauen verbreitet. Mit intelligenten Lösungen ebnen wir gemeinsam den Weg für mehr Verständnis und einen nachhaltigen Wandel im Bereich der Solarenergie", appelliert Nowak an einen internationalen Schulterschluss, um die Energiewende erfolgreich zu gestalten. Neben dem Fokus auf Forschung und der ständigen Verbesserung der Produktpalette legt Huawei auch einen großen Wert auf höchste Sicherheitsstandards seiner Produkte. So zählen die Wechselrichter von Huawei zu den meistgeprüften der Welt und erfüllen etliche internationale Cybersicherheitsstandards wie beispielsweise die ISO-Zertifizierung.

Solarenergie ist lokal verfügbar, klimafreundlich und wirtschaftlich attraktiv.

„Alle Daten, die lokal von unseren Wechselrichtern verarbeitet werden, werden ausschließlich in Europa gespeichert, liegen in der Cloud eines bekannten europäischen Unternehmens und werden von unabhängigen europäischen Teams unter Einhaltung der Datenschutzrichtlinien verwaltet. Die Cloud ist dabei nichts anderes als ein besonders gesicherter Speicherort in einem Rechenzentrum – vergleichbar mit einem digitalen Tresor, der rund um die Uhr geschützt und kontrolliert wird. Wenn Kunden das nicht möchten, haben sie außerdem die Möglichkeit, ihre Wechselrichter komplett vom Internet zu trennen und sie funktionieren auch ohne Updates weiter", so Nowak weiter.

Gemeinsam schneller vorankommen

Die technologischen Voraussetzungen für eine erfolgreiche Energiewende sind schon gesetzt. Damit sie auch gelingt, braucht es neben innovativen Lösungen auch den politischen Willen, wirtschaftlichen Mut und ein breites gesellschaftliches Bewusstsein für die Chancen erneuerbarer Energie. Photovoltaik wird dabei eine zentrale Rolle spielen: als lokal verfügbare, klimafreundliche und wirtschaftlich attraktive Energiequelle. Denn nur wenn alle an einem Strang ziehen, wird aus dem sonnigsten Monat des Jahres auch ein Symbol für eine nachhaltige Energiezukunft.

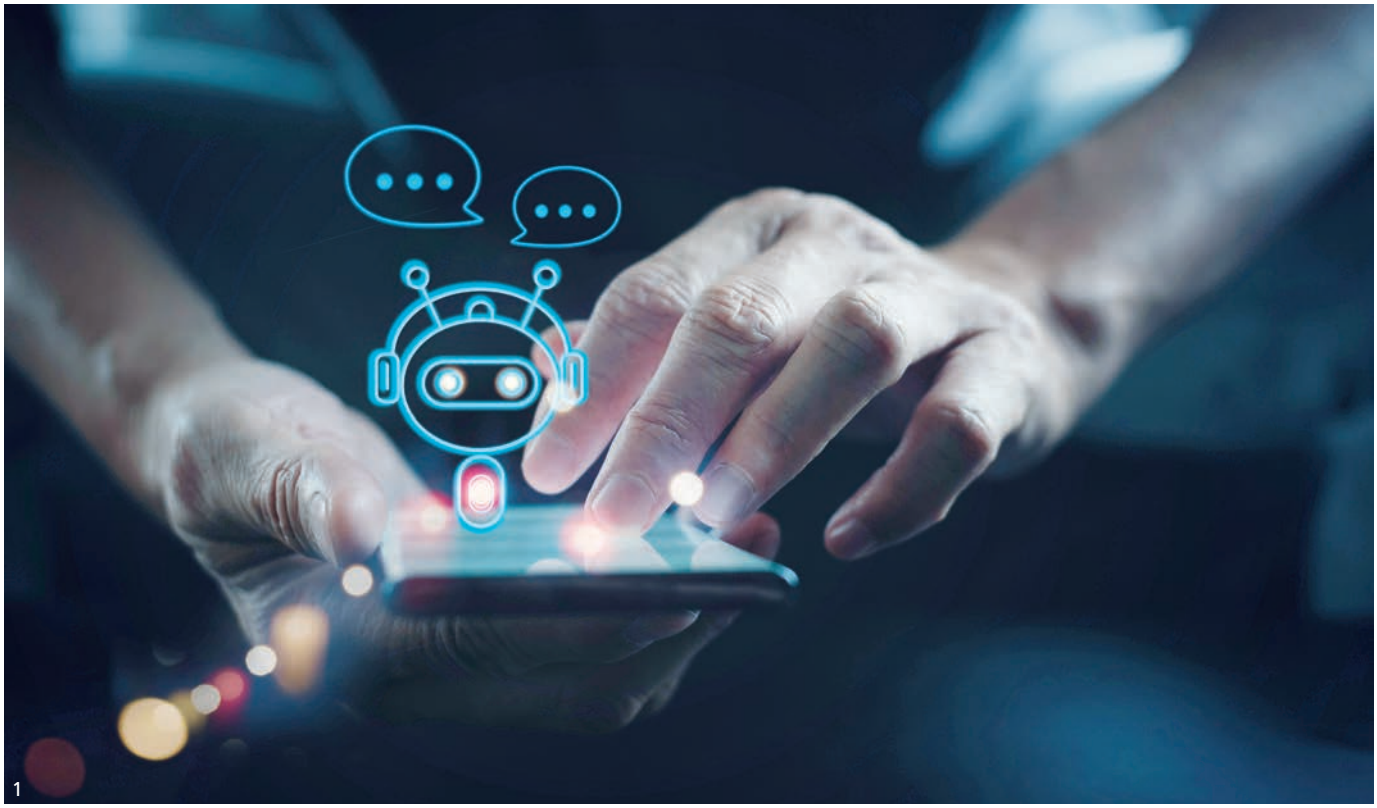
Michael Nowak, Unternehmenssprecher von Huawei Austria

HUAWEI

RÜCKFRAGEN & KONTAKT

Huawei Technologies Austria GmbH
IZD Tower 9. Stock
Wagramer Straße 19, 1220 Wien
https://e.huawei.com/at

Anzeige • Fotos: Huawei



1

CHATBOT INFORMIERT ZU AI ACT

Künstliche Intelligenz bietet viele Chancen, birgt aber auch Risiken. Daher setzt die Regierung mit einem Chatbot der KI-Servicestelle auf Informationsvermittlung, Verständlichkeit und Zugänglichkeit.

Wer Fragen rund um die europäische KI-Verordnung hat, bekommt jetzt Antworten über den neuen Chatbot der österreichischen Rundfunk und Telekom Regulierungs-GmbH (RTR GmbH). Die Antworten basieren auf relevanten Fachdokumenten – darunter der AI Act der EU selbst sowie Informationsmaterialien der KI-Servicestelle zu den regulatorischen Rahmenbedingungen für den Einsatz von künstlicher Intelligenz. Die bereitgestellten Inhalte sind verständlich aufbereitet und dienen als erste Orientierung. Rechtlich bindend sind sie allerdings nicht. „Als staatliche Einrichtung hat die RTR die Aufgabe, Service für die Bürgerinnen und Bürger zu bieten. Das tut sie, indem sie darüber informiert, was der wichtige AI Act der EU für uns alle bedeutet; und das passenderweise mit einem Chatbot, der auf künstlicher Intelligenz basiert. Künstliche Intelligenz bietet viele Chancen, birgt aber auch Risiken. Dem müssen wir nicht nur in der Gesetzgebung gerecht werden, sondern eben auch in der Information darüber für die Menschen in unserem Land“, sagt Vizekanzler Andreas Babler, der für die RTR GmbH ressortzuständig ist. „Der AI Act ist ein Meilenstein für den verantwortungsvollen Einsatz von künstlicher Intelligenz in Europa. Mit dem neuen Chatbot schafft die KI-Servicestelle bei der RTR einen leicht zugänglichen Einstieg in dieses komplexe Regelwerk – für Bürgerinnen und Bürger, Organisationen und Unternehmen. Ziel ist es, transparent zu informieren und Bewusstsein zu schaffen. Die Unternehmen sollen wissen, was rechtlich möglich ist – und was nicht. Die Bürgerinnen und Bürger versorgen wir im Rahmen der Digitalen Kompetenzoffensive mit Wissen rund um KI. Technologiekompetenz und Technologieoffenheit gehen so Hand in Hand“, so Alexander Pröll, Staatssekretär für Digitalisierung. Der Chatbot zeichnet sich durch ein hohes Maß an

Im Rahmen der CDO-Taskforce (Chief Digital Officer) wurde beschlossen, eine einheitliche Kennzeichnung von KI-Systemen künftig ressortübergreifend als Verhaltenskodex einzuführen.

Transparenz aus: Seine gesamte Funktionsweise wird offengelegt – von der ursprünglichen Eingabe (Prompt) über die Informationsbeschaffung bis hin zur Generierung der Antwort. Damit zeigt das System nicht nur die Stärken, sondern auch die Grenzen moderner Interaktionssysteme auf und dient als Vorzeigeprojekt für den verantwortungsvollen Einsatz von KI.

TRANSPARENT UND NACHVOLLZIEHBAR

Ein zentrales Merkmal ist die ausführliche technische Dokumentation, die anderen Organisationen detaillierte Einblicke in Konzeption, Aufbau und Funktionslogik bietet. So können Interessierte nachvollziehen, wie ein themenspezifisches Sprachmodell aufgebaut ist – und dieses Wissen für eigene Entwicklungen nutzen. Ein besonderes Highlight des Projekts ist die erstmalige Darstellung des Stromverbrauchs pro Anfrage. Diese Innovation schafft Bewusstsein für die Umweltauswirkungen von KI-Anwendungen. Um die Werte anschaulich zu machen, vergleicht der Chatbot den Energiebedarf einzelner Prompts mit alltäglichen Geräten wie Haartrocknern oder Handy-Akkus.

Die KI-Servicestelle der RTR weist darauf hin, dass die vom Chatbot generierten Antworten – wie bei allen generativen KI-Systemen – potenziell fehlerhaft sein können. Eine sorgfältige Qualitätskontrolle bleibt daher unerlässlich. Für weiterführende Fragen und fachliche Unterstützung steht das Team der KI-Servicestelle jederzeit zur Verfügung. Der AI Act Chatbot ist ab sofort erreichbar unter: https://chat.ki.rtr.at.

AUSBLICK: KI IN DER VERWALTUNG STÄRKEN

Auch auf gesamtstaatlicher Ebene wird der Aufbau einer vertrauenswürdigen KI-Infrastruktur in der Verwaltung konsequent vorangetrieben. Der von Staatssekretär Pröll initiierte Schwerpunkt „KI in der Verwaltung" ist ein zentraler Bestandteil der österreichischen Digitalisierungsstrategie und verfolgt das Ziel, Effizienz, Qualität und Transparenz im öffentlichen Dienst durch den verantwortungsvollen Einsatz von künstlicher Intelligenz nachhaltig zu stärken.

Einen wichtigen Meilenstein setzte die CDO-Taskforce der Bundesministerien Anfang Mai: Die einheitliche Kennzeichnung von KI-Systemen wird künftig ressortübergreifend als Verhaltenskodex sukzessive eingeführt. Bürgerinnen und Bürger sollen klar erkennen können, ob ein digitales Verwaltungsservice auf KI basiert und in welchem Ausmaß es eigenständig agiert oder Entscheidungsprozesse beeinflusst. BS

LEICHTER EINSTIEG

»Mit dem neuen Chatbot schafft die KI-Servicestelle bei der RTR einen leicht zugänglichen Einstieg in dieses komplexe Regelwerk.«

Alexander Pröll, Staatssekretär für Digitalisierung

Fotos: Evgenymedia/Freepik (1), BKA (2+3)

GENAI MADE IN EUROPE, PLEASE!

Wie fit sind Österreich und Europa für generative KI? Dieser Frage geht der IT-Dienstleister adesso in seinem aktuellen „GenAI Impact Report“ nach. Die Ergebnisse: Unternehmen sehen die österreichische Wirtschaft deutlich besser auf GenAI vorbereitet als im letzten Jahr. Sie verlangen aber Anwendungen aus Europa.

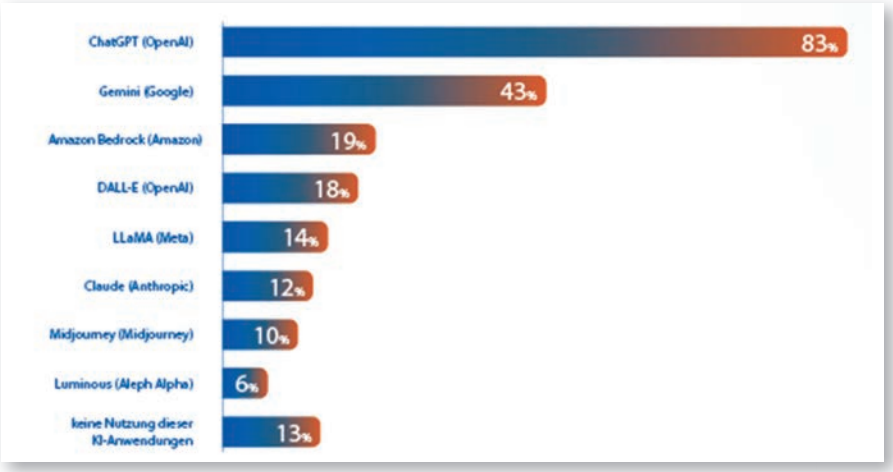
Österreich und die EU spielen im weltweiten KI-Rennen nicht die erste Geige. Das soll sich ändern. Im Februar kündigte die Europäische Union auf dem KI-Gipfel in Paris umfangreiche Investitionen in die KI-Branche an, um im globalen Wettbewerb aufzuholen und die technologische Souveränität Europas zu stärken. Gemeinsam mit einem klaren Fokus auf die Entwicklung von sicherer und ethischer KI sollen diese Investitionen Europa zu einer weltweiten Führungsrolle verhelfen.

In seiner GenAI-Studie untersucht adesso, wie österreichische Unternehmen Österreich und Europa in Sachen generative KI aktuell einschätzen, wie fit sie sich selbst sehen und welche Rolle GenAI inzwischen in ihrem Arbeitsalltag spielt. Dafür befragte der IT-Dienstleister 100 Führungskräfte aus der österreichischen Wirtschaft.

„Österreichische Unternehmen fühlen sich immer besser für generative KI aufgestellt. Das ist ein deutliches Zeichen für die zunehmende Akzeptanz dieser Technologie. Mit Blick auf strategische Nutzung besteht aber noch erheblicher Nachholbedarf“, kommentiert Tom Strube, Head of Consulting der adesso Austria. „Der Report macht aber auch den Bedarf an europäischen Lösungen sichtbar. Die Unternehmen warten auf Lösungen aus der EU, die das Zeug haben, sichere und ethische GenAI-Anwendungen zu werden.“

ZENTRALE ERGEBNISSE DER UMFRAGE:

- Unternehmen warten auf „GenAI made in Europe“. Die Befragten senden ein klares Signal für den Bedarf an europäischen Alternativen. Für 66 Prozent ist es wichtig oder sehr wichtig, dass die GenAI-Anwendungen, die ihr Unternehmen nutzt oder nutzen könnte, in der Europäischen Union entwickelt wurden. Damit zeigen sie ein großes Bewusstsein für digitale Souveränität und den starken Wunsch, sich nicht von außereuropäischen Anbietern abhängig zu machen.
- Regulierung ist ein notwendiges Instrument. Die Mehrheit der Befragten befürwortet eine stärkere Regulierung von KI-Anwendungen wie ChatGPT: 52 Prozent stimmen dem „eher“ zu, 27 Prozent sogar „voll und ganz“. Diese Zahlen zeigen, dass Unternehmen Regulierung nicht nur akzeptieren, sondern dass sie von vielen als notwendiges Instrument angesehen wird, um verantwortungsvoll mit KI umzugehen und mögliche Risiken zu kontrollieren.
- Die Zahlen zeigen: Die österreichische Wirtschaft ist auf GenAI noch längst nicht ausreichend vorbereitet. Nur 5 Prozent der Befragten halten den aktuellen Stand für sehr gut, 21 Prozent für gut – das ist ein niedriger Anteil angesichts der Dynamik des Themas. Gleichzeitig bewerten 35 Prozent die Vorbereitung als mangelhaft, weitere 15 Prozent nur als ausreichend. Diese Einschätzungen machen deutlich: Wenn Unternehmen das Potenzial von GenAI künftig ausschöpfen wollen, braucht es jetzt gezielte Investitionen, Qualifizierung und strategische Weichenstellungen.
- GenAI-Fitness der Unternehmen steigt. Auch sich selbst sehen die Unternehmen inzwischen besser auf GenAI vorbereitet. Der Anteil der Firmen, die sich gut oder sehr gut gerüstet fühlen, stieg gegenüber dem Vorjahr von 22 Prozent auf 39 Prozent. Auf der strategischen Ebene kommt GenAI aber erst zaghaft in den Unternehmen an. Lediglich 48 Prozent haben bereits eine KI-Strategie entwickelt – und 20 Prozent von diesen Unternehmen berücksichtigen dabei lediglich die klassische KI. BO



Auch wenn die Nachfrage nach europäischen GenAI-Lösungen wächst, setzen österreichische Unternehmen aktuell noch überwiegend auf Lösungen US-amerikanischer Anbieter.

Foto: adesso

TRÜGERISCHE SICHERHEIT

Backups sind zweifellos ein essenzieller Bestandteil jeder IT-Sicherheitsstrategie – gleichzeitig vermitteln sie oft eine trügerische Sicherheit. Denn wer glaubt, dass ein solides Backup allein ausreicht, um ERP-Systeme vor Cyberangriffen zu schützen, setzt auf eine gefährliche Fehleinschätzung.

Am 31. März erinnert der World Backup Day Unternehmen weltweit daran, ihre Daten regelmäßig zu sichern. Lange Zeit war das größte Risiko von Ransomware-Angriffen, dass Unternehmen den Zugriff auf ihre Daten verlieren. Doch da viele Organisationen mittlerweile über robuste Backup-Strategien verfügen, setzen immer mehr Cyberkriminelle auf eine neue Taktik mit doppelter und sogar dreifacher Erpressungsmethode: Verschlüsselung, Datenexfiltration und Erpressung durch Veröffentlichungsdrohungen. Statt „nur" Daten zu verschlüsseln, stehlen Angreifer sensible Informationen, beispielsweise aus ERP-Systemen – etwa Kundendetails, Lieferantenkonditionen oder strategische Finanzdaten oder technische Unterlagen wie Baupläne, Produktionsverfahren und Softwarecodes – und drohen, diese offenzulegen oder zu verkaufen. Dieser Ansatz ist nicht nur potenziell existenzbedrohend und rufschädigend, sondern auch besonders gefährlich für Unternehmen mit strengen Datenschutz- und Compliance-Anforderungen, da eine Veröffentlichung erhebliche regulatorische Konsequenzen nach sich ziehen kann. In vielen Fällen sind Unternehmen dann gezwungen, hohe geforderte Summen zu zahlen, selbst wenn Backups eine Wiederherstellung der Systeme ermöglichen würden.

BACKUPS SIND WICHTIG – ABER NICHT GENUG

Ein Backup schützt also vor Datenverlust, aber nicht vor ungewollten Veränderungen oder gezielten Angriffen auf kritische Geschäftsprozesse. ERP-Systeme enthalten hochsensible Informationen, die nicht nur gesichert, sondern aktiv geschützt und überwacht werden müssen. Ohne eine ganzheitliche Sicherheitsstrategie können Angreifer unbemerkt Zugriff auf ERP-Daten erlangen, bösartige Änderungen vornehmen oder mit der Veröffentlichung gestohlener Daten erpressen.

WIE UNTERNEHMEN IHRE ERP-DATEN UMFASSEND ABSICHERN

Neben regelmäßigen Backups, die eine bewährte Methode zur Schadensminimierung bei Systemausfällen oder klassischen Ransomware-Attacken mit Verschlüsselung sind, braucht es ein mehrschichtiges Sicherheitskonzept, das potenzielle Angriffsflächen frühzeitig erkennt, Schwachstellen automatisch schließt, Manipulationen verhindert und die Systemintegrität sicherstellt. Dazu gehören:

- Automatisiertes Log-Monitoring und 24/7-Überwachung auf Anomalien und verdächtige Aktivitäten in ERP-Systemen
- Zero-Trust-Sicherheitsmodelle mit strikten Zugriffskontrollen, um unautorisierte Zugriffe und Änderungen sowie Exfiltrationen zu verhindern
- Automatisiertes Patching von Schwachstellen, um zu verhindern, dass sich Angreifer überhaupt erst Zugang zu Netzwerken und Systemen verschaffen
- Transaktions- und Code-Überprüfungen, um versteckte Manipulationen zu erkennen

WERTVOLLE ERINNERUNG

Der World Backup Day ist eine wertvolle Erinnerung für Unternehmen, sich der essenziellen Rolle der Datensicherung bewusst zu werden. Ein reines Wiederherstellungskonzept kann angesichts modernster Angriffstaktiken jedoch nicht verhindern, dass Geschäftsdaten und -prozesse kompromittiert oder regulatorische Vorgaben verletzt werden. Daher muss ein ganzheitlicher Sicherheitsansatz darüber hinausgehen. Unternehmen sollten auf präventive Maßnahmen wie kontinuierliches Log-Monitoring, Schwachstellen-Scanning und Zero-Trust-Konzepte setzen, um Bedrohungen frühzeitig zu erkennen und abzuwehren. Ergänzend dazu sind automatisierte Security-Lösungen essenziell, um Fehlkonfigurationen in Echtzeit zu identifizieren und Compliance-Anforderungen durchgehend einzuhalten. Letztlich gilt: Ein Backup ist gut – Sicherheitsmaßnahmen, die verhindern, dass es überhaupt zum Ernstfall kommt, sind besser. VE

Foto: Onapsis

ANGRIFFSTAKTIKEN

»Ein reines Wiederherstellungskonzept kann angesichts modernster Angriffstaktiken jedoch nicht verhindern, dass Geschäftsdaten und -prozesse kompromittiert oder regulatorische Vorgaben verletzt werden.«

Volker Eschenbächer, VP Sales International Onapsis

DER AUTOR

Volker Eschenbächer ist VP Sales International (EMEA & APAC) bei Onapsis

TREND MICRO

Künstliche Intelligenz wird unverzichtbar, um wachsende Security-Herausforderungen zu meistern und KI-basierte Software-Architekturen abzusichern. Eine wichtige Rolle spielen dabei KI-Agenten.

Proaktive statt reaktive Cybersecurity

1

■ Künstliche Intelligenz hat sich vom experimentellen Add-on zum integralen Bestandteil moderner Geschäftsprozesse entwickelt. Auch in der Cybersicherheit kommt die neue Technologie zum Einsatz – und das bereits seit 20 Jahren. Tatsächlich gibt es kaum noch eine Security-Lösung, in die nicht irgendeine Art von künstlicher Intelligenz integriert ist, sei es in Form von maschinellem Lernen, Deep Learning oder generativer KI. Angesichts immer komplexerer IT-Umgebungen, einer professionalisierten Bedrohungslandschaft und zunehmend KI-basierten Software-Architekturen gewinnt künstliche Intelligenz stark an Bedeutung für die Verteidigung. Künftig werden intelligente Algorithmen entscheidend dafür sein, ob wir uns resilient gegen immer raffiniertere Angreifer aufstellen können.

Wachsende Herausforderungen erfordern optimale Unterstützung

Cyberkriminelle sind heute meist keine Einzeltäter mehr, sondern in einer hoch professionellen Schattenindustrie organisiert, die aus Hacking-Services, Angriffs-Tools, erbeuteten Daten und Erpressung lukrative Geschäftsmodelle aufgebaut hat. Sie entwickeln ihre Angriffstechniken immer weiter und setzen dafür modernste Technologie ein. Neben monetär motivierten Cybercrime-Organisationen sehen wir – bedingt durch die angespannte geopolitische Lage – verstärkt auch staatlich unterstützte Gruppierungen, die das Ziel verfolgen, unsere Gesellschaft zu destabilisieren. Für kleine IT- oder IT-Security-Teams wird die Verteidigung immer mehr zu einem Kampf wie David gegen Goliath. Sie stehen nicht nur einer mächtigen cyberkriminellen Industrie gegenüber, sondern sind auch mit einer wachsenden Angriffsfläche und einer Flut an Warnmeldungen konfrontiert, die es erschwert, kritische Indikatoren zu erkennen. Dazu kommen neue regulatorische Anforderungen. Nur mit optimaler technologischer Unterstützung sind Securityteams noch in der Lage, die zunehmenden Herausforderungen zu meistern.

Superkräfte fürs Securityteam

KI ist wie ein Zaubertrank, der selbst kleinen Securityteams Superkräfte verleiht. Die neue Technologie unterstützt sie dabei, die komplexe Angriffsfläche stets im Blick zu behalten, Risiken zu bewerten, Schwachstellen proaktiv zu schließen und im Ernstfall schnell zu reagieren. Maschinelles Lernen kann An-

2

Eine einheitliche Cybersecurity-Plattform ermöglicht proaktiven Schutz für die gesamte IT-Umgebung.

3

KI reduziert die Komplexität und ermöglicht umfassende Sichtbarkeit über das Cyberrisikoniveau des Unternehmens.

zeichen für Cyberangriffe verhaltensbasiert erkennen und auch bisher unbekannte Bedrohungen aufdecken. Außerdem kommen Machine Learning und Deep Learning zum Beispiel zum Einsatz, um Phishing-Mails herauszufiltern oder Deepfakes als ungebetene Gäste in Videokonferenzen zu identifizieren. Auch Large Language Models (LLMs) übernehmen eine wichtige Rolle: Sie helfen Mitarbeitern etwa dabei, technische Informationen leichter zu verstehen und schnell die richtigen Handlungsempfehlungen zu finden.

Spezialisierte Cybersecurity-KI-Agenten

Der nächste Schritt in der Entwicklung sind KI-Agenten, die wie virtuelle Securitymitarbeiter selbstständig Aufgaben übernehmen und im Team zusammenarbeiten. Dabei lernen die Agenten dynamisch dazu. Auf diese Weise können Sicherheitsverantwortliche ihre Strategie kontinuierlich validieren und optimieren. Da die KI-Agenten die Verteidiger in die Lage versetzen, Angriffspfade und -taktiken vorherzusehen, können sie schneller sein als der Gegner. So ermöglicht die neue Technologie einen proaktiven Security-Ansatz, der die Resilienz erheblich steigert.

KI-Architekturen erfordern eine dynamische Absicherung

Dieser Paradigmenwechsel von einer reaktiven zu einer proaktiven Security-Strategie ist nicht nur angesichts der Bedrohungslage unverzichtbar, sondern auch im Hinblick auf den zunehmenden Einsatz von KI in Geschäftsprozessen. Denn mit der neuen Technologie verändern sich Software-Architekturen und Angriffsflächen. KI-Workloads führen neue Architekturschichten ein, sind datengetrieben und verändern sich kontinuierlich.

Auch die Cybersicherheit muss sich daher dynamisch ausrichten und KI-Modelle, den Datenfluss sowie deren Infrastrukturen laufend überwachen. So lassen sich neue, KI-spezifische Risiken mindern, die darauf abzielen, KI-Modelle zu kompromittieren oder sensible Daten zu extrahieren. Wichtig ist, Security in alle Ebenen der KI-Infrastruktur zu integrieren und die gesamte Lieferkette zu berücksichtigen – von der Hardware über die Cloud-Umgebung und Schnittstellen zu Drittsystemen bis zum Foundation-Modell und Nutzer-Interface. Voraussetzung dafür schafft eine integrierte und KI-gestützte Cybersecurity-Plattform.

Die intelligente Security-Schaltzentrale

Diese stellt sicher, dass sämtliche Security-Systeme und KI-Agenten nahtlos interagieren und auf die bestmögliche Datenbasis zugreifen können. Hier laufen alle Security-relevanten Informationen zusammen und werden alle Security-Prozesse zentral gemanagt. Das reduziert die Komplexität erheblich und schafft umfassende Transparenz über Aktivitäten, Risiken und Bedrohungen in der gesamten IT-Umgebung.

Damit dient eine solche Plattform als „Single Source of Truth" und erleichtert mit übersichtlichen Reports und Kennzahlen den IT-Verantwortlichen wie der Geschäftsleitung die Kommunikation und das Management von Cyberrisiken. Diese stellen laut dem Allianz Risk Barometer das größte Geschäftsrisiko weltweit dar. Mit der weiter voranschreitenden Digitalisierung von Geschäftsprozessen und der rasanten Entwicklung im Bereich KI wird sich das noch verschärfen. Umso wichtiger ist es, dass Geschäftsführungen ein grundlegendes Verständnis für die Cyberrisiken haben, denen ihr Unternehmen ausgesetzt ist, und deren Management als Leitungsaufgabe vorantreiben.

Die Zukunft der Cybersicherheit ist proaktiv und KI-gestützt

Während sich Bedrohungslandschaften, IT-Infrastrukturen und Software-Architekturen weiterentwickeln, muss auch die Security Schritt halten. Reaktive Cybersicherheit ist nicht mehr zeitgemäß. Mit einer proaktiven Security-Strategie, die das Potenzial von KI-Agenten ausschöpft, können Unternehmen dagegen Risiken vorausschauend mindern und auch künftige Herausforderungen meistern. Entscheidend für die Wirksamkeit ist ein Plattformansatz, der Security-Daten, -Systeme und -KI-Modelle zusammenführt und zentral steuert. So lässt sich die nötige Transparenz und Effizienz erzielen, um die Verteidigung kontinuierlich an wachsende Anforderungen anzupassen.

www.trendmicro.com

Anzeige • Fotos: Frolopiaton Palm/Freepik (1), Trend Micro (2+3) • Text: Hannes Steiner, Vice President DACH

1

NEUES SICHERHEITSPROGRAMM

Microsoft hat ein neues europäisches Sicherheitsprogramm ins Leben gerufen, um die Cybersicherheit in Europa zu stärken. Es beinhaltet eine verstärkte Zusammenarbeit mit Regierungen, zusätzliche Investitionen und den Ausbau von Partnerschaften zur Abwehr von Cyberangriffen.

Mit dem Fortschritt von KI und digitalen Technologien entwickelt sich auch die Cyberbedrohungslage in Europa weiter und stellt uns vor neue Herausforderungen, die stärkere Partnerschaften und verbesserte Lösungen erfordern. Ransomware-Gruppen und staatlich geförderte Akteure aus Russland, China, dem Iran und Nordkorea werden größer und immer raffinierter. Der europäische Cyberschutz kann es sich nicht leisten, stillzustehen. Aus diesem Grund kündigte Microsoft Anfang Juni eine neue Initiative an, mit der das Unternehmen sein langjähriges Engagement zur Verteidigung von Europas Cybersicherheit ausweiten will. „Wir starten heute ein neues Europäisches Sicherheitsprogramm und setzen damit eine unserer fünf digitalen Zusicherungen für Europa um, die ich vor fünf Wochen in Brüssel vorgestellt habe. Dies ergänzt unser seit Langem bestehendes Government Security Program für Regierungen“, so Brad Smith, Vice Chair und Präsident von Microsoft, in einer Aussendung.

Das neue Programm erweitert den geografischen Umfang der bisherigen Arbeit und fügt neue Elemente hinzu, die für den Schutz Europas von entscheidender Bedeutung sein werden. KI wird damit als Instrument zum Schutz von Cybersicherheit in den Mittelpunkt der Arbeit gestellt und der Schutz von digitaler und KI-Infrastruktur gestärkt. Das Europäische Sicherheitsprogramm startet mit drei neuen Elementen: verstärkter Austausch von KI-basierten Bedrohungsinformationen mit Europäischen Regierungen, zusätzliche Investitionen zur Stärkung von Cybersicherheitskapazitäten und Resilienz sowie Ausbau von Partnerschaften zur Abwehr von Cyberangriffen und Zerschlagung cyberkrimineller Netzwerke.
Dieses Programm stellt Microsoft allen europäischen Regierungen kostenlos zur Verfügung, darunter allen 27 Mitgliedsstaaten der Europäischen Union sowie den EU-Beitrittsländern, den Mitgliedern der Europäischen Freihandelsassoziation (EFTA), dem Vereinigten Königreich, Monaco und dem Vatikan.

Microsoft warnt vor anhaltenden Cyberangriffen staatlicher Akteure auf europäische Netzwerke – gleichzeitig entwickeln Kriminelle neue Ransomware-as-a-Service-Tools.

Fotos: Adobe Stock/AI.noevation (1), Adobe Stock/MrJeans (2), Adobe Stock/mozZz (3)

NEUE MASSNAHMEN SIND NOTWENDIG – DAS AKTUELLE BEDROHUNGSUMFELD

Microsoft beobachtet weiterhin anhaltende Bedrohungsaktivitäten von staatlichen Akteuren, die europäische Netzwerke angreifen. Akteure aus Russland und China sind in Europa besonders aktiv. Es überrascht nicht, dass Russland weiterhin besonders auf Ziele in der Ukraine sowie auf die europäischen Staaten fokussiert ist, die die Ukraine unterstützen. Staatliche Akteure und Bedrohungsaktivitäten aus dem Iran und Nordkorea verfolgen in Europa vor allem Spionagezwecke, indem sie Zugangsdaten stehlen oder Schwachstellen ausnutzen, um sich Zugang zu Unternehmens- und Regierungsnetzwerken zu verschaffen. Mehrere Kampagnen, darunter auch solche aus China, haben es auch auf akademische Einrichtungen abgesehen. In diesem Kontext kompromittieren sie etwa Nutzer:innen-Konten, um auf vertrauliche Forschungsdaten zuzugreifen oder geopolitische Spionage gegen Thinktanks zu betreiben. Neben den Bedrohungen durch Nationalstaaten setzen Cyberkriminelle auch weiterhin auf die Entwicklung von Ransomware-as-a-Service-Tools. Microsoft beobachtet die zunehmende Popularität illegaler Websites, die durch Ransomware gewonnene Erkenntnisse veröffentlichen und diese dann kriminellen Gruppen für die Durchführung von Angriffen in ganz Europa zur Verfügung stellen. Und die wachsende Bedeutung von KI verändert auch das Verhalten der Bedrohungsakteure. Microsoft hat festgestellt, dass KI von Bedrohungsakteuren für die Aufklärung, Schwachstellenforschung, Übersetzung, LLM-verfeinerte operative Befehlstechniken, Ressourcenentwicklung, Skripting-Techniken, Umgehung von Erkennungsmaßnahmen, Social Engineering und Brute-Force-Angriffe eingesetzt wird. Aus diesem Grund verfolgt Microsoft jetzt jede böswillige Nutzung der neuesten KI-Modelle und verhindert proaktiv, dass bekannte Bedrohungsakteure die KI-Produkte von Microsoft nutzen. Dies soll auch die Bedeutung sicherer Entwicklung und strikter Tests von KI-Modellen, der Nutzung von KI für Cyberabwehr sowie enger öffentlich-privater Partnerschaften zum Austausch neuester Erkenntnisse über KI und Cybersicherheit unterstreichen.

VERSTÄRKTER AUSTAUSCH VON KI-BASIERTEN BEDROHUNGSINFORMATIONEN MIT REGIERUNGEN

Das Government Security Program (GSP) von Microsoft stellt Regierungen seit Langem vertrauliche Sicherheitsinformationen und Ressourcen zur Verfügung, die ihnen helfen, Produkte und die sich entwickelnde Bedrohungslandschaft besser zu verstehen – dies gilt insbesondere für Bedrohungen durch nationalstaatliche Akteure. Das Europäische Sicherheitsprogramm verbessert den Informationsfluss und erweitert den Zugang zu verwertbaren Bedrohungsdaten für europäische Regierungen. Dieses Programm ist auf nationale Bedrohungsumgebungen zugeschnitten, wird durch modernste KI-Informationen ermöglicht und nach Möglichkeit in Echtzeit bereitgestellt. Das soll Regierungen helfen, neuesten Cyberbedrohungen einen Schritt voraus zu sein. Erreicht werden soll das etwa durch die Nutzung von Erkenntnissen aus Bedrohungsdaten. Microsoft verfolgt die Cyberaktivitäten von Nationalstaaten und bietet zeitnahe Einblicke in sich entwickelnde globale Bedrohungen. Dazu wird KI zur Unterstützung der Analysen genutzt. Das verbessert die Sicht-

Im Rahmen eines Pilotprogramms mit dem European Cybercrime Center (EC3) von Europol werden Ermittler:innen der Microsoft Digital Crimes Unit (DCU) im EC3-Hauptquartier in Den Haag eingesetzt.

barkeit von Bedrohungen und beschleunigt die Fähigkeit zum Informationsaustausch und zur Weitergabe der neuesten Erkenntnisse über die Taktiken, Techniken und Vorgehensweisen – einschließlich des böswilligen Einsatzes von KI. Durch die schnellere und umfangreichere Bereitstellung solcher Informationen unterstützt Microsoft europäische Regierungen dabei, ihre Cyberresilienz zu stärken und eine proaktive Verteidigung zu ermöglichen. Auch die Microsoft Digital Crimes Unit (DCU) spielt eine entscheidende Rolle bei der Aufdeckung und Zerschlagung globaler cyberkrimineller Infrastrukturen. Über das Cybercrime Threat Intelligence Program (CTIP) stellen die Expert:innen diese Informationen vertrauenswürdigen europäischen Partnern zur Verfügung, um schnelle Reaktionen und koordinierte Durchsetzungsmaßnahmen möglich zu machen.

Außerdem beobachtet das Microsoft Threat Analysis Center (MTAC), dass Operationen zur Einflussnahme in Europa zunehmend KI einsetzen, um mit künstlichen „Deepfake"-Inhalten in die Irre zu führen und zu täuschen. MTAC wird daher regelmäßig Informationen über ausländische Einflussnahme bereitstellen, die zeitnahe Einblicke in die Taktiken, Narrative und digitalen Plattformen staatlich gelenkter Akteure bieten werden.

Diese Briefings sollen politischen Entscheidungsträger:innen und Sicherheitsakteur:innen helfen, den sich entwickelnden Desinformationskampagnen und hybriden Bedrohungen, die auf demokratische Institutionen und das öffentliche Vertrauen abzielen, immer einen Schritt voraus zu sein. Microsoft hat sich außerdem zu einer proaktiven und transparenten Sicherheitskommunikation verpflichtet, insbesondere im Hinblick auf neue Bedrohungen und sich entwickelnde Schwachstellen. Durch strukturierte Programme wie den „Threat Microsoft Security Update Guide", den „Vulnerability Reporting Process" und das „Microsoft Defender Vulnerability Management" sollen Kund:innen mit zeitnahen, praxisorientierten Informationen versorgt werden. Im Rahmen dieser nun ausgeweiteten Verpflichtung will Microsoft seinen Partnern im Europäischen Sicherheitsprogramm mit Vorrang sicherheitsrelevante Informationen geben, einschließlich Anleitungen zur Behebung von Sicherheitslücken – mit dem Ziel, das Situationsbewusstsein zu verbessern und schnellere Reaktionen zu ermöglichen.

ZUSÄTZLICHE INVESTITIONEN ZUR STÄRKUNG VON CYBERSICHERHEITSKAPAZITÄTEN UND RESILIENZ

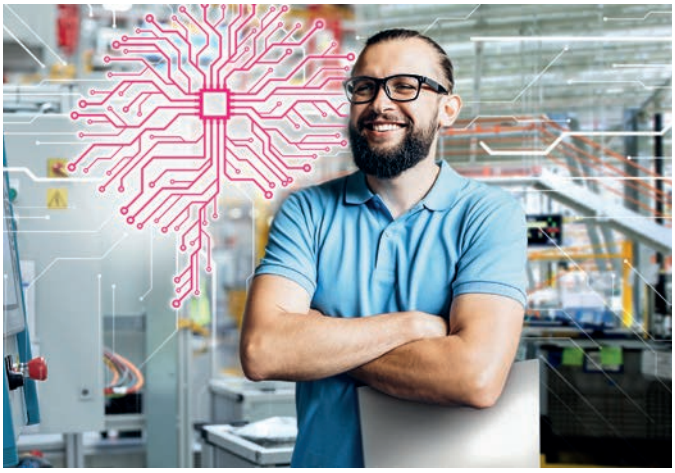
Digitale Resilienz – also die Fähigkeit, Cyberbedrohungen und -störungen zu antizipieren, ihnen zu widerstehen, sich von ihnen zu erholen und sich auf sie einzustellen – erfordert mehr als nur Technologie. Sie erfordert Investitionen in Menschen, Institutionen und Partnerschaften. Im Rahmen des Europäischen Sicherheitsprogramms will Microsoft zusätzliche Ressourcen bereitstellen und die Zusammenarbeit mit Regierungen, der Zivilgesellschaft und Innovatoren ausbauen, um lokale Fähigkeiten zu stärken und nachhaltige Resilienz aufzubauen. Zu den Schwerpunkten gehört u. a. die Stärkung der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Microsoft hat ein neues Pilotprogramm mit dem European Cybercrime Center (EC3) von Europol gestartet, in dessen Rahmen Ermittler:innen der Microsoft Digital Crimes Unit (DCU) im EC3-Hauptquartier in Den Haag eingesetzt werden, um den Informationsaustausch und die operative Koordination zu verbessern. Ein weiterer Punkt ist die Unterstützung der Zivilgesellschaft und Schutz vor Ransomware. Microsoft hat dazu seine dreijährige Partnerschaft mit dem CyberPeace Institute verlängert, um Nichtregierungsorganisationen zu unterstützen und bösartige Akteure zur Rechenschaft zu ziehen. Fast 100 Microsoft-Mitarbeiter:innen stellen ehrenamtlich ihre Zeit und ihr Fachwissen zur Verfügung, um die am meisten gefährdeten Menschen im Cyberspace zu schützen. Durch eine neue Zusammenarbeit mit dem Western Balkans Cyber Capacity Centre (WB3C) wird Microsoft die Cybersicherheit in einer Region ausbau- ››

Foto: Adobe Stock/Menyhert

KUMAVISION GMBH

Die Automatisierung und der Einsatz von künstlicher Intelligenz (KI) senken Kosten, entlasten das Personal und ermöglichen eine Skalierung des Business. ERP-Lösungen von KUMAVISION kombinieren dazu branchenspezifische Best-Practice-Prozesse mit serienmäßiger KI-Unterstützung und einer schnellen Einführung.

Dream-Team für mehr Produktivität



In allen Unternehmensbereichen lassen sich zentrale Abläufe digitalisieren und automatisieren. Einige Beispiele: die automatisierte Verarbeitung von Eingangsrechnungen, das systemgesteuerte Erstellen von Bestellvorschlägen im Einkauf, die softwaregestützte Sanktionslistenprüfung, die Zollabwicklung direkt aus der ERP-Lösung, die tagesaktuelle Material- und Produktionsplanung für eine optimale Auslastung von Maschinen und Ressourcen, die automatisierte Abrechnung von wiederkehrenden Leistungen oder die Einsatzplanung von Servicetechnikern. In vielen Fällen spielt es dann auch keine Rolle, ob 10, 100 oder 1.000 Vorgänge vom System ohne Nutzereingriffe bearbeitet werden.

Künstliche Intelligenz als Effizienzturbo

KI ist ein Schlüsselfaktor bei der Automatisierung: Sie bereitet unstrukturierte Daten – wie z. B. natürliche Sprache – auf, vervollständigt die Daten und stellt ggf. Rückfragen bei fehlenden Informationen, damit die ERP-Software mit ebenso strukturierten wie vollständigen Daten Prozesse systemgesteuert bearbeiten kann. Ebenso entlastet KI das Personal von Routineaufgaben, wie z. B. Suchen nach Informationen, Beantworten von E-Mails, Analysieren von Daten, Zusammenfassen von Meetings … Viele Unternehmen wollen das Potenzial von KI nutzen, stehen aber vor der Frage, wie sie diese wegweisende Innovation in ihre Geschäftsprozesse einbinden. Die Einführung externer KI-Lösungen ist immer mit einem großen Zeit- und Kostenaufwand verbunden. Zudem ist die Zielsetzung oft unscharf: „Irgendwas mit KI" reicht nicht aus.

Serienmäßige KI-Unterstützung

Die ERP-Branchenlösungen von KUMAVISION für Industrie, Handel, Medizintechnik und Projektdienstleister bringen Dutzende Best-Practice-Prozesse mit und ermöglichen damit eine schnelle Time-to-Value. Sie basieren auf Microsoft Dynamics 365 und verfügen damit bereits im Standard über eine integrierte KI-Unterstützung. Der virtuelle KI-Assistent Microsoft Copilot setzt auf der führenden ChatGPT-Technologie auf und wurde von Microsoft an die Anforderungen von Business-Kunden angepasst und erweitert.

Ein echtes Alleinstellungsmerkmal: Microsoft Copilot steht im gesamten Microsoft-Ökosystem zur Verfügung. Unternehmen können damit nicht nur im ERP-System, sondern auch in der CRM-Software sowie Office, Outlook und Teams verschiedenste Aufgaben beschleunigen und automatisieren. Schnell und einfach, ganz ohne aufwendige Einführungsprojekte.

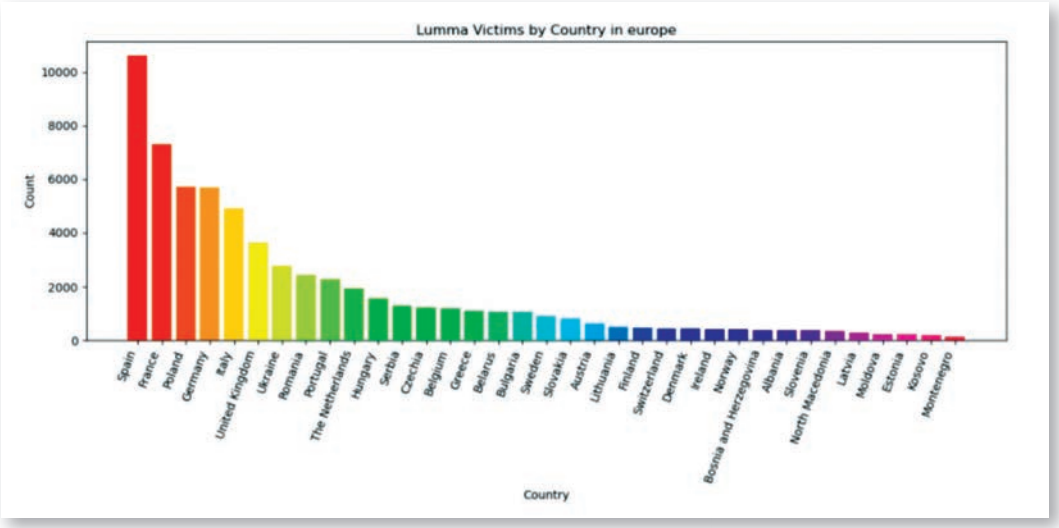
Kurze Innovationszyklen, nachhaltige Wettbewerbsvorteile

Cloud-Lösungen, die sich wie die ERP-Lösungen von KUMAVISION jeden Monat im Hintergrund automatisch aktualisieren, sind Voraussetzung dafür, um die Vorteile von Automatisierung und künstlicher Intelligenz zeitnah nutzen zu können. Angesichts des Tempos, mit dem sich künstliche Intelligenz weiterentwickelt und laufend neue Unterstützungsfunktionen bereitstellt, ist das ein echter Wettbewerbsvorteil gegenüber Unternehmen, die ihre ERP-Software nur im Abstand von mehreren Jahren mit einem Update-Projekt aktualisieren.

KUMA VISION ERP CRM DMS CLOUD

RÜCKFRAGEN & KONTAKT
KUMAVISION GmbH
Millennium Park 4
6890 Lustenau
Tel.: +43 5577 890 62-100
lustenau@kumavision.com
www.kumavision.at

Anzeige • Fotos: KUMAVISION GmbH



Zwischen März und Mai 2025 wurden mehr als 394.000 von Lumma infizierte Windows-Systeme weltweit entdeckt – darunter viele in Europa.

›› en, in der böswillige Akteure seit Langem versuchen, die an die EU angrenzenden Länder zu destabilisieren. Microsoft stellt zusätzliche Ressourcen bereit, um die Forschung zu unterstützen, den Nachwuchs im Bereich Cybersicherheit zu fördern und fortschrittliche, KI-gestützte Sicherheitstools in realen Umgebungen unter Verwendung von Microsofts Security Stack sowie der Funktionen von Azure und Copilot zu testen. Dazu arbeitet Microsoft mit dem britischen Laboratory for AI Security Research (LASR) zusammen, einer öffentlich-privaten Partnerschaft, die gegründet wurde, um die KI-Sicherheit zur Unterstützung der nationalen Sicherheit und des wirtschaftlichen Wohlstands Großbritanniens voranzutreiben. Gemeinsam wurde ein Forschungsprogramm gestartet, das sich auf Herausforderungen im Bereich der KI-Cybersicherheit mit Schwerpunkt auf kritischer Infrastruktur und agentenbasierter KI-Sicherheit konzentriert.

AUSBAU VON PARTNERSCHAFTEN UND ZERSCHLAGUNG CYBERKRIMINELLER NETZWERKE

Im Rahmen des Europäischen Sicherheitsprogramms baut Microsoft gezielt die Partnerschaften mit Strafverfolgungsbehörden und regionalen Akteuren aus. Das Ziel ist es, proaktiv neue und innovative Wege zur Bekämpfung böswilliger und krimineller Aktivitäten zu finden. So hat beispielsweise die Digital Crimes Unit (DCU) von Microsoft im vergangenen Monat in Zusammenarbeit mit Europol und anderen Stellen Lumma ausgeschaltet, eine weit verbreitete Infostealer-Malware, die zum Diebstahl von Passwörtern, Finanzdaten und Krypto-Wallets verwendet wurde. In nur zwei Monaten infizierte Lumma weltweit fast 400.000 Geräte, viele davon in Europa. Im Rahmen der Operation wurden über 2.300 Command-and-Control-Domains beschlagnahmt und gesperrt. Aufbauend auf dieser Maßnahme arbeitet Microsoft mit Europol zusammen, um neue Möglichkeiten zu identifizieren, mit denen wir Cyberkriminelle weiterhin wirksam bekämpfen und ihre Aktivitäten verhindern können.

Um künftige Takedowns zu beschleunigen, wurden im April 2025 das Statutory Automated Disruption (SAD)-Programm gestartet. Diese Initiative automatisiert die Benachrichtigung von Hosting-Anbietern über Rechtsverstöße und ermöglicht eine schnellere Entfernung bösartiger Domains und IP-Adressen. SAD konzentriert sich zunächst auf Europa und die USA und erhöht die Geschäftskosten für Cyberkriminelle und erschwert es ihnen, in großem Maßstab zu operieren. Darüber hinaus gibt es Kooperationen mit lokalen Internetanbietern, um betroffene Nutzer:innen zu schützen und sicherzustellen, dass Regierungen einen besseren Überblick über aufkommende Bedrohungen haben.

Die DCU spielt seit Langem eine führende Rolle bei der proaktiven Bekämpfung von Cyberbedrohungen, einschließlich solcher, die von staatlichen Akteuren ausgehen. Seit 2016 hat Microsoft sieben Klagen eingereicht, um staatliche Bedrohungsakteure aus Ländern wie Russland, China, dem Iran und Nordkorea ins Visier zu nehmen und zu stören. Zuletzt leitete Microsoft im September 2024 eine Aktion zur Unterbrechung gegen den oben genannten russischen Akteur Star Blizzard ein, der dafür bekannt ist, politische Ziele im Zusammenhang mit den Wahlen im Vereinigten Königreich 2022 gehackt und NATO-Länder ins Visier genommen zu haben, um seine geopolitischen Interessen in Bezug auf die Ukraine voranzutreiben. Microsoft hat die russischen Akteure enttarnt und insgesamt über 140 bösartige Domains direkt beschlagnahmt, wodurch die laufenden Kampagnen erheblich beeinträchtigt wurden und Star Blizzard gezwungen war, seine Angriffsmethoden auf andere Plattformen umzustellen, was Microsoft Threat Intelligence anschließend in einem Sicherheitsblog öffentlich bekannt gab.

Diese Bemühungen sind Teil der umfassenden Strategie zur Zusammenarbeit mit Strafverfolgungsbehörden in ganz Europa. Dazu wird bereits an koordinierten Maßnahmen zum Schutz des digitalen Ökosystems gearbeitet. Außerdem sind die Expert:innen vom Microsoft überzeugt, dass Abschreckung ein wichtiger Pfeiler der modernen Cybersicherheit ist. Die Cyber-Diplomacy-Toolbox der EU spielt dabei eine wichtige Rolle, indem sie die Koordinierung der Krisenreaktion unterstützt und ein klares Signal sendet, dass böswillige Aktivitäten nicht ohne Folgen bleiben – weder rechtlich, operativ noch in Bezug auf die Reputation. BS

Foto: Microsoft

BE-TERNA GMBH

Um in der Praxis tatsächlich von KI-Szenarien zu profitieren, ist die richtige Vorarbeit entscheidend. Der Spezialist für Business-Software BE-terna setzt dabei auf ein dreistufiges Vorgehen.

KI-Einführung nach Plan – mit Plan!


1


2

Für den erfolgreichen Einsatz von künstlicher Intelligenz sind die richtigen Schritte entscheidend.

Der Druck auf Unternehmen steigt, möglichst schnell auf den KI-Zug aufzuspringen. Doch noch immer kommen zahlreiche KI-Projekte nicht über die Konzeptphase hinaus: Erhoffte Vorteile stellen sich nicht ein, die Ergebnisse der Technologie liefern nicht die benötigte Qualität, eine solide Umsetzung gestaltet sich als zu aufwendig.

Wer nicht frühzeitig beginnt, gerät Mitbewerbern gegenüber ins Hintertreffen. Doch Geschwindigkeit ist nicht alles: Eine schnelle KI-Einführung ohne echten Nutzen bringt kein Unternehmen voran. Um tatsächlich und langfristig von den Vorteilen der intelligenten Technologie zu profitieren, sollten Interessenten mit einem Plan vorgehen. Dazu empfehlen sich drei Stufen:

1. Wissenserwerb

Wer sich ein grundlegendes Verständnis der Funktionsweise der intelligenten Technologie aneignet, kann Chancen und Risiken in der Praxis deutlich besser einschätzen. Auch sollten Unternehmen ihre interne „KI-Readiness" evaluieren. Welche Kompetenzen sind bereits vorhanden? Wie stehen Mitarbeitende zu KI? Welche Qualität haben vorhandene Daten?

2. Aktivierung von Potenzialen

Nicht jedes KI-Szenario ist für jedes Unternehmen geeignet oder sinnvoll. Es empfiehlt sich, Potenziale genau zu prüfen und mit „Low Hanging Fruits" zu beginnen: Bereiche, in denen Mitarbeitende viel Zeit durch manuelle Routine verlieren, sollten zunächst im Fokus stehen. Jedes Projekt muss über eine konkrete, messbare Zielsetzung verfügen.

3. Nachhaltige Umsetzung

Erst dann erfolgt die eigentliche Implementierung des KI-Szenarios. Dazu zählt auch, interne Richtlinien zu definieren, wie die Technologie in der Praxis genutzt werden kann und soll. Daneben empfiehlt sich der Aufbau interner Ressourcen zur kontinuierlichen Betreuung und Weiterentwicklung der Lösung.

Künstliche Intelligenz – intelligent implementiert

Mit seinem dreistufigen Ansatz bietet BE-terna Unternehmen ein modulares KI-Beratungsprogramm, das Unternehmen genau auf der Stufe abholt, auf der sie sich gerade befinden. So begleitet Sie der Beratungs- und Implementierungsspezialist mit seinem umfassenden KI-Know-how aus zahlreichen erfolgreich realisierten Projekten Schritt für Schritt in die intelligente Zukunft.

BE terna
Part of Telefónica Tech

RÜCKFRAGEN & KONTAKT

BE-terna GmbH
Grabenweg 3a, 6020 Innsbruck
Tel.: +43 512 36 20 60
office@be-terna.com
www.be-terna.com

1

ANGRIFF AUF DIE LIEFERKETTEN

Die Europäische Cybersicherheitsbehörde ENISA hat Software-Supply-Chain-Angriffe zur größten Bedrohung erklärt. Damit besteht akuter Handlungsbedarf auch für industrielle IT- und OT-Systeme. Die Zahl der Vorfälle zu Software-Lieferketten hat sich in der EU seit 2020 mehr als verdoppelt.

Die Industrie sieht sich zunehmend mit Software-Supply-Chain-Cyberattacken auf smarte Systeme, sogenannte Embedded Systems, konfrontiert. Dies sind Angriffe, die gezielt über externe Komponenten, Software-Bibliotheken oder Firmware-Updates eingeschleust werden. Darauf weist das Düsseldorfer Cybersicherheitsunternehmen Onekey hin, das unter dem Namen Product Cybersecurity & Compliance Platform (OCP) eine Plattform zur automatisierten Überprüfung von Software in Embedded Systems auf Schadcode oder Schwachstellen betreibt. Diese Form der Cyberkriminalität nutzt Sicherheitslücken bei Zulieferern, Dienstleistern oder Softwareanbietern aus, um in der Lieferkette nachgelagerte Unternehmen oder gar den Endkunden anzugreifen. Besonders betroffen sind Industrieanlagen, Maschinensteuerungen (OT-Systeme, Operational Technology), IoT-Komponenten (Internet of Things) und andere eingebettete Systeme, die meist langjährige Betriebszyklen haben und selten sicherheitskritisch untersucht, überwacht und aktualisiert werden. „Hier besteht akuter Handlungsbedarf“, wendet sich der CEO von Onekey, Jan Wendenburg, an die Industrie. Er erklärt: „Cybersecurity muss die gesamte Wertschöpfungskette umfassen, um wirksam zu sein.“

Die Marktforschungsfirma Cybersecurity Ventures veranschlagt in einer aktuellen Studie den durch Supply-Chain-Angriffe verursachten Schaden auf weltweit 80 Milliarden Dollar jährlich. „Die Komplexität globaler Lieferketten verschärft das Problem“, sagt Jan Wendenburg. Er verweist auf einen Bericht der Europäischen Agentur für Cybersicherheit (ENISA), wonach zwei Drittel der Unternehmen in der EU mindestens schon einmal von kompromittierten Zulieferern betroffen waren. Laut ENISA gehören Supply-Chain-Angriffe zu den Top-5-Bedrohungen für industrielle IT- und OT-Systeme und werden im „ENISA Foresight 2023 Report“ als die Top-1 Cybersecurity-Gefahr herausgestellt.

JEDES VORPRODUKT STELLT EINE POTENZIELLE GEFAHR DAR

Die deutsche Wirtschaft ist traditionell stark internationalisiert. Der Wert der importierten Vorprodukte, die von der deutschen Industrie aus aller Welt bezogen und in ihre Produkte eingebaut werden, liegt in der Größenordnung von 370 Milliarden Dollar. Diese Importe von sogenannten „intermediate goods" sind von zentraler Bedeutung für die Produktion in Deutschland. „Jede verwendete Software und jedes mit vernetzter Digitaltechnik ausgerüstete Vorprodukt stellt eine potenzielle Gefahr dar", umreißt Jan Wendenburg die Dimension der Bedrohung. Dabei besteht das große Gefährdungspotenzial von Supply-Chain-Angriffen darin, dass nicht nur das jeweilige Unternehmen mit Schadsoftware infiziert wird, sondern diese über Produktauslieferungen an Kunden weitergegeben wird. So wäre es beispielsweise möglich, dass ein Maschinenbauer an seine Kunden Anlagen mit industriellen Steuerungen abgibt, die ein Schadprogramm in sich tragen. Dabei kann der bösartige Code über zwei Wege aus der Lieferkette kommen: entweder als Software, die in die Produktentwicklung einfließt, oder als Teil eines Vorprodukts, das im Endprodukt verbaut wird.

STEIGENDE NACHFRAGE NACH SICHERHEITSÜBERPRÜFUNGEN

„Dieser Trend ist alarmierend, da die Lieferketten der deutschen Industrie hochgradig vernetzt sind und ein einziger Angriff weitreichende Folgen haben kann", erklärt Jan Wendenburg. Er sagt: „Daher sollten Embedded Systems, die in Steuerungstechnik, Automatisierung oder IoT-Geräten zum Einsatz kommen, einer umfassenden Prüfung im Hinblick auf Cybersecurity unterzogen werden." Das gelte ausnahmslos für alle Komponenten, also nicht nur die im eigenen Unternehmen entwickelten, sondern auch für die von Zulieferern übernommenen Vorprodukte.

Nach seinen Angaben erfährt Onekey derzeit eine „stark steigende Nachfrage" nach Sicherheitsüberprüfungen von Geräten, Anlagen und Systemen mit Echtzeit-Betriebssystemen (Real-Time Operating Systems, RTOS), wie sie in Embedded Systems typischerweise zum Einsatz kommen. Das Düsseldorfer Sicherheitsunternehmen hatte erst vor wenigen Monaten seine Product Cybersecurity & Compliance Platform (OCP) weiterentwickelt, sodass diese auch RTOS-Firmware auf Schwachstellen und Sicherheitslücken überprüfen kann. Dies galt zuvor in der Branche als schwierig bis unmöglich, insbesondere bei sogenannten monolithischen Binärdateien, wie sie bei marktgängigen Echtzeit-Betriebssystemen wie etwa FreeRTOS, Zephyr OS, ThreadX und anderen im Einsatz sind.

2

Fotos: Freepik (1), Frolopiaton Palm/Freepik (2)

OPEN SOURCE UND DER FALL LOG4SHELL

Als ein besonders kritisches Einfallstor in der Lieferkette gelten Open-Source-Komponenten, die in rund 80 Prozent aller Firmware-Stacks für Embedded Systems enthalten sind. Sicherheitslücken in weitverbreiteten Bibliotheken wie uClibc, BusyBox oder OpenSSL können eine Vielzahl von Systemen gleichzeitig betreffen. Der Fall Log4Shell im Jahr 2021 – eine Schwachstelle in der weitverbreiteten Java-Bibliothek Log4j – hatte gezeigt, wie gefährlich eine unsichere Softwarekomponente sein kann, selbst wenn sie nur in einem Subsystem verwendet wird. Der Log4Shell-Fall gilt als eine der gravierendsten Sicherheitslücken der letzten Jahrzehnte, weil die Software Bestandteil von Millionen Java-Anwendungen ist, darunter auch Zehntausende OT- und IoT-Systeme.

„Die zunehmende Komplexität industrieller Systeme, die Vielzahl externer Anbieter und die Langzeitnutzung von Embedded Systems lassen Supply-Chain-Angriffe zu einer immer größeren Bedrohung werden", sagt Jan Wendenburg. Er verweist auf Prognosen der Gartner Group, wonach bis 2026 über 45 Prozent aller Unternehmen mindestens einen Cybervorfall über die Lieferkette erleiden werden, der ihre Betriebsfähigkeit beeinträchtigt.

ES STEHT VIEL AUF DEM SPIEL: PRODUKTION, REPUTATION, LIEFERFÄHIGKEIT

„Die immer stärkere Integration von Industrial-IoT-Systemen und Robotik bis hin zu autonomen Produktionslinien öffnet geradezu ein Scheunentor für Attacken aus der Lieferkette", erklärt Jan Wendenburg. Er appelliert an die Unternehmensführungen: „Es ist höchste Zeit, Software für Embedded Systeme, unabhängig ob aus eigenem Haus oder von Lieferanten, systematisch vor dem Einsatz und laufend zu überprüfen. Wer das unterlässt, setzt nicht nur seine Produktion, sondern auch seine Reputation und Lieferfähigkeit aufs Spiel."

Hinzu kommt der rechtliche Aspekt: Die Radio Equipment Directive EN18031 und der EU Cyber Resilience Act (CRA) und andere gesetzliche Vorgaben schreiben die Verantwortung der Hersteller für die Cybersicherheit vernetzter Geräte, Maschinen und Anlagen zwingend vor. Die Product Cybersecurity & Compliance Platform (OCP) von Onekey ermöglicht mit dem Compliance Wizard eine automatisierte Überprüfung der Konformität zum CRA und weiteren cybersicherheitsrelevanten Normen. Dies erleichtert die Vorbereitung auf Audits erheblich und reduziert den bürokratischen Aufwand, der durch neue Gesetze entsteht. BO

SYSTEMATISCHE DOPPELSTRATEGIE

Die Ausgaben von Unternehmen für künstliche Intelligenz (KI) haben sich von 2023 bis 2024 zwar auf knapp 14 Mrd. US-Dollar versechsfacht, doch bisher hat erst gut ein Viertel KI vollständig in die Betriebsabläufe integriert. So das zentrale Ergebnis der Studie „The Data Imperative“ der Strategieberatung Roland Berger.

Als größte Hürden für die Umsetzung von KI-Projekten nannten 28 Prozent das Thema Daten, 25 Prozent die Komplexität der Integration von KI-Anwendungen in bestehende Systeme und Prozesse sowie 15 Prozent die Schwierigkeit, ausreichend KI- und Datenspezialisten zu finden. Die Studienautoren kommen daher unter anderem zu dem Schluss, dass für eine erfolgreiche Umsetzung von KI-Technologien in Unternehmen eine systematische Doppelstrategie unverzichtbar ist.

„Nur wenn strukturierte und unstrukturierte Daten in ihrem Kontext prozessübergreifend zusammengeführt werden, kann KI ihr volles Potenzial entfalten“, sagt Edeltraud Leibrock, Global Managing Director bei Roland Berger. „Semantische Graphen als Meta-Layers ermöglichen genau das: Sie schaffen eine dynamische und interpretierbare Datenbasis, die Agentensysteme mit kontextuellem Verständnis versorgt und so echte Ende-zu-Ende-Automatisierung erst möglich macht.“

Für die Studie wurden Unternehmen befragt, die mindestens 250 Mitarbeiter haben und bereits aktiv an KI-Initiativen arbeiten. Als wichtigstes Hindernis auf dem Weg zur Umsetzung entsprechender Projekte sehen 28 Prozent von ihnen Probleme rund um das Thema Daten: von deren Qualität über ihre Zugänglichkeit und Verwaltung bis hin zu Problemen beim Datenschutz. Vor allem in der Gesundheitsbranche und im Einzelhandel ist der Zugang zu zuverlässigen Daten schwierig, während in der Technologie- und IT-Dienstleistungsbranche die Hälfte der Befragten angeben, dass sie selten oder nie Probleme mit der Datenqualität haben.

Als weitere Herausforderung nennen 25 Prozent die Komplexität der Integration von KI-Technologien in bestehende Systeme und Abläufe. Mit Abstand folgen der Mangel an entsprechenden Fachkräften (15 %), ethische Bedenken (12 %) sowie Kosten und mangelndes Vertrauen von Kunden und anderen Stakeholdern (jeweils 10 %).

WETTBEWERBSVORTEILE DURCH ZWEIGLEISIGEN ANSATZ

Die Studie belegt die Wichtigkeit einer passenden Organisationsstruktur für den Erfolg: Unternehmen, die spezielle Teams für das Datenmanagement eingeführt haben (41 % der Befragten), sind in der Umsetzung von KI-Projekten erfolgreicher als Unternehmen, die das Thema lediglich als zusätzliche Aufgabe in bestehende Verantwortungsbereiche integrieren (49 %). Zudem sind 93 Prozent der Befragten der Meinung, dass sich umgekehrt auch die Arbeit an KI-Initiativen positiv auf die Praxis der Datenverwaltung auswirkt. Es lohnt sich daher, die Strategie anzupassen und an beiden Themen gleichzeitig zu arbeiten.

„Wer ausschließlich auf langfristige Datenstrategien setzt, läuft Gefahr, von agileren Mitbewerbern abgehängt zu werden. Wer sich hingegen nur auf kurzfristige KI-Erfolge konzentriert, limitiert künftige Handlungsmöglichkeiten durch eine unzureichende Datengrundlage. Entscheidend ist es deshalb, eine bewusste Balance zwischen unmittelbarem Nutzen in der Verwertung und dem nachhaltigen Aufbau eines belastbaren Datenfundaments zu finden“, erklärt der KI-Experte Alexander Türk, Partner bei Roland Berger Österreich. BO

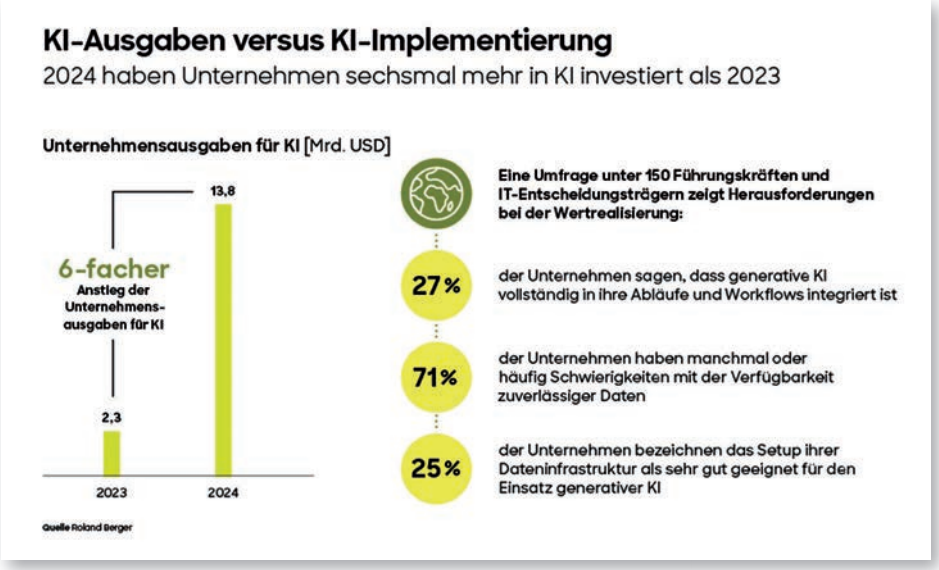


Foto: Roland Berger

VEEAM

In einer zunehmend digitalisierten Welt ist Datenresilienz nicht länger nur ein IT-Thema – sie ist ein strategischer Imperativ.

Datenresilienz beginnt im Vorstand


1


2

Mario Zimmermann, Senior Regional Director DACH, ist überzeugt: Datenresilienz ist heute ein Top-Thema für die Unternehmensführung!

■ Eine aktuelle Studie von Veeam und McKinsey zeigt: Die Mehrheit der Unternehmen überschätzt ihre Widerstandsfähigkeit gegenüber Ausfällen und Cyberangriffen massiv. Die Folgen sind gravierend – jährlich entstehen Verluste von über 400 Milliarden Dollar durch Ausfälle, Rufschädigung und Betriebsunterbrechungen weltweit.

Für Führungskräfte entwickelt: Data Resilience Maturity Model

Mit dem Data Resilience Maturity Model (DRMM) liefert Veeam ein neues Framework, das speziell für Führungskräfte entwickelt wurde. Es ermöglicht eine objektive Standortbestimmung und zeigt konkrete Wege auf, wie Unternehmen ihre Datenstrategie, Prozesse und Technologien auf ein resilientes Fundament stellen können.

„Datenresilienz ist heute ein Top-Thema für die Unternehmensführung", sagt Mario Zimmermann, Senior Regional Director DACH. „Sie entscheidet darüber, ob ein Unternehmen bei einem Ausfall handlungsfähig bleibt – oder zum Stillstand kommt."

Mehr zum Veeam Data Resilience Maturity Model hier oder unter www.veeam.com

Das DRMM unterscheidet vier Reifegrade – von reaktiv bis autonom – und bietet klare Handlungsempfehlungen für den Weg zur Best-in-Class-Resilienz. Unternehmen auf diesem Niveau erholen sich siebenmal schneller von Ausfällen, verzeichnen deutlich weniger Datenverluste und sichern sich einen nachhaltigen Wettbewerbsvorteil.

Besonders kritisch

Über 30 Prozent der CIOs in den am wenigsten resilienten Unternehmen überschätzen ihre Fähigkeiten – ein Risiko, das sich vermeiden lässt. Das DRMM schafft Transparenz und liefert die Grundlage für fundierte Investitionsentscheidungen. Führungskräfte können den Reifeprozess aktiv gestalten – etwa durch die Teilnahme an Veeam-Executive-Workshops, die gezielt auf strategische Steuerung, Risikominimierung und Innovationsförderung ausgerichtet sind.

„Datenresilienz schützt nicht nur Informationen – sie schützt Geschäftsmodelle, Kundenbeziehungen und Markenvertrauen", so Zimmermann. „Sie ist die Basis für digitale Transformation, regulatorische Sicherheit und unternehmerische Zukunftsfähigkeit."

Die wichtigsten Ergebnisse der Veeam DRMM-Studie:

■ 74 Prozent der Unternehmen sind nicht auf dem Stand der Best Practices und arbeiten auf den beiden niedrigsten Reifegraden.

■ Unternehmen mit dem höchsten Reifegrad erholen sich siebenmal schneller von Ausfällen, haben dreimal weniger Ausfallzeiten und erleiden viermal weniger Datenverluste als ihre Mitbewerber.

■ Alarmierend ist, dass mehr als 30 Prozent der CIOs in den am wenigsten resilienten Unternehmen ihre Datenresilienz-Fähigkeiten überschätzen – und damit ihr Unternehmen einem potenziellen Ausfall aussetzen.

INFO-BOX

Über die Studie

Das Veeam DRMM basiert auf umfangreichen Untersuchungen in Zusammenarbeit mit McKinsey & Company und Erkenntnissen von mehr als 500 IT-, Sicherheits- und Betriebsleitern. Es wurde durch reale Kundenergebnisse validiert, darunter ein Gesundheitssystem, das fünf Millionen US-Dollar pro Ausfall einsparen konnte, und eine globale Bank, die nach der Implementierung des Modells mit der Veeam-Plattform keine Cybervorfälle mehr hatte.

FAKE PRESIDENT INCIDENT

Die im Jahr 2016 im Anschluss an den Fake President Incident in China sichergestellten Gelder in Höhe von 10,8 Millionen Euro wurden Ende März 2025 von der Republik Österreich an die FACC AG rücküberwiesen.

Nachdem die FACC Ende 2015 Opfer eines Betrugsfalles wurde (Fake President Incident), konnten aufgrund der intensiven Zusammenarbeit zwischen chinesischen und österreichischen Behörden von diesen Geldern Anfang 2016 rd. 10,8 Mio. Euro auf chinesischen Konten eingefroren werden. Diese wurden 2019 an das Oberlandesgericht Wien überwiesen und nun, nach einer Dauer von ca. sechs Jahren und umfangreichen juristischen Verfahren, von der Verwahrstelle des Oberlandesgerichts Wien an die FACC rückerstattet. Da die eingefrorenen Gelder als Forderung verbucht waren, ist der Erhalt der Gelder nicht ergebniswirksam, erhöht aber die Liquidität.

„Wir bedanken uns bei allen Behörden für die konstruktive Zusammenarbeit in den letzten Jahren. Die schlussendliche Rücküberweisung der Gelder an die FACC beendet ein langjähriges juristisches Kapitel", unterstreicht CEO Robert Machtlinger.

1

LANGE VERFAHRENSDAUER

Die lange Gesamtdauer ist der Komplexität dieses Verfahrens geschuldet, welches nicht nur die internationale Zusammenarbeit mehrerer Behörden, sondern auch umfangreiche juristische Abklärungen der österreichischen Gerichtsbarkeit umfasste.

Wolf Theiss unterstützte die FACC über mehrere Jahre hinweg bei der Koordination mit nationalen und internationalen Behörden, der rechtlichen Absicherung der Ansprüche sowie im Strafverfahren und bei der prozessualen Abwicklung der Ausfolgung. Die Auszahlung markiert den erfolgreichen Abschluss eines der bedeutendsten Asset-Tracing-Fälle eines österreichischen Industrieunternehmens.

Das Wolf-Theiss-Team bestand aus Clemens Trauttenberg (Partner), Nikolaus Laudon (Partner), Theresia Welser (Senior Associate) und Angelika Lange (Senior Associate) – alle Disputes Resolution.

„Die Ausfolgung der Gelder ist das Ergebnis jahrelanger konsequenter juristischer Arbeit und internationaler Kooperation. Die rechtlichen Herausforderungen in diesem Fall waren beachtlich, zuletzt besonders auch auf der strafprozessualen Ebene im Inland. Umso mehr freut es uns, gemeinsam mit unserer Mandantin diesen wichtigen Erfolg erzielt zu haben. Ebenso wichtig ist, dass in Zukunft aufgrund der auch dadurch angestoßenen Änderung in der StPO eine Rückerstattung an die Opfer deutlich effizienter erfolgen kann", Clemens Trauttenberg, Partner Wolf Theiss. BO


2

KONSTRUKTIVE ZUSAMMENARBEIT

»Wir bedanken uns bei allen Behörden für die konstruktive Zusammenarbeit in den letzten Jahren. Die schlussendliche Rücküberweisung der Gelder an die FACC beendet ein langjähriges juristisches Kapitel.«

Robert Machtlinger, CEO FACC AG

Fotos: FACC/Gortana (1), FACC AG (2)

IMPULSE FÜR DEN WANDEL

Mit dem Transformations-Forum schafft die Plattform Industrie 4.0 Raum für Austausch, Praxisbeispiele und neue Perspektiven auf die Triple Transformation Digitalisierung, Nachhaltigkeit und Menschzentrierung.

Die Transformation der Industrie betrifft Unternehmen auf allen Ebenen: Neue Technologien, veränderte Geschäftsmodelle, flexible Arbeitsweisen, neue Kompetenzen und eine lebendige Unternehmenskultur müssen zusammen gedacht werden. Diese sogenannte Triple Transformation – Digitalisierung, Nachhaltigkeit und Menschzentrierung – fordert Organisationen ganzheitlich heraus. Erfolgreiche Unternehmen gestalten diese Veränderungen nicht isoliert, sondern integriert als abgestimmten Wandel von Strukturen, Strategien und Haltungen. Dabei stehen zentrale Fragen im Raum: Wie lässt sich eine Organisation zukunftsfähig und resilient aufstellen? Welche Rolle spielen Führung, Kommunikation und Zusammenarbeit? Und vor allem: Wie gelingt die Verbindung von technologischer Innovation mit sozialen und ökologischen Zielen?

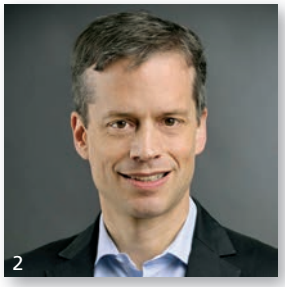
UNTERNEHMEN IM WANDEL STÄRKEN

Das Transformations-Forum der Plattform Industrie 4.0 startete Mitte Mai und bietet dazu einen Raum für Austausch, Reflexion und Vernetzung. Ziel ist es, Unternehmen in ihrem Wandel zu stärken – mit wissenschaftlicher Fundierung, praktischen Erfahrungen und interaktiven Formaten. Die drei Vorträge beim ersten Transformations-Forum beleuchteten den Transformationsprozess aus unterschiedlichen Perspektiven: Sebastian Schlund von Fraunhofer Austria und der TU Wien sprach über die „Triple Transformation", ergänzt um die Perspektive der Wettbewerbsfähigkeit. Peter Obermair, Business Development & Consulting bei formways GmbH, und Stefan Novoszel, Principle Consultant Automotive & Manufacturing bei Tietoevry, zeigten anhand konkreter Fallbeispiele, warum viele Digitalisierungsprojekte scheitern und wie sie erfolgreich sein können.

1

Thomas Welser, CEO der Unternehmensgruppe Welser Profile, gab Einblick in den umfassenden Wandel seines Unternehmens – ein langfristiger Kulturprozess, getragen von Mitarbeiter:innenbeteiligung, werteorientierter Haltung und einem eigenen „Operating System".

„Transformation ist weit mehr als ein technologisches Thema. Sie erfordert klare Visionen, kulturellen Wandel und Zusammenarbeit über Sektorengrenzen hinweg. Mit dem Transformations-Forum schaffen wir einen Raum für interaktiven Austausch, das Teilen von Best Practices und die Entwicklung gemeinsamer Lösungsansätze. Ich freue mich auf die nächste Ausgabe des neuen Formats im kommenden Herbst," erklärt Roland Sommer, Geschäftsführer der Plattform Industrie 4.0. Die Veranstaltung fand im Rahmen des EU-Interreg-Projekts „Twin City Future Innovation Manufacturing Hub" statt, einer grenzüberschreitenden Initiative zwischen der Slowakei und Österreich. BS



2

RAUM FÜR WANDEL UND ZUSAMMENARBEIT

»Mit dem Transformations-Forum schaffen wir einen Raum für interaktiven Austausch, das Teilen von Best Practices und die Entwicklung gemeinsamer Lösungsansätze.«

Roland Sommer, GF der Plattform Industrie 4.0

Fotos: Piten/Freepik (1), Zinner (2)

CRIF GMBH

Zum dritten Mal führten Business Circle, CRIF und EY Österreich eine jährliche Studie durch, um aktuelle Entwicklungen und zukünftige Herausforderungen im Risikomanagement zu analysieren. Diese zeigt: Unternehmen überschätzen ihre Krisenfestigkeit – Mangel an Daten und Technologie bleibt zentrale Schwachstelle.

Risikomanagement-Studie 2025

Unternehmen in Österreich sehen sich in Zeiten geopolitischer Unsicherheiten, technologischer Umbrüche und zunehmender Regulierungen als widerstandsfähig – gleichzeitig zeigt sich aber, dass wichtige Hebel wie Datenverfügbarkeit, Agilität und strategische Einbindung von Risikomanagement oft noch nicht voll ausgeschöpft werden. Das ist das zentrale Ergebnis einer gemeinsamen Umfrage von EY Österreich, CRIF und Business Circle, an der Vertreter:innen von 55 Unternehmen unterschiedlicher Branchen und Größen teilgenommen haben. „In einer Welt, die sich rasch ändert, braucht es mehr als punktuelle Krisenreaktionen. Risikomanagement muss heute ein integraler Bestandteil der Unternehmensstrategie sein – und Daten bilden dabei das Fundament", betont Markus Hölzl, Partner bei EY Österreich.

Zur Risikomanagement-Studie 2025

Strukturelle Defizite und ungenutzte Chancen im Risikomanagement

Laut Analyse schätzen fast neun von zehn Unternehmen (87,3 %) ihre Organisation als stark oder sehr stark widerstandsfähig gegenüber Krisen ein. Doch der kritische Blick offenbart Schwächen: 38,2 Prozent messen ihre Resilienz nicht. „Diese Lücke zwischen Selbstbild und Realität ist riskant. Gerade in Krisenzeiten zeigt sich, wie wichtig es ist, Resilienz nicht nur zu behaupten, sondern messbar zu machen und kontinuierlich weiterzuentwickeln", sagt Anca Eisner-Schwarz, Geschäftsführerin von CRIF Österreich. Mehr als ein Fünftel der Unternehmen (21,8 %) haben keine eigene Risikomanagement-Abteilung oder -funktion. Bei knapp der Hälfte (47,3 %) ist weniger als eine Vollzeitkraft dafür zuständig. 30 Prozent der Firmen mit weniger als 50 Mitarbeitenden geben auch an, dass sie keine Ressourcen für Risikomanagement bereitstellen.

Krisenlandschaft: Aktuelle Risiken und künftige Gefahren im Fokus

Die Unternehmen sehen aktuell vor allem Marktrisiken (69,1 %) als größte Herausforderung, gefolgt von Technologierisiken (45,5 %), Finanzrisiken (43,6 %) und geopolitischen Risiken (40,0 %). Auch Personalrisiken (29,1 %) gewinnen zunehmend an Bedeutung. Für die kommenden Jahre erwarten die Unternehmen einen Anstieg bei geopolitischen Risiken (47,3 %) und Personalrisiken (45,5 %), während Marktrisiken (56,4 %) und Technologie-/Cyberrisiken (41,8 %) weiterhin auf hohem Niveau bleiben. Gerhard Pichler, Geschäftsführer des Business Circle, dazu: „Diese Einschätzungen verdeutlichen, dass Unternehmen immer stärker vernetzte und globale Zusammenhänge im Blick behalten müssen, um langfristig erfolgreich zu bleiben."

Selbstbild oft stark, Datenmangel hemmt die Umsetzung

Die Studie zeigt: 70,9 Prozent der Unternehmen schätzen ihre Reaktionsfähigkeit auf Veränderungen als agil oder sehr agil ein. Dennoch überwacht etwa ein Drittel (34,5 %) externe Entwicklungen zur Ableitung akuten Handlungsbedarfs nur schwach. Positiv ist jedoch, dass 78,2 Prozent Erkenntnisse aus vergangenen Krisen zumindest teilweise in die Strategie einfließen lassen.

Ein zentrales Hindernis für proaktives Risikomanagement bleibt der Mangel an Daten. 45,5 Prozent der Unternehmen geben an, dass ihnen die notwendigen Informationen für eine aktive und agile Steuerung nicht zur Verfügung stehen. Nur 14,5 Prozent haben vollständigen Zugriff auf Echtzeitdaten, während 27,3 Prozent kaum oder gar keine Echtzeitinformationen nutzen können. Die Studie zeigt deutlich, dass Unternehmen vor allem in der konsequenten Nutzung von Daten und Technologien noch aufholen müssen, um Risiken wirklich als Chancen zu verstehen. Wer heute datengetrieben arbeitet, kann nicht nur schneller und präziser reagieren, sondern auch Wettbewerbsvorteile schaffen

Geplante Technologieinvestitionen stärken künftige Agilität

Österreichische Unternehmen planen verstärkt, in moderne Technologien zu investieren, um ihr Risikomanagement agiler und datengetriebener zu gestalten. Laut Studie wollen 43,6 Prozent der Unternehmen künftig verstärkt Datenanalyse-Tools einsetzen, um Risiken präziser identifizieren und steuern zu können. Zudem plant etwa ein Drittel (32,7 %) die Nutzung von Automatisierungslösungen, beispielsweise Robotic Process Automation (RPA), um Prozesse effizienter zu gestalten und schneller auf Krisenszenarien reagieren zu können. Dies zeigt, dass die Bedeutung digitaler Tools zunehmend erkannt wird, jedoch die tatsächliche Umsetzung und Integration in bestehende Risikomanagement-Systeme noch deutlich verbessert werden muss. „Datengetriebenes Risikomanagement schafft nicht nur Transparenz, sondern ermöglicht auch proaktive Entscheidungen, die Unternehmen resilienter machen“, so Eisner-Schwarz. Pichler ergänzt: „Unsere Umfrage zeigt klar, dass Unternehmen ihre Widerstandskraft gegenüber Krisen objektiv messen und kontinuierlich verbessern müssen, um langfristig erfolgreich zu sein.“

Technologielücke: Kaum Vorbereitung auf AI Act

Zwar setzen bereits 36,4 Prozent der Unternehmen Technologien wie KI oder Automatisierung im Risikomanagement ein -, aber gleichzeitig ist die Vorbereitung auf die neue EU-Verordnung (AI Act) erschreckend gering: Fast zwei Drittel (63,6 %) der durch den AI Act betroffenen Unternehmen haben bisher kaum oder keine Maßnahmen gesetzt, 27,3 Prozent sind sich der Anforderungen noch nicht bewusst. Nur 22,7 % der Unternehmen bewerten ihr Wissen über die Anforderungen des AI Acts als sehr hoch. „Der Anpassungsbedarf wird unterschätzt. Unternehmen müssen schnell handeln, um regulatorische Anforderungen nicht nur zu erfüllen, sondern auch als Innovationschance zu nutzen“, ergänzt Hölzl abschließend.

www.crif.at, www.businesscircle.at
www.ey.com/de_at

INFO-BOX

Die Highlights der Ergebnisse:

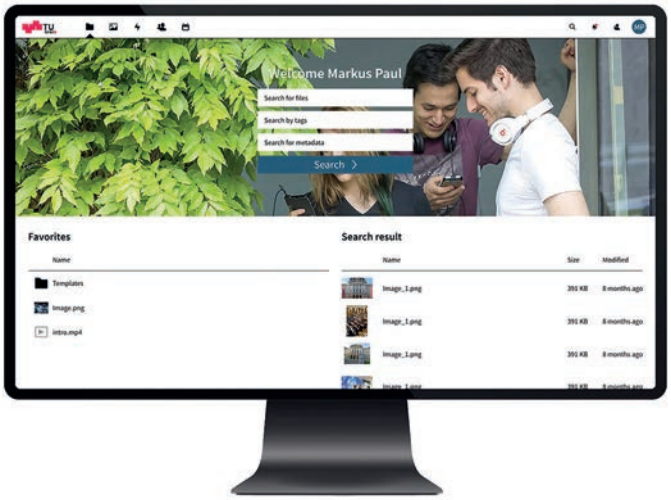
- Österreichische Unternehmen schätzen ihre Widerstandsfähigkeit gegen Krisen als hoch ein, vernachlässigen aber die Messung tatsächlicher Resilienz.
- Knapp die Hälfte der Unternehmen klagt über unzureichende Datenverfügbarkeit für effektive Risikosteuerung.
- Mehrheit noch unvorbereitet auf kommende regulatorische Anforderungen (AI Act).

Anzeige • Foto: shutterstock

UNIVERSITÄRE BUSINESS GMBH

Die Technische Universität Graz gründet die erste universitäre Business GmbH zur Softwareverwertung in Österreich. Ziel der TU Graz Business GmbH ist es, universitäre Softwareentwicklungen aktiv zu verwerten und so anderen Bildungseinrichtungen und Unternehmen aus der Industrie zugänglich zu machen.

Die TU Graz Business GmbH versteht sich als zentrale Partnerin für Softwareprodukte, Consulting-Leistungen und maßgeschneiderte IT-Lösungen. Dabei reicht das Portfolio von Produkteinführungen über Support bis hin zur Weiterentwicklung im Dialog mit den Anwender:innen. „Mit der Gründung dieser GmbH schaffen wir eine innovative Plattform, um universitäre Entwicklungen effizienter in den Markt zu bringen", erklärt Vizerektorin Andrea Hoffmann. „Gleichzeitig reagieren wir auf zentrale Herausforderungen, mit denen Universitäten heute konfrontiert sind: die Notwendigkeit zur Digitalisierung, steigenden Effizienzdruck und den verantwortungsvollen Umgang mit begrenzten Ressourcen."
Geschäftsführer Tobias Solacher ist überzeugt: „Wir schaffen einen professionellen Rahmen, um hochqualitative universitäre IT-Lösungen zu verbreiten – skalierbar, rechtssicher und mit Mehrwert für viele Hochschulen. Die positive Resonanz aus ersten Kooperationen zeigt: Wir haben den richtigen Nerv getroffen."



Die Softwarelösung Digital Asset Management ermöglicht die zentrale Verwaltung von Bildern, Lizenzen und Dokumenten.

ERSTE TOOLS BEREITS AM MARKT

Zum Start bietet die TU Graz Business GmbH gleich eine recht umfangreiche Produktlösung an: Die Software-Suite TUULS, speziell für die Bedürfnisse von Universitäts-Kommunikationsabteilungen entwickelt, wurde bereits erfolgreich gemeinsam mit der international tätigen Digitalagentur Conversory umgesetzt. Sie bündelt mehrere zentrale Tools. Dazu gehört das Redaktionssystem „Elmar", mit dem sich Inhalte auf einer intuitiven und responsiv programmierten Oberfläche gemeinsam planen und verwalten lassen. Ebenfalls Teil von TUULS ist ein Digital Asset Management, das die zentrale Verwaltung von Bildern, Lizenzen und Dokumenten ermöglicht, womit langes Suchen der Vergangenheit angehört. Ein Digital Publishing Tool ist auch an Bord, mit dem digitale Publikationen multimedial, ressourcenschonend und datensicher auf smartem Weg veröffentlicht werden können.
Alle Tools laufen DSGVO-konform auf europäischen Servern – die volle Datenkontrolle bleibt somit garantiert. Für Kommunikationsabteilungen, die mit ähnlichen Zielen und Herausforderungen kämpfen – wie der Digitalisierung interner Prozesse, wachsender Wissenschaftsskepsis und sinkenden Budgets –, stellt TUULS ein attraktives Angebot dar. Statt individuell teure Lösungen zu entwickeln, können Hochschulen eine gemeinsame Plattform nutzen. Wartung, Weiterentwicklung und Support erfolgen über günstige Wartungsverträge – inklusive Zugang zur TUULS-Community: ein Raum für Austausch, Tutorials, Demovideos und strategische Diskussionen rund um Wissenschaftskommunikation.
Als Entwicklerin der Softwarelösungen hat die TU Graz die Tools bereits erfolgreich im Eigenbetrieb im Einsatz. BO


Andrea Hoffmann, TU Graz-Vizerektorin, und Tobias Solacher, Geschäftsführer der TU Graz Business GmbH.

Fotos: Lunghammer/TU Graz

KOMPETENTER UMGANG MIT KI

Im Mai fand die zweite Veranstaltung der „KI-Schmiede“ der ARS Akademie und des ETC – Enterprise Training Center statt. Das Thema lautete „AI Act in der Praxis: Was Entscheider jetzt wissen müssen“.

V. l. n. r.: Christoph Becker, Oliver Bernecker, Martina Saller, Richard Melbinger, Clemens Wasner

Künstliche Intelligenz ist eines der meistdiskutierten Themen der heutigen Zeit – ein echtes „heißes Eisen“. Was macht man mit heißen Eisen? Man schmiedet sie. Genau das ist das Ziel der Initiative „KI-Schmiede“ der ARS Akademie und des ETC – Enterprise Training Center. Die Plattform leistet konkrete Unterstützung und versetzt Unternehmen in die Lage, von innen heraus KI-fit zu werden. Nach dem Startschuss im März folgte im Mai die zweite kostenlose Veranstaltung der „KI-Schmiede“. Sie fand in den Wiener Räumlichkeiten von ETC statt und stand unter dem Motto „AI Act in der Praxis: Was Entscheider jetzt wissen müssen“.

JEDER JOB WIRD EIN KI-JOB

„Der verantwortungsvolle Umgang mit künstlicher Intelligenz ist nicht nur eine technologische, sondern vor allem eine Kompetenzfrage. KI verändert nicht irgendwann die Arbeitswelt – sie tut es bereits. Und sie betrifft nicht nur IT-Abteilungen. Jeder Job wird ein KI-Job – ob in der Buchhaltung, im Marketing oder im Kundenservice. Deshalb brauchen wir jetzt flächendeckende Qualifizierungsinitiativen, die Menschen befähigen, KI zu verstehen, anzuwenden und kritisch zu hinterfragen. Als führender Anbieter im Bereich IT-Training sehen wir es als unsere Verantwortung, Unternehmen und Einzelpersonen genau auf diesem Weg zu begleiten“, sagt Christoph Becker, CEO von ETC – Enterprise Training Center, über die Idee hinter der „KI-Schmiede“.

Nach der Begrüßung der Gäste durch die Initiatoren Richard Melbinger, CEO ARS Akademie, sowie ETC-CEO Christoph Becker, folgte ein Vortrag von Clemens Wasner, der einen Überblick lieferte, was Unternehmen hinsichtlich des EU AI Acts wissen müssen. Außerdem hatte Wasner, CEO von EnliteAI, einem österreichischen AI-Start-up, sowie Mitgründer und Vorsitzender von AI Austria, einem unabhängigen Verein zur Förderung von AI in Österreich, auch praktische Tipps für die Umsetzung im Gepäck.

Im Anschluss daran diskutierte ein Panel, bestehend aus Martina Saller, Vertriebsleiterin für den öffentlichen Sektor bei Microsoft Österreich, Oliver Bernecker, Geschäftsführer der Know Center Research GmbH, einem führenden europäischen Innovations- und Forschungszentrum für vertrauenswürdige KI und Data Science, sowie Christoph Becker unter Beteiligung des Publikums Fragen im Zusammenhang mit dem Herstellen von Compliance mit der EU-Richtlinie, berichtete von ersten Erfahrungen aus der Praxis und erläuterte konkrete Handlungsschritte.

Seinen Ausklang fand der Nachmittag für die Teilnehmerinnen und Teilnehmer auf der ETC-Dachterrasse, um in entspanntem Rahmen die Informationen noch einmal in persönlichen Gesprächen Revue passieren zu lassen und die Gelegenheit fürs Networking zu nutzen.

„KI-FAILS“ VERMEIDEN

„KI hat schon in zahlreichen Unternehmen Einzug gehalten. Die große Frage ist jedoch, wie kann man mit und durch KI einen Wettbewerbsvorteil und damit einen – finanziellen – Mehrwert schaffen, der dann auch zu einem echten Profit führt? Aktuell gibt es nur sehr wenige Unternehmen, so zum Beispiel Klarna, die hier mutig vorangegangen sind. Der Einsatz von generativer KI hat beigetragen, Kosten im Kundenservice zu senken und Gewinne zu erhöhen, aber auf Kosten der Customer Experience. Gute Vorbereitung und Kenntnis der Grenzen von KI sind notwendig, um solche ‚KI-Fails‘ zu vermeiden“, so ARS-CEO Richard Melbinger abschließend. RNF

www.ars.at, www.etc.at

Foto: RNF

1

KI-NUTZUNG STEIGT, WISSEN FEHLT

Immer mehr Menschen in Österreich nutzen künstliche Intelligenz im Berufsleben und wünschen sich mehr davon. Doch viele fühlen sich unzureichend vorbereitet, wie eine neue Studie von PwC und Microsoft zeigt.

Der Einsatz von KI nimmt in Österreich an Fahrt auf: Bereits 28 Prozent der Menschen nutzen KI im Berufs- oder Ausbildungsalltag – deutlich mehr als noch vor zwei Jahren (2023: 18 %). Gleichzeitig wünschen sich 45 Prozent einen verstärkten Einsatz von KI im Arbeitsleben. Besonders groß ist die Offenheit bei der Generation Z, wo sich fast sechs von zehn mehr KI-Unterstützung wünschen. Das zeigt die aktuelle repräsentative KI-Studie von PwC Österreich und Microsoft Österreich. 52 Prozent der Befragten sehen in der Nutzung von KI im Arbeitsalltag mehr Vor- als Nachteile. Besonders der erwartete Effizienzgewinn überzeugt: Zwei Drittel glauben, dass KI ihnen lästige oder zeitintensive Aufgaben abnehmen und den Arbeitsalltag erleichtern kann. Im Vergleich zu 2023 (57 %) ist das ein deutlicher Anstieg.

Während KI zunehmend Teil des Arbeitsalltags wird, fühlen sich viele Menschen noch nicht ausreichend vorbereitet. Lediglich 32 Prozent der Befragten glauben, gut

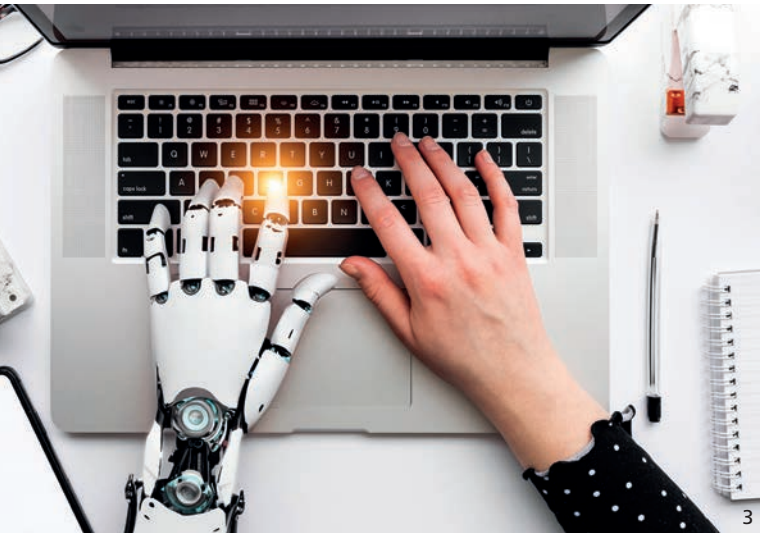

2

ALLE MÜSSEN MIT

»Wenn wir das volle Potenzial von KI ausschöpfen wollen, müssen wir alle Menschen befähigen, mitzuhalten – unabhängig von Alter, Geschlecht oder Vorbildung.«

Rudolf Krickl, CEO von PwC Österreich

Fotos: Frolopiaton Palm/Freepik (1), PwC Österreich (2)



OHNE KI KEIN FORTSCHRITT

»Der Ausbau der KI-Fähigkeiten ist essenziell, um die digitale Transformation in Österreich zu beschleunigen und die Wettbewerbsfähigkeit sowie die Innovationskraft des Landes zu sichern.«

Hermann Erlach, General Manager bei Microsoft Österreich

für eine KI-geprägte Arbeitswelt gerüstet zu sein. Selbst unter der technologieaffinen Generation Z sieht sich nur etwas mehr als die Hälfte entsprechend vorbereitet. Auffallend ist auch der Unterschied zwischen den Geschlechtern: 40 Prozent der Männer schätzen ihre Fähigkeiten im Umgang mit KI als ausreichend ein, bei den Frauen sind es nur 25 Prozent. „Wenn wir das volle Potenzial von KI ausschöpfen wollen, müssen wir alle Menschen befähigen, mitzuhalten – unabhängig von Alter, Geschlecht oder Vorbildung. Lebenslanges Lernen ist kein Nice-to-have mehr, sondern ein Muss für die Zukunft unserer Arbeitswelt“, so Rudolf Krickl, CEO von PwC Österreich.

BILDUNG TRIFFT TECHNOLOGIE

Besonders hohes Potenzial schreiben die Befragten dem Einsatz von KI im Gesundheitswesen zu: 39 Prozent sehen hier den größten Nutzen. Gleichzeitig wächst der Wunsch nach mehr Aufklärung und Kompetenzaufbau. Drei von vier Personen sprechen sich für ein eigenes Schulfach zum Thema künstliche Intelligenz aus. „Die Ergebnisse zeigen, wie sehr der Gesellschaft das Potenzial von KI bewusst wird – insbesondere in der Arbeitswelt und im Bildungswesen. Der Ausbau der KI-Fähigkeiten ist daher essenziell, um die digitale Transformation in Österreich zu beschleunigen und die Wettbewerbsfähigkeit sowie die Innovationskraft des Landes zu sichern“, betont Hermann Erlach, General Manager bei Microsoft Österreich. BS

Fotos: Freepik (3), Microsoft Österreich (4)

ERP FÜR MEHR EFFIZIENZ

Der Maschinenbauer Jenz GmbH implementiert das ERP-System PSIpenta von PSI Software SE, um zentrale Prozesse standortübergreifend zu steuern – inklusive PLM-Anbindung, mobiler Apps und hoher Selbstverwaltung.

Betriebsmittelverwaltung im PSIpenta/ERP

Die PSI Software SE wurde vom Maschinen- und Anlagenbauer Jenz GmbH mit der Implementierung des ERP-Systems PSIpenta beauftragt. Das familiengeführte Unternehmen ist Hersteller von Maschinen zur Aufbereitung von Biomasse. Mit rund 250 Mitarbeitenden entwickelt und produziert das Unternehmen hochmoderne Maschinen, die für die effiziente Zerkleinerung von Holz- und Grünabfällen sowie Biogassubstraten eingesetzt werden. Neben dem Auftragsmanagement werden unter anderem die integrierten Module der Lagerplatzverwaltung sowie das Änderungs- und Servicemanagement geliefert. Zusätzlich wird PSIpenta/ERP mit der Mehrwerksteuerung Multisite zukünftig den Standort Österreich in allen Kernprozessen zentral vom Firmensitz in Petershagen im deutschen Brandenburg aus unterstützen. Neben der Kostenrechnung wird der Finanzbereich für die Aufgaben Finanzen, Lohn- und Gehalt sowie Personal, einschließlich des Einsatzes einer automatischen Archivierung des Rechnungseingangs, komplettiert.

SELBSTVERWALTUNG MÖGLICH

Einen wesentlichen Baustein der Gesamtlösung bildet die zeitgleiche Implementierung eines neuen Product-Lifecycle-Management-Systems (PLM) der Firma Contact Software aus Bremen. Dieses ermöglicht mit einer „Single-Source-of-Truth"-Strategie für alle digitalen Prozesse eine Transparenz über die gesamte Wertschöpfung von der Konstruktion und der Produktion über den Vertrieb bis hin zum Service. Ausschlaggebende Faktoren für den Zuschlag waren für Jenz das PSI-Click-Design, die Möglichkeiten der Selbstverwaltung des gesamten ERP-Systems sowie der Einsatz vielfältiger mobiler ERP-Prozesse über die PSIpenta/Industrial-Apps. Das Projekt wurde über die ERP-Auswahlplattform der Trovarit gestartet und erfolgreich vom Beratungsunternehmen Leannova GmbH aus Lingen durchgeführt BS

INFO-BOX

PSI Software

Der PSI-Konzern entwickelt Softwareprodukte zur Optimierung des Energie- und Materialflusses bei Versorgern und Industrie. Als unabhängiger Softwarehersteller mit über 2.300 Beschäftigten ist PSI seit 1969 Technologieführer für Prozesssteuerungssysteme, die durch die Kombination von KI-Methoden mit industriell bewährten Optimierungsverfahren für eine nachhaltige Energieversorgung, Produktion und Logistik sorgen. Die innovativen Branchenprodukte können vom Kunden selbst oder in der Cloud betrieben werden.

www.psi.de

Foto: PSI Software SE

COMM-IT EDV DIENSTLEISTUNGSGMBH

Das Unternehmen comm-IT ist Digitalisierungstreiber und zugleich solider Backbone: Beratung, Entwicklung, Betrieb und Integration aus einer Hand. Von der Idee bis zur Umsetzung ist comm-IT Ihr Sparringspartner.

Unser Credo: We make IT easy

1

2

Die UniFi World Conference 2025 in Berlin bot Gelegenheit zum Austausch mit Ubiquiti-Ingenieur:innen und Partner:innen aus aller Welt.

Informationstechnologie ist heute überall und stellt einen wesentlichen Baustein des Unternehmenserfolgs dar. Während sich moderne IT-Lösungen einerseits ein höchstmögliches Maß an Einfachheit in Nutzung und Bedienung an ihre Fahnen heften, steigen andererseits die Komplexität durch den Umfang der IT-Landschaften und ihre Bedeutung als zentraler Bestandteil fast aller Businessprozesse stetig weiter an. Das bedeutet eine große Herausforderung. Aber es muss nicht immer kompliziert sein – wenn man einen verlässlichen Partner mit langjähriger Erfahrung an seiner Seite hat.

„Wir unterstützen Unternehmen dabei, ihre Digitalisierungsvorhaben effizient und erfolgreich umzusetzen, indem wir maßgeschneiderte Lösungen aus einer Hand anbieten", so Dennis Wagner, Geschäftsführer der Wiener comm-IT EDV Dienstleistungs-gmbH. Ein breites Spektrum an IT-Dienstleistungen ermöglicht es comm-IT, IT-Bedürfnisse ganzheitlich abzudecken – von Infrastrukturplanung und -implementierung über Support und Wartung bis hin zu Sicherheit und Datenschutz. „Wir verfügen über umfassende Expertise, insbesondere in den Branchen Steuerberatung, Rechtswesen, Medienagenturen und Versicherungsmakler. Unser Leistungsspektrum umfasst alles, von moderner Telefonie – Telefonanlagen und SIP-Trunks – über Highspeed-Internet bis hin zu umfassender IT-Betreuung, Beschaffung von Hardware und strategischer Beratung", geht Wagner ins Detail und ergänzt: „Auch in der Immobilien- und Hospitality-Branche – etwa Hotels, studentisches Wohnen, Mikroapartments oder Kurzzeitvermietungen – haben wir viel Erfahrung in Bereichen wie Haustechnik (Netzwerk, Wi-Fi) und Sicherheitssysteme (moderne KI-gestützte Kamerasysteme, zentrale Schließsysteme etc.)."


3

Dennis Wagner ist Geschäftsführer der Wiener comm-IT EDV Dienstleistungs-gmbH.

LIVE AUS BERLIN:
UniFi World Conference 2025

Eben noch in der Keynote von Ubiquiti-CEO Robert Pera, jetzt schon voller Eindrücke: Auf der UniFi World Conference 2025 in Berlin wurde klar, wohin die Reise für Netzwerke und Sicherheitslösungen geht. Ohne ins Detail zu gehen – Vertraulichkeit muss sein –, so viel sei verraten: Die kommenden UniFi-Generationen heben Performance, Skalierbarkeit und KI-gestützte Analyse auf ein völlig neues Niveau.

Für uns bei comm-IT bedeutet das: noch mehr Möglichkeiten, Unternehmen in Österreich mit zukunftssicheren Netzwerk- und Wi-Fi-Infrastrukturen und intelligenter Video-Überwachung zu unterstützen. Besonders spannend ist, wie nahtlos sich die neuen Features in bestehende Umgebungen einfügen – ein echter Gewinn für Effizienz und Datenschutz zugleich.

Neben Vorträgen und Live-Demos nutzte Dennis Wagner die Gelegenheit zum Austausch mit Ubiquiti-Ingenieur:innen und Partner:innen aus aller Welt. Die Diskussionen reichten von praktischen Deployment-Tipps bis hin zu Visionen für AI-basierte Automatisierung im Netzwerk- und Protect-Umfeld.

Dieses geballte Know-how bringen wir direkt zu unseren Kund:innen – verlässlich, transparent und dedicated to progress.

comm-IT Your connection is our commITment

RÜCKFRAGEN & KONTAKT

comm-IT EDV DienstleistungsgmbH
Adamsgasse 1/20
1030 Wien
Tel.: +43 1 205 210
office@comm-IT.at
www.comm-IT.at

Anzeige • Fotos: comm-IT (1+2), Lars Ternes (3)

ZUKUNFTSFITTES RECHENZENTRUM

Mit dem ersten Umweltzeichen für ein Rechenzentrum setzt Wien ein starkes Zeichen für eine klimafitte Digitalisierung. Die Stadt zeigt vor, wie Effizienz, Technologie und Nachhaltigkeit erfolgreich zusammenspielen.

Mit dem Ziel, zur nachhaltigen Digitalisierungshauptstadt Europas zu werden, schreitet die Stadt Wien mit gutem Beispiel voran: Das Rechenzentrum der Stadt Wien erhält als erstes Rechenzentrum des Landes das Österreichische Umweltzeichen. „Der steigende Verbrauch von Rechenleistung wird beispielsweise durch künstliche Intelligenz verstärkt und stellt für die erfolgreiche Energiewende eine weitere Herausforderung dar. Umso wichtiger ist uns, mit der Richtlinie für Rechenzentren einen Leitfaden zu geben, wie ein nachhaltiges Rechenzentrum aussehen kann. Dabei gibt es viele Optimierungsmöglichkeiten, die nicht nur nachhaltig, sondern auch wirtschaftlich sinnvoll sind. Eine tolle Möglichkeit ist, beispielsweise die überflüssige Abwärme für anliegende Unternehmen oder Haushalte zum Heizen zu nutzen“, unterstreicht Christian Kornherr, Projektleiter im Umweltzeichen-Team des Vereins für Konsumenteninformation (VKI). „Ziel ist es natürlich, noch mehr Rechenzentren zu zertifizieren, damit gegenseitig nachhaltige Lösungen geteilt werden können und neue Vorzeigeprojekte entstehen“, betont Kornherr.

NACHHALTIGKEIT ALS INNOVATIONS- UND EFFIZIENZFAKTOR

Das Rechenzentrum der Stadt Wien im 22. Gemeindebezirk ist ein Unternehmen der WSE Wiener Standortentwicklung GmbH und wird von Wien Digital, der IT-Abteilung der Stadt Wien, genutzt. Dort wird das Data-Center auf dem neuesten Stand der Technik mit höchster Leistung und Sicherheit betrieben, um IT-Services für Bürger:innen der Stadt Wien verlässlich zur Verfügung zu stellen. Eine umweltverträgliche und ressourcenschonende Ausrichtung wird u. a. durch ein umfangreiches Energiemonitoring-System und die Nutzung der Außenluft und des lokalen Grundwassers zur Kühlung erreicht. Geschäftsführer Christian Altenberger zieht ein positives Fazit nach dem erfolgreichen Zertifizierungsprozess: „In den vergangenen Jahren haben wir ein umfangreiches System zur Überwachung des Energieverbrauchs implementiert. Durch kontinuierliches Messen erfassen wir wichtige Kennzahlen, um unsere Effizienzfortschritte zu überprüfen und gezielte Energiesparmaßnahmen zu treffen. Durch die Auszeichnung wurde unser bisheriger Weg bestätigt. Wir übernehmen Verantwortung und arbeiten weiter daran, unser Rechenzentrum noch energieeffizienter, umweltverträglicher und ressourcenschonender zu betreiben. Unser Ziel ist es, den steigenden Bedarf an IT-Services in Wien zu decken und gleichzeitig zur Erreichung der Klimaziele der Stadt beizutragen. Darüber hinaus möchten wir mit unserem nachhaltigen Ansatz als Vorbild fungieren und demonstrieren, dass umweltfreundliche Praktiken in der IT-Branche realisierbar sind.“

ZERTIFIZIERUNG SEIT ENDE 2024 MÖGLICH

Seit über 30 Jahren steht das Österreichische Umweltzeichen für geprüften Umweltschutz und zeichnet Unternehmen, Produkte, Dienstleistungen und Events aus. Seit knapp sechs Monaten können Rechenzentren die österreichische UZ-80-Zertifizierung erhalten. Die neue Zertifizierung reagiert auf den zunehmenden ökologischen Fußabdruck der Branche und fördert unter anderem die sinnvolle Nutzung von Abwärme. Das Rechenzentrum der Stadt Wien, als erster Lizenznehmer der UZ 80, nimmt als öffentliche Hand eine Vorreiterposition für interessierte Rechenzentren ein. Je nach Bundesland stehen diesen individuelle Beratungs- und Förderungsangebote zur Verfügung, in Wien etwa durch das Angebot von OekoBusiness Wien. BS

Foto: Stadt Wien

AUCOTEC GMBH

Aucotec integriert IEC 61850 nahtlos in Engineering Base und zeigt, wie KI und zentrale Datenmodelle das Engineering digitaler Umspannwerke revolutionieren.

Vollintegration der IEC 61850

■ Auf der internationalen Fachmesse CIRED 2025 in Genf präsentierte Aucotec die vollständige Integration der IEC 61850 in die eigene Kooperationsplattform Engineering Base. Diese bahnbrechende Entwicklung macht das Engineering digitaler Umspannwerke effizienter, durchgängiger und zukunftssicherer. Darüber hinaus zeigte Aucotec, wie eine KI-gestützte Lösung zur automatisierten Umsetzung normkonformer Schutz- und Leittechnikmodelle funktioniert.

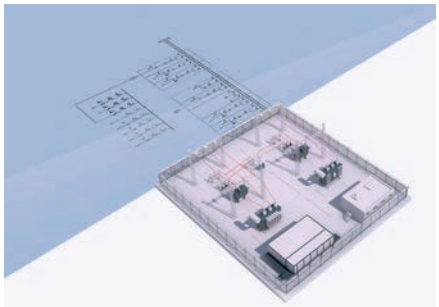
Das ist Engineering Base: Alle Disziplinen, einschließlich der Schutz- und Leittechnik, haben Zugriff auf das konsolidierte Datenmodell – so entsteht konsistente Aktualität und die Tool- und Systemlandschaft wird deutlich verschlankt

IEC 61850 nahtlos integriert – erstmals durchgängig in einer Plattform

Die Digitalisierung und Dekarbonisierung der Energienetze stellen neue Anforderungen an Planung und Betrieb moderner Umspannwerke. In dieser neuen Ära übernehmen Server und Datenbus-Systeme den Informationsaustausch – klassische, dokumentenbasierte Tools stoßen dabei zunehmend an ihre Grenzen. Die Norm IEC 61850 hat sich dabei als zentrale Grundlage für digitale Umspannwerke etabliert.

Engineering Base ist die weltweit erste Plattform, in der sich IEC-61850-konforme Datenmodelle ohne externe Tools direkt modellieren und mit dem Produktaspekt, also der Hardware-Welt, verknüpfen lassen. Die gesamte Definition erfolgt zentral, normgerecht und medienbruchfrei – vom Datenobjekt bis zur fertigen Konfiguration.

Alle Disziplinen – von Primär- bis Leittechnik – arbeiten parallel und zentral mit denselben Daten. Eigene Bibliotheken, Änderungsverfolgung und eine einheitliche Datenbasis sorgen für hohe Effizienz und maximale Transparenz. Durch die enge Verbindung zwischen funktionalem Modell und realer Hardware wird die Systemlandschaft deutlich verschlankt, IT-Ressourcen werden entlastet und Engineering-Zeiten verkürzt.



Transparenter, stets aktueller Digital Twin des Umspannwerks in Engineering Base.

Der AI DB Builder: Intelligente Datenmodellierung

Ein Paradebeispiel für die neue Flexibilität und Automatisierung ist der vom Technologiepartner SM Energy entwickelte AI DB Builder. Er wird derzeit noch als Custom Solution eingesetzt und zeigt bereits jetzt, wie zukünftige Innovationen in Engineering Base aussehen können. Der AI DB Builder extrahiert technische Informationen aus Engineering-Dokumenten und überführt sie in objektorientierte Modelle innerhalb von Engineering Base. Dabei werden verschiedenste Datenquellen – etwa zur Netzstruktur oder zu Schutzkonzepten – automatisiert in strukturierte Engineering-Daten umgewandelt. So entstehen automatisch Geräte-Modelle, IEC-61850-Datenstrukturen, Verbindungsinformationen, Signaldefinitionen und mehr – und damit wird die Lücke zwischen klassischer Dokumentation und den Anforderungen moderner Stationsautomatisierung geschlossen. Dank der offenen Architektur von Engineering Base lässt sich der AI DB Builder nahtlos in den digitalen Engineering-Prozess integrieren. Schutzfunktionen, Verriegelungslogiken und IED-Strukturen werden dabei automatisiert erstellt, validiert und mit der realen Hardware verknüpft – fehlerfrei und in Rekordzeit.

Der AI DB Builder bietet handfeste Vorteile für Netzbetreiber ebenso wie für Ingenieurbüros: deutlich reduzierte Engineering-Zeiten, weniger manuelle Fehler, vollständige Normenkonformität und zukunftsfähige Workflows – einschließlich der direkten Umsetzung von Schutzkonzepten und Verriegelungslogiken.

RÜCKFRAGEN & KONTAKT

Aucotec GmbH
Ignaz-Köck-Straße 10, 1210 Wien
Tel.: +43 1 270 85 77-0
sales.at@aucotec.com
www.aucotec.at

BMD WÄCHST WEITER

Mit einem Umsatzplus von über acht Prozent und erstmals einem neunstelligen Konzernumsatz blickt BMD auf ein starkes Geschäftsjahr. Wachstumstreiber sind gezielte KI-Investitionen, digitale HR- und ESG-Lösungen sowie eine konsequente Internationalisierungsstrategie.

Im Wirtschaftsjahr 2024/2025 erzielte die international tätige BMD Systemhaus GesmbH ein besonderes Ergebnis. „Der Umsatz des Unternehmens lag im Geschäftsjahr 2024/2025 bei 97 Mio. Euro, was einem Anstieg von über acht Prozent gegenüber dem Wirtschaftsjahr 2023/2024 entspricht“, erläutert Markus Knasmüller, Geschäftsführer der BMD. Im Konzern ist man sogar zum ersten Mal wohl neunstellig. „Unser Ziel bleibt klar: Wir gestalten die digitale Zukunft für Unternehmen und Kanzleien aktiv mit – als Innovationsführer, verlässlicher Partner und Arbeitgeber mit Haltung“, betont Knasmüller und sagt weiter „Unser kontinuierlicher Fokus auf Innovation und Kundennutzen hat sich einmal mehr ausgezahlt. Wir investieren gezielt in zukunftsweisende Technologien wie künstliche Intelligenz, nachhaltige Softwarelösungen und moderne Arbeitswelten. Das kommt unseren Kundinnen und Kunden ebenso zugute wie unseren Mitarbeiterinnen und Mitarbeitern. Unsere Innovationsstrategie trägt Früchte – besonders im Bereich der KI-gestützten Prozessautomatisierung, der digitalen HR-Lösungen und beim Ausbau unserer ESG-Angebote.“

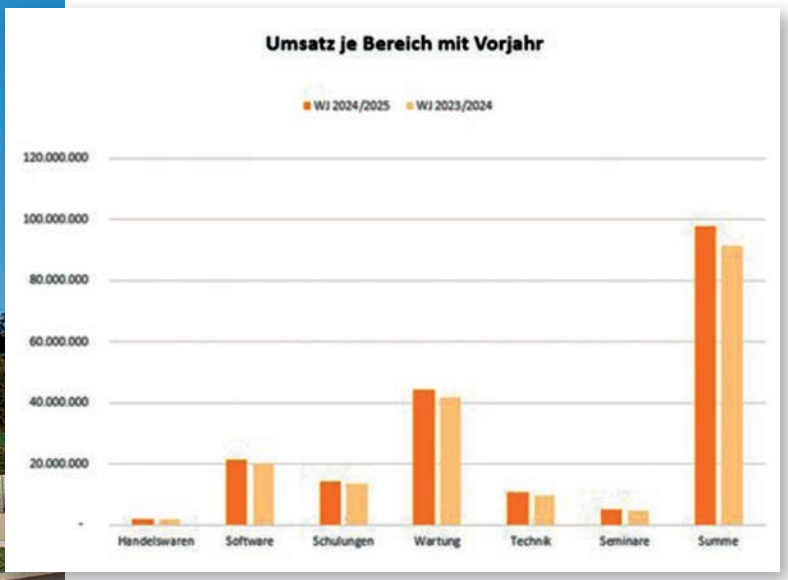
VIEL INVESTMENT

»Wir investieren gezielt in zukunftsweisende Technologien wie künstliche Intelligenz, nachhaltige Softwarelösungen und moderne Arbeitswelten.«

Markus Knasmüller, Geschäftsführer BMD

INTERNATIONALISIERUNG WIRD WEITER FORCIERT

Ein wichtiges Thema ist die Internationalisierung der BMD mit besonderem Fokus auf den deutschsprachigen Raum. In Deutsch-



land wurde die erste Akquisition erfolgreich abgeschlossen: Es wurde ein Teilbereich eines Softwareunternehmens übernommen. In der Schweiz hat BMD eigenen Angaben zufolge als Marktführer im Bereich Wirtschaftsprüfung seine Position gehalten. Aktuell zeigt sich das Wirtschaftsjahr aus der Sicht von BMD International in einem sehr erfreulichen Licht. So konnte der Umsatz in allen Niederlassungen deutlich gesteigert werden. Fest steht, dass auch hier weitere Unternehmensakquisitionen folgen werden, um das Wachstum weiter voranzutreiben.

FORTSCHRITTE BEI DER KI

Künstliche Intelligenz ist heute nicht mehr wegzudenken. BMD setzt sie gezielt in den unterschiedlichsten Anwendungsfeldern ein. Einerseits kommt sie im Support selbst zum Einsatz: BMD Fox ist ein Chatbot, der bereits Tausende Anfragen pro Woche beantworten kann. Andererseits ergänzt sie die BMD-Software auf wertvolle Weise. So gibt es etwa Textgeneratoren, automatische Auslegungen von betriebswirtschaftlichen Auswertungen und Anomalie-Erkennungen. Auch im Ausbildungsbereich spielt KI eine wesentliche Rolle.

BMD AKADEMIE

Ein besonderer Vorteil der BMD-Seminare ist, dass jede:r Teilnehmende einen eigenen PC-Arbeitsplatz mit zwei Bildschirmen hat. Der Zugriff erfolgt dabei via Remote Desktop, wodurch der Vorteil einer zentralen Wartung genutzt werden kann. Auf Knopfdruck kann so ein ursprünglicher Stand wiederhergestellt werden, sodass die Teilnehmenden beliebig „experimentieren" können. Diese zentrale Wartung wird derzeit neu aufgestellt und ist eines der ersten Projekte der Microsoft-Cloud-Region Österreich.

NEUE ENTWICKLUNGEN

Das Mehrwertsteuer-Modernisierungspaket wurde am 11. März vom Rat der Europäischen Union endgültig verabschiedet. BMD-Geschäftsführer Markus Knasmüller wurde sowohl von der Kammer der Steuerberater und Wirtschaftsprüfer als auch von der WKO als Experte in verschiedene Gremien entsandt, unter anderem Anfang April zum Fiscalis-Workshop der EU. Der große Wurf, nämlich die Einführung strukturierter digitaler Rechnungen, blieb vorläufig aus. Erst ab Juli 2030 sind diese im innergemeinschaftlichen Verkehr verpflichtend. Der nationale Gesetzgeber kann hier aber schon früher tätig werden. So ist etwa in Deutschland seit Jahresbeginn der Empfang von digitalen Rechnungen verpflichtend und ab 2027 dürfen nur noch digitale Rechnungen versendet werden. Die EU-Transparenzrichtlinie ist im Juni 2023 in Kraft getreten und muss bis Juni 2026 in österreichisches Recht umgesetzt werden. Ziel ist es, den Grundsatz des gleichen Lohns für gleiche oder gleichwertige Arbeit zu stärken. Derzeit finden Generalkollektivverhandlungen statt, um zu klären, wie genau dies in österreichisches Recht umgesetzt werden muss. Auch die Frage, wie genau die Meldung erfolgen sollte, ist noch zu klären. Unabhängig davon müssen sich die Betriebe darauf vorbereiten. Daher ist es von Bedeutung, den Gap bereits für die Jahre 2024 und 2025 feststellen zu können, um zu wissen, ob Maßnahmen nötig sind oder nicht. BMD hat in der Lohnverrechnung bereits jetzt die idealen Werkzeuge dafür. BS

Fotos: BMD Systemhaus GesmbH/Gabor Bota

V.l.n.r.: Andreas Kugi, AIT Scientific Director, Peter Schwab, AIT-Aufsichtsratsvorsitzender, Brigitte Bach, AIT Managing Director & Spokesperson of the Management Board und Alexander Svejkovsky, AIT Managing Director. Im Rahmen der Bilanzpressekonferenz wurde auch der aktuelle „Impact Report" des AIT präsentiert.

AIT MIT KLARER VISION

Das AIT präsentierte ein solides Jahresergebnis für das vergangene Jahr, hohe Investitionen und starken Impact und verzeichnet eine hohe Nachfrage nach anwendungsorientierter Forschung.

Das AIT Austrian Institute of Technology blickt auf ein wirtschaftlich erfolgreiches Jahr 2024 zurück. Mit einem Ergebnis nach Steuern von 5,42 Mio. Euro konnte das Ergebnis auf einem Niveau gehalten werden, das weitere Investitionen in strategische Zukunftsfelder ermöglicht. Die Summe der betrieblichen Erträge erreichte 218 Millionen Euro – ein Plus von neun Prozent gegenüber dem Vorjahr. Wesentlichen Anteil daran hatten die externen Erlöse aus Auftrags- und kofinanzierter Forschung, die um 11,3 Prozent auf insgesamt 130,7 Millionen Euro anwuchsen. Trotz eines erwartbaren Rückgangs beim Auftragseingang – bedingt durch hohe Einmaleffekte im Vorjahr – konnte der Auftragsstand des AIT zum Jahresende um sechs Prozent auf 276,2 Millionen Euro gesteigert werden. Auch personell wuchs das Institut: Das AIT zählt aktuell 1.653 Mitarbeitende aus mehr als 50 Nationen. „Am AIT verfolgen wir eine klare Vision: We make innovation a driving force in Europe", betont Brigitte Bach, Managing Director und Spokesperson of the Management Board des AIT, bei der Präsentation der Bilanz 2024. „Angesichts des zunehmenden globalen Wettbewerbs braucht Europa gezielte Investitionen in Forschung und Innovation sowie eine enge Zusammenarbeit zwischen Wissenschaft, Industrie und öffentlicher Hand. Innovation heißt, dass Forschung am Markt ankommt. Und darum geht es letztlich beim AIT." Deshalb steht die Wettbewerbsfähigkeit Österreichs und Europas im Zentrum der Forschungs- und Entwicklungsaktivitäten des AIT.

AIT GEHÖRT ZU SPITZENGRUPPE

„Wie sehr wir – gemäß unserer Vision – hier Leadership zeigen, sieht man an unseren Beteiligungen im aktuellen EU-Forschungsrahmenprogramm Horizon Europe: Das AIT ist bisher in 127 Projekten aktiv, in 26 davon in der Koordinatorrolle. Mit einer Gesamtfördersumme von über 77 Millionen

Euro mit Ende 2024 zählen wir zu den Top 3 Forschungseinrichtungen in Österreich", so Brigitte Bach.

IMPACT DER AIT-FORSCHUNG

Die Dreier-Geschäftsführung des AIT legt im Rahmen der Bilanzpressekonferenz auch den aktuellen „Impact Report" vor und betont, dass die AIT-Forschung konkrete Lösungen für reale Herausforderungen liefert. „Der Impact Report zeigt anhand zahlreicher Beispiele, wie AIT-Technologien direkt in Wirtschaft und Gesellschaft wirken", erläutert Andreas Kugi, Scientific Director des AIT. Künstliche Intelligenz kommt etwa beim Schutz vor Onlinebetrug durch den Fake-Shop Detector sowie in der Stahlindustrie zur Qualitätskontrolle und beim autonomen Betrieb von Maschinen zum Einsatz. Mit der AI Factory Austria beteiligt sich das AIT maßgeblich am Aufbau eines Supercomputer-Hubs mit einem AI-One-Stop-Shop für Unternehmen. Im Bereich nachhaltiger und resilienter Infrastrukturen reicht die Bandbreite von führender Quantenkommunikationstechnologie bis hin zu optimierten Energiekonzepten mit Hochtemperatur-Wärmepumpen für die CO_2-neutrale Ziegelproduktion und innovativen Mixed-Reality-Lösungen für das Training von Einsatzkräften.

STRATEGISCHE ZUKUNFTSFELDER

Andreas Kugi hebt bei der Bilanzpressekonferenz mehrere strategische Zukunftsfelder des AIT hervor: „In den kommenden Jahren bauen wir unsere nationale und internationale Vernetzung weiter aus und stärken gezielt jene Felder, in denen wir bereits führend sind, und nutzen gezielt Synergien der Kooperation." Darunter fallen Bereiche wie Applied AI Engineering, Digitalisierung und Dateninfrastrukturen; weiters Sicherheitsforschung und Quantentechnologien sowie die Optimierung industrieller Prozesse durch AI, Automatisierung, Energie- und Ressourceneffizienz und neue innovative Mensch-Maschine-Konzepte.

AIT IST IN WICHTIGEN ZUKUNFTSTHEMEN INVESTIERT

Das AIT investierte auch im Geschäftsjahr 2024 intensiv in Forschungsthemen und -infrastruktur. „Mit einem Investitionsvolumen von 13 Millionen Euro wurden zentrale Projekte angestoßen und fortgeführt", erläutert AIT Managing Director Alexander Svejkovsky: In Wien nahm ein neues Feststoff-Batterielabor den Betrieb auf. In Seibersdorf wurde der Aufbau des AIT H2Lab als nationale Testumgebung für Wasserstofftechnologien gestartet. Ergänzt wurde dies durch den Baubeginn eines Großprüfstands für Wärmepumpen bis 100 kW.

Ein besonders dynamisches Feld ist der Technologietransfer über Spin-offs und Entrepreneurship-Initiativen: „2024 haben wir drei neue Spin-off-Projekte in der Vorgründungsphase begleitet. Ziel ist ein marktnaher und erfolgreicher Einstieg", sagt Alexander Svejkovsky. „Wir gestalten ein Ökosystem für Spin-offs in Österreich und Europa mit. Dieses Ökosystem soll stark getragen sein von Kooperation mit Universitäten, Inkubatoren, Förderagenturen und anderen etablierten Akteuren der Start-up-Welt in Österreich. Österreich muss in diesem Bereich mehr Gewicht auf die Waage bringen, um europäisches Kapital anzuziehen", so Alexander Svejkovsky. BS

Fotos: AIT/APA-Fotoservice/Rudolph

AXFLOW GESMBH

Mit der Integration der Tochterunternehmen TUMA Pumpensysteme (Wien) und VIP Tehnika (Duplek/Maribor) setzt AxFlow neue Maßstäbe in der Fluidtechnik. Die Synergie der jeweiligen Expertise und Kompetenzen dieser drei Standorte erlaubt es, umfassende und maßgeschneiderte Lösungen zu bieten.

Individuelle Fluidtechnik neu gedacht

Die Flüssigkeitsring-Vakuumpumpen von TUMA fördern und verdichten Gase in diversen Anwendungen und werden in besonderen Ausführungen auch zum Fördern von explosiven Gasen, z. B. von Wasserstoff und Dämpfen, eingesetzt.

■ Seit mehr als 35 Jahren ist AxFlow ein kompetenter Partner in der Fluidtechnik. Als Kompetenzzentrum für Verdrängerpumpen und Fluid Handling bietet das Unternehmen ein breites Portfolio an Pumpen, Mischern, Rührwerken, Homogenisatoren und Wärmetauschern. Durch die enge Zusammenarbeit mit führenden Herstellern und ein umfassendes „Rundum-sorglos-Paket" – von der Planung über die Entwicklung bis zur Installation – hat sich AxFlow als bevorzugter Partner für hygienische und industrielle Anwendungen etabliert.

AxFlow ist spezialisiert auf Verdrängerpumpen, die für Anwendungen mit hoher Dosiergenauigkeit und wechselnden Viskositäten von Flüssigkeiten benötigt werden. Die Produktpalette umfasst Schlauch-, Dosier-, Exzenterschnecken-, Drehkolben- und Membranpumpen. Für Anwendungen, die eine gleichmäßige Textur und verbesserte Haltbarkeit erfordern, bietet AxFlow eine breite Palette an Homogenisatoren, die besonders in der Lebensmittel-, Pharma-, Chemie- und Kosmetikindustrie sowie in biotechnologischen Prozessen gefragt sind. Im Bereich Sustainability können Wärmetauscher einen großen Beitrag leisten.

TUMA – Vakuumtechnik für höchste Ansprüche

TUMA Pumpensysteme, ein wichtiges Tochterunternehmen von AxFlow, ist auf innova-

VIP Tehnika bietet Druckerhöhungsanlagen, die einen konstanten Druck in Wasserversorgungssystemen gewährleisten.

tive Vakuumpumpenlösungen spezialisiert. Die umfangreiche Produktpalette umfasst Drehschieber-, Schrauben- und Flüssigkeitsringpumpen, die für alle Industriezweige wie Chemie, Pharma und Lebensmittel ideal geeignet sind. TUMA bietet maßgeschneiderte Lösungen, die den höchsten Qualitäts- und Leistungsstandards entsprechen, und zeichnet sich durch umfassende Engineering- und Projektmanagement-Fähigkeiten aus.

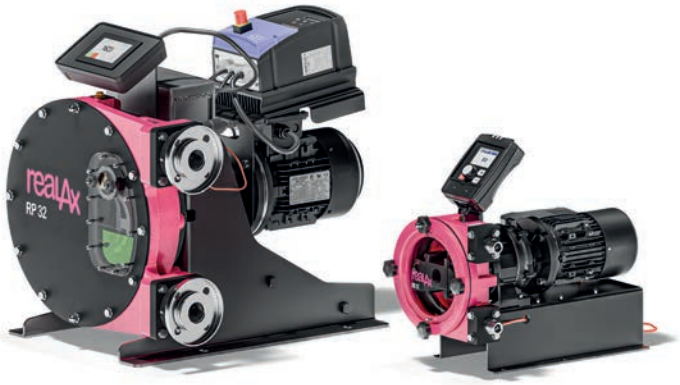
Durch die Verwendung von Pumpenkomponenten international führender Hersteller und Elektromotoren realisiert TUMA energieeffiziente Anlagen und verfügt über umfangreiche Erfahrung im Bau von schlüsselfertigen Spezialanlagen, die höchsten Sicherheitsstandards entsprechen. Bedeutende Projekte sind die Lieferung einer Vakuumanlage für eine der weltweit effizientesten Müllverbrennungsanlagen und hochwertige Vakuumaggregate für die Pharmaindustrie.

VIP Tehnika – Kompetenz in Druckerhöhungsanlagen, Anlagenbau und Pumpensystemen

Als Kompetenzzentrum für Kreiselpumpen und Anlagenbau ist VIP Tehnika – ein weiterer wichtiger Teil der AxFlow GesmbH Österreich – führend in der Branche. Das Unternehmen bietet umfassende Lösungen für Wasser- und Abwasseranwendungen und erweitert die Aktivitäten von AxFlow auf dem Balkan. Mit fast 30 Jahren Erfahrung bietet VIP Tehnika eine breite Palette renommierter Marken und konstruiert maßgeschneiderte Pumpensysteme. Die Produktpalette von VIP Tehnika für die Industrie umfasst Pumpen für die Wasserversorgung, landwirtschaftliche Bewässerung, Pharma- und Lebensmittelindustrie, Kesselanlagen, Abwasserentsorgung und Reinigungssysteme. VIP Tehnika bietet Druckerhöhungsanlagen, die einen konstanten Druck in Wasserversorgungssystemen gewährleisten und sich durch Energie- und Wassereffizienz, qualitativ hochwertige Komponenten und eine robuste Konstruktion auszeichnen.

Ein engagiertes Expertenteam für optimale Prozessintegration

Die AxFlow-AT-Gruppe vereint die Fähigkeiten der Kompetenzzentren AxFlow, TUMA und VIP Tehnika, um jede Flüssigkeitsanwendung effizient zu bedienen. Das Unternehmen legt großen Wert auf nachhaltige Lösungen und bietet umfassende Dienstleistungen von der Beratung über die Installation bis hin zur Wartung. Mit einem engagierten Expertenteam sorgt AxFlow dafür, dass jede Pumpe optimal in den jeweiligen Prozess integriert wird. AxFlow steht für Qualität, Innovation und einen kontinuierlichen Betrieb, der durch das Firmenmotto „fluidity.nonstop“ perfekt verkörpert wird.



realAx Schlauchpumpen decken ein breites Spektrum unterschiedlicher Förder- und Dosieranwendungen ab. NEU mit Dosiercomputer.

AxFlow
fluidity.nonstop

RÜCKFRAGEN & KONTAKT

AxFlow GesmbH
Seering 2/2. OG, 8141 Premstätten
Tel.: +43 316 68 35 09
office@axflow.at, **www.axflow.at**

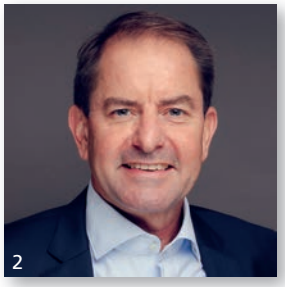
Anzeige • Fotos: Axflow

V.l.: Philipp Guth, CTO Rittal, Ulrich Engenhardt, CBO Rittal, Marc Wucherer, CEO Lenze SE, Christian Eberhard, Senior Vice President Sales EMEA Central bei Lenze, und Raphael Görner, Geschäftsbereichsleiter Energy & Power Solutions bei Rittal.

TECHNOLOGIEPARTNERSCHAFT

Im Maschinen- und Anlagenbau gilt es gerade jetzt, alle Optimierungspotenziale zu heben. Lenze und Rittal haben eine Technologiepartnerschaft geschlossen, um gemeinsam Stromverteilung und Antriebstechnik in die Zukunft zu führen.

Die Anforderungen im Maschinenbau steigen. Komplexe Antriebslösungen müssen flexibel, verlässlich und immer kompakter aufgebaut werden. Fachkräftemangel und Kostendruck erfordern zudem ein neues Effizienz-Level bei Engineering, Aufbau und Inbetriebnahme von Maschinen und Anlagen. Hier setzen Lenze und Rittal jetzt gemeinsam als Technology Partner an. „Lenze ist ein Taktgeber der Automatisierung und hat mit dem Dreiklang aus Elektromechanik, Elektronik und Software die Prozesse der Kunden weit über die Komponenten hinaus im Blick. Das passt zu Rittal und macht das Unternehmen zu einem exzellenten Technologiepartner im RiLineX-Ökosystem“, sagt Ulrich Engenhardt, Chief Business Units Officer bei Rittal. „Mit der Systemplattform RiLineX setzt Rittal neue Maßstäbe bei der Stromverteilung im Schaltschrank. Durch den Einsatz von Lenze-Umrichtern erweitern wir diesen Nutzen auf die Antriebstechnik und schaffen damit für unsere Kunden kompaktere Lösungen.



KOMPAKTERE LÖSUNGEN

»Mit der Systemplattform RiLineX setzt Rittal neue Maßstäbe bei der Stromverteilung im Schaltschrank. Durch den Einsatz von Lenze-Umrichtern erweitern wir diesen Nutzen auf die Antriebstechnik und schaffen damit für unsere Kunden kompaktere Lösungen.«

Dr. Marc Wucherer, CEO Lenze SE

für unsere Kunden kompaktere Lösungen“, ergänzt Marc Wucherer, CEO Lenze SE.

DOPPELT PLATZ UND ZEIT GESPART

Ein Praxisbeispiel für Anwender-Synergien ist der Frequenzumrichter i550 cabinet von Lenze. Der kompakte Umrichter bietet einen außergewöhnlich breiten Temperaturbereich von –30 bis +60 °C und offene Schnittstellen zu allen gängigen Steuerungen, mit skalierbarer Funktionalität für Förderantriebe, Fahrantriebe, Wickelantriebe, Hubantriebe, Extruder, Verpackungsmaschinen oder industrielle Klimatechnik. „Der Lenze i550 cabinet ist der weltweit kompakteste Frequenzumrichter seiner Klasse. Dieser wesentliche Pluspunkt wird mit RiLineX noch verstärkt“, erläutert Christian Eberhard, Senior Vice President Sales EMEA Central bei Lenze. „Auf der Plattform wird er noch platzsparender und einfacher installiert.“
Wie das geht? Der sonst übliche Einbauort auf der Montageplatte wird für andere Komponenten frei, da der Umrichter mitsamt Absicherung per „Click&Work“ auf einem einzigen Adapter auf dem RiLineX Board Platz findet – und zwar mit höchster Packungsdichte. Denn der schmale Frequenzumrichter ist nahtlos auf dem vollständig überbaubaren Board anreihbar. Auch Verkabelung und entsprechende Fehler sind damit Vergangenheit. Das Ergebnis für die Kunden: Nach 30 Prozent Zeitvorteil beim Engineering und bis zu 75 Prozent bei der Montage von RiLineX geht es auch bei der Umrichter-Installation mit hohem Tempo und deutlichem Platzvorteil im Schrank weiter. Die Datenverbindung des Frequenzumrichters über WLAN beschleunigt später zudem die Inbetriebnahme. „In der Konfigurationssoftware RiPower schlagen wir aus gutem Grund zuerst Komponenten aus unserem Technology-Partner-Ökosystem vor. Wir bieten den Kunden damit einfachen Zugang zu geprüften Komponenten wie den Lenze-Umrichtern, die sich besonders für zukunftsfähigen Maschinen- und Anlagenbau eignen und umfassende Daten für das Engineering mit Eplan bieten“, erläutert Raphael Görner, Geschäftsbereichsleiter Energy & Power Solutions bei Rittal.

DATENQUALITÄT FÜR SCHNELLERE PROZESSE

Hohe Datenqualität ist Voraussetzung für effiziente Prozesse schon bei Engineering und Konfiguration. Hier verfolgen beide Partner ähnliche Ansätze. Rittal RiPower setzt auf enge Integration mit der Eplan Software. Lenze nutzt als Eplan Technology Partner ebenfalls solche hochwertigen Daten für seine Kunden. Das Eplan Data Portal mit über vier Millionen Artikeldaten ist beispielsweise auch Datenquelle für den EASY Product Finder (EPF) von Lenze, ein Onlinetool, das für die Kunden die Suche, Konfiguration, Angebotsanfrage und Bestellung von Lenze-Produkten vereinfacht. Zusätzlich zum konfigurierten Produkt erzeugt das System einen kompletten Satz an Eplan-Daten inklusive Verdrahtungslisten, Schaltschrankaufbauten und Fertigungsdokumentationen aus Eplan Pro Panel. Lenze-Kunden können sämtliche Fertigungsdaten auf Knopfdruck im Eplan-Format herunterladen.
Auch im EASY System Designer, dem webbasierten Engineering-Tool von Lenze für die Antriebsauslegung und komplette Planung von Maschinenlösungen, kommen diese Daten zum Einsatz – für kürzere Entwicklungszeiten und höhere Qualität bei geringerem Personalaufwand durch einfache Systemauslegung. BO

www.rittal.at
www.lenze.com

3

4

Der i550 cabinet von Lenze ist in seiner Klasse der kompakteste Frequenzumrichter am Markt. Bei der Montage auf RiLineX wird noch weiterer Bauraum frei (3). RiLineX spart bis zu 75 Prozent Zeit bei der Montage. Schon vor dem Verkaufsstart hat Rittal ein Ökosystem mit Technologiepartnern angestoßen (4).

Fotos: Rittal GmbH (1+4), Lenze (2+3)

PRODUKTIVE NEUHEITEN

Von neuen Absolut-Encodern über selbstständige Rastbolzen bis zu selbst produzierten Schaltern und Tastern – die Produkt-Highlights im Juli und August.

Neue Absolut-Encoder-Generation
Mit dem neuen ANS/ANM58 Profinet präsentiert Sick eine Absolut-Encoder-Generation, die auf höhere Maschinen- und Anlagenproduktivität ausgelegt ist. Das verbesserte, optische Messsystem ermöglicht eine hochpräzise Bewegungssteuerung, während zugleich die Echtzeitübertragung von Bewegungs- und Positionsdaten kurze Zykluszeiten sowie Profinet-IRT-taktsynchrone Prozesse ermöglichen. Die Best-in-Class-Kompaktheit und große mechanische Varianz der Encoder bietet erhebliche Vorteile bei der mechanischen Integration in enge und anspruchsvolle Einbausituationen. Die steuerungstechnische Anbindung erfolgt auf einfache Weise über das Siemens TIA-Portal oder das Sick-Tool Sopas. Darüber hinaus unterstützen die Absolut-Encoder ANS/ANM58 mit ihren prozessrelevanten Diagnosedaten auch die zustandsabhängige Anlagenwartung. Damit decken sie das breite Spektrum industrieller Anforderungen an State-of-the-Art-Encoder in vollem Umfang ab, wie sie unter anderem in der Verpackungstechnik, im Maschinenbau sowie in der Lager- und Fördertechnik relevant sind.
www.sick.at

Performant, robust, vielseitig
Industrielle Temperaturmessgeräte sind oftmals anspruchsvollen Bedingungen wie hohen Temperaturen, Staub, Feuchtigkeit oder elektromagnetischen Störungen ausgesetzt. Die drei neuen Pyrometer thermoMETER UC (Universal Controller), SE (Separate Electronic) und FI (Fully Integrated) von Micro-Epsilon meistern all diese Herausforderungen durch ein robustes Metallgehäuse und eine exzellente Temperaturstabilität, auch bei hohen Umgebungstemperaturen. Die Pyrometer messen schnell, präzise und berührungslos Oberflächentemperaturen von –50 bis +900 °C mit einer äußerst hohen Signalqualität und Signalstabilität. Die drei Varianten unterscheiden sich vor allem im Aufbau und damit in ihren Einsatzmöglichkeiten: die hochperformante Variante UC mit abgesetztem, robustem Controller für hohe Temperaturbereiche, die Miniaturvariante SE mit miniaturisiertem Controller im Kabel als Lösung mit geringem Installationsaufwand und die vollintegrierte Kompaktlösung FI mit Sensor und Controller in einem Gehäuse. Weitere Vorteile sind der parallele Digital- und Analogbetrieb sowie die integrierte Alarmfunktion. Alle Modelle sind werkseitig voreingestellt und sofort einsatzbereit. Nutzer:innen profitieren von einfachen Ka-

librier- und Parametrieroptionen sowie umfangreichen Signalverarbeitungs- und Einstellmöglichkeiten über die sensorTool-Software. Die Integration kann über zahlreiche Schnittstellen erfolgen – analog, digital, Ethernet und Feldbus.
www.micro-epsilon.at

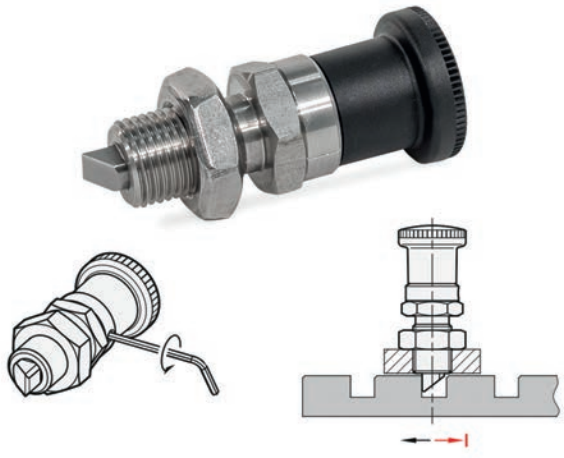
Flexibel und widerstandsfähig
Für den Transport von Medien wie Wasser oder Luft kommen in der Regel Spezialschläuche zum Einsatz. Damit diese umfassende Flexibilität und hohe Widerstandsfähigkeit miteinander kombinieren, hat der Automatisierungsspezialist SMC die Serie TUE entwickelt. Die doppelwandigen Schläuche aus zwei verschiedenen Materialien vereinen Umweltbeständigkeit mit Biegsamkeit, decken einen breiten Betriebstemperaturbereich ab und sind in vier Farbvarianten sowie fünf unterschiedlichen Außendurchmessern erhältlich. Gemeinsam bieten sie optimale Eigenschaften, um für eine große Bandbreite an Anwendungen einen zuverlässigen Medientransport zu gewährleisten. Die äußere Schicht der Serie TUE besteht aus Fluorpolymer, das besonders widerstandsfähig gegen Umwelteinflüsse wie Flammen oder Chemikalien ist, und sie erfüllt die Vorschrift UL 94 nach den Kriterien V-0 zur Brennbarkeit von Kunststof-

Fotos: Sick, Micro Epsilon

fen. Der Schlauch ist so auch für Anwendungen mit Schweiß- oder Kühlmittelspritzern geeignet und realisiert durchgehend hohe Prozesssicherheit. Die innere Schicht aus Polyurethan sorgt dagegen für hohe Flexibilität mit einem minimalen Biegeradius zwischen 11 und 44 mm sowie 14 und 61 mm. Damit lässt sich der Schlauch problemlos für verschiedene Applikationen und auch bei engen Platzverhältnissen einsetzen. Dank der vorhandenen Außendurchmesser von wahlweise 4, 6, 8, 10 und 12 mm eignet sich die Serie TUE für unterschiedliche Applikationsspezifikationen. Im Vergleich zur Vorgängerserie TU hat sich der Querschnitt um bis zu 44 Prozent vergrößert. Ergänzt wird dies u. a. durch die Vielzahl an verwendbaren Steckverbindungen KQB2/KQG2, KF (als Polyamid- oder Messing-Buchse) und KFG2 von SMC. Dabei sind die Schläuche insgesamt für einen breiten Betriebstemperaturbereich geeignet – bei Druckluft und inerten Gasen von –20 bis +80 °C bzw. bei Wasser von 0 bis 70 °C –, was den Einsatzbereich auf verschiedene Anwendungen und Industriezweige weiter ausdehnt.
www.smc.com

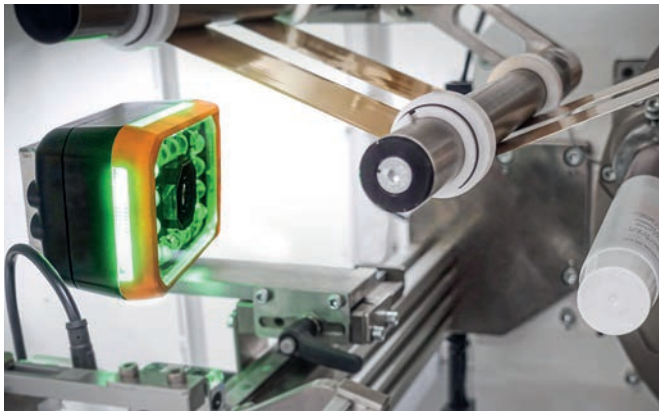
Selbstrastend dank Anlaufschräge

Sie sind geradezu universelle Elemente, nahezu überall anzutreffen, wenn es ums Verriegeln, Fixieren und Arretieren geht: Rastbolzen. So unterschiedlich die Bauformen und Dimensionierungen, eines haben die bisher existierenden Elemente gemeinsam: Der Rastvorgang erfolgt normalerweise an einer zylindrischen Bohrung, die zum Durchmesser des Raststifts ausgerichtet ist und die von diesem ohne Hindernisse erreicht werden kann. Es existieren aber auch Fälle, bei denen zum Rasten nur eine Kante oder eine Nut genügen muss, die zudem seitlich nicht genau zum Raststift positioniert werden kann. Für solche Anwendungen hat Elesa+Ganter nun eine neue Art von Rastbolzen entwickelt, die selbstständig an Kanten und Nuten einrasten kann. Möglich macht dies ein angeschrägter Raststift. Stößt dieser mit seiner Anlaufschräge auf eine erhabene Rastgeometrie, so fährt er ein, um danach federbeaufschlagt wieder auszufahren, sobald die Raststelle erreicht ist. Bestellbar sind die neuen Rastbolzen unter der Elesa+Ganter-Norm GN 824, mit axialer Gewindefixierung und schwarzem Kunststoffknopf zur Betätigung. Damit die Anlaufrastung zuverlässig abläuft, baut Elesa+Ganter Raststifte aus gehärtetem und robustem Edelstahl mit quadratischem Querschnitt und gängiger Dimensionierung ein. Wird der Rastbolzen über eines der Standardgewinde M12 bis M20 eingeschraubt und gekontert, dann nimmt die Anlaufschräge zunächst eine willkürliche Winkellage ein. Damit diese tatsächlich senkrecht auf ihr Gegenüber auftrifft, kann der Raststift um 360 Grad justiert werden – ganz einfach durch Lösen eines Gewindestifts im Sockelring. Eine Markierung am Ring zeigt die Ausrichtung der Anlaufschräge an – auch wenn der Blick auf den Raststift selbst verdeckt ist. Soll der Rastbolzen zeitweise außer Betrieb gesetzt werden, sodass er nicht mehr automatisch einrastet, stehen die Formen C und CK mit Rastsperre zur Verfügung. Hierzu wird der Knopf nach dem Einziehen des Stiftes um 90° gedreht und dann durch eine Rastkerbe im Knopf in dieser Position gehalten. Ausführungen, die eine Kontermutter im Lieferumfang enthalten, lassen sich im Montagegewinde individuell auf die Rasttiefe einstellen. Rastbolzen mit Anlaufschräge eignen sich besonders für Anwendungen, bei denen Transportgestelle, Vorrichtungen oder Klappen schnell und sicher, aber vor allem ohne manuelles Zutun verriegelt werden müssen.
www.elesa-ganter.at



Echtzeit-Vision im Maschinenprozess

B&R hat eine Smart Camera der nächsten Generation vorgestellt, die künstliche Intelligenz direkt in die Maschinensteuerung einbindet. Mit diesen integrierten KI-Funktionen ermöglicht die neue Kamera Bildverarbeitung in Echtzeit, dynamische Modellwechsel und hybride KI-basierte Inspektion – ganz ohne externe Hardware und ohne die Produktion zu unterbrechen. Maschinenbauer und Hersteller erhalten eine kompakte Plug-



Fotos: SMC, elesa+ganter, B&R

and-play-Lösung, die höhere Qualität, schnelleren Durchsatz und geringere Makulatur erzielt, selbst bei stark variierenden Produktionsbedingungen. Die neue Smart Camera kann direkt in den Regelkreis eingebunden werden, sodass Maschinen im laufenden Betrieb angepasst werden können. So erkennen Maschinen Produktfehler nicht nur, sondern reagieren unmittelbar darauf. Ein weiterer Vorteil der Smart Camera ist ihr flexibler Einsatz. Kunden können Modelle wechseln und KI-Funktionen in benutzerdefinierten Sequenzen kombinieren – ohne Produktionsunterbrechung. Diese Eigenschaft ermöglicht, den Prozess schnell an neue Produktvarianten anzupassen oder auch neuartige Fehlertypen zu erkennen. Zudem unterstützt die B&R-Lösung die schrittweise Integration von KI in bestehende regelbasierte Systeme. Im Gegensatz zu herkömmlichen Lösungen, die auf externe PCs oder Steuerungen angewiesen sind, verarbeitet die Smart Camera von B&R Bilddaten lokal. Die KI-Inferenz erfolgt in Echtzeit, angetrieben von einem Edge-KI-Prozessor, der laut Hailo-Benchmarks bis zu 15-mal effizienter ist als vergleichbare Chips.
www.br-automation.com

Neuer High-Performance-Controller
Mit der N6 bringt Nanotec einen kompakten und leistungsstarken Motorcontroller auf den Markt, der sich für Schrittmotoren mit Flanschgrößen von NEMA 14 bis 34 sowie für BLDC-Motoren bis NEMA 23 eignet. Die feldorientierte Regelung (FOC) sorgt für hohe Laufruhe und Effizienz, während die sensorlose Closed-Loop-Regelung Drehmoment und Drehzahl hochpräzise steuert. Die N6 verarbeitet Signale von Hallsensoren, inkrementellen Gebern (QEI) und SSI-Encodern. Ein externer Bremswiderstand kann direkt angeschlossen werden. Mit einem Nennstrom von 6 A und einem Spitzenstrom von bis zu 18 A ist die N6 für Anwendungen bis 300 W ausgelegt. Sechs digitale und zwei analoge Eingänge, drei Feedback-Kanäle sowie ein Bremsenausgang stehen für die Einbindung in komplexe Systeme bereit. Die Programmierung erfolgt über Plug&Drive Studio, die Parametrierung wahlweise per EtherCAT, CANopen, Ethernet/IP, Modbus TCP oder Modbus RTU. Der Motorcontroller N6 eignet sich besonders für anspruchsvolle Anwendungen in der Laborautomatisierung, Medizintechnik, Verpackungstechnik, SMD-Bestückung sowie in Wickelanlagen.
www.nanotec.com

Mit IO-Link-Schnittstelle
Mit dem MSS-IO betritt Schurter das Feld der bidirektionalen Kommunikation via Taster in der industriellen Automation. Der MSS-IO basiert auf dem erfolgreichen elektronischen Taster Schurter MSS, welcher um ein IO-Link-Modul erweitert wurde. Statt kapazitiver Technologie wird eine präzise Änderung

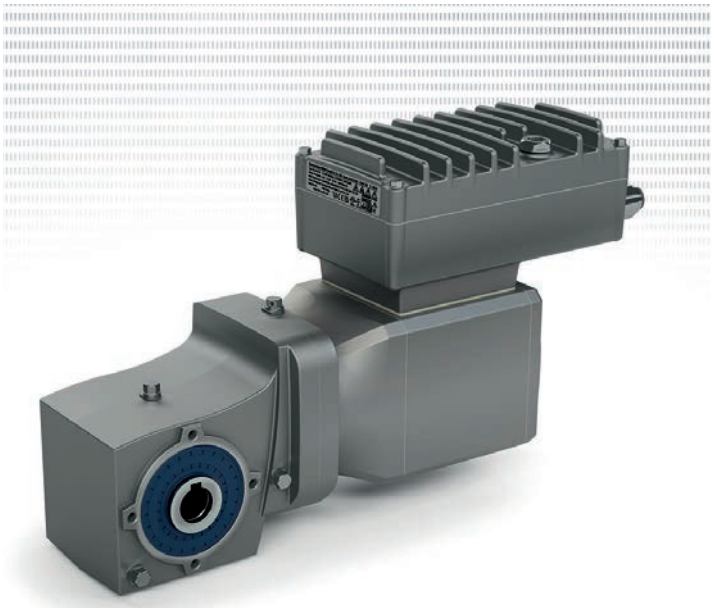
des elektrischen Widerstands zur Schalterkennung genutzt – sensibel genug, um kleinste Druckveränderungen zu erkennen, robust genug für industrielle Serienprozesse. Ultralanglebig, präzise und leicht integrierbar. Durch die geschlossene Oberfläche ist der Schalter unempfindlich gegenüber Wasser, Schmutz und Reinigungsmitteln. Dies ist ein klarer Vorteil in hygienisch sensiblen Bereichen wie Lebensmittelverarbeitung oder Laborautomatisierung. Der Verzicht auf bewegliche Teile minimiert den Wartungsaufwand und erhöht die Lebensdauer enorm. Die IO-Link-Schnittstelle erlaubt bidirektionale Kommunikation, Parametrierung im laufenden Betrieb und Echtzeit-Diagnostik. Der Anschluss erfolgt über M12-Standardstecker. Vorausschauende Wartung sowie einfache Integration in bestehende Industrie-4.0-Umgebungen sind gewährleistet.
www.schurter.com

Fotos: Nanotec, Schurter

Schalter und Taster aus eigener Produktion
Rose Systemtechnik wird einen Teil der Taster und Schalter für sein Gehäuseprogramm in Zukunft selbst produzieren. Die Abmessungen der eigengefertigten Komponenten sind deutlich kompakter als die bisher auf dem Markt zur Verfügung stehenden. Maschinen-, Geräte- und Anlagenbauer sparen dadurch viel Bauraum – die kleineren Gehäuse fügen sich optisch auch optimal in die Anwendung ein.
Zu den in Eigenfertigung hergestellten Tastern und Schaltern gehören unter anderem Wahlschalter, Druckknöpfe, Anzeigelampen und Not-Aus-Schalter. Alle Ausführungen sind ATEX- bzw. IECEx-konform (Zone 1 und 2, Zone 21 und 22), die meisten gibt es auch in abschließbarer Ausführung. Die Taster und Schalter erfüllen die Anforderungen der Schutzart IP66 (IEC 60529) und können in Temperaturbereichen zwischen –60 °C und +70 °C eingesetzt werden. Sie werden in den klassischen Farben Rot, Gelb, Grün, Blau und Bernstein sowie in Weiß und Schwarz gefertigt.
Die Module für die Steuerung bzw. Beleuchtung der Taster und Schalter produziert Rose künftig ebenfalls selbst. Die Breite der Module konnte im Vergleich zu denen von Wettbewerbs-

produkten um zwei Drittel reduziert werden. Damit sind die Kontakt- und LED-Module von Rose gerade einmal 10 mm stark und beanspruchen nur sehr wenig Bauraum.
www.rose-systemtechnik.com

Langlebig, effizient und leicht zu reinigen
Antriebslösungen für die Prozesse in der Lebensmittel- und Getränkeindustrie müssen auch unempfindlich gegen Reinigungsmittel sein, denn wegen der hohen Hygienestandards werden sie oft gereinigt und desinfiziert. Edelstahl ist in Wash-down-Bereichen das bevorzugte Material, doch in der Applikation für Antriebstechnik weist es entscheidende Nachteile auf. Die von Nord entwickelte Oberflächenveredelung NXD tupH macht Aluminium zu einer interessanten Alternative für Anwendungen



in der Branche Food & Beverage. Mit ihr werden Oberflächen von Antriebskomponenten wie Getriebe, Glattmotoren und Frequenzumrichter widerstandsfähig gegen raue Umwelteinflüsse – auch gegen aggressive Reinigungsmittel, Chemikalien, Säuren und Laugen. Antriebe aus Aluminium sind zudem signifikant leichter und laufen kühler.
NXD tupH ist speziell für Anwendungen geeignet, in denen lebensmittelkonforme Oberflächen gefordert sind. Regelmäßige Reinigungen und Desinfektionen überstehen die so veredelten Aluminiumoberflächen über lange Zeit. Die NXD-tupH-Veredelung entsteht in zwei Schritten. Im ersten wird die obere Schicht des Aluminiumkörpers in eine korrosionsbeständige, harte Schicht umgewandelt. Im zweiten wird ein Sealer aufgetragen, der eine hohe Widerstandsfähigkeit gegen Chemikalien erreicht. NXD-tupH-Oberflächen sind PFAS-frei und lebensmittelkonform gemäß FDA, der EU-Verordnung 1935/2004 sowie den Bestimmungen der Schweiz und der Mercosur-Staaten. Sie können damit in hygienekritischen Bereichen in der Lebensmittel-, Getränke- oder Verpackungsindustrie sowie in der Pharma- und Chemieindustrie eingesetzt werden.
Die innovative Oberflächenveredelung NXD tupH ist der jüngste Baustein in der Reihe für Antriebslösungen von Nord, die speziell für die Lebensmittel- und Getränkeindustrie mit ihren zunehmend strengeren Vorschriften maßgeschneidert sind. Weltweit sind bereits Tausende solcher Antriebe für Food & Beverage im Einsatz. Sie stehen für hohe Investitionssicherheit, sind robust gebaut und für einen langen Lebenszyklus konzipiert. Moderne IE5+-Antriebe stellen die hohe Effizienz sicher und senken damit Betriebskosten. Für den Einsatz in hygienesensiblen Bereichen finden Nord-Kunden eine Auswahl an lüfterlosen Glattmotoren, die leicht, schnell und gründlich zu reinigen sind. Mit der optionalen Veredelung durch NXD tupH sind diese Antriebe wash-down-fähig und korrosionsbeständig, nachhaltig und montagefertig ab Lager verfügbar.
www.nord.com

Fotos: ROSE Systemtechnik, NORD


START
NOW
ÖSTERREICHS NUMMER 1 FÜR
DIGITALE KOMPETENZ
• IT-Trainings und Zertifizierungen
• Suche und Entwicklung von IT-Talenten
für Ihr Unternehmen
Starten Sie jetzt auf etc.at
ETC