Report (+) PLUS

MEHRWERT FÜR MANAGER

# BUSINESS RESILIENCE

Wie Unternehmen widerstandsfähig werden und gestärkt aus Krisen kommen.

# CYBER-SICHERHEIT

Was Datensouveränität in der Cloud bedeutet und welche Technologie dahintersteht.

# NACHHALTIG & DIGITAL

Warum sich Resilienz-Strategien positiv auf den $CO_2$-Fußabdruck auswirken.

04 AUSGABE 2023
20. JAHRGANG

P. b. b. Verlagspostamt 1160 Wien, Vertriebskennzahl GZ 02Z034501, Einzelheftpreis: EUR 4,–

# Magenta Telekom und T-Systems stärken Partnerschaft für Österreichs digitale Zukunft

- 5-jährige Verlängerung der strategischen Partnerschaft bis 2027
- Transformation der operativen Services und Bestshoring zur Unterstützung der strategischen Ziele von Magenta
- Schnellere Time-to-Market durch Nutzung moderner hybrider Cloud-Umgebungen

Magenta Telekom und T-Systems verlängern ihre strategische Partnerschaft bis 2027. Hauptziel der Kooperation ist es, die Transformation zur Leading Digital Telco (LDT) abzuschließen, indem strategische IT-Prioritäten definiert werden, die eine schnelle Entwicklung neuer Dienste und Lösungen sicherstellen. Zu diesen Prioritäten gehören eine verstärkte Verlagerung in die Cloud sowie die Modernisierung wichtiger Anwendungen. Damit verwirklichen Magenta Telekom und T-Systems die übergeordnete Mission des Konzerns Deutsche Telekom.

Die Herausforderungen unterstreichen die Notwendigkeit eines zuverlässigen, innovativen Digitalisierungspartners mit globaler Präsenz. Seit 2002 ist T-Systems operativer Partner für Magenta in den Bereichen Managed IT Infrastructure, Application Management, SAP und Digital Solutions. Jetzt verlängern beide Unternehmen diese gemeinsame Reise um mindestens fünf weitere Jahre. »Durch diese Vertragsverlängerung wird für Magenta Telekom der Grundstein für den Wandel hin zu einem schnelleren Time-to-Market gelegt, indem die Vorteile und Chancen der Hybrid- und Multi-Cloud, sowie unseres gesamten T-Systems Portfolios, genutzt werden«, führt Peter Lenz, Vorsitzender der Geschäftsführung von T-Systems Austria, aus.

***Francois Mairey,*** Senior Vice President IT bei Magenta Telekom über die Erneuerung der Partnerschaft: »Während des gesamten Designprozesses bildeten die strategischen Ziele von Magenta die Leitlinien für T-Systems. So sind wir künftig in der Lage, ein IT-Framework auf Basis einer Hybrid Cloud zu nutzen, um so unser Geschäft zu transformieren.«

T-Systems trägt mit kosteneffizienten digitalen Lösungen und Cloud-Diensten dazu bei, Wachstumschancen zu nutzen, Innovationen zu fördern und neue zielgerichtete Dienste einzuführen. Als Partner von Magenta erweitert T-Systems die bestehende Zusammenarbeit mit den Schwerpunkten Cloudification, Agile Collaboration und Bestshoring. »Bei dem von T-Systems vorgeschlagenen attraktiven Bestshoring-Sourcing-Ansatz kombinieren wir die weltweit bestmöglichen Fähigkeiten. Dadurch erhalten wir einen Mix aus lokalen österreichischen Experten und weiteren globalen Kompetenzen zu einem wettbewerbsfähigen Preisniveau«, ergänzt Helmut Legat, Vice President Procurement bei Magenta Telekom, zum letzten Punkt.

## Die wichtigsten Vorteile der Partnerschaft sind folgende:

- **Cloudification:** professionelle Unterstützung bei der Transformation in eine zukunftssichere hybride Cloud-Architektur, bestehend aus einer individuellen Private Cloud und einer skalierbaren Public Cloud-Umgebung.
- **Best of Breed:** neue Bereitstellungsoptionen für alle Services mit lokalen Experten und globalen Kompetenzzentren für eine schnellere Markteinführung
- **Cloud Center of Excellence:** Alle Kompetenzen gebündelt in einem funktionsübergreifenden Team, um Anwendungsbetrieb und Dev Ops-Services in der Cloud zu ermöglichen
- **Flexibilität:** Ein attraktives Preismodell ohne Grenzen ermöglicht es Magenta, sein Geschäft basierend auf der tatsächlichen Nachfrage zu skalieren
- **Skaleneffekte:** Wettbewerbsfähige Konditionen durch strategische Partnerschaften von T-Systems mit allen führenden Drittanbietern und Cloud-Anbietern

***Timo Heyl,*** Senior Vice President Sales DTAG, hebt den kundenzentrierten Ansatz hervor: »Manche würden meinen, dass eine so langfristige Partnerschaft Innovation und Agilität blockiert. Das Gegenteil ist der Fall. Wir haben erneut unsere Fähigkeit unter Beweis gestellt, unsere Dienste in Übereinstimmung mit den strategischen Anpassungen unseres Kunden Magenta Telekom zu transformieren.«

Des Weiteren einigten sich Magenta und T-Systems auf den weiteren Ausbau der starken Partnerschaft für die Zukunft. Daher wurden bereits mehrere gemeinsame Initiativen über die genannten Themen hinaus gestartet, um Magenta auch in anderen Bereichen zu unterstützen. Das umfasst vor allem die Kompetenzen von T-Systems in den Bereichen Big Data & Analytics, Customer Experience, Automatisierung sowie Nachhaltigkeit.



**Gemeinsam für ein starkes digitales Österreich – Magenta Telekom und T-Systems.**

EDITORIAL

## Kalkuliertes Risiko

Vor 36 Jahren beschrieb der Soziologe Ulrich Beck die »Risikogesellschaft« und deren Leben mit der Ungewissheit: Die Suche nach Lösungen aufzuschieben, statt zu handeln, erzeuge nur noch komplexere, vielschichtigere Problemlagen. Heute befindet sich die Welt im Dauerkrisenmodus. In Angststarre zu verfallen und sich nicht zu bewegen, ist mehr denn je die falsche Reaktion.

Resiliente Unternehmen überstehen nachweislich Krisen besser und starten danach erfolgreicher durch. Sie zeichnen sich durch ihr Anpassungsvermögen aus, aber auch durch die Fähigkeit, mit Unsicherheit gut umgehen zu können. Resilienz erfordert ein Umdenken beim Risikomanagement. Wer jedes Risiko vermeidet, nimmt sich auch die Möglichkeit, aus Fehlern zu lernen. Denn Fortschritt und Innovation gehen oft mit dem bewussten Eingehen von Risiken, dem Mut zu Fehlern einher.

***Angela Heissenberger***
*Redakteurin Report(+)PLUS*

# INHALT

REPORT PLUS | MEHRWERT FÜR MANAGER




Report Verlag HERAUSGEBER/CHEFREDAKTEUR: Dr. Alfons Flatscher [flatscher@report.at] VERLAGSLEITUNG: Mag. Gerda Platzer [platzer@report.at] Chef vom Dienst: Mag. Bernd Affenzeller [affenzeller@report.at] REDAKTION: Mag. Angela Heissenberger [heissenberger@report.at], Martin Szelgrad [szelgrad@report.at] AUTOR*INNEN: Sarah Bloos B.A., Mag. Rainer Sigl LAYOUT: Anita Troger PRODUKTION: Report Media LLC LEKTORAT: Johannes Fiebich, MA DRUCK: Styria MEDIENINHABER: Report Verlag GmbH & Co KG, Lienfeldergasse 58/3, A-1160 Wien TELEFON: (01) 902 99 E-MAIL: office@report.at WEB: www.report.at

# INSIDE

Was brisant ist und
was Sie wissen müssen

## KURZ ZITIERT

»Schauen wir, dass wir die Impfstoffe haben, nicht nur wenn, sondern auch weil wir sie brauchen.«
*PHARMIG-Generalsekretär Alexander Herzog plädiert für verstärkte Versorgungssicherheit.*

»Es ist an der Zeit, zu einer Normalisierung der Geldpolitik zurückzukehren.«
*Barbara Kolm, Austrian Economics Center, bricht eine Lanze für den freien Markt.*

»Keine Region der Welt kann es sich leisten, hier den Anschluss zu verlieren.«
*AT&S-CEO Andreas Gerstenmayer sieht in der Mikroelektronik die Schlüsseltechnologie für effiziente Verkehrs-, Kommunikations- und Energienetze.*

»Es ist bemerkenswert, dass wir in Österreich immer noch um nachhaltige Forschungsmittel und zukunftsweisende Rahmenbedingungen kämpfen müssen.«
*Ulrike Prommer, Präsidentin der österreichischen Fachhochschul-Konferenz (FHK), fordert eine Investitionsoffensive für FHs.*

»Österreich hat mit der ELGA und der E-Health-Struktur stark begonnen, aber mittlerweile noch stärker nachgelassen.«
*Siegfried Meryn, Professor für innere Medizin und ORF-Gesundheitsexperte, kritisiert die lahmende Digitalisierungsstrategie.*

»Jede Kilowattstunde, die nicht erzeugt werden muss, beschleunigt die Energiewende enorm.«
*Matthias Nadrag, Geschäftsführer enixi, bringt Energieeffizienz in KMU und Gemeinden.*

»Die Menschen glauben an die KI, wenn es um ›bessere‹ Rechenaufgaben geht, aber sonst eher nicht.«
*Manfred Hämmerle, imh Institut, analysierte für eine Studie den Einsatz von künstlicher Intelligenz am Arbeitsplatz.*

# KARRIERESPRUNG NACH ZÜRICH

*Nach vier Jahren an der Spitze von Google Austria übernimmt die Österreicherin Christine Antlanger-Winter nun die Leitung von Google Schweiz. Ihre Nachfolge in Österreich ist noch ungeklärt.*

TEXT | ANGELA HEISSENBERGER

In ihre künftige Funktion in Zürich konnte sich Christine Antlanger-Winter bereits einarbeiten. Seit ihr Vorgänger Patrick Warnking im November 2022 als Osteuropa-Chef nach Warschau berufen wurde, hatte sie interimistisch auch das Geschäft in der Schweiz verantwortet. Die gebürtige Oberösterreicherin studierte Medientechnik und Mediendesign an der FH Hagenberg – bis dahin stand ein IT-Beruf nicht auf ihrem Radar. Das Studium ermöglichte der passionierten Musikerin, Technik mit kreativen Interessen zu verbinden. Mädchen und Frauen die Scheu vor Technologien zu nehmen, ist ihr deshalb aus eigener Erfahrung ein wichtiges Anliegen. Ab 2003 war Antlanger-Winter in der Mediaagentur Mindshare tätig und baute dort die Digital-Market-Unit auf. Im Februar 2018 übernahm sie die Geschäftsführung, wechselte jedoch bereits im November 2018 als Country Director zu Google Austria.

Zürich zählt mit den Schwerpunkten Software-Engineering und Forschung und rund 5.000 Mitarbeiter*innen zu den wichtigsten Entwicklungsstandorten des Konzerns weltweit. »Die neue Aufgabe in Zürich ist sehr spannend für mich, an kaum einem anderen Standort außerhalb der USA wird weltweit an so vielen Innovationen für Nutzerinnen und Nutzer gearbeitet wie bei Google in der Schweiz«, freut sich Antlanger-Winter auf den Karrieresprung. Zusätzlich zur Geschäftsleitung von Google Schweiz wird die 42-Jährige künftig auch das Kerngeschäft für die Region Schweiz/Österreich übernehmen. Ihre bisherige Position in Österreich wird vorerst interimistisch besetzt.

Foto: Inge Prader

**Innovation**

# Globale Erfolgsgeschichte

*Zahlreiche deutsche Kläranlagen setzen auf Know-how aus Österreich. Durch eine innovative Belüftungstechnologie wird der Energieverbrauch beinahe halbiert.*

*Die Technologie des Traiskirchner Unternehmens Aquaconsult wird weltweit in 2.500 Kläranlagen eingesetzt.*

Kläranlagen beanspruchen oft bis zu 20 Prozent des Elektrizitätsverbrauchs von Gemeinden. Die Kläranlage Zweibrücken in Rheinland-Pfalz zeigt vor, wie man kommunale Stromfresser effektiv vermeiden kann: Durch die Umrüstung der Anlage auf Streifenbelüfter des Traiskirchner Unternehmens Aquaconsult konnte der spezifische Stromverbrauch von über 30 kWh/a auf 18 kWh/a gesenkt werden. Neben dem geringeren Ressourcenverbrauch konnte auch die Reinigungsleistung verbessert werden.

Zur Belüftung wurden 440 Aerostrip Streifenbelüfter eingebaut. Moderne Gebläse, die aufeinander abgestuft im optimalen Wirkungsgradbereich betrieben werden, übernehmen nun die Luftversorgung. Übergeordnet stimmt ein Lastmanagement die Reinigungsvorgänge und den erforderlichen Lufteintrag bestmöglich aufeinander ab. Auch die flache Bauweise des Streifenbelüfters trägt zur Energieeinsparung bei. Mit einer Aufbauhöhe von nur fünf Zentimetern kann die gesamte Wassertiefe für den Sauerstoffeintrag genutzt werden. »Dank permanenter Forschungs- und Entwicklungsarbeit sowie regelmäßig durchgeführter Leistungstests kann unser Aerostrip als einer der effizientesten Vertreter feinblasiger Tiefenbelüfter angesehen werden«, betont Rüdiger Vrabac, Niederlassungsleiter bei Aquaconsult Anlagenbau in Deutschland. »Die Investition zahlt sich unmittelbar aus. Der Return on Invest liegt durchschnittlich bei drei Jahren.«

Die innovative Technologie aus Traiskirchen in Niederösterreich wird weltweit in mehr als 2.500 industriellen und kommunalen Kläranlagen eingesetzt. Aktuelle Referenzprojekte sind die Kläranlage »Jeddah Airport 2« in Saudi-Arabien, drei Abwasserreinigungsanlagen in Kopenhagen sowie die »Alte Emscher« in Duisburg, eine der größten Kläranlagen Deutschlands.

Foto : UBZ

Reges Interesse bei der Microsoft TC23 in der neuen Location Colosseum 21.

# KI IM FOKUS

*Mit mehr als 800 Besucher*innen stellte die Microsoft Tech Conference (TC23) einen neuen Rekord auf. Für zwei Tage verwandelte sich das Colosseum 21 in einen Innovation- und Tech-Hub, in dem sich alles um die Themen Digitalisierung, Internet of Things und Modern Workplace drehte.*

Über 40 internationale IT-Expert*innen diskutierten in spannenden Talks und Workshops über die Chancen und Risiken von Künstlicher Intelligenz. Isabell Claus, Mitgründerin der Suchmaschine thinkers.ai, betonte in ihrer Keynote, dass KI von immer mehr Unternehmen als wesentlicher Treiber der digitalen Transformation gesehen wird, wobei die KI-Transformation weit über die digitale hinausgeht. Claus forderte dazu auf, die eigene Innovationskraft vor das »Problemdenken« zu stellen, »dass KI und Technologie unseren Wohlstand prägen, so wie es Jahrzehnte lang die industriellen Innovationen getan haben.«

## CYBERCRIME VERÄNDERT SICH

Der finnische Windows-Sicherheitsexperte Sami Laiho sprach in seiner Keynote über die veränderten Sicherheitsbedrohungen für Unternehmen im Jahr 2022. Laut einer Studie haben 83 Prozent der europäischen Unternehmen zwei oder mehr Sicherheitsverletzungen erlitten. Ransomware dringt häufiger durch Angriffe auf ungepatchte Schwachstellen in Unternehmen ein als durch Phishing. »Die Ransomware-Industrie wächst und wird immer aggressiver. Wir können also davon ausgehen, dass mehr Unternehmen als je zuvor betroffen sein werden«, erklärte Laiho anhand aktueller Beispiele, wie Angreifer*innen vorgehen und welche Sicherheitskontrollen am sinnvollsten sind.

Viele betroffene Unternehmen zahlen nach Ransomware-Angriffen das geforderte Lösegeld, aber nur 65 Prozent erhalten ihre Daten zurück. Deshalb sei es essenziell, einen Aktionsplan parat zu haben, um die Geschäftskontinuität zu gewährleisten. Dieser sollte ein Business Impact Assessment, eine Kopie wichtiger Systeme und regelmäßige Tests der Disaster-Recovery-Pläne beinhalten, wie Stefan Bartram, Cybersecurity-Experte von AvePoint, ausführte. Denn mit einem guten Backup müsse sich ein Unternehmen erst gar nicht mit Lösegeldforderungen auseinandersetzen.

## DIGITALER ZWILLING

Dagmar Heidecker, IT-Sicherheitsexpertin bei Microsoft, unterstützt Unternehmen, die von Hacker*innen angegriffen wurden oder ihre IT neu aufsetzen müssen. In ihrem Talk führte sie aus, wie Hacker*innen Azure und Active Directory ausnutzen können und wie man sich davor schützen kann. Der KI-Spezialist Sebastiano Galazzo zeigte in seinem von der Netflix-Serie »Black Mirror« inspirierten Vortrag, wie man eine digitale Kopie von sich selbst erstellen kann, die Persönlichkeit, Gedanken und Hobbys abbildet und verschiedene Aufgaben erledigen kann. Lukas Keller und Anne Marchal von Tietoevry Austria präsentierten anhand der »Billa-Filiale der Zukunft«, wie durch IoT-Vernetzung ein effizienteres Energiemanagement und eine nachhaltigere Nutzung der Handelsfiliale erreicht wird. Abgerundet wurde der Auftritt von XR-Experte Helmut Krämer mit einer Live-Demo des »Metaverse for Business«, die u. a. Extended-Reality-Lösungen für Trainings an industriellen Maschinen ermöglicht.

## SPANNENDE ZEITEN

»Der Wunsch der Unternehmen, Arbeitsprozesse zu automatisieren und zu vereinfachen, ist sehr groß«, sagte Michael Swoboda, Veranstalter der TC23 und Geschäftsführer von ETC. Für über 800 Microsoft-Partner*innen und -Kund*innen aus ganz Österreich bot sich die ideale Möglichkeit, sich zu vernetzen. »Wir haben ein enormes Cloud-Wachstum in Österreich und sind deshalb dabei, unter die Topnationen innerhalb der Microsoft-Community aufzurücken«, sagte Hermann Erlach, General Manager Microsoft Österreich. »Wir erleben gerade besonders spannende Zeiten, da wir erst am Anfang der AI-Journey sind und die volle Revolution noch gar nicht absehen können«, zeigte sich auch Doris Lippert, Global Partner Solutions Lead von Microsoft Österreich, begeistert.

Foto: Ludwig Schedl_ETC

Studie

# Kernproblem Arbeitskräftemangel

*Österreich ist – dem aktuellen Deloitte Wirtschaftsradar zufolge – im europäischen Vergleich der Wirtschaftsstandorte »bestenfalls Mittelmaß«. Das schlägt sich auch auf den Arbeitsmarkt nieder: Für Arbeitskräfte aus dem Ausland ist Österreich »vollkommen unattraktiv«.*

*Die fehlenden Arbeitskräfte sind die größte Bremse für Österreichs Wirtschaftswachstum.*

Der Faktor Lebensqualität war lange Zeit für den Wirtschaftsstandort Österreich »ein echtes Ass im Ärmel«, meint Elisa Aichinger, Partnerin bei Deloitte Österreich. Dieser Vorteil zieht nicht mehr, wie der »Deloitte Radar 2023« des Beratungsunternehmens zeigt. 41 Prozent der 185 befragten Führungskräfte sehen die Verfügbarkeit von Arbeitskräften als »genügend« oder »nicht genügend« an. Bei Fachkräften sind es sogar mehr als zwei Drittel. Es gebe praktisch keine Branche mehr, die vom Arbeitskräftemangel verschont sei, so Aichinger bei der Präsentation der Studie: »Unsere Arbeitsmarktsituation ist die größte Bremse für unser Wirtschaftswachstum.«

Im internationalen Vergleich kann Österreich beim Ringen um Fachkräfte nicht mithalten. »Wir sind vollkommen unattraktiv für Arbeitskräfte aus dem Ausland«, macht Herbert Kovar, Deloitte Österreich Managing Partner Tax & Legal, die hohen Steuern verantwortlich: »Mit derart hohen Kosten auf dem Faktor Arbeit werden wir die Personalressourcen aus anderen Ländern nicht anziehen können.« Auch Osteuropa könne bereits mit guten Löhnen und Arbeitsbedingungen aufwarten – Migration ist für die Menschen kein Thema mehr.

Die Analyse der wichtigsten globalen Standort-Indizes zeige über die letzten zehn Jahre eine ernüchternde Entwicklung, erklärt Harald Breit, CEO von Deloitte Österreich: »In internationalen Rankings kommt Österreich seit Jahren nicht vom Fleck. Das Land ist auch heuer wieder bestenfalls Mittelmaß und bleibt unter seinen Möglichkeiten.« Im Europa-Ranking belegt Österreich nur Platz 10. Die Schweiz und die skandinavischen Länder – Volkswirtschaften, die mit Österreich durchaus vergleichbar sind – liegen klar voran.

Foto: iStock

# UMFRAGE

Der Report Verlag hat nachgefragt

# BUSINESS RESILIENCE

*Resiliente Unternehmen haben die Fähigkeit, auf Störungen oder Veränderungen ihres Geschäftsfeldes rasch zu reagieren. Beginnend beim Risikomanagement umfasst Business Resilience alle Prozesse und Organisationsbereiche. Wie bereiten sich österreichische Unternehmen auf mögliche Krisensituationen vor?*

## 1 *Welche Maßnahmen hat Ihr Unternehmen ergriffen, um sich gegen unvorhergesehene Ereignisse und Bedrohungen zu wappnen?*

**ANDREAS THÖNI**
*Leitung Konzernstrategie, Digital & Innovation der Österreichischen Post AG*

Grundsätzlich gilt es, die strategische und taktische Dimension zu unterscheiden, wobei ein zentrales, geprüftes Risikomanagement (auf Basis COSO/ERM) sowie Controlling den übergreifenden Blick sicherstellen. Diese Aktivitäten zielen auf eine nachhaltige Steigerung des Unternehmenswertes ab. Strategisch wird das Risiko von einseitigen Ausfällen durch markt- bzw. geschäftsmodellseitige und geografische Diversifizierung reduziert. Taktisch sind im Unternehmen auf verschiedenen Ebenen Regelkreise mit Planung, Steuerung und Kontrolle auf Basis eines integrierten finanziellen und operativen Berichtswesens etabliert.

**VOLKER LIBOVSKY**
*Chief Technology & Innovation Officer der Magenta Telekom*

Bei Magenta Telekom haben wir auf verschiedenen Ebenen vorgesorgt. Unsere Netze sind durch Redundanzen abgesichert. Wenn es also zum Beispiel in einem Rechenzentrum zu einem Ausfall kommt, können wir sofort auf ein anderes Datencenter umschalten. Für größere unvorhergesehene Ereignisse gibt es einen ständigen Krisenstab, der im Ernstfall schnell zur Stelle ist. Das hat zum Beispiel beim Ausbruch der Coronapandemie sehr gut geklappt. Eine große Hilfe ist auch der Austausch innerhalb unseres Mutterkonzerns Deutsche Telekom, weil wir so Erfahrungen zwischen den verschiedenen Ländergesellschaften austauschen können.

**KURT SVOBODA**
*Chief Financial Officer und Chief Risk Officer der UNIQA Insurance Group AG*

Als Versicherungsunternehmen ist das proaktive Management von unvorhergesehenen Ereignissen und Bedrohungen eine unserer Kernkompetenzen. Dazu haben wir im Haus eine eigene Abteilung geschaffen, die sich mit dem Management dieser Risiken befasst. Dies umfasst sowohl klassische Risiken aus dem Versicherungsgeschäft sowie dem Kapitalmarkt als auch neue Risiken wie zum Beispiel das Cyberrisiko. Neben der Identifikation dieser Risiken befasst sich diese Abteilung auch damit, dass diesen Risiken mit entsprechenden Maßnahmen begegnet wird.

Foto: iStock

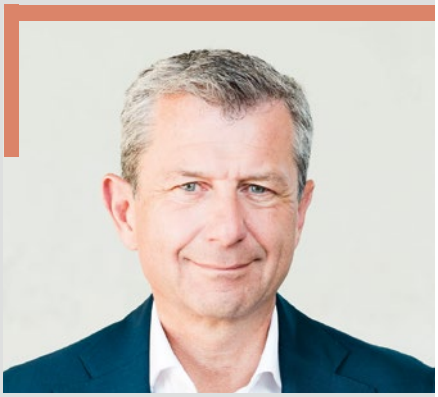
## 2 *Welche Technologien werden zur Unterstützung der Business Resilience verwendet?*

### ANDREAS THÖNI

Es werden unterschiedlichste Technologien in den verschiedenen Geschäftsfeldern zum Erkennen von Bedrohungen (aber auch Chancen) eingesetzt – in einer Bank ist dies z. B. anders als im Paketbereich. Für das Nachvollziehen übergreifender Risiken werden spezifische Software-Systeme genutzt, die in Kombination mit den »klassischen« Accounting- bzw. Controlling-Systemen zu sehen sind. In den operativen Bereichen liegt der Kern in oftmals eigenentwickelten Systemen, die Daten sowohl für den tagtäglichen Betrieb als auch für das Erkennen von Abweichungen liefern. Für die Bereiche Krisen und Cyber-Security sind wiederum spezifische Systeme nennenswert.

### VOLKER LIBOVSKY

Digitalisierung ist da ein guter Oberbegriff. Die Bandbreite reicht hier von Lösungen zur Fernwartung von Systemen bis hin zum Mobile Working. Krisen halten sich eben leider nicht an Dienstpläne – und deshalb ist es so wichtig, digital und vernetzt zu denken. Im besten Fall lassen sich kleine und große Krisen durch digitale Lösungen verhindern, etwa durch Prognosen auf Basis gesammelter Daten.



### KURT SVOBODA

Nicht erst seit der Covid-19-Pandemie ist bekannt, dass der sinnvolle Einsatz moderner Technologien einen positiven Beitrag auf die Resilienz einer Organisation haben kann. Die wesentlichsten Fokusthemen diesbezüglich sind bei uns die Umsetzung unserer Cloud-Strategy, die Prozessautomatisierung durch den Einsatz von Robotern sowie angemessene Technologien zur Gewährleistung der IT-Sicherheit durch die neue Arbeitswelt und Homeoffice.

## 3 *Wie werden Mitarbeiter*innen eingebunden, um ein hohes Maß an Widerstandsfähigkeit sicherzustellen?*

### ANDREAS THÖNI

Mitarbeiter*innen sind neben Prozessen die Grundlage eines resilienten Unternehmens. Bereits die Kultur legt die Ausgangsbasis für den Umgang mit laufenden Herausforderungen. Hier sind in der Post die Kulturwerte Freude, Sinn und Leistung auf Basis eines gemeinsamen Wir-Gefühls etabliert, welche die organisatorische Resilienz neben den fachlichen Fähigkeiten unterstützen. Darüber hinaus sind die Mitarbeiter*innen tief in die laufenden Kontrollprozesse eingebunden und tragen aktiv zum Erkennen von Abweichungen bei. Schließlich tragen auch die Reputation als attraktive Arbeitgeberin und die damit verbundene Attraktivität für Talente zur Widerstandsfähigkeit bei.

### VOLKER LIBOVSKY

Das Wichtigste ist die Sicherstellung einer guten internen Kommunikation. Um beim Beispiel Corona zu bleiben: Damals haben wir anfangs wöchentlich in Livestreams über die aktuelle Lage und die Vorgehensweise informiert. Die Kolleginnen und Kollegen konnten live im Chat Fragen stellen. So haben wir es geschafft, die Strategie für die Krise über Livestreams, verstärkte Team-Meetings und Kommunikation über das Intranet zu vermitteln. Gute und offene Kommunikation – das ist das A und O.

### KURT SVOBODA

Die Einbindung der Mitarbeiter*innen ist bei uns ein sehr wichtiges Thema. Durch eine Vielzahl von Maßnahmen wollen wir die Awareness unserer Kolleg*innen zu den vorhandenen Bedrohungen – und wie sie darauf angemessen reagieren sollen – sicherstellen. Es gibt bei uns im Haus verpflichtende Trainings, die von allen Mitarbeiter*innen regelmäßig zu absolvieren sind. Die interne Kommunikation erfolgt unter einer eigenen internen Marke namens »UNIQA Protection«. Dafür gibt es auch einen eigenen Bereich, wo alle Informationen zu finden sind und wo neben klassischen Artikeln auch neue Formate wie Podcasts angeboten werden. Auch Angriffssimulationen wie z. B. Phishing E-Mails werden regelmäßig durchgeführt.

Fotos: Magenta Telekom_Marlena König, Natascha Unkart & Isabelle Köhler, Österreichische Post AG

# STARK DURCH D

UNTERNEHMEN MÜSSEN VORAUSSCHAUEND PLANEN, UM FÜR NOTFÄLLE UND KRISEN JEGLICHER ART GERÜSTET ZU SEIN. BUSINESS RESILIENCE UND BUSINESS CONTINUITY SICHERN NICHT NUR DEN FORTBESTAND DER GESCHÄFTSTÄTIGKEIT – DIESE STRATEGIEN BEFÄHIGEN ORGANISATIONEN, AUS SCHWIERIGEN SITUATIONEN GESTÄRKT HERAUSZUGEHEN.

TEXT | ANGELA HEISSENBERGER

Fotos: iStock

# IE KRISE

Corona, Lieferkettenprobleme und schließlich der russische Angriffskrieg gegen die Ukraine haben viele Unternehmen auf eine harte Probe gestellt und hinterlassen bis heute Spuren in der globalen Wirtschaft. Doch warum kommt ein Unternehmen besser durch schwierige Zeiten und wächst geradezu über sich hinaus, während andere an den Herausforderungen scheitern? Wirtschaftsexpert*innen sind sich einig: Die Resilienz ist entscheidend. In unsicheren Zeiten müssen sich Unternehmen widerstandsfähig gegen Krisen und Angriffe machen.

Die Unternehmensberatung McKinsey analysierte die Fähigkeit von Unternehmen, trotz zyklischer Veränderungen von Angebot und Nachfrage weiterhin Gewinn zu erwirtschaften. Rund 1.500 Unternehmen wurden für die Studie nach dem »Z-Score«, der die Wahrscheinlichkeit eines Firmenkonkurses misst, bewertet. Dabei zeigte sich: Wer eine Krise gut übersteht, wächst später stärker. Die besten 20 Prozent der untersuchten Betriebe konnten ihren Gewinn um fünf Prozent steigern, während die anderen Unternehmen 19 Prozent verloren. Resili-

RESILIENTE UNTERNEHMEN GELANGEN RASCH WIEDER AUF DEN WACHSTUMSPFAD.

ente Firmen gehen gestärkt aus wirtschaftlichen Extremsituationen hervor, weil sie in der Lage sind, Schocks nicht nur zu absorbieren, sondern sogar zum Aufbau von Wettbewerbsvorteilen zu nutzen. »Resiliente Unternehmen sind gut in der Verteidigung und gehen zugleich in die Offensive«, meint Thomas Poppensieker, Senior Partner bei McKinsey. »Schutz ist ein Muss, Wachstum aber auch. Die Gewinner von morgen bilden sich bereits heraus.«

Fünf Merkmale zeichnen resiliente Unternehmen aus: Sie treffen frühzeitig Entscheidungen. Sie bewegen sich rascher und gelangen bald wieder auf den Wachstumspfad. Sie schränken ihre Investitionen nicht ein und reinvestieren. Sie sind digitale Vorreiter, die frühzeitig auf innovative Technologien setzen. Sie verwirklichen einen stakeholder-orientierten Blick auf die Wirtschaft.

## SCHWACHSTELLEN ERKENNEN

Die »Kronjuwelen« eines Unternehmens sind die zentralen Prozesse, die Gebäude, die IT-Infrastruktur sowie die wichtigsten Mitarbeiter*innen und Lieferant*innen. Fällt eines dieser Elemente aus, drohen der gesamten Organisation Schäden und Verluste. Störun-

Fotos: iStock

FACTS

## Fünf Merkmale eines resilienten Unternehmens

Quelle: WU Executive Academy

### 1 LIQUIDITÄT

Resiliente Unternehmen haben Kapitalreserven, die es ihnen ermöglichen, eine längere wirtschaftliche Durststrecke, etwa durch unerwarteten Umsatzrückgang, zu überbrücken. Für den Aufbau von Kapitalreserven gibt es drei Hebel: Überschüsse nicht ausschütten, Eigenkapital erhöhen, Schulden strukturell reduzieren. Alle cash-relevanten Prozesse sind optimiert und nach Fristen getaktet. Zusätzlich überprüfen resiliente Unternehmen ihren Investitionsplan laufend auf Investitionen, die maximalen Return liefern, und vermeiden weniger relevante Investitionen.

### 2 GESCHÄFTSMODELL

Um neue Kund*innensegmente und -gewohnheiten frühzeitig zu entdecken und zu besetzen, wird der Fokus auf Innovationen, Service, Vertrieb, Digitalisierung und Mitarbeiter*innen gerichtet. Das digitale Unternehmen umfasst eine zentrale Serviceplattform für Kund*innen und Lieferant*innen, digitale Skills der Mitarbeiter*innen und einen gestärkten digitalen Vertrieb.

gen des Geschäftsbetriebs, hervorgerufen durch schwerwiegende Zwischenfälle oder Ausfälle, ziehen meist finanzielle Einbußen und einen Reputationsverlust nach sich. Dieses Risiko ist existenzbedrohend und nicht versicherbar.

»Unternehmen stehen in der Krise unter Zeitdruck. Es müssen viele Entscheidungen in kurzer Zeit und bei unvollständiger Informationslage getroffen werden«, sagt Georg Beham, Leiter des Bereichs Cybersecurity & Privacy bei PwC.

Für das Fortführen der Geschäftstätigkeit ist es daher essentiell, die Kernleistungen unabhängig von äußeren Einflüssen in mög-

## DIGITAL COMPLIANCE

Compliance-Maßnahmen stellen sicher, dass ein Unternehmen ethische und rechtliche Verpflichtungen einhält. Ein Compliance Management System (CMS) umfasst Prozesse zur Überwachung, Überprüfung und Überarbeitung dieser Regeln sowie zur Meldung und Behandlung von Verstößen. Compliance stärkt die Resilienz eines Unternehmens und sollte in Zusammenhang mit dem Business Continuity Management stehen.

Ein softwaregestütztes CMS kann den Aufbau und die Wartung erheblich erleichtern. Es ist jedoch nur dann effektiv, wenn es den spezifischen Anforderungen des Unternehmens entsprechend konfiguriert und regelmäßig überprüft und angepasst wird.

**Vorteile eines digitalen CMS:**

- Zentralisierung und Standardisierung von Compliance-Prozessen und Compliance-Informationen
- Automatisierte Überwachung und Überprüfung von Geschäftspraktiken
- Bessere Überwachung und Überprüfung von Compliance-Risiken
- Effizientere Überwachung und Überprüfung von Compliance-Verstößen
- Verfügbarkeit von aktualisierten rechtlichen und regulatorischen Anforderungen in Echtzeit
- Automatisierte Überwachung und Überprüfung von Compliance-Schulungen
- Unterstützung bei der Überwachung und Überprüfung der Wirksamkeit des CMS

3

### FLEXIBILITÄT

Unternehmen müssen rasch auf Kund*innenbedürfnisse reagieren und gleichzeitig versuchen, möglichst unabhängig von globalen Märkten zu agieren. Ein schlankes Headquarter und klare Führungsverantwortung sorgen für innerbetriebliche Synergien und dienen als Katalysator für funktionsübergreifende Plattforminnovationen. Dezentrale, in wesentlichen Zielmärkten autonom agierende Supply Chains sichern die Versorgung auch bei geschlossenen Grenzen. Eine Auslegung der Kapazitäten auf maximale kontinuierliche Auslastung statt auf Spitzenabdeckung wird durch modularen Aufbau der Fixkostenmodule, die je nach Bedarf zugeschaltet werden, ermöglicht. Weitere Elemente: Shared Services, zentralisierte Datenhoheit in Echtzeit und agile Organisationsstrukturen

4

### PURPOSE

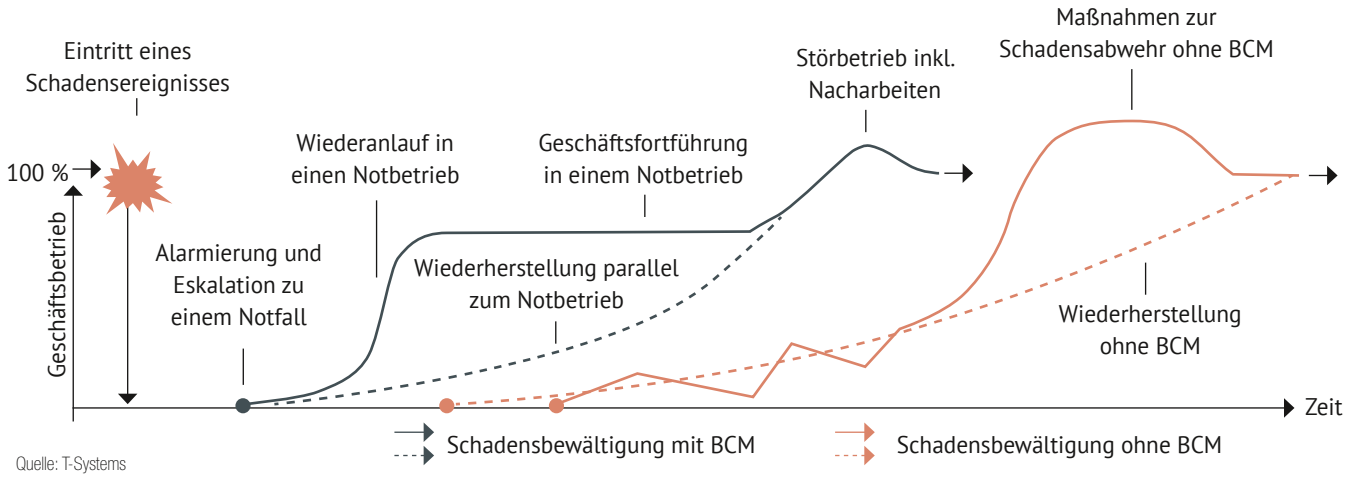
Unternehmen müssen glaubwürdig agieren, um jüngere Generationen anzusprechen und sich erfolgreich als »Employer of Choice« zu positionieren. Das gelingt nur, wenn der Unternehmenssinn definiert und tatsächlich gelebt wird und die Themen Diversität, Nachhaltigkeit und Umweltschutz im Unternehmen zentral verankert sind.

5

### LEADERSHIP

Führungskräfte in resilienten Unternehmen zeichnen sich durch Authentizität, Empathie, Transparenz und klare, unmittelbare Kommunikation aus. Weitsicht und die Fähigkeit, exponentiell zu denken, wird angesichts der zunehmenden Komplexität im Business immer wichtiger. Schnelle Entscheidungen werden durch dezentrales Empowerment der Mitarbeiter*innen und ein hohes Maß an Interaktivität ermöglicht.

# SCHADENSBEWÄLTIGUNG MIT BUSINESS CONTINUITY MANAGEMENT




Quelle: T-Systems

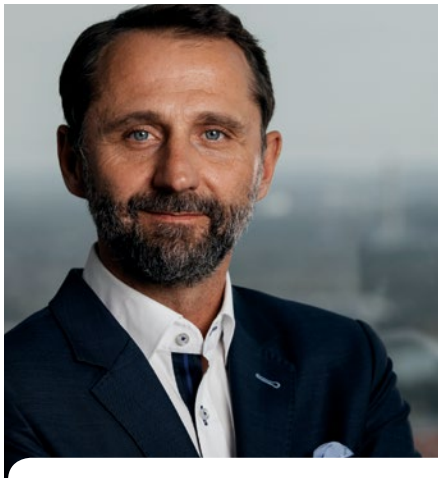
*In Unternehmen mit Business Continuity Management (BCM) erfolgt die Reaktion auf Notfall- oder Krisensituationen früher und der Normalbetrieb ist rascher wiederhergestellt.*

lichst jeder Situation aufrechterhalten zu können. Laut einer Umfrage der Beratungsgesellschaft PwC verfügen aber nur rund 45 Prozent der befragten Unternehmen über Business-Continuity-Pläne zur Absicherung besonders kritischer Geschäftsprozesse. Darunter fallen die Einrichtung eines Krisenstabs, die Festlegung eines Eskalationsmechanismus sowie vorbereitete Unterlagen und Handlungsanweisungen. Nur 16 Prozent der Unternehmen, die entsprechende Vorkehrungen getroffen haben, führen aber auch regelmäßige Notfallübungen durch.

»Unternehmen müssen in der Lage sein, unerwartete Umstände zu verkraften und schnell, oft mit unklaren Annahmen, Entscheidungen zu treffen und sich anzupassen und manchmal neu auszurichten«, umreißt Vladimir Preveden, strategischer Berater von Unternehmen in Zentral- und Osteuropa, die Herausforderungen.

Unternehmen haben sich in der Vergangenheit vorwiegend auf resiliente Führungskräfte fokussiert – das reicht in multiplen Krisen nicht aus, um mögliche Schwachstellen vorzeitig zu erkennen, wie Christof Stögerer, Leiter des Bereichs Continuing Education an der WU Executive Academy, meint: »Das gesamte Unternehmen muss auf seine Resilienz hin betrachtet werden – die Organisation, die Struktur, die Produkte, die Partnerschaften und Kooperationen.«

*Frank Roselieb, Institut für Krisenforschung: »Führungskräfte stehen vor besonderen Herausforderungen.«*



*Georg Beham, PwC: »Unternehmen stehen in der Krise unter Zeitdruck.«*

## HANDLUNGSFÄHIG BLEIBEN

Schon in ruhigeren Zeiten sollten Unternehmen ein umfassendes Business Continuity Managementsystem (BCM) implementieren. Treten nämlich Disruptionen bereits auf, ist es unter hohem Zeit- und Finanzdruck kaum möglich, Reibungsverluste zu vermeiden. Je besser eine Organisation, ihre Prozesse und ihre IT vorbereitet sind, desto erfolgreicher wird sie durch die Krise kommen.

Der durch Corona erfolgte Digitalisierungsschub, der sich häufig auf Homeoffice-Lösungen und Videokonferenzen beschränkte, hat damit nur wenig zu tun. In der Post-Pandemie-Welt spielt New Work zwar eine bleibende Rolle, echte Resilienz-Strategien gehen jedoch weit darüber hinaus. Unternehmen müssen bei drei Bereichen ansetzen, um widerstandsfähiger zu werden: Kundenerlebnis, Prozesse und Technologie. Eine digitale Kundenschnittstelle verbindet Vertrieb und Service, die Zentralisierung der Daten und optimierte Prozesse steigern die Effizienz, Kollaborationsplattformen fördern die funktionsübergreifende Zusammenarbeit der Mitarbeiter*innen.

»Business Resilience kann man als Ausfallsicherheitsstrategie des gesamten Unternehmens verstehen«, sagt Andrea Trapp, Director of Business EMEA bei Dropbox. Die Business-Continuity-Strategie sollte

Fotos: Institut für Krisenforschung

BUCHTIPP


## In Krisen richtig handeln

Störungen des Regelbetriebs von Unternehmen oder Katastrophen, von denen ganze Volkswirtschaften betroffen sind, können viele Ursachen haben. Business Continuity Management zielt darauf ab, solche Beeinträchigungen nach Möglichkeit zu vermeiden, frühzeitig zu erkennen, systematisch zu bewältigen und adäquat nachzubereiten. 15 renommierte Fachleute erklären anhand von Fallbeispielen aus unterschiedlichsten Branchen wie Notfall- und Krisenmanagementsysteme funktionieren und welche internationalen Standards bei der Umsetzung helfen. Die Autor*innen gewähren dabei Einblick in Krisenmanagementsysteme namhafter Unternehmen und Organisationen und nehmen auch zwei Bereiche unter die Lupe, denen oft weniger Bedeutung zugemessen wird: Krisenkommunikation und Krisentraining.

***Frank Roselieb (Hg.): Business Continuity Management in der Praxis.***
***Erich Schmidt Verlag 2022***
***ISBN: 978-3-503-20960-6***

Fotos: Deutsche Bank

# ECHTE RESILIENZSTRATEGIEN GEHEN WEIT ÜBER DIGITALE NOTKONZEPTE DER CORONA-ZEIT HINAUS.

sich »nicht ausschließlich auf Werterhaltung, sondern stets auf Wertschöpfung konzentrieren«: »Um das zu gewährleisten, brauchen wir agile Technologien, basierend auf mobilen Lösungen.«

### GUTE KRISENKOMMUNIKATION

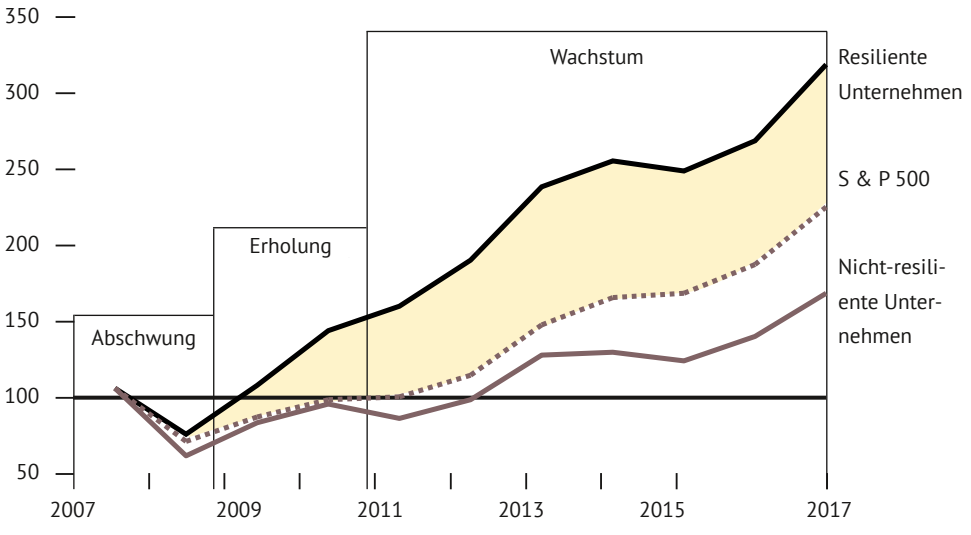
Das beste BCM-System nützt jedoch nichts, wenn es nicht von Führungskräften und Mitarbeiter*innen getragen wird. Die Bereitschaft zur Umsetzung muss da sein – nicht weil es vorgeschrieben ist, sondern weil alle davon überzeugt sind. Idealerweise lässt sich das Risikomanagement in das Qualitätsmanagement integrieren.

So sollte neben der Aufrechterhaltung der technischen und finanziellen Handlungsfähigkeit nicht auf die wichtige Funktion einer geordneten Krisenkommunikation vergessen werden. »Bei multiplen Krisen stehen die Führungskräfte vor einer dreifachen Herausforderung: Sie müssen die Mitarbeiter*innen immer wieder neu für ihre Tätigkeit motivieren, der zunehmenden Krisenmüdigkeit der Menschen begegnen sowie während des Krisenmarathons das Vertrauen in betriebliche und politische Entscheidungen aufrechterhalten«, verweist Frank Roselieb, geschäftsführender Direktor des Kieler Instituts für Krisenforschung, auf zwei weitere wichtige Aspekte: »Zu den Grundregeln guter Krisenkommunikation zählen neben der Schnelligkeit auch die Wahrheit und Offenheit.« ■

*Thomas Poppensieker, McKinsey: »Resiliente Unternehmen gehen in die Offensive.«*

## RESILIENTE UNTERNEHMEN KOMMEN BESSER DURCH DIE KRISE

Gesamtrendite der Shareholder, n = 1.140 Unternehmen (2007 = 100)




Quelle: Trendbook Business Resilience

*Unternehmen, die eine Krise gut überstehen, wachsen danach stärker und sind wirtschaftlich erfolgreicher.*

# »Es sind alle gut beraten, sich damit rechtzeitig zu beschäftigen«

TEXT | MARTIN SZELGRAD

IM REPORT-TALK ZUM GROSSEN THEMENKREIS BUSINESS RESILIENZ: THOMAS MASICEK, LEITER DES BEREICHS CYBERSECURITY BEI T-SYSTEMS INTERNATIONAL, UND MANAGING DIRECTOR VON T-SYSTEMS ÖSTERREICH PETER LENZ, DER AUCH DEN NACHHALTIGEN UMGANG MIT RESSOURCEN UND INFRA-STRUKTUREN VERANTWORTET.

Was bedeutet Business Resilienz und aus welchen Gründen sollten sich Unternehmen damit beschäftigen?

**Peter Lenz:** Business Resilienz ist die Fähigkeit von Unternehmern, sich auf – zum Teil rasch – ändernde Umgebungen einzustellen. Das können Krisen sein, wie wir sie in den letzten Jahren erlebt haben: Corona, Störungen in den Lieferketten oder ein Angriffskrieg auf die Ukraine, der auch Teuerungen bei Energie und Kraftstoffen gebracht hat. Business Resilienz steht für Krisenfestigkeit, für das »Krisenfestmachen« eines Unternehmens oder einer Organisation, um auf Veränderungen im Geschäftsfeld entsprechend reagieren zu können.

Welche Bereiche umfassen Maßnahmen dazu?

**Lenz:** Das beginnt beim Risikomanagement, es umfasst die Flexibilität von Organisationen, aber auch eine gewisse Kontinuitätsplanung, und geht bis in die Innovationsfähigkeit und letztlich auch um Resilienz bei den Mitarbeiter*innen. Denn deren Fähigkeiten und auch ihre Verfügbarkeit spielen bei der Standhaftigkeit eines Unternehmens eine große Rolle. Business Resilienz umfasst alle Geschäftsprozesse eines Unternehmens. Das kann je nach Branche in dem einen oder anderen Bereich stärker gewichtet sein – zum Beispiel in der Papierindustrie, die stark von den Preisen des Rohstoffs Gas abhängig ist. Andere Themen betreffen Unternehmen über alle Sektoren auf ähnliche Weise, wie etwa Lockdown-Maßnahmen in einer Pandemie.

In welcher Weise hat sich das Thema Cybersicherheit in den vergangenen Jahren verändert? Auf welchen Bereich fokussieren Sie bei T-Systems?

**Thomas Masicek:** Ich verantworte im Konzern international den Bereich Cybersecurity – und damit unsere Plattformen, die gängigen Normen und Standards entsprechen müssen, ebenso wie unsere schlagkräftigen Cybersecurity-Lösungen für die Kunden. Diese Lösungen sind entweder in die Cloud und in alle unsere digi-

Fotos: Sigrid Moser-Sailer

*Peter Lenz (li.), Managing Director T-Systems Austria, und Thomas Masicek, SVP Cyber Security T-Systems International*

talen Lösungen integriert, sie werden aber auch als Service angeboten.

Für die Business Resilienz hat Cybersicherheit insbesondere durch die Ukraine-Krise mit allen ihren Folgen an Bedeutung gewonnen. Man hat gesehen, dass in der ersten Phase des Ukraine-Krieges auch ein digitaler Krieg geführt wurde. Es wurden gezielt kritische Infrastrukturen angegriffen. Man hat versucht, Zahlungssysteme zu beeinflussen und hat die Bereiche Bildung und Energieversorgung attackiert – zuerst virtuell und in der zweiten Phase auch physisch. IT ist maßgeblich von Stromversorgung abhängig. Hat ein Rechenzentrum keine Stromversorgung, sind Services des Alltags und des Wirtschaftslebens nicht verfügbar. Diese Themen hängen stark zusammen und somit bedeutet Business Resilienz auch resilient gegen jegliche Art von Cyberbedrohungen zu sein. Diese können uns tagtäglich widerfahren, auch wenn es den Angreifern »nur« darum geht, mit Ransomware Geld zu verdienen.

Wie gut sind die Unternehmen in Österreich in der Praxis hinsichtlich ihre Resilienz aufgestellt? Was ist hier Ihre Erfahrung?

**Lenz:** Wie immer variiert es hier: Manche sind sehr gut aufgestellt und haben ein durch sämtliche Geschäftsbereiche durchgängiges Prozessverständnis und Know-how. Andere gehen es ein wenig hemdsärmeliger an.

Ist dies auch eine Frage der Unternehmensgröße?

**Lenz:** Nicht unbedingt, wobei natürlich große Unternehmen aufgrund ihrer Unternehmensstruktur, ihrer Eigentümer oder aufgrund gesetzlicher Vorgaben anders aufgestellt sind. Da werden schon vom Aufsichtsrat ganz andere Fragen gestellt. Letztlich hängt es auch von der »Exposure« und Betroffenheit ab, welchem Risiko man über die letzten Jahre ausgesetzt war. Ausschlaggebend ist auf jeden Fall, ob in einem Unternehmen und in einer Organisation bereits eine Awareness dazu geweckt worden ist – und man damit weiß, an welchen Hebeln noch zu drehen ist.

**Masicek:** Wenn ein Cybersicherheitsvorfall zu einer Bedrohung des Fortbestands eines Unternehmens ausartet – das kann bis zur Insolvenz gehen –, sind die Awareness und auch Mittel für Maßnahmen schnell da. Durch Ransomware-Attacken auf die Industrie ist das Thema Verfügbarkeit von Unternehmensprozessen in den Führungsebenen angekommen. Jeder kennt inzwischen ein Unternehmen, das bereits einmal betroffen war und auch die Schadensausmaße sind bekannt. Doch ist die Verfügbarkeit von Unternehmensprozessen nicht nur von der IT, sondern auch von Energie und von Rohstoffen abhängig. Eine Veränderung eines Marktes und auch die Verteuerung von Betriebsmitteln kann ebenso den Fortbestand eines Unternehmens gefährden.

Von energieerzeugenden Unternehmen und ihren kritischen Infrastrukturen ist de facto das öffentliche Leben abhängig. Genauso gilt dies für Krankenhäuser, die wir zu unseren Kunden zählen. Eine Ausfallsicherheit in der IT hat hier mehrere Aspekte. Man muss den digitalen Bedrohungsaspekt ebenso betrachten wie alle Abhängigkeiten von Rohstoffen, Vordienstleistern – eben alles, was ich benötige, um meine IT tatsächlich am Leben zu erhalten.

Im Bereich der Cybersicherheit sind die Großen generell merklich besser vorbereitet. Bei kleineren Betrieben hängt es meist davon ab, ob dieses Thema jemand im Unternehmen antreibt. Es gibt hier viele Bestrebungen und auch Hilfestellungen, etwa von der Wirtschaftskammer oder der Interessenvertretung Internetoffensive Österreich. Am Ende des Tages sollten Entscheider*innen mit dem nötigen Wissen in der Lage sein, eine Risikobewertung treffen zu können. Idealerweise haben Unternehmen ab einer gewissen Größe auch einen Sicherheitsbeauftragten – so wie es bereits Datenschutzbeauftragte gibt. Sie oder er treibt dann Sicherheits- und Resilienz-Maßnahmen im Interesse des Unternehmens voran und verantwortet diese. Dann ist auch gewährleistet, dass tatsächlich etwas unternommen wird.

Können Resilienz und Sicherheit an einen IT-Dienstleister ausgelagert werden?

**Masicek:** Die Tätigkeit kann ausgelagert werden, die Verantwortlichkeit dazu nicht. Es gibt aus meiner Sicht ein großes Problem: Viele glauben, dass das Thema mit einem Stück Technik oder einem Stück Software, das man kauft, erledigt wird. Das reicht aber bei weitem nicht. De facto brauche ich immer ein Gesamtkonzept, wie in einem Haus. Wenn ich die Eingangstür mit fünf Schlössern absichere, aber auf der Rückseite bleibt eine Tür offen oder die Fenster können einfach geöffnet werden, dann funktioniert es nicht. Wenn es viele Möglichkeiten der Verwundbarkeit gibt, ist das Gesamtsystem nicht effizient. Zudem geht das Thema Resilienz über Informationstechnologie hinaus. So haben Krankenhäuser im Rahmen der Blackout-Vorsorge Notfall-Prozeduren in einer analogen Form etabliert – mit Laufzetteln, wie es sie früher gab, um im Fall eines Ausfalls der IT den Krankenhausbetrieb aufrechterhalten zu können.

Wo helfen Nachhaltigkeitsthemen, resilienter bei Veränderungen und Krisen aufgestellt zu sein?

**Lenz:** Nehmen wir ein österreichisches Paradeunternehmen wie die OMV. Sie vollzieht mit ihrer »Strategie 2030« einen Wandel vom traditionellen Energieunternehmen zu einem nachhaltigen Akteur in einer Kreislaufwirtschaft. Die Umstellung auf $CO_2$-armes Geschäft bis hin zum völligen Stopp der Produktion von Öl und Gas für die energetische Nutzung bis 2050 ist für mich ein hervorragendes Beispiel für Veränderung, um auch in einer künftig klimaneutralen Wirtschaft gut aufgestellt zu sein. Das betrifft auch die Tochter Borealis, bei der man intensiv an den Möglichkeiten des

*Thomas Masicek: »Jeder kennt ein Unternehmen, das von einer Cyberattacke betroffen war – auch die Schadensausmaße sind bekannt.«*

Recyclings von Kunststoffen bis hin zu geschlossenen Stoffkreisläufen arbeitet.

Nachhaltigkeit im Sinne für den Fortbestand eines Unternehmens erfordert auch eine Diversifizierungsstrategie. So sponsert Red Bull mittlerweile nicht nur traditionelle Sportarten, sondern auch E-Sports, um neue Kundenschichten anzusprechen. Bei meinen eigenen Kindern sehe ich, dass auch solche Events Interesse schüren – in diesem Ausmaß gab es das vor einigen Jahren noch nicht. Die Firma Engel wiederum hat in der Pandemie ihr Produktportfolio umgestellt. Man hat schnell reagiert und mit seinen Spritzguss-Maschinen Kunststoffmasken produziert. Auch Banken und Versicherungen mussten ihr Geschäft entsprechend gesetzlicher Vorgaben neu ausrichten. Auf die produzierende und energieintensive Industrie in der EU kommt künftig eine neue Bewertung von Produkten und eben auch ganzer Unternehmen aufgrund ihres $CO_2$-Fußabdrucks zu. Nachhaltigkeit ist für eine Organisation die Antwort auf die Frage, wo man in zwanzig, dreißig Jahren stehen wird und wofür man eigentlich stehen will.

Welche Vorgaben und Regelwerke kommen hier generell auf Unternehmen zu?

**Lenz:** Die ISO 22301 regelt das Business Continuity Management, die KRITIS-Verantwortung zielt auf die Betreiber kritischer Infrastrukturen, der »Sustainable Finance Disclosure Regulation Act« der EU forciert die angesprochenen ESG-Themen (Anm. Environmental, Social, Governance) in Unternehmen...

**Masicek:** ... im Cybersicherheitsbereich wird mit der neuen NIS-2-Regelung die Cybersicherheitsrichtlinie der EU ab Oktober 2024 auf eine weitaus größere Zahl an Unternehmen ausgedehnt. Das ist eine Riesenherausforderung, denn bisher waren relativ wenige Unternehmen gesetzlich zu Sicherheitsmaßnahmen und Meldungen bei Sicherheitsvorfällen verpflichtet. Der Gesetzgeber ist hier auch noch in einer Findungsphase, etwa zur Frage, wie diese Menge an Unternehmen überhaupt geprüft werden kann. Auch sind von NIS 2 betroffene Unternehmen nicht mehr so klar von den Behörden definiert. Sie müssen selbstständig anhand eines Kriterienkatalogs bewerten, ob sie unter die Richtlinie fallen. Der Gesetzgeber muss erst lernen, mit diesen Anforderungen an kleinere Unternehmen umzugehen. Umso schwerer ist es für die Unternehmen selbst, zu wissen, wie ich es konkret für mich umsetzen kann: Ohne entsprechende Hilfe sind diese Unternehmen in der Regel eher verloren.

*Peter Lenz: »Nachhaltigkeit ist die Antwort auf die Frage, wofür ein Unternehmen stehen will.«*

Was bedeutet NIS 2 beispielsweise für ein Unternehmen, das nun erstmals betroffen ist?

**Masicek:** Es gibt einen konkreten Anforderungskatalog, der von organisatorischen bis zu technischen Maßnahmen reicht. Doch Geschäftsführer*innen müssen sich auch vergewissern, dass die nötigen Maßnahmen umgesetzt sind. Dafür braucht es ein Managementsystem, mit dem die Wirksamkeit des Gesamtsystems bewertet wird und daraus Risiken und Maßnahmen abgeleitet werden. Im Mittelstand bedeutet das Prozesse oder Verfahren, die noch nicht in dieser Art und Weise vorhanden sind. Großunternehmen haben eigene Abteilungen, die sich mit den Themen Sicherheit, Risikomanagement und Notfallvorsorge auseinandersetzen. Hier ist sicherlich noch der Gesetzgeber gefordert, mit einer Art Branchenstandards – wie es sie in Ländern wie Deutschland bereits gibt – eine Anleitung zu bieten. Damit muss das Rad für diese kleineren Unternehmen nicht jedes Mal neu erfunden werden.

Hat T-Systems in Österreich ebenfalls Unternehmenskunden, die unter NIS 2 fallen?

**Masicek:** Wir sind eine laut NIS-Verordnung qualifizierte Stelle, die Unternehmen prüfen kann und auch Beratung zur »NIS Readiness« bietet, damit diese entsprechenden Prüfungen absolvieren können. Wir sind diesbezüglich täglich mit Unternehmen in Kontakt.

**Lenz:** Mit Regelwerken wie NIS und der politischen Fokussierung auf Nachhaltigkeitsthemen ist ein völlig neuer Markt entstanden: Auch die großen Beratungshäuser setzen darauf, aber auch Softwareanbieter. So gibt es mittlerweile über 100 Softwareprodukte, die sich mit Portfolio-Screening und der EU-Taxonomie auseinandersetzen. Das beginnt bei intelligenten Excel-Sheets als Basis und geht bis zu ausgeklügelten Programmen, die laufend bei gesetzlichen Änderungen adaptiert werden. Denn es sind tatsächlich lebende Regelwerke, die etabliert werden müssen – und es sind alle gut beraten, sich damit rechtzeitig zu beschäftigen. Man ist dann nicht überrascht, wenn zum Tag X der entsprechende Ausweis eingefordert wird.

Hat sich der Trend zur Digitalisierung zu einer Chance oder mit all den Cybersicherheitsgefahren vor allem zu einem Risiko entwickelt?

**Lenz:** Für mein Dafürhalten stehen klar die Chancen im Vordergrund. Selbst ein kleiner Tischlereibetrieb kommt an einer CNC-Bearbeitung, die auf IT setzt, nicht mehr vorbei. Ich sehe die Digitalisierung auf jeden Fall ab dem österreichischen Mittelstand verpflichtend – sei es für die Kundenbindung, bei der Ansprache der Mitarbeiter*innen und natürlich für effiziente Prozesse. Lässt sich ein Geschäft heute noch rein mit manuellen Abläufen beherrschen?

Fotos: Sigrid Moser-Sailer

*Thomas Masicek: »Mit NIS 2 und der Taxonomie-Verordnung kommen erhebliche Anforderungen auf Unternehmen zu.«*

Man darf auch nicht vergessen, dass Mitarbeitende auf dem knappen Arbeitsmarkt in Österreich spannende und wertstiftende Tätigkeiten suchen. Hat man immer die gleichen Arbeiten, ohne technische Unterstützung, sucht man sich vielleicht höherwertige Aufgabenbereiche in einem anderen Unternehmen. Allein aus diesem Aspekt – der Entlastung von Routinetätigkeiten – ist die Digitalisierung dringend erforderlich.

Die Risiken sind also beherrschbar?

**Masicek:** Wir sehen die Digitalisierung in unserem Bereich der »Incident Response« auch als Risiko – wenn etwa durch die Ausbreitung von Ransomware in einem Firmennetz schlagartig alle Geschäftsprozesse zum Stillstand kommen. Doch sofern man die Hausaufgaben macht, ist dieses Risiko kalkulierbar. Wenn ich aber einfach nur Technik einsetze, ohne mich damit weiter zu beschäftigen, ist das ein massives Risiko fürs Unternehmen. Ich bin dann vielleicht bei der Verschlüsselung meiner geschäftskritischen Systeme durch Schadsoftware in der Zwickmühle, ob ich die geforderte Summe bezahle und damit ein kriminelles Geschäftsmodell finanziere – oder ob ich nicht mehr produktionsfähig bin. Wir sehen häufig, dass sich Unternehmen nicht um Backup- und Recovery-Prozeduren kümmern. Ich meine hier auch nicht die reine IT, sondern Notfallmaßnahmen, um auch in Krisen weiter agieren zu können. Wenn es keine Sicherheitskopien gibt, die auch rasch wieder eingespielt werden können, ist ein Unternehmensnetzwerk offen wie ein Scheunentor. Auch die Angreifer werden effizienter, Attacken erfolgen zunehmend zielgerichtet. Cybercrime arbeitet heute in Strukturen, die ähnlich jener herkömmlicher Unternehmen sind – mit Qualitätsmaßnahmen, Mitarbeiterführung und sogar Bonusprogrammen. Das resultiert auch in Zukunft in effizienten Prozessen mit großer Trefferwahrscheinlichkeit.

Wie viel darf oder soll Cybersicherheit kosten?

**Masicek:** Als Erfahrungswert hat sich eine Größe von zehn Prozent des IT-Budgets etabliert, die man für die Absicherung der Infrastruktur inklusive Backup und Recovery ausgeben muss. Gehe ich in Richtung fünf Prozent, dann mache ich schon wieder Abstriche und decke nur einzelne Bereiche ab. Ich habe möglicherweise immer noch ein kalkulierbares Risiko, das ich vertreten kann. Die Voraussetzung ist aber, dass dieses Risiko klar bewertet werden kann.

Was bedeutet die moderne Arbeitswelt mit teilweise entkoppelten Arbeitsorten für die IT-Sicherheit in Unternehmen?

**Masicek:** Die Pandemie hat teilweise gezeigt, wie wenig Unternehmen auf das Thema mobiles Arbeiten vorbereitet waren. Mitunter mussten die Stand-PCs abgebaut und in die Homeoffices transportiert werden. Die Mitarbeiter*innen konnten dann lokal arbeiten, hatten aber keine sicheren Zugänge zum Firmennetz. Mittlerweile haben sich die Unternehmen mit den nötigen Sicherheitslösungen versorgt und ihre Mitarbeitenden geschult. Denn weiterhin ist der Faktor Mensch der Eintrittspunkt Nummer eins: Man kann nicht alles technisch abfangen.

Früher war es einfacher, die Sicherheit einer Infrastruktur hinter der Firewall eines Unternehmensnetzwerkes mit all ihren Parametern zu gewährleisten. Heute ist ein Notebook, ein Tablet oder Smartphone in irgendeinem Netz eingebucht. Ist dann die Sicherheit der Geräte nicht vollinhaltlich abgedeckt, habe ich sofort ein Risiko. Das Thema Remote-Zugang ist bei den Unternehmen weitgehend gelöst. Die Absicherung der Arbeitsplätze ist oft immer noch mangelhaft.

Wie bieten Sie dazu Unternehmen an?

**Masicek:** Wir führen eine Bedrohungsanalyse durch, abhängig von der Branche, vom Unternehmenszweck und den Anforderungen an die Sicherheit. Hier gibt es auch normenspezifische Unterschiede, wie zum Beispiel im Bereich der Automobilbranche oder in der Gesundheitsbranche. Neben den technischen Hausaufgaben als Basis können dann Arbeitsplätze nicht nur mit Antivirussoftware, sondern mit modernen Detection-Response-Lösungen abgesichert werden. Sie können dann auch auf einen Phishing-Angriff, der zunehmend besser getarnt via E-Mail geschickt wird, reagieren und die Menschen dahingehend unterstützen. Weitere Punkte sind die Absicherung der Applikationen, die ich nach außen hin verfügbar mache, sowie eine Transparenz in meiner Infrastruktur. Ich brauche die nötige Sichtbarkeit auf meine Systeme, um ein Problem zu erkennen und gegenzusteuern. Eine Zusammenarbeit beginnt häufig mit einem Beratungsgespräch inklusive Assessments. Wo stehe ich als Unternehmen aktuell? Wo sind meine Baustellen und wo kann ich vielleicht Geld sparen? Denn es geht nicht immer nur darum, mehr zu investieren, sondern manchmal auch weniger, aber trotzdem ein abgestimmtes Sicherheitskonzept zu erarbeiten.

Wie resilient ist T-Systems selbst in Österreich aufgestellt?

**Lenz:** Als Betreiber kritischer Infrastrukturen und IT-Services für unsere Kunden – darunter auch für unsere Konzernschwester Magenta Telekom – müssen wir sehr resilient aufgestellt sein. Das fängt bei Prozeduren im Haus an, die sicherstellen, dass wir unsere Datacenter im Fall eines Blackouts weiterbetreiben können. Unsere Mitarbeitenden wissen in einer Krise auch ohne weitere Verständigung, was zu tun ist und haben hier Notfallpläne auch im persönlichen Bereich – beispielsweise wer im Fall des Falles das Kind von Kindergarten abholt. Mit unserem Cybersecurity-Team von über 100 Mitarbeiter*innen wissen wir natürlich, was in dem Bereich gefordert ist.

Zusätzlich bauen wir auch den $CO_2$-Fußabdruck im gesamten Konzern Schritt für Schritt ab. Das bekommen die Führungskräfte in ihre Zielerreichung geschrieben. Dieses Jahr hat man sich vorgenommen, 50 Prozent der $CO_2$-Emissionen in der Deutschen Telekom zu reduzieren. Das fängt an mit der Verwendung von Green Energy, geht über zum sparsamen Umgang mit Energie, der Vermeidung von Geschäftsreisen und dem Einsatz von E-Mobilität in unserer Fahrzeugflotte.

# #FACT

## 97 %

der Führungskräfte weltweit sind überzeugt, dass Resilienz wichtig ist, doch beinahe die Hälfte der Umfrageteilnehmer*innen findet, dass ihr Unternehmen nicht ausreichend vorbereitet ist, um Disruptionen zu bewältigen. Als besondere Herausforderungen beurteilen sie die Bereiche Datensicherheit (48 %), Produktivität (47 %) und technologische Innovation (46 %).

Quelle: »Resiliency Rules Report«, SAS

## 59 %

der Unternehmen, die 2022 von Ransomware-Verschlüsselungen betroffen waren, haben die Zahlung von Lösegeld verweigert. Als Grund für diesen Trend vermuten Analyst*innen unter anderem Compliance-Regelungen und Vorgaben aus Cyberversicherungen. 2019 wurde noch in 76 % der Fälle Forderungen von Erpressern nachgegeben.

Quelle: Chainalysis, Coveware

## 7 VON 10

Für 72 % der unter 30-Jährigen in Österreich ist die Haltung eines potenziellen Arbeitgebers zum Klima ein wichtiges Kriterium bei der Jobwahl. Für 21 % hat dieser Aspekt sogar oberste Priorität.

Quelle: European Investment Bank (EIB) Climate Survey

# 456,8 MILLIONEN

Dollar wurden 2022 weltweit mit Ransomware erpresst – wobei die Dunkelziffer wesentlich höher ist. Trotzdem bedeutet das einen Rückgang von rund 40 Prozent im Vergleich zu 2021 (765,6 Mio. Dollar). Als Grund dafür vermuten Analyst*innen die gesunkene Bereitschaft der Unternehmen zu Zahlungen an Erpresser*innen.

Quelle: Chainalysis

## 44 %

der Befragten halten digitale Lösungen für ein Mittel zur besseren Krisenbewältigung. Besonders Familien hat die Covid-Pandemie dahingehend geprägt: Haushalte mit zwei Elternteilen und Kindern empfinden digitale Angebote etwa im Gesundheitsbereich als entlastend.

Quelle: Digital Healthcare-Studie von Cisco

## 1/3

der Befragten von größeren Unternehmen in Österreich mit verpflichtender EU-Nachhaltigkeits-Berichterstattung (CSRD) fehlt eine ausreichende Datenbasis aus Geschäftsbereichen wie Produktion, Energiemanagement und Fuhrpark, um transparente Nachhaltigkeitsentscheidungen fällen zu können.

Quelle: Umfrage von TQS Research & Consulting und Tietoevry Austria

# 8 VON 10

Entscheider*innen attestieren der Digitalisierung eine große Rolle in der Erreichung ihrer Nachhaltigkeitsziele. Vier von zehn Unternehmen mit 250 bis 500 Mitarbeiter*innen in Österreich haben jedoch keine*n Hauptverantwortliche*n für die Umsetzung von Nachhaltigkeitsagenden.

Quelle: Umfrage von TQS Research & Consulting und Tietoevry Austria

## 3/4

Knapp drei Viertel (73 %) der befragten Führungskräfte in Industrieunternehmen in Europa berichten über Personalengpässe in den Bereichen Engineering, Forschung und Entwicklung. Die Pensionierungswelle der Babyboomer hat begonnen, zudem wechseln Ingenieur*innen mit zunehmendem Alter häufig in andere Funktionen, wodurch die Personalnot in der Entwicklung noch größer wird.

Quelle: »Global Engineering and R&D Report«, Bain & Company

# Der freundliche Nachbar von gegenüber

TEXT | MARTIN SZELGRAD

*Otmar Lendl ist Senior Information Technology Security Analyst bei der staatlichen Stelle CERT.at, wo es seine Aufgabe ist, die IT-Sicherheit Österreichs zu unterstützen.*

CERT.at wurde in einer Kooperation des Bundeskanzleramts mit der Domain-Registrierungsstelle nic.at gegründet. In welcher Weise arbeiten Sie für die IT-Sicherheit des Landes?

**Otmar Lendl:** Wir beobachten seit unserer Gründung 2008 Entwicklungen im Cybersicherheitsbereich, sammeln Informationen von IT-Security-Unternehmen oder beispielsweise Microsoft und anderen IT-Konzernen, generieren Warnungen daraus und informieren Entscheidungsträger und auch Medien. Dann holen wir unterschiedlichste Informationen zu Sicherheitslücken, Schwachstellen und auch kompromittierter IT-Infrastruktur in Österreich ein – und geben diese Informationen an die betroffenen Betreiber und Unternehmen weiter. Selbst können wir nichts anordnen, dafür gibt es keine rechtliche Grundlage und mit unserem kleinen Team können wir selten bei Sicherheitsvorfällen vor Ort unterstützen – aber wir geben sehr wohl Empfehlungen ab.

CERT.at ist so etwas wie der freundliche Nachbar von gegenüber, der auf das eingeschaltete Licht beim geparkten Auto aufmerksam macht. Wir fungieren primär als Informationsdrehscheibe zum Thema IT-Sicherheit: sowohl innerhalb Österreichs als auch als Schnittstelle zu internationalen Kooperationen. Seit März 2019 übernimmt CERT.at die Rolle des »Nationalen Computer-Notfallteams« laut NIS-Gesetz.

Wie gefährdet sehen Sie Unternehmen und Verwaltung in Österreich? Wie hat es dazu in den letzten Jahren ausgesehen? Können Sie einen Trend erkennen?

**Lendl:** Wir befinden uns seit vielen Jahren in einem Wettrüsten. Es gibt, ähnlich wie im menschlichen Immunsystem, keinen absoluten Zustand der Sicherheit oder der Unsicherheit. Werden Firmen angegriffen? Das ist klar mit einem Ja zu beantworten. Jedes einzelne Unternehmen wird täglich attackiert, gleich dem Abwehrkampf des Körpers gegenüber Viren. Sich etwa einmal in den Finger zu schneiden, ist nicht gleich eine Katastrophe – vorausgesetzt, man hat eine Tetanus-Impfung und versorgt die Wunde. Neben den Dauerbrennern wie rein finanziell motivierten Ransomware- und CEO-Fraud-Attacken und den üblichen Spionageversuchen kam im Vorjahr mit dem Krieg in der Ukraine ein weiterer großer Unsicherheitsfaktor dazu.

Hat sich der Ukraine-Krieg auch auf die Cybersicherheit in Österreich niedergeschlagen? Wenn ja, wie?

**Lendl:** Zunächst war unklar, ob sich die Cyberaktionen beider Seiten auf die Kriegsparteien beschränken, oder ob auch Unterstützer betroffen sein werden. Das hat bei einigen Organisationen zu mehr Investitionen in die IT-Sicherheit geführt, inzwischen ist der Effekt aber vorbei. Glücklicherweise ist bis auf wenige Aktionen von Aktivisten in Österreich nichts passiert.

Welche Lücken sind oft für erfolgreiche Ransomware-Attacken auf Organisationen verantwortlich?

**Lendl:** Die Einbruchsvektoren variieren stark, manchmal kaufen die Ransomware-Gruppen einfach den Zugang zu Firmennetzen von anderen Tätergruppen ein. Aus technischer Hinsicht geht es grob um zwei Problembereiche. Zum einen der Arbeitsplatz eines Mitarbeiters: Hier wird mit einer Mischung aus technischer Raffinesse und kreativem Social Engineering versucht, eingeschleuste Programmfragmente zur Ausführung zu bringen. Zum anderen sind es Server, die Anfragen aus dem Internet verarbeiten. Im Jahr 2022 waren insbesondere die Unternehmens-Collaboration-Plattform Confluence und das Webinterface von Microsoft Exchange betroffen. Es sind komplexe, weitverbreitete Plattformen, die oft von außen erreichbar sind, falls man diese nicht mittels VPNs oder vorgelagerten Schutzmaßnamen absichert. Wichtig sind schnelles Patchen und eine durchgehende Implementation einer Mehr-Faktoren-Authentifikation.

Auch die Industrie hat in den letzten Jahren ihre Betriebsumgebungen für den Zugriff von außen geöffnet. Wie sind dazu die Unternehmen aufgestellt?

**Lendl:** Den Industrieunternehmen ist zu einem guten Teil sehr bewusst, mit welchen Gefahren sie operieren. Eine OMV zum Beispiel weiß seit vielen Jahren, dass sie auf der Liste von Zielen diversester Tätergruppen ganz oben ist – angefangen bei Spionage bis hin zu Ransomware und Sabotage. Entsprechend sind diese Unternehmen dann aber auch bei ihrer IT-Sicherheit aufgestellt. Gerade Wirtschaftsspionage ist ein heißes Thema,

Fotos: iStock, CERT.at

ebenso die Abhängigkeit von IT-Prozessen in der Produktion. Vernetzte, auf einzelne Stückzahlen flexibel produzierende Unternehmen benötigen heute die Anbindung an Workflow-Systeme wie etwa SAP. Ein Hack kann hier sehr schnell zu großem Schaden führen – man sichert entsprechend gut seine Umgebungen ab.

Gilt dies auch für das kleine Zulieferunternehmen?

**Lendl:** Je kleiner, desto spannender wird es. Unsere Wirtschaft ist kleinteiliger als in anderen Staaten und damit haben wir viele KMU, denen gebündeltes IT-Security-Know-how vor Ort und die Ressourcen dazu fehlen. Hier stellt sich generell auch die Frage, wie weit der Staat regulierend eingreifen sollte. Mit den Informationssicherheitsgesetzen NIS1 und ab Oktober nächsten Jahres NIS2 werden Betrieben bestimmter Größen und Branchen Maßnahmen vorgeschrieben. Es wird aber praktisch nicht sinnvoll sein, die Prüfprozesse aus NIS1 auf jedes kleine Unternehmen bei NIS2 auszuweiten. Es ist heute noch nicht ganz klar, wie die Behörden die Kontrolle von Auditberichten auf mehrere tausend Unternehmen skalieren werden. Die gesetzlichen Regelungen haben aber auf jeden Fall bewirkt, dass so mancher in den letzten Jahren von der Geschäftsführung belächelte IT-Sicherheitsverantwortliche nun ernst genommen wird.

*Otmar Lendl, CERT.at: »IT-Sicherheitsverantwortliche in den Unternehmen werden nun ernst genommen.«*

Können sich Unternehmen überhaupt auf Dauer gegen Angriffe mit den vorhandenen Möglichkeiten schützen?

**Lendl:** Ja. Das ist aber nicht gratis – weder in Bezug auf die aufzuwendenden Ressourcen noch in puncto Komfort: einfach und bequem ist nicht immer sicher. Ein sinnvoller Ansatz dreht sich um die Angriffsfläche, die wir nach außen präsentieren: je weniger hier sichtbar oder angreifbar ist, desto besser.

Gefährden Falschinformationen die Sicherheit unserer Unternehmen und Gesellschaft?

**Lendl:** Die Frage ist sehr wichtig. Russland betreibt aktive »Information Operations« gegen die Unterstützer der Ukraine. Das ist aber außerhalb unseres Zuständigkeitsbereiches.

# KOMMENTAR

Was Meinung ist und wer Position bezieht

*Jedes Unternehmen wird seinen eigenen Weg suchen und gehen müssen.*

Gertrud Götze / Vice Preisdent HR / T-Systems Austria

# Die Mitarbeitenden sagen an

*Der Arbeitskräftemangel ist großteils hausgemacht. Unternehmen müssen endlich in den »Driver-Seat«, Verantwortung übernehmen und handeln. T-Systems testet die Viertagewoche – die ersten Ergebnisse sind überzeugend.*

Laut Statistik Austria waren in Österreich letztes Jahr durchschnittlich 206.500 Stellen unbesetzt. Allein in der IT-Branche fehlen rund 24.000 Arbeitskräfte. Der direkte und indirekte Wertschöpfungsverlust pro unbesetzter Stelle beläuft sich auf 175.000 Euro pro Jahr, insgesamt also 4,2 Milliarden Euro. Meine provokante Hypothese: Das Problem ist von uns allen selbst verursacht. Profitdenken, kontinuierliches Wachstumsdenken um jeden Preis, Ausblenden von offensichtlichen Entwicklungen und Handeln für den kurzfristigen Erfolg haben uns das eingebrockt. Und als wäre das nicht schon eine harte Nuss für sich, die es zu knacken gilt, sind wir zudem weiteren multidimensionalen Bedrohungen ausgesetzt, die unser aller Wertegefüge neu sortieren.

Egal welche Altersgruppe betrachtet wird: Die Pandemie, der Ukraine-Konflikt, die Klimakrise, die Flucht oder Vertreibung unzähliger Menschen verändern uns. Auf die arbeitende Gesellschaft gespiegelt, zeigt sich das in unserer Arbeitsmotivation und bei unseren Arbeitsmotiven. Wir müssen alle für unseren Lebensunterhalt arbeiten – an dieser Tatsache hat sich nichts geändert. Geändert hat sich aber der Ort und die Menge an Zeit, die wir bereit sind, für unser tägliches Auskommen zu investieren. Wurde man früher für Siebzig- oder Achtzigstundenwochen im Büro bewundert, so wird man heute eher für den offensichtlichen Knochenjob bemitleidet.

Man kann es drehen und wenden, wie man will: Die Mitarbeitenden von heute sagen an, wo und wie viel sie arbeiten wollen. Geändert hat sich darüber hinaus, dass die arbeitende Generation für die Zeit, die sie in Unternehmen investieren, Sinnstiftung, ein gutes soziales Klima und Selbstbestimmung fordern, außerdem dabei die Möglichkeit haben möchten, selbst zu lernen und zu wachsen. Unternehmen, die sich weiterhin vor dieser Entwicklung verschließen und den Kopf in den Sand stecken – oder schlimmer noch: darauf warten, dass Regierungen oder undefinierte »andere« ihr Problem lösen –, werden nicht überleben. Jedes Unternehmen, das noch einen (Über-)Lebensgeist in sich spürt, muss wieder in den Driver-Seat, die Verantwortung übernehmen und handeln. Und es muss dabei flexibel sein, denn gäbe es eine klare Lösungsstrategie aus der aktuellen Lage, die für alle passt, hätte man sie vermutlich schon gefunden und weitflächig umgesetzt. Nein, jedes Unternehmen wird seinen eigenen Weg suchen und gehen müssen.

## DEUTLICHE STEIGERUNG

Wir bei T-Systems haben uns durch unzählige Studien und Austrittsinterviews ehemaliger Kolleg*innen gelesen, um daraus zu lernen, was unsere Mitarbeitenden hält bzw. neue anzieht. Flexibilität und Zeit haben wir als größten Hebel hinsichtlich Nachhaltigkeit und Resilienz unserer Belegschaft gefunden. Deshalb starteten wir Anfang Jänner 2023 ein Pilotprojekt mit der Viertagewoche: 36 Stunden an vier Tagen arbeiten, bei gleichem Gehalt, aber auch gleichem Leistungsergebnis. Wir konnten zehn Prozent unserer Mitarbeitenden dafür gewinnen, das neue Modell mit kontinuierlicher Begleitung durch unser Controlling, dem Betriebsrat, unserer HR-Abteilung und unter strenger Beobachtung unserer Konzernmutter zu testen.

Die ersten Ergebnisse sind enorm: Nach einer Umgewöhnungsphase berichtet die Pilotgruppe über eine deutliche Steigerung ihrer allgemeinen Zufriedenheit und Work-Life-Balance bei gleichzeitig geringem bis keinen negativen Impact auf ihre Leistung und Ergebnisse. Auch die Führungskräfte berichten weder von Kommunikations- noch von Leistungsengpässen. Um weitere Schritte besonnen setzen zu können, brauchen wir noch mehr Daten und Erfahrungswerte. Daher haben wir beschlossen, den Beobachtungszeitraum um ein Quartal zu verlängern. Ein ganzes Unternehmen mit einem neuen Arbeitszeitmodell zu versehen, ist ein großer Kraftakt. Einer, der sich lohnt – davon bin ich schon jetzt überzeugt.

Foto: T-Systems

# Nachlese zum
## 28. **quality**austria Forum

*Hybrid-Event vom 22. März 2023*

**Erfolgsfaktoren der Zukunft:**

**Der Mensch macht den Unterschied**

SABINE HÜBNER, BERATERIN UND AUTORIN: »SERVICE IST KEIN PROJEKT, SONDERN EINE HALTUNG.«

*Steffi Burkhart, Human Capital Evangelist*

Mehr als 700 Teilnehmer*innen begrüßten die Geschäftsführer der Quality Austria, Werner Paar und Christoph Mondl, am 22. März im Salzburg Congress und online vor den Bildschirmen. Wie im Vorjahr fand der Branchenevent für Qualitätsmanager*innen aus dem In- und Ausland als Hybrid-Veranstaltung statt. Im Mittelpunkt stand die Arbeitswelt, die sich – Stichwort Homeoffice und Viertagewoche – merklich im Umbruch befindet. »Wir haben in jüngster Zeit gesehen, dass unsere Abläufe und Gewohnheiten veränderbar sind. Anpassung ist möglich, wenn wir es wollen oder müssen«, verwies Werner Paar im Eingangsstatement auch auf die gesellschaftliche Verantwortung: »Wie die Welt in Zukunft aussieht, liegt an uns.«

Wirtschaftlicher Erfolg hängt von unterschiedlichen Faktoren ab. Im Mittelpunkt stehe aber immer ein Mensch als Mitarbeiter*in,

Fotos: Anna Rauchenberger

Sabine Hübner, Service-Performance-Beraterin

# DER FAKTOR MENSCH

*Aktuelle Herausforderungen wie die Klimakrise, Digitalisierung, Gesundheit und Nachhaltigkeit verlangen ein Umdenken und neue Strukturen. Welche Erfolgsfaktoren in Zukunft entscheidend sind und welche Rolle der Mensch einnehmen wird, diskutierten Expert*innen beim 28. qualityaustria Forum.*

TEXT | ANGELA HEISSENBERGER

Führungskraft, Kund*in, Auftraggeber*in oder Geschäftspartner*in, so Paar: »Integrierte Managementsysteme schaffen verlässliche Strukturen, um diese Herausforderungen zu bewältigen.«

Christoph Mondl skizzierte das Bild einer vernetzten, digitalisierten und resilienten Wirtschaft, »weg von der Value Chain, hin zum Value Network«. Rangierten früher etwa ein attraktiver Standort oder die Bekanntheit des Arbeitgebers noch weit oben, sind heute flexible Arbeitszeiten, sinnstiftende Tätigkeiten und eine hohe Work-Life-Balance entscheidend für die Jobwahl. 52 Prozent der Befragten würden ein attraktives Angebot ausschlagen, wenn sie im Bewerbungsprozess negative Erfahrungen machen.

## DER MENSCH-MOMENT

»Talente sind der Schlüssel der Zukunft«, betonte Steffi Burkhart, Human Capital Evangelist, in ihrem Vortrag. Ab 2035 werden bereits 75 Prozent der Belegschaft aus den Generationen Y (1980–1995), Z (1995–2010) und Alpha (2010–2025) bestehen. Sie sind die Treiber, die technologische und marktrelevante Entwicklungen künftig beeinflussen. Einigen Ländern fehlt aufgrund niedriger Geburtenraten dieser frische Input der jüngeren Generationen – Japan oder China sind bereits stark von Überalterung betroffen.

Aber wie gelingt es Organisationen, junge Talente zu gewinnen, um Zukunftsthemen voranzubringen? »Viele Unternehmen schöpfen den Talentepool nur zur Hälfte aus, indem sie auf Frauen verzichten«, erklärte Burkhart. Darüber hinaus seien die Rahmenbedingungen entscheidend: »Junge Menschen werden in Zukunft nicht mehr Geld gegen Arbeit tauschen. Wir brauchen fluidere, flexiblere Formen von Arbeit, die klassischen fünf Arbeitstage und die 40-Stunden-Woche sind ein Auslaufmodell.«

*Werner Paar, Geschäftsführer Quality Austria*

Wie Führungskräfte diesen veränderten Erwartungen begegnen können, strich Unternehmerin und Autorin Kerstin Plehwe heraus: »Kommunikation ist die neue Königsdisziplin.« Nahbarkeit, Authentizität, häufiges und wertschätzendes Feedback sowie Individualität zeichnen echtes Leadership aus. Entscheidend sei der positive Umgang mit Veränderungen: Statt die gesamte Energie auf die Gestaltung der

*Christoph Mondl, Geschäftsführer Quality Austria*

*Wolfgang Glatz, Director of Quality Management bei Plansee HPM*

*Kerstin Plehwe, Unternehmerin und Autorin*

Zukunft zu richten, lassen sich aber viele Menschen von Misstrauen und Bedenken bremsen. Resilienz erfordere innere Stärke und Widerstandskraft, so Plehwe: »Wenn von außen ein Sturm kommt, knicken nur jene Palmen um, die nicht fest verankert sind.«

Service-Performance-Beraterin Sabine Hübner richtete in ihrer Keynote den Fokus auf den Kontakt zwischen Unternehmen und Kund*innen, der immer mehr zum Prüfstein wird: »Service ist kein Projekt, sondern eine Haltung. Je digitaler unsere Welt wird, desto mehr steigt der Anspruch der Menschen an die Qualität der persönlichen Begegnung.« Unzufriedene Konsument*innen machen ihre Erfahrungen öffentlich kund. Gleichzeitig steckt in jeder Begegnung die Chance auf »einen einprägsamen Mensch-Moment, mit dem wir uns selbst ein Gesicht geben«, wie ihn Hübner anhand eines eigenen Erlebnisses anschaulich schilderte: »Am Ende bleibt immer ein Gefühl haften.«

## DIE WEICHEN STELLEN

Auch Axel Dick, Prokurist Business Development Umwelt und Energie der Quality Austria, nahm auf die zentrale Rolle der jungen Bevölkerung Bezug: »Wir müssen bis 2030 die Weichen richtig stellen, damit die Generationen Z und Alpha eine Perspektive für die Zukunft haben.« Die Agenda sei angesichts der drängenden Probleme – War for Talents, Energieeffizienz, Klimaschutz, Kreislaufwirtschaft, Biodiversitätsverlust – lang: »Prozesse, die wir für selbstverständlich gehalten haben, laufen nicht mehr so ab wie gewohnt.« Es gelte, diese Themen ernst zu nehmen, auch wenn praktikable Lösungen (noch) nicht überall bereitstehen. Hinsichtlich neuer Regelungen wie der europäischen Taxonomie-Verordnung oder der Richtlinie zur Nachhaltigkeitsberichterstattung CSRD geben Managementsysteme und Normen den betroffenen Unternehmen das nötige Rüstzeug.

Einen Blick in die praktische Umsetzung einer »Qualitätsmatrix« öffnete Wolfgang Glatz, Director of Quality Management

Fotos: Anna Rauchenberger

bei Plansee HPM. Das 1921 in Reutte gegründete Unternehmen erzeugt Hochleistungswerkstoffe und ist Weltmarktführer im Bereich Refraktärmetalle. »Wir sind ein typischer Hidden Champion, aber meist auch Enabler von Produkten für unsere Kunden«, erläuterte Glatz die Prinzipien des Erfolgs: »Qualität leben und Kundenversprechen in Leistung umsetzen.« Der PDCA-Zyklus (»Plan-Do-Check-Act«) dient als Drehscheibe: Die Planung der Ziele erfolgt im Jahreskreis, die Umsetzung wird mit den Stakeholder*innen abgestimmt und an festgelegten Checkpoints geprüft. Alle Prozesse werden visualisiert und transparent abgebildet und Probleme entsprechend des Eskalationsmodells bearbeitet: »Diese Problemlösungskompetenz aus der Organisation nimmt die Last von den Schultern der Mitarbeiter*innen.«

Dem interessierten Publikum gab Glatz einen wichtigen Rat mit auf den Weg: »Integrieren Sie das Management – sonst ist das Ding nicht mal die Hälfte wert!« ■

*Axel Dick, Prokurist Business Development Umwelt und Energie, CSR bei Quality Austria*


*Strahlende Gewinner*innen (v.l.n.r.): Werner Paar (CEO Quality Austria), Michael Danzl (Qualitäts-Champion 2022), Alexander Woidich (Vorsitzender der Jury), Valerie Primas (Qualitäts-Talent 2022), Christoph Mondl (CEO Quality Austria)*

# Qualitäts-Champion & Qualitäts-Talent

*Auf Initiative der Österreichischen Vereinigung für Qualitätssicherung (ÖVQ) werden jährlich im feierlichen Rahmen des qualityaustria Forums zwei Persönlichkeiten für ihre herausragenden Projekte im Bereich Qualitätsmanagement ausgezeichnet.*

Zum »Qualitäts-Champion 2022« wurde heuer der Qualitätsmanager Michael Danzl gekürt. Dem 47-Jährigen gelang die erfolgreiche Implementierung eines auf die Unternehmensbedürfnisse zugeschnittenen Managementsystems. Die firmeninterne Plattform dient zur Dokumentation und Verbesserung der Unternehmensprozesse und leistet inzwischen einen wichtigen Beitrag zur Erreichung der innerbetrieblichen strategischen Ziele. »Das übergreifende Informationssystem unterstützt sieben Sprachen und deckt die Themen Qualitäts-, Umwelt-, Sicherheits- und Energiemanagement ab. Neben mehreren Tausend Dokumenten wird der gesamte Verbesserungsprozess mit derzeit zig-tausend Einzelmaßnahmen in dem Integrierten Managementsystem gesteuert«, zeigte sich die Jury in ihrer Begründung beeindruckt. Als neuer Qualitäts-Champion ist Michael Danzl automatisch für den European Quality Leader Award der European Organization for Quality (EOQ) nominiert.

Für die Auszeichnung Qualitäts-Champion können sich Personen bewerben, die in den vergangenen drei Jahren ein Projekt durchgeführt haben, das wesentlich zur Verbesserung von Produkten oder Dienstleistungen beigetragen hat. Auch mit herausragenden Ideen für neue Methoden und Werkzeuge im Projektmanagement (etwa im Bereich Qualität, Umwelt oder Sicherheit) ist eine Teilnahme am Bewerb möglich.

Mit dem Nachwuchspreis »Qualitäts-Talent 2022« wurde die 23-jährige Projektmanagerin Valerie Primas ausgezeichnet. Ihr Projekt »Gute Gesundheitsinformationen« hebt am Universitätsklinikum Graz »mit einer neu geschaffenen Systematik die Qualität der vielfältig vorhandenen Informationen für Patient*innen strukturell und inhaltlich auf ein neues Niveau«, befand die Jury in ihrer Würdigung. Die neu geschaffene Methodik sichert eine einheitliche Struktur, die fachliche Aktualität der Gesundheitsinformationen sowie deren Verfügbarkeit für alle Mitarbeitenden. Für den Nachwuchspreis »Qualitäts-Talent« können sich Personen zwischen 16 und 30 Jahren bewerben, die Auszeichnung ist mit 3.000 Euro dotiert (die Hälfte davon als Bildungsgutschein der Quality Austria).

**Info und Anmeldung für den kommenden Wettbewerb:**
www.qualityaustria.com/qualitaets-champion

# DIGITALE UNABHÄNGIGKEIT

*Ohne Cloud werden Wertschöpfungsketten nicht mehr funktionieren – Schutzmechanismen sind erforderlich.*

IM ZUGE IHRER DIGITALISIERUNGSSTRATEGIE NEHMEN VIELE UNTERNEHMEN ZUNEHMEND CLOUD-SERVICES IN ANSPRUCH. WO DIE DATEN GESPEICHERT SIND, WER SIE VERWALTET UND WELCHE TECHNOLOGIE DAHINTER STEHT, WIRD DABEI ZUM ENTSCHEIDUNGSKRITERIUM. EUROPÄISCHE BESTREBUNGEN FÜR EINE »SOUVERÄNE CLOUD« SOLLEN DATENSCHUTZ UND RECHTSSICHERHEIT GEWÄHRLEISTEN.

TEXT | ANGELA HEISSENBERGER

Dienste von Cloud-Anbietern werden für die Verarbeitung und Speicherung großer Datenmengen genutzt. Daten in einer Public Cloud können auf mehrere Rechenzentren verteilt sein und unterliegen grundsätzlich den Vorschriften des jeweiligen Landes, in dem die Daten gespeichert sind.

Viele Unternehmen, die diese Services zur Umsetzung ihrer Digitalisierungsprojekte in Anspruch nehmen, sind um die Sicherheit ihrer Daten und der ihrer Kund*innen besorgt – insbesondere in Zusammenhang mit der DSGVO und anderen Regulatorien. Vor allem in der Finanzindustrie, im öffentlichen Sektor und im Gesundheitsbereich sind Schutzmechanismen dringend erforderlich. Doch auch in anderen Branchen zeichnet sich bereits ab: Ohne Cloud werden Wertschöpfungs- und Lieferketten nicht mehr funktionieren. Doch Datenschutz und Cloud müssen kein Widerspruch sein.

## VOLLSTÄNDIGE KONTROLLE

Unter einer »Sovereign Cloud« versteht man eine Cloud-Computing-Lösung, die ein bestimmtes Land oder eine Organisation vollständig selbst hostet und verwaltet. Solche »souveränen« Clouds gewinnen zunehmend an Bedeutung, vor allem wenn es um den Schutz sensibler oder personenbezogener Daten geht. Der Betreiber der Cloud

Fotos: iStock, T-System International GmbH

*Timo Levi, T-Systems International.*

## »Resilienz hat an Bedeutung gewonnen«

*Digitale Souveränität sei nicht erst seit Corona ein brisantes Thema, meint Timo Levi, Tribe Lead Technology & Innovation der T-Systems International GmbH. In Europa werde nur offener darüber diskutiert.*

Hat das Thema Datensouveränität durch aktuelle geopolitische Entwicklungen zusätzlich an Bedeutung gewonnen?

**Timo Levi:** Digitale Souveränität beinhaltet Datensouveränität, betriebliche Souveränität und technologische Souveränität. Man will damit unabhängiger von Abhängigkeiten werden und sich gegen nachteilige Entwicklungen vorbereiten, seien es einseitige Veränderungen in der Produktpolitik von Herstellern oder der fehlende Zugriff auf Technologien, wie es bei Lieferkettenproblematiken oder geopolitischen Herausforderungen entstehen kann. Dies zeigen uns der russische Angriffskrieg auf die Ukraine und der drohende Konflikt zwischen China und Taiwan sehr deutlich. Wir nehmen dazu mehr Bemühungen bei unseren Kund*innen wahr, sich gegen diese Herausforderungen zu stellen. Ob es der Ersatz eines russischen Virenscanners oder die Absicherung gegen Cyberangriffe aus russischer Hand ist – Resilienz hat an Bedeutung gewonnen.

Ergeben sich durch die strengeren Schutzmaßnahmen möglicherweise Wettbewerbsnachteile für den Wirtschaftsstandort Europa?

**Levi**: Digitale Souveränität sollte nicht als die Einführung strenger Schutzmaßnahmen verstanden werden, sondern als vorausschauende Betrachtung der Gesamtrisiken und ihrer Mitigation. Ein aufgeräumter und gesunder Garten widersteht auch jedem Sturm nahezu unbeschadet. Oder anders formuliert: Die Wettbewerbsnachteile bei Nichtbeachtung von digitaler Souveränität oder Resilienz sind mit Sicherheit schwerwiegender.

Inwieweit ist ein eigener Weg Europas im Cloud-Markt auch wirtschaftlich sinnvoll?

**Levi:** Es ist nicht richtig, dass Europa mit digitaler Souveränität seinen eigenen Weg geht. Viele der großen Volkswirtschaften haben sich seit vielen Jahren auf die Reise zu mehr Resilienz und digitaler Souveränität gemacht.
Die große Abhängigkeit von verteilten, globalen Lieferketten ist nicht erst seit Corona ein Problem geworden. Denken Sie an die Piraterie in Asien, an die Sperrung bedeutender Schiffswege, an die vielfältigen politischen Bemühungen der US-Amerikaner, Technologien wieder zurück ins Land zu holen oder an den stark zunehmenden Einsatz von Open Source in asiatischen Ländern. Europa geht insofern keinen eigenen Weg, sondern spricht aufgrund der engen föderalen Vernetzung der Partnerländer offener darüber.

besitzt die vollständige Kontrolle über die gesamte Infrastruktur, einschließlich der Daten, der Anwendungen, der Plattformen und der Dienste.

Die Bestrebungen der europäischen Gaia-X-Initiative zur Schaffung gemeinsamer Rahmenbedingungen prägten den Begriff, unter dem die Aspekte Datensouveränität, operative Souveränität und Softwaresouveränität subsumiert werden. Während Datensouveränität darauf abzielt, wem die Daten gehören und wie damit umgegangen wird, betrifft die operative Souveränität die technische Seite der Cloud – welche Infrastruktur, welche Hersteller, welche Technologien ihr zugrunde liegen. Die Softwaresouveränität beschäftigt sich mit der Art der Software und welche Dienstleister sie implementieren und weiterentwickeln.

### KEIN UNBERECHTIGTER ZUGRIFF

Eine Voraussetzung für Datensouveränität ist volle Transparenz. Sie stellt sicher, dass Anwendungen auch im Krisenfall und unabhängig vom Hersteller weiterbetrieben werden können. »Souveräne Cloud-Dienste sind für Kunden aller Branchen inklusive der öffentlichen Verwaltung relevant. Sie stärken Resilienz und digitale Souveränität und erhalten unseren Kund*innen ihre Handlungsfähigkeit«, verweist Timo Levi, Tribe Lead Technology & Innovation bei T-Systems International, auf einen weiteren Vorteil: »Nebenbei sorgen Sie auch für geringere Kosten.«

Offene Plattformen, wie die souveränen Cloud-Services von T-Systems und Google, sind in der Lage »containerisierte sowie virtualisierte Workloads auszuführen, die sich konsistent über unterschiedliche Cloud-Landschaften hinweg verwalten und damit auch jederzeit auf andere Plattformen verschieben lassen«, erklärt Alexander Bruckner, Public Cloud Sales Expert bei T-Systems. Die Services basieren auf Open Source Software und kommunizieren auf Basis offener Schnittstellen miteinander. Dadurch wird die Abhängigkeit von einem Hersteller verhindert. Das Verschlüsselungsmanagement von T-Systems garantiert zudem, dass kein unberechtigter Zugriff auf die Kundendaten möglich ist – und zwar weder aus Europa noch aus den USA.

Einschränkungen müssen bei der Nutzung nicht in Kauf genommen werden. »Ein Umdenken ist im Einzelfall notwendig und manch liebgewonnene Praxis muss kritisch hinterfragt werden, gegebenenfalls müssen neue Skills aufgebaut werden und Partnerschaften überdacht werden«, sagt Innovationsexperte Levi. »So ist der Einsatz von Open Source Software ein wesentlicher Beitrag für Souveränität und kann im Unternehmen eine Vielzahl an Vorteilen bringen.«

# Unterstützung bei Sicherheitsfragen

TEXT | MARTIN SZELGRAD

Welchen Stellenwert räumen Unternehmen dem Thema Cybersicherheit ein? Und wo setzen Sie hier mit Ihrer Arbeit an?

**Thomas Stubbings:** Die großen Unternehmen haben dahingehend eine starke Awareness und setzten bereits viele Maßnahmen um. Doch der Mittelbau, der auch das Rückgrat der Wirtschaft in Österreich ist, tut viel zu wenig. KMU haben all die Risiken, die die Großen auch haben – sie sind sich dessen aber oft nicht bewusst.

Ich bin seit über 20 Jahren im Bereich Cybersicherheit in verschiedensten Rollen tätig. Seit acht Jahren berate ich Unternehmen zu diesem Thema. Seit der Gründung des Unternehmens Cyber Trust Services beschäftige ich mich mit einem Gütesiegel für Cybersicherheit, der als Nachweis für eine Basissicherheit in Unternehmen und Organisationen dient. Daneben bin ich ehrenamtlich in Funktionen wie etwa im Vorsitz der Cybersicherheitsplattform der Bundesregierung tätig – mit der Zielsetzung, Österreich sicherer zu machen. Das Thema treibt mich seit Jahren an.

Ist das eine Frage des Budgets, der fehlenden Fachkräfte oder einfach nur des mangelnden Know-hows?

**Stubbings:** Es kommt alles zusammen. Zunächst fehlt in vielen Fällen das Bewusstsein, da sich die Geschäftsführung eines mittelständischen Unternehmen meistens nicht mit Cybersecurity auskennt und auch nicht dazu tendiert, Berater zu konsultieren. Man ist zumeist darauf reduziert, was man über die Medien erfährt. Das ist sicher nicht ausreichend. Dann ist Geld ein Faktor. KMU müssen jeden Euro zweimal umdrehen und haben 1.000 Dinge auf ihrer Agenda. Nicht zuletzt fehlen die Personalressourcen. Es gibt zu wenige qualifizierte Fachkräfte in Österreich, um die Unternehmen im Bereich Cybersicherheit zu unterstützen. Man wird künftig deshalb verstärkt über Pooling und auch Outsourcing nachdenken müssen. Das ist aus meiner Sicht auch nicht falsch, denn nicht jedes kleinere Unternehmen braucht einen eigenen CISO (Anm. Chief Information Security Officer). CISO-Leistungen können zugekauft werden und das muss auch keine Vollzeitstelle sein. Wenn sich ein Externer zwei Tage in der Woche um das Thema kümmert, ist das immer noch besser, als gar keine Maßnahmen zu setzen.

Fehlende Ressourcen in Unternehmen für die Cybersicherheit bedeutet in der Regel, das Risiko dazu nicht beziffern zu können. Gehandelt wird oft erst nach einem erfolgreichen Angriff – wenn der Schaden bereits da ist.

**Stubbings:** Üblicherweise gibt es kein strukturiertes Risikomanagement in KMU, ausgenommen vielleicht bei Unternehmen im Finanzdienstleistungsbereich. Daher gibt es auch kein Risikobewusstsein. Wenn ich ein Risiko nicht greifen kann, habe ich auch keinen Anlass, etwas dagegen zu tun. Aus meiner Sicht ist die größte Herausforderung für uns alle, die allgemeine Risikolage in der gesamten Unternehmenslandschaft bewusst zu machen.

Foto: Cyber Trust Services

*Thomas Stubbings, Geschäftsführer von Cyber Trust Services, bietet mit einem Gütesiegel den Nachweis für Sicherheitsmaßnahmen in Unternehmen. Warum dies auch für nicht von NIS 2 betroffene Unternehmen spannend ist – darüber spricht er mit Report(+)PLUS.*

In der jüngsten Zeit gab es kaum Mangel an Berichten über Ransomware-Attacken in den Medien. Damit müsste doch ein Grundwissen darüber bestehen?

**Stubbings:** Ja, aber offensichtlich reicht es nicht aus. Frei nach dem Floriani-Prinzip fühlen sich viele nicht selbst davon betroffen oder gefährdet. Man betrachtet sich vermeintlich als unwichtig – die klassische Lebenslüge. Denn Angreifer suchen sich nicht das teuerste oder das wichtigste Opfer, sondern jenes, das am einfachsten angegriffen werden kann – selbst dann, wenn man dort vielleicht nur 5.000 Euro abzocken kann.

Beim Schaffen des Bewusstseins dafür sehe ich auch die Standesvertretungen in den Branchen in der Pflicht. Wenn Information zu Cybersicherheitsthemen und Gefahren über die Peer-Group verbreitet werden, ist das besonders effektiv. Ein Logistikunternehmen, das mit einem Partner-Unternehmen aus demselben Sektor über einen Sicherheitsvorfall spricht – da hat man einen besonderen Bezug.

Darüber hinaus gibt es in Österreich bereits wenige Branchen-CERTs (Anm. Computer Emergency Response Team) – wie etwa für die Energiewirtschaft –, die bereits hervorragende Arbeit machen und auf einem Niveau sind, von dem andere nur träumen können. Sie beschäftigen sich mit aktuellen Bedrohungen und Schwachstellen, informieren dazu und geben auch Hilfestellungen. Auch CERT.at ist eine sehr gute Infodrehscheibe, aber sie ist nicht die Kavallerie, die bei jeder Verschlüsselung bei einem KMU einmarschiert. Dazu sind die CERTs auch nicht personell aufgestellt.

Warum sollten Unternehmen auf ein Gütesiegel für Cybersicherheit setzen?

**Stubbings:** Das Cyber Trust Austria Gütesiegel wurde vor zwei Jahren in Zusammenarbeit mit dem Kompetenzzentrum Sicheres Österreich und dem KSV1870 geschaffen, um Transparenz im Bereich Cybersicherheit zu schaffen und Unternehmen den Nachweis ihrer Sicherheit zu erleichtern. Grundlegend wäre es ausreichend, die dazu geforderten Maßnahmen umzusetzen. Aber wir leben in einem vernetzten Markt mit Partnern und Kunden, die in einer Zusammenarbeit ebenfalls auf ihre Wahl des Partners achten.

Einen aktuellen Rechtsrahmen bildet NIS 1, das in Österreich rund 100 Unternehmen reguliert. Diese sind verpflichtet, eine Sorgfaltspflicht gegenüber Lieferanten anzulegen. Mit NIS 2 wird das Thema »Partner Risk Management« explizit in die Breite gebracht. Die Wirtschaftskammer geht derzeit von 3.000 bis 4.000 Unternehmen aus, die ab Oktober 2024 unter die neue Regelung fallen werden. Auch diese Unternehmen in Österreich werden dann verpflichtet, einen Nachweis zu ihrem Lieferantenrisiko in geeigneter Weise zu erbringen. Das kann eine Zertifizierung wie ISO 27001 sein, die mit Stand vor zwei Jahren aber eine verschwindende Minderheit von nur 170 Unternehmen in Österreich hatten. Weiters ist ein Nachweis durch Audits der Lieferanten und Partner möglich, was aber naturgemäß aufwendig ist. Und dann gibt es einen neutralen Qualitätsnachweis wie das »Cyber Trust Austria«-Gütesiegel. Damit erfüllen die Unternehmen validierte Mindestsicherheitsmaßnahmen und dieser Nachweis wird auch von den zuständigen Behörden im Rahmen des Lieferantenrisikomanagements akzeptiert werden. Betreibt dann ein Betreiber nach NIS 2 wesentlicher oder wichtiger Dienste ein Risikomanagement und fordert das Gütesiegel von seinen Lieferanten ein, wird dies bei einer Prüfung positiv angerechnet.

Wie aufwendig ist die Qualifikation für das Gütesiegel?

**Stubbings:** Anders als eine ISO-Zertifizierung, deren Kosten sich mindestens in einem fünfstelligen Euro-Bereich bewegen, kostet das Cyber Trust-Standardlabel 890 Euro. Kriterien hier sind beispielsweise ein Ansprechpartner für Cybersicherheit intern oder extern, eine Policy für den Umgang mit Sicherheit im Unternehmen, die Schulung von Mitarbeitenden das Testen von Notfallplänen und technische Grundvoraussetzungen wie Patchmanagement, Antivirus, Firewall und Nutzerauthentifizierung. Wenn diese Anforderungen erfüllt werden – die wahrlich keine Raketenwissenschaft sind –, ist das Gütesiegel in ein bis zwei Wochen machbar. Wir sind von der Win-win-Situation überzeugt: Der Kunde, der Auftraggeber bekommt einen Nachweis in NIS-gültiger Form. Der Lieferant macht den Nachweis einmal und kann ihn gegenüber allen Kunden und Partnern vorweisen.

An wen richten Sie ihren Service vorrangig?

**Stubbings:** KMU sind unsere Hauptzielgruppe, aber wir haben im Moment das interessante Phänomen, dass überdurchschnittlich viele große Unternehmen ein Gütesiegel im höheren Silber- oder Gold-Level durchführen – wie zum Beispiel Siemens, Hornbach oder PwC. Auch hier zeigt sich, dass das Bewusstsein bei den Großen da ist. Wir erwarten, dass größere Unternehmen künftig das Gütesiegel auch von ihren kleineren Partnern einfordern werden. Damit werden indirekt auch die Lieferanten der unter NIS 2 fallenden Unternehmen reguliert.

Genaue Zahlen gibt es dazu nicht, aber die IKT-Branche (Anm. Wirtschaftskammer-Sparte Information und Consulting) wird von rund 100.000 Unternehmen in Österreich gebildet. Gemäß einer Studie der Industriellenvereinigung generieren zwei Drittel der österreichischen KMU zumindest ein Drittel ihres Umsatzes mit den österreichischen Leitbetrieben. Diesen Unternehmen wollen wir das Angebot des Gütesiegels machen. Es ist niederschwellig, leistbar und behördlich anerkannt. ■

# #REFERENZ

# Datenschutz aus einem Guss

*Für den Baustoffspezialisten Wienerberger hat T-Systems ein Datenschutzmanagement implementiert. Seitdem laufen nahezu alle Prozesse, die für die Einhaltung der europäischen Datenschutzverordnung nötig sind, auf einer hochsicheren Cloud-Plattform und verursachen nur noch minimalen Administrationsaufwand – und die Lösung ist äußerst userfreundlich.*

Die Vielfalt der Niederlassungen der Wienerberger AG hängt mit dem Geschäftsmodell zusammen. Weil Ziegel, Rohrsysteme und Betonsteine nicht weit transportiert werden können, produziert der Baustoffspezialist in 30 Ländern in Zentral- und Osteuropa sowie in Nordamerika jeweils lokal an knapp 210 Produktionsstandorten. Die Umsetzung der europäischen Datenschutzgrundverordnung hat Wienerberger vor die Herausforderung gestellt, bis Mai 2018 ein funktionierendes Tool zu implementieren, das dem Unternehmen hilft und die gesetzlichen Anforderungen erfüllt. Es musste auch ein System gefunden werden, das sich auf die länderspezifisch unterschiedlichen Wienerberger-Strukturen anpassen kann und dennoch ein stimmiges Ganzes ergibt.

Dass die Wahl am Ende auf eine Datenschutzmanagementlösung von T-Systems gefallen ist, lag zunächst einmal an der hohen Sicherheits- und Datenschutzexpertise, die die Österreich-Tochter der Deutschen Telekom mitbringt. Schließlich gehört zur gesetzeskonformen Verarbeitung von personenbezogenen Daten auch die sichere Speicherung. Die Daten für die Wienerberger-Lösung werden daher in einer von T-Systems betriebenen, mehrfach abgesicherten GRC-Cloud gelagert, die dazugehörige Infrastruktur befindet sich im Twin-Core-Rechenzentrum in Wien. Bei etwaigen Problemen ist T-Systems somit auch der direkte Ansprechpartner für Wienerberger.

## VOLLER SERVICE

Doch die GRC-Cloud – GRC steht für Governance, Risk and Compliance – hat noch einen weiteren Vorteil: »Weil die gesamte Lösung von T-Systems in der Cloud betrieben wird, müssen wir uns nicht mit Updates, Patches und sonstigen Revisionen herumschlagen. Wir bekommen das gar nicht mit«, erklärt Christoph Schacher, Corporate Information Security Manager bei Wienerberger. Kurzer Nachsatz: »Okay, manchmal kommt eine E-Mail, dass das System am Wochenende kurz down sein wird. Das war's dann aber wirklich.«

BIC GRC, wie die dafür verwendete GRC-Plattform des Softwareherstellers GBTEC heißt, ermöglicht in Verbindung mit den von T-Systems entwickelten Kontrollkatalogen, Workflows und Prozessen den DSGVO-Verantwortlichen in den einzelnen Bereichen des Unternehmens nicht nur mögliche Verstöße gegen die EU-DSGVO aufzudecken, sondern sie bietet auch Lösungen an, die – wieder direkt über die Plattform – gesetzt werden können, um zu einem rechtskonformen Status zu kommen. Zudem erlaubt die Plattform die Erweiterung des reinen Datenschutzmanagements um zusätzliche Bereiche wie z. B. Informationssicherheits- oder Risikomanagement. »Das sind fertige Bausteine, die man sehr schnell an etwaige individuelle Kundenwünsche anpassen und auch in bestehende IT-Landschaften integrieren kann«, sagt Thomas Masicek, Senior Vice President und Tribe Lead Cyber Security der T-Systems International GmbH.

## ERFAHRUNG ALS ASSET

In seinem Kern umfasst die Datenschutzmanagementlösung, die T-Systems anbietet, alle zur Einhaltung der EU-DSGVO notwendigen Teilbereiche, also ein revisionssicheres Verzeichnis der Verarbeitungstätigkeiten, die Durchführung und Dokumentation von Datenschutzfolgeabschätzungen sowie Workflows für die Bearbeitung von Datenpannen und Anfragen durch betroffene Personen. Zu einer Anwendung mit Mehrwert wird das System aber durch das DSGVO-spezifische Knowhow des T-Systems GRC-Teams. »Es war schon sehr stark zu merken, dass die Kollegen von T-Systems nicht nur Daten- und IT-Spezialisten sind, sondern auch bei der

Fotos: Wienerberger AG, Otto Group

# Ganzheitliches Risikomanagement

*Das Enterprise Risk Managementsystem von T-Systems ermöglicht der Otto Group höchste Flexibilität durch kundenspezifische Konfiguration.*

Umsetzung der gesetzlichen Vorgaben in der Praxis bereits sehr viel Erfahrung haben«, blickt der Wienerberger-CISO Christoph Schacher auf das Projekt zurück. »Sie wissen wirklich auch in praktischer Hinsicht, wovon sie reden.« Was wohl auch damit zu tun hat, dass die Deutsche Telekom, die Mutter von T-Systems, in den Landesorganisationen genau jene Datenschutzmanagementlösung verwendet, die sie auch ihren Kunden anbietet. »Allein dadurch haben wir sehr viele praktische Erfahrungen, weil wir in diesem Fall eben nicht nur Anbieter der Lösung sind, sondern sie in unserem Bereich auch selbst nutzen«, erklärt Masicek. Zugleich profitiere man von den inzwischen zahlreichen Use-Cases. Denn jeder einzelne bringt neue Erkenntnisse, die zukünftigen Usern zugutekommen. Dass inzwischen auch sehr viele Großkonzerne für ihren Datenschutz die von T-Systems angebotene Lösung verwenden, befeuert diese Entwicklung zusätzlich.

## BLICK FÜR DIE PRAXIS

»Viele Berater konzentrieren sich, wenn es um die EU-DSGVO geht, ausschließlich auf das Gesetz. Wir kennen auch die Praxis, und das ist neben IT-technischer Expertise unser großer Vorteil«, so Masicek. Praxisorientiert ist aber auch das Frontend des Systems, in dem Risikohöhen mittels grafischer Heat Maps festgelegt werden können.

Die Implementierung der Lösung bei Wienerberger lief ebenfalls sehr userfreundlich ab – mit Onlineschulungen, die nicht nur den Umgang mit der Software zeigten, sondern zugleich auch eine jeweils dem Anwenderlevel angepasste Einführung in die EU-DSGVO enthielten. Seit das System läuft, merkt man indessen kaum noch etwas davon. Nach der Technik im Hintergrund gefragt, kann sich Christoph Schacher von Wienerberger daher eine recht entspannte Antwort leisten: »Wir konzentrieren uns hier voll auf die Inhalte. Die Technik dahinter muss funktionieren – und das tut sie.« ■

Die Otto Group mit Sitz in Hamburg zählt mit einem Onlineumsatz von 7,7 Milliarden Euro zu den weltweit größten Onlinehändlern. Ihr Portfolio deckt die ganze Bandbreite des Einzelhandels vom Spielzeug-Shop über den SaaS-Anbieter bis hin zur Open-Commerce-Plattform ab. Im Frühjahr 2019 beauftragte die Otto Group den Digitaldienstleister T-Systems mit dem technischen Konzept, der Implementierung sowie der Integration eines ganzheitlichen Enterprise Risk Managementsystems. Ziel war es, die Anwendungsfälle so schlank wie möglich zu halten, um ein schnelles Roll-out und Onboarding der Nutzer*innen zu ermöglichen. Die Basis bildete die Software BIC GRC des österreichischen Softwareunternehmens GBTEC.

Die Softwarelösung ermöglicht höchste Flexibilität durch kundenspezifische Konfiguration im BIC-GRC-Systemstandard. T-Systems verfolgt einen dualen Consulting-Ansatz und kombiniert fachliche mit technischer Expertenberatung. Um den Kund*innen schnellstmögliche Ergebnisse und eine größere Anpassungsfreiheit zu ermöglichen, wird ein agiler Implementierungsansatz mit Fokus auf Kernfunktionalitäten gewählt, der mit späteren Roll-outs sukzessive erweiterbar ist.

Um die vorgegebene Deadline einzuhalten, wurde das sogenannte »Minimum Viable Product« des Enterprise Risk Managementsystems innerhalb einer anspruchsvollen Timeline durch das GRC-Team umgesetzt. Der Go-live der ersten Welle für das Enterprise Risk Management der Otto Group erfolgte im Juli 2019. Bereits Ende August wurde die erste Datenerhebung im Konzern erfolgreich abgeschlossen. Ein wichtiger Erfolgsfaktor war die von Anfang an stattfindende Einbindung der relevanten Stakeholder in die Lösungsentwicklung: Das frühzeitige Onboarding der Nutzer*innen schaffte eine hohe Akzeptanz.

Ein gleichbleibendes Projektteam bei T-Systems, bestehend aus Fachspezialist*innen aus dem GRC-Bereich, arbeitete von Anfang an eng mit der Otto Group zusammen. In der Kommunikation und Abstimmung fungierte T-Systems als einziger Ansprechpartner. Die individuelle und intensive Betreuung war für die erfolgreiche Durchführung des Projekts entscheidend. Die Otto Group und T-Systems arbeiten derzeit an der Erweiterung des bestehenden Serviceumfangs, welcher auch eine Weiterentwicklung des Tools mit sich bringen wird . ■

*Die Otto Group implementierte mit Unterstützung von T-Systems und GBTEC ein ganzheitliches Enterprise Risk Managementsystem.*


# PERFEKTES DOPPEL

*Unternehmensnetze stoßen bei der Nutzung von Cloud-Services zunehmend an ihre Grenzen. Eine Netzwerkarchitektur auf Basis von Secure Access Service Edge (SASE) verbindet Sicherheit mit verlässlicher Netzanbindung.*

TEXT | ANGELA HEISSENBERGER

Die Cloud ist zu einer Drehscheibe geworden, die auch Auswirkungen auf Unternehmensnetze hat. Nutzer*innen greifen aus dem Homeoffice oder mobil auf cloudbasierte Apps und Dienste zu, auch vernetzte Maschinen und Standorte benötigen einen direkten Zugang. Die dezentrale Infrastruktur wird immer komplexer. So manches Unternehmensnetz stößt an seine Grenzen, wenn Mitarbeiter*innen im Außendienst aufgrund langsamer Verbindungen ausgebremst werden. Dazu kommt die Sicherheitsfrage: Wie lassen sich das Netzwerk und alle seine Endpunkte umfassend schützen? Das nötige Sicherheitsniveau zu erreichen, ohne die User Experience (UX) zu beeinträchtigen, kann sich schwierig gestalten.

Gartner stellte bereits Ende 2019 das Konzept »Secure Access Service Edge« vor. »Bis 2025 werden mindestens 60 Prozent der Unternehmen explizite Strategien und Zeitpläne für die Einführung von SASE haben: von Nutzer- über Zweigstellen- bis Edge-Zugriff«, hieß es damals. 2020 waren es erst zehn Prozent der Unternehmen. Seit im Zuge der Coronapandemie Remote Work zum bleibenden Faktor wurde, ist das Thema jedoch verstärkt in den Fokus gerückt: Viele Unternehmen haben erkannt, dass SASE die Möglichkeit bietet, eine Zero-Trust-Sicherheitspolitik umzusetzen, ohne die Komplexität zu erhöhen.

## DYNAMISCHER MARKT

»Wir beobachten, dass der SASE-Markt Fahrt aufnimmt und sich weiterentwickelt. In den kommenden Monaten werden die Implementierungen sicher zunehmen«, erklärt Christopher Ehmsen, Managing Director Deutsche Telekom Cyber Security Austria GmbH. »Auch der Wettbewerb unter den Anbietern verschärft sich. Sie bieten eine Reihe von Vorteilen, die sich auf höhere ROIs konzentrieren und ein robustes, nutzerorientiertes Security-Framework ermöglichen sollen.«

SASE (gesprochen: »sässi«) steht für die Synthese von Sicherheit, Netzwerkkommunikation und Optimierung – die meist auch gleich in einem Cloud-Umfeld stattfindet.

Fotos: iStock

## GLOSSAR

Das IT-Sicherheitsmanagement mit SASE (Secure Access Service Edge) besteht aus folgenden Komponenten:

- **Security Service Edge (SSE):** gewährleistet die zentrale Bereitstellung aller Sicherheitsdienste
- **Software-Defined Wide Area Network (SD-WAN):** leitet den Datenverkehr über ein WAN, ohne ihn zum Hub zurückzuleiten (im Gegensatz zum üblichen WAN-Prozess).
- **Secure Web Gateway (SWG):** bietet durch die Durchsetzung von Sicherheitsrichtlinien Schutz in der Cloud.
- **Cloud Access Security Broker (CASB):** bietet ein einziges Control Panel für das plattformübergreifende IT-Sicherheitsmanagement.
- **Zero Trust Network Access (ZTNA):** Zugriff auf Basis der Nutzeridentität.
- **Firewall as a Service (FWaaS):** eine Cloud-Firewall mit erweiterten Funktionen, um Skalierung zu ermöglichen.

Die Verknüpfung von Sicherheitsaspekten mit den Themen Connectivity und Automatisierung ist heute das zentrale Thema im Cloud-Business. Nachdem ein Gutteil der Anwendungen bereits in der Wolke stattfindet, sollte die Cloud konsequenterweise gleich auch als Zugangsknotenpunkt für die Vernetzung von Standorten verstanden werden.

Ein traditioneller Sicherheitsansatz ist in einem dynamischen Arbeitsumfeld völlig unzureichend. Unternehmen setzen vermehrt auf Cloud-Services, um agiler zu sein – die IT-Infrastruktur wächst aber nicht im gleichen Ausmaß mit. Im Durchschnitt greift ein*e Remote-User*in auf etwa zwölf SaaS-basierte Apps zu.

Eine weitere Herausforderung ist das Backhauling des Datenverkehrs zu Rechenzentren, beispielsweise mit einem VPN zu Prüfungszwecken. Dies beeinträchtigt die Nutzer*innen der Applikationen aufgrund der hohen Latenzzeiten. Darüber hinaus sind herkömmliche VPN-Infrastrukturen anfälliger für Bedrohungen. Schwache Sicherheitsrichtlinien eines Drittanbieters können die Angriffsfläche erhöhen.

### DIGITALE IDENTITÄTEN

Die Sicherheitsarchitektur SASE vereint hohe Performance im Netz und Cybersicherheit zu einem perfekten Doppel – ohne Umweg über das Firmennetz. Applikationen werden per Konnektoren in der Cloud abgebildet und können nur einzeln von legitimierten Anwender*innen genutzt werden. Damit ausschließlich berechtigte User*innen auf die Daten zugreifen, werden die digitalen Identitäten – und nicht wie früher die IP-Adressen – überprüft.

»Wir erfinden nichts neu, sondern kombinieren bewährte Technologien gleich direkt in der Cloud. So entfaltet sich die Stärke von SASE, nämlich direkt an der Edge zu sein – im Headquarter, in der Zweigniederlassung, überall, wo wir mobil arbeiten«, streicht Thomas Masicek, SVP Cyber Security T-Systems International, hervor.

Die Funktionen werden über eine cloudbasierte Plattform bereitgestellt: Die hauseigene IT muss somit weder Hard- noch Software installieren, auch Upgrades und Wartung laufen automatisiert ab und binden somit keine personellen und finanziellen Ressourcen. Alle Sicherheitsfeatures befinden sich stets auf dem aktuellen Stand und schützen vor Cyberangriffen. Ein einheitliches Portal sorgt für Übersichtlichkeit. IT-Teams können sämtliche Standorte, User*innen und Geräte, die über eine einzige Schnittstelle auf Geschäftsanwendungen zugreifen, überwachen und verwalten.

Begonnen sollte mit einer SASE-Machbarkeitsstudie werden. Expert*innen ermitteln den Ist-Zustand der IT-Infrastruktur und planen eine geeignete Sicherheitsarchitektur. Ist das ideale Framework gefunden und integriert, ist das Netzwerk fit für das Cloud-Zeitalter.

»Digitalisierung und die Cloud treiben Produktivität und Wachstum voran, bringen aber auch neue Herausforderungen mit sich«, so Masicek. »Durch eine Security-Service-Edge-Architektur ermöglichen Unternehmen ihren Mitarbeiter*innen einen ortsunabhängigen Arbeitsplatz, um produktiv Applikationen im Rechenzentrum und in mehreren Cloud-Umgebungen nahtlos, performant und vor allem sicher zu nutzen.« ■

## Was für Security Service Edge (SSE) spricht

1

**Weniger Risiken:** Eine Cloud-Plattform bietet Schutz; Security ist nicht mehr an einen Standort oder ein Netzwerk gebunden. Einheitliche Sicherheitsdienstleistungen schließen die Lücken zwischen Einzelprodukten und verringern Risiken. SSE verbessert die Sichtbarkeit der Benutzer*innen unabhängig von deren Standort. Es automatisiert auch alle Sicherheitsupdates in der gesamten Cloud, sodass manuelle IT-Aufgaben reduziert werden.

2

**Bessere Benutzererfahrung:** Bei der globalen Verteilung von SSE werden Inhalte überprüft, wenn die Endbenutzer*innen eine Verbindung zur SSE-Cloud herstellen. Dies führt zu geringerer Latenz und verbesserter Leistung. Der Wegfall der VPN-Nutzung und der Wechsel zu cloudbasierten Apps tragen dazu bei.

3

**Weniger Kosten und Komplexität:** SSE vereint mehrere Sicherheitsdienstleistungen wie SWG, ZTNA, CASB, FWaaS, Cloud DLP, CSPM und CBI. Durch die Verfügbarkeit unter einem Dach reduzieren sich Kosten und Komplexität, da alle Kanäle, auf die Benutzer*innen zugreifen, einheitlich geschützt sind.

4

**Zero-Trust-basierter Zugriff:** SSE schafft einen sicheren Remote-Zugriff mit Zero-Trust-Richtlinien für Geräte, Anwendungen, Inhalte und vor allem Benutzer*innen. Die Gewährung des Zugriffs ist streng richtlinien- und benutzerbasiert. Da sich die Benutzer*innen nicht im Netzwerk befinden und die Apps hinter der SSE-Plattform, wird die Verbindung sicherer. Angriffsfläche und Geschäftsrisiken werden so gemindert.

# #REFERENZ

# Dynamische Cloud-Lösung

*Öffentliche Ladestationen sind wichtig, aber die Zukunft liegt im Aufbau eigener entsprechender Infrastrukturen für Unternehmen, Kommunen und Institutionen. ENIO, ein europaweit führender Anbieter von E-Mobilitäts-Lösungen aus Österreich, vertraut seine sensiblen Daten der T-Systems Sovereign Cloud powered by Google Cloud an.*

70 bis 80 Prozent aller Ladungen erfolgen nicht im öffentlichen Bereich, sondern in eigenen Ladenetz-Infrastrukturen. Die ENIO GmbH sieht das größte Potenzial bei großen Fuhrparks, Bauträgern und Hausverwaltungen, der Logistikbranche oder Garagen- und Parkplatzbetreibern. So ist auch beim Laden von immer mehr Elektroautos die wichtigste technische Herausforderung, Stromspitzen zu vermeiden, die das Netz belasten. Innovative Ladetechnologien, die bedarfsorientiertes, netzschonendes und umweltfreundliches Laden ermöglichen, sind der Erfolgsschlüssel. Neben der Betriebssteuerung und der Verrechnung bietet ENIO seinen Kund*innen auch das Lastmanagement sowie das Energiemanagement an. Aufgrund der vielen ursprünglich monolithischen Applikationen hatte das Unternehmen hohe Aufwände in der Wartung.

## VOLLE TRANSPARENZ

Gesucht wurde deshalb eine Cloud-Lösung, die eine dynamische Ressourcenbereitstellung für Lastspitzen ermöglicht und darüber hinaus auch bei der Einführung neuer Whitelabel-Services unterstützt. Eine weitere Herausforderung lag in der Transformation der Applikationen in eine flexiblere Microservice-Architektur.

*Markus Litzlbauer (li.) und Michael Viktor Fischer, Geschäftsführung ENIO.*

Um all diese Herausforderungen zu meistern, entschied sich ENIO für die T-Systems Sovereign Cloud powered by Google Cloud als Trusted Plattform für sensible Daten. Auf Basis einer Containerplattform werden die dynamischen Applikationsservices nun in der Public Cloud betrieben. Zur Unterstützung der cloudnativen Entwicklung der Services erfolgen die automatisierten Deployments nun mittels CI/CD-Pipelines. »Für uns liegen die Vorteile der T-Systems Sovereign Cloud powered by Google Cloud eindeutig in der Flexibilisierung und einfachen Skalierung des Business-modells, der höheren Ausfallsicherheit sowie verringerter Störwegweite als auch in der Verkürzung der Releasezyklen sowie in der DSGVO-konformen Verarbeitung und Speicherung unserer sensiblen Kundendaten«, erklärt Michael Viktor Fischer, CEO und geschäftsführender Gesellschafter von ENIO. »Darüber hinaus bietet diese Cloud-Lösung volle Kostentransparenz durch ein Pay-as-you-go-Preismodell.«

## DAS UNTERNEHMEN

Die herstellerunabhängigen Softwarepakete von ENIO ermöglichen eine intelligente Steuerung von Ladestationen, sichere Zahlungsvorgänge und eine optimale Verteilung der zur Verfügung stehenden Energie. In der Unternehmenszentrale in Wien entwickelt und vertreibt das 2013 gegründete Unternehmen europaweit Software für die Infrastruktur der Elektromobilität sowie für die Steuerung und Abrechnung von Dienstleistungen mit Elektrogeräten. ENIO betreut Kund*innen aus 14 Ländern mit mehr als 5.000 Ladepunkten.

www.enio.at

Fotos: ENIO

# Klimafreundlicher Wasserstoff

*Wasserstoff, der mit geringem $CO_2$-Ausstoß erzeugt wird, entwickelt sich zu einem vielversprechenden Instrument zur Dekarbonisierung. Insbesondere die energieintensive Industrie hat das Potenzial des Energieträgers für sich entdeckt.*

TEXT | ANGELA HEISSENBERGER

Die Nachfrage nach Wasserstoff ist in den letzten drei Jahren branchen- und länderübergreifend um mehr als zehn Prozent gestiegen. In den klassischen Einsatzbereichen, etwa in Erdölraffinerien, Chemie- und Düngemittelunternehmen, wird sich dieser Trend noch weiter verstärken. Doch auch andere Bereiche wie der Schwerlastverkehr und die Luft- und Schifffahrt haben das Potenzial von Wasserstoff erkannt. Obwohl die Technologien hier noch nicht ausgereift sind, könnte vor allem in Sektoren, in denen Elektrifizierung keine Option ist, Wasserstoff eine mögliche Alternative zu fossilen Energieträgern sein.

Laut der Studie »Low-Carbon Hydrogen – A Path to a Greener Future« des Capgemini Research Institute prüfen 62 Prozent der Unternehmen aus energieintensiven Industriezweigen bereits den Umstieg auf $CO_2$-arm erzeugten Wasserstoff. »Unternehmen, die in Wasserstoff-Technologien investieren, können nicht nur ihre $CO_2$-Bilanz verbessern, sondern auch von neuen Geschäftsmöglichkeiten in einer kohlenstoffarmen Wirtschaft profitieren«, erklärt Martina Sennebogen, Managing Director von Capgemini in Österreich. Daher sei es entscheidend, die Entwicklung von klimafreundlichem Wasserstoff voranzutreiben und innovative Strategien zur Nutzung dieser Technologie zu entwickeln.


*62 Prozent der Unternehmen aus energieintensiven Industriezweigen prüfen bereits den Umstieg auf Wasserstoff.*

## NEUE PARTNERSCHAFTEN

Als klimafreundlich wird Wasserstoff in der EU eingestuft, wenn er durch Pyrolyse von Biomasse, durch Elektrolyse mit erneuerbaren Energien (»grüner« Wasserstoff) oder Atomkraft (»pinker« Wasserstoff) hergestellt wurde. Trotz der steigenden Nachfrage nach Wasserstoff gibt es bei seiner Produktion bekanntermaßen Probleme. Die derzeit angewandten Methoden sind weder kosteneffizient noch sind sie immer umweltfreundlich.

Um das zu ändern, brauche es umfangreiche Investitionen, so die Studienautor*innen. Möglich wäre das durch Partnerschaften zwischen den etablierten Akteuren der Wasserstoffbranche und neuen Marktteilnehmern sowie durch transparente und offene Märkte.

Trotz der Herausforderungen bei der Beschaffung von erneuerbarer Energie und den aktuell hohen Kosten für die Elektrolyse zeigen sich die Energieversorger zuversichtlich: Fast die Hälfte der Befragten erwarten, dass die Kosten zur klimafreundlichen Wasserstofferzeugung bis 2040 stetig sinken werden. Vorerst sind die meisten Unternehmen freilich noch mit Machbarkeitsstudien beschäftigt oder befinden sich in der Pilotphase. Erst elf Prozent der Energieunternehmen weltweit – in Deutschland sind es mit 22 Prozent fast doppelt so viele – und sieben Prozent der Endverbraucher haben Projekte mit klimafreundlichem Wasserstoff bereits vollständig in ihrem Markt eingeführt.

*Martina Sennebogen, Managing Director Capgemini Österreich.*

## VIELE HERAUSFORDERUNGEN

Neben der Kosten- und Energiefrage sind noch technische und infrastrukturelle Probleme zu lösen. So betrachten 65 Prozent der Unternehmen im Schwerlastverkehr die Ausweitung der Produktion von Wasserstoff-Brennstoffzellen als größte Herausforderung. In der Luftfahrt müsste zunächst die Bauweise von Flugzeugen geändert werden, um Wasserstoff als Kraftstoff nutzen zu können. In der Stahlindustrie halten 72 Prozent der Befragten die Modernisierung der Infrastruktur in großem Maßstab für erforderlich.

Zu den finanziellen, infrastrukturellen und technischen Fragen kommt ein eklatanter Mangel an Expertise. Wie in den meisten Branchen fehlt es auch in der Entwicklung der Wasserstofftechnologie an qualifizierten Fachkräften – 60 Prozent der Unternehmen sehen dies als die größte Bremse für ihre Wasserstoff-Projekte. ■

Fotos: iStock, Capgemini

# KOMMENTAR

Was Meinung ist und wer Position bezieht

*Die Sicherheit von Maschinen und Produktionsanlagen wird oft vernachlässigt.*

Christopher Ehmsen / Managing Director / Deutsche Telekom Cyber Security Austria GmbH

# Mehr Schutz gegen Cyber-Angriffe

*Von NIS 2 bis zum Cyber Resilience Act befasst sich eine ganze Reihe neuer Richtlinien mit IT-Security. Durch sie soll die Resilienz von Unternehmen europaweit gestärkt werden.*

Die Zahl der Cyberangriffe steigt nach wie vor weltweit kontinuierlich an. Jede Minute sind weltweit vier Unternehmen von einer Ransomware-Attacke betroffen und jeden Tag werden 560.000 neue Malware-Bedrohungen entdeckt. Diese Entwicklung stellt eine immense Gefahr für Organisationen dar, deren Prozesse, Produkte und Zusammenarbeit immer umfassender auf digitalen Technologien beruhen. Nicht nur das wirtschaftliche Überleben von Unternehmen ist von diesen Risiken betroffen, auch unsere lebenserhaltenden Systeme – vom Krankenhaus bis zum Energieversorger – erweisen sich als genauso angreifbar wie digital gesteuerte Produktionsanlagen, Verkehrsmittel oder auch Smartphones.

Vernetzte Produktionsanlagen und Betreiber kritischer Infrastrukturen geraten dabei immer öfter ins Visier der Angreifer. Inzwischen sind sich auch Regulierungsbehörden und Gesetzgeber darüber im Klaren, dass Cybersecurity uns alle betrifft. Während Europa in der Vergangenheit Datenschutz-Pionier war, ziehen zahlreiche Länder und Regionen nach und etablieren entsprechende Reglements. So soll die NIS-Richtlinie einen hohen Sicherheitsstandard der Netz- und Informationssysteme innerhalb der Europäischen Union gewährleisten. Umgesetzt wird die Richtlinie in Österreich durch das NIS-Gesetz (NISG), das seit Ende 2018 in Kraft ist. Die Anforderungen betreffen Betreiber wesentlicher Dienste (BwD) und Anbieter digitaler Dienste (AdD) und beinhalten die Implementierung von Sicherheitsmaßnahmen und die unverzügliche Meldung von Sicherheitsvorfällen. Des Weiteren müssen betroffene Einrichtungen mindestens alle drei Jahre die Sicherheitsmaßnahmen für ihre Netz- und Informationssysteme nachweisen.

## UMFASSENDES RISIKOMANAGEMENT

Als Reaktion auf die sich entwickelnde Bedrohungslage für Cybersicherheit haben das Europäische Parlament und der Rat der EU nun auch die NIS-2-Richtlinie verabschiedet. Diese wurde Ende 2022 veröffentlicht und trat am 16. Jänner 2023 in Kraft. Die EU-Mitgliedstaaten haben nun bis 17. Oktober 2024 Zeit, die darin enthaltenen Vorgaben in nationales Recht umzusetzen. Diese Richtlinie nimmt Einrichtungen, die für grundlegende gesellschaftliche und wirtschaftliche Tätigkeiten von entscheidender Bedeutung sind, in die Pflicht, sich mit Cybersicherheits-Agenden zu befassen, um so die Resilienz von Unternehmen gegenüber Cyberangriffen europaweit zu stärken. Während sich in der ersten Generation der NIS-Richtlinie vor allem Betreiber kritischer Infrastrukturen verantworten mussten, so erweitert die zweite Generation, NIS-2, ihren Umfang um eine Vielzahl weiterer Unternehmen, mit dem Ziel, die Cyber-Resilienz EU-weit auf ein höheres Niveau anzuheben. Unternehmen stehen nun vor der Herausforderung in dieser kurzen Zeit die in der Richtlinie vorgegebenen Maßnahmen umzusetzen. Bei Nichteinhaltung drohen hohe Geldstrafen.

Der Kern der neuen NIS-2-Regelung basiert auf der Durchführung eines Risikomanagements zur Ermittlung und Bewertung von möglichen IT-Sicherheitsrisiken und potenziellen Cyberangriffen. Zudem sind Unternehmen dazu verpflichtet, Sicherheitsvorfälle, die Auswirkungen auf die kritische Dienstleistung haben, an die Behörden sowie an die Empfänger dieser Dienstleistung zu melden. Auch die Sicherheit der Lieferkette findet erstmalig Berücksichtigung in der Richtlinie. Organisationen müssen nun auch Risiken direkter Zulieferer im Rahmen ihres Risikomanagements

Fotos: Deutsche Telekom Cyber Security Austria, iStock

## Erste Schritte zu einer sinnvollen IT- und OT-Resilienz sehen so aus:

1

**Risikoanalyse durchführen:** Die Identifikation und Bewertung von IT- und OT-Sicherheitsrisiken dient nicht nur einer frühzeitigen Erkennung von potenziellen Schäden, sondern kann auch die Reaktionszeit im Falle eines Angriffes wesentlich verkürzen.

2

**Abhängigkeiten lokalisieren:** Identifizieren und halten Sie Ihre kritischen Systeme und Kommunikationspfade fest.

3

**Schwachstellen managen:** Arbeiten Sie nicht einfach die Liste der Schwachstellen der Reihe nach ab, sondern beginnen Sie mit denen, die ein tatsächliches Risiko darstellen. Meist sind das jene Systeme, die auf den Kommunikationspfaden zu kritischen Systemen liegen.

4

**Mitarbeiter*innen schulen:** Eine gute Verteidigungsposition basiert auf dem Zusammenspiel zwischen Know-how, Technik und Prozessen. Geschulte Mitarbeiter*innen sind ein kritischer Faktor für eine gute Verteidigungsbasis.

5

**Threat Hunting durchführen:** Unternehmen sollten sich nicht damit begnügen, während oder nach einem Sicherheitsvorfall aufzuräumen, sondern auch aktiv nach Hinweisen für künftige Angriffe suchen.

6

**Patches einspielen:** Patchen Sie regelmäßig Ihre IT- und OT-Systeme. Lassen sich ältere Systeme, wie sie vor allem in Produktionsumgebungen zu finden sind, nicht direkt patchen, so kann man eventuell ein Upstream Patching im kritischen Kommunikationspfad durchführen.

7

**Systeme visualisieren:** Einen hundertprozentigen Schutz gegen Cyberangriffe gibt es leider nicht, daher kann gerade im Schadensfall die Visualisierung der Systeme die Wiederherstellungszeit signifikant reduzieren.

bedenken und bewerten. Damit rückt auch die Sicherheit von Produktionsanlagen zunehmend in den Fokus. Die Einführung smarter Maschinen und Lieferketten macht Unternehmen unweigerlich von externen Prozessen und dynamischen Daten abhängig.

### IT-RESILIENZ STÄRKEN

Doch während Organisationen im IT-Sicherheits-Umfeld meist schon zumindest rudimentäre Security-Lösungen zur Abwehr und Detektion von potenziellen Angriffen implementiert haben, wird die Sicherheit von Produktionsanlagen und Maschinen oft vernachlässigt. Schafft es ein Angreifer allerdings einmal in die Produktionsumgebung vorzudringen, kann dies fatale Folgen haben. Es drohen hohe Erpressungssummen, Imageschäden, Diebstahl von sensiblen Daten und Intellectual Property und schlimmstenfalls die Gefährdung von Menschenleben.

Die NIS-2-Richtlinie beinhaltet demnach neben Vorgaben zur Sicherheit von IT- und OT-Systemen auch Vorgaben zu physischer Sicherheit. Damit soll nicht nur die IT-Resilienz gestärkt werden, sondern auch die Resilienz produktionsfähiger Anlagen. Beide brauchen aber eine unterschiedliche Betrachtung. Während im IT-Security-Umfeld vor allem die Vertraulichkeit und der Schutz von Daten im Vordergrund steht, betrachtet man in der OT-Security Steuersignale oder Kommandos, bei denen Verfügbarkeit und Laufzeit kritisch sind. So sind zum Beispiel Verfahren wie die in der IT übliche Datenverschlüsselung im OT-Umfeld unter Umständen ein Risiko für die Verfügbarkeit von Echtzeitsignalen. Eine Konvergenz zwischen IT und OT zu schaffen, ist für einen optimalen Schutz vor Cyberangriffen unerlässlich. Der Schutz von Industrieanlagen erfordert Maßnahmen, die Skills, Technologien und Prozesse im IT- und OT-Umfeld berücksichtigen.

Ihr Unternehmen zählt zur kritischen Infrastruktur – was nun? Als Deutsche Telekom Cyber Security Austria empfehlen wir, langfristig zu denken, auch wenn der sehr enge Umsetzungszeitplan zur Eile drängt. Eine einmalige Bewertung der Risikolandschaft und der Maßnahmen kann Ihre Geschäftsprozesse und Assets nicht nachhaltig schützen – und wird auch die Prüfenden nicht überzeugen. Nur mit einem funktionierenden Managementsystem können Sie den Anforderungen von NIS sinnvoll begegnen. Wir unterstützen Sie bei der Umsetzung der geforderten Sicherheitsmaßnahmen, von der Beratung über Assessment zur Bestimmung Ihres aktuellen Sicherheitsniveaus bis hin zur Implementierung konkreter Sicherheitslösungen um Ihre IT/OT-Resilienz nachhaltig zu stärken.

# WERKZEUGE FÜR VERANTWORTUNG

*Eryn Devola, Vice President Sustainability im Industriebereich bei Siemens, über Nachhaltigkeit in Prozessen und Produkten.*

TEXT | MARTIN SZELGRAD

*»Dort Maßnahmen ergreifen, wo es wirklich am meisten Sinn macht«, plädiert Eryn Devola, Siemens, für den Einsatz von Datenwerkzeugen und Analysen für Ressourceneinsparungen in der Wirtschaft.*

Sie sind für Nachhaltigkeit im Industriebereich bei Siemens weltweit verantwortlich. Welche Themen umfasst Ihre Arbeit?

**Eryn Devola:** Im Bereich unseres Portfolios für digitale Industrien sind das unsere Automatisierungslösungen für Prozesse, für diskrete Industrien, unser Motion-Control-Geschäft und das Servicegeschäft, ebenso Engineering-Software. Zum einen geht es um die Nachhaltigkeit bei den eigenen Betriebsabläufen: Fuhrpark, Produktionsstandorte, Geschäftsreisen – wie groß ist der Fußabdruck, den wir in unserer Arbeit hinterlassen? Dann fokussieren wir auf unsere eigenen Hardwareprodukte – wie sie herstellt werden, wie Lieferketten gestaltet sind, wie lange die Produkte dann genutzt werden. Drittens bieten wir Kund*innen Lösungen und Werkzeuge, damit diese selbst in ihrem Geschäft nachhaltiger werden. Das beinhaltet zum Beispiel Konstruktionssoftware, Simulationslösungen oder auch energieeffiziente Motoren und Antriebssysteme. Wir betrachten das Themenfeld Nachhaltigkeit also von innen, ebenso wie von außen mit unserem Angebot am Markt – jeweils angepasst an die Herausforderungen in den unterschiedlichen Branchen. Mit unserer Business-Plattform Xcelerator ergänzen wir unser Portfolio auch mit Lösungen von Partnern.

Sehen Sie hier Herausforderungen, die sich über alle Sektoren, in denen Unternehmen tätig sind, ähneln?

**Devola:** Wir beschäftigen uns stark mit einer neuen Notwendigkeit zu Transparenz und mit Effizienzen und Einsparungen in den Betrieben. Die Menschen müssen wissen, welche Maßnahmen besonders sinnvoll sind und welche Auswirkungen auch ihr eigenes Tun hat. Wir können nur kontrollieren und verbessern, was wir messen können. Meist haben Unternehmen aber keinen Überblick über ihre Daten und Prozesse. Und wenn es bereits Transparenz gibt, dann nur innerhalb des Firmengeländes – nicht über Unternehmensgrenzen hinweg. Nun verlangen Gesetze und Regulierungen aber den Blick auf gesamte Wertschöpfungsketten, von der Herstellung, über die Nutzung bis zum Lebensende und der Wiederverwertung eines Produkts. Das ist ein Riesenwandel, der mit enormer Komplexität verknüpft ist. In den Unternehmen kommt mitunter das Gefühl auf, die Kontrolle über das, was man kennt, zu verlieren. Viele haben sich auch zu Klimazielen bis 2025 oder 2030 bekannt. Diese Jahre rücken jetzt rasch näher. Die selbst auferlegten Ziele, gemeinsam mit dem Regulierungsdruck in der EU durch Richtlinien wie der »Corporate Sustainability Reporting Directive«, erfordern künftig auch eine wesentlich breitere Offenlegung von Daten.

Wie kann eine Transparenz von Ressourcenverbrauch in der Industrie hergestellt werden? Wie ist hier die richtige Strategie für Einsparungen?

**Devola:** Das kommt auf die Branche an. In einer energieintensiven Industrie, wie es etwa die chemische Industrie ist, kann vieles

Fotos: iStock

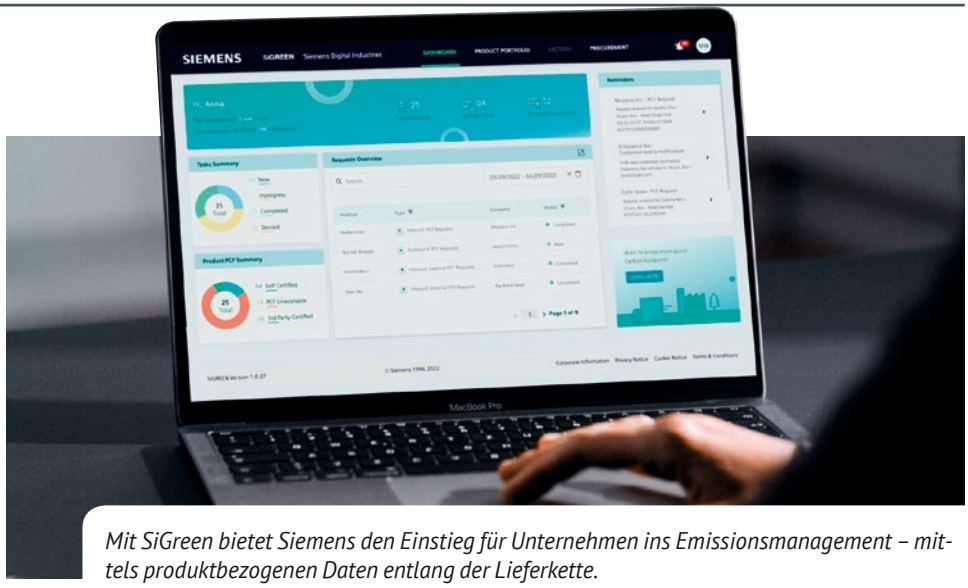
innerhalb der eigenen Prozesse umgesetzt werden. Mit Energiemonitoring können Verbräuche analysiert und optimiert werden. Mit Zählern im oder vor dem Gebäude werden Ressourcenströme gemessen. Ebenso ist das vor jeder Maschine möglich, vor jedem Gerät, rund um die Uhr. Auf dieser Datenbasis können dann auch präzise Maßnahmen ergriffen werden.

Betrachten wir ein Unternehmen in der Automobilbranche, liegen die Herausforderungen zu einem großen Teil außerhalb der eigenen Hallen. Die Wertschöpfungsketten bis zum fertigen Produkt sind hier besonders ausgeprägt. Die Emissionen eines einzelnen Unternehmens sind meist wesentlich geringer als »upstream« bei Partnern in der Lieferkette und »downstream« in der Nutzung des Produkts. Der Trick ist herauszufinden, wo mit dem geringsten Einsatz die größten Effekte erzielt werden. Bei einem Bierproduzenten, der zu unseren Kunden zählt, war das zum Beispiel die Lkw-Flotte in der Logistik. Bei einem Hersteller in einem anderen Markt kann es etwas ganz anderes sein.

Welche Rolle spielen IT und Rechenzentren bei Maßnahmen zur Emissionsreduktion?

**Devola:** Je mehr ich auf digitaler Ebene umsetzen kann, desto weniger muss ich das in der physischen Welt tun. Simulationen, Modellierungen und Analysen können enorm helfen, Ressourcen einzusparen. Doch ist natürlich auch der Energieverbrauch von Rechenzentren ein Faktor – das geht bis zur Art der Software und Anwendungsarchitektur.

Die Klimakrise, der Druck zu Einsparungen und die Auswirkungen von Unternehmen und ihren Produkten auf die Umwelt – das kann den Einzelnen überfordern. Aber ich bin überzeugt: Wenn viele diese Verantwortung erkennen und gemeinsam etwas bewegen, wird dieser Druck weniger. Es gibt sie bereits, die Lösungen, die eine Transparenz auch zum $CO_2$-Fußabdruck in Wertschöpfungsketten ermöglichen – Werkzeuge wie SiGreen von Siemens. Wenn wir alle zusammenhelfen, schaffen wir das. ■




*Mit SiGreen bietet Siemens den Einstieg für Unternehmen ins Emissionsmanagement – mittels produktbezogenen Daten entlang der Lieferkette.*

# Dekarbonisierung beginnt mit Daten

*Nachhaltigkeit gewinnt in der Industrie immer mehr an Bedeutung. Technologieunternehmen und Konsortien zeigen, wie Unternehmen ihre Nachhaltigkeitsziele umsetzen können.*

Sie heißen »SiGreen«, »Catena-X« oder »digitaler Produktpass« – Werkzeuge, Ökosysteme und politisch getriebene Modelle für eine nachhaltige, ressourcenschonende und vor allem transparente Industrie in Europa. Auf der Hannover Messe im April beherrschten die Themen Nachhaltigkeit und Klimawandel Gespräche, Produktvorstellungen und manche Hoffnung auf den Messeständen. So bietet der Technologiekonzern Siemens mit SiGreen Unternehmen die Grundlage, Emissionswerte von Produkten effektiv zu managen – über die ganze Wertschöpfungskette hinweg. Ziel ist, die in Europa gesetzten Klimaziele auch auf Produktebene zu erreichen. Die Lösung liefert die Antwort auf das steigende Bedürfnis nach Transparenz für den $CO_2$-Fußabdruck von Komponenten.

Mit dem europäischen Datenökosystem Gaia-X im Hintergrund, will die Industrie nun in Deutschland mit Catena-X durchstarten. Es sind die großen OEMs im Automobilmarkt und ihre vielen Zulieferer (auch in Österreich), die sich bei diesem ersten kollaborativen und offenen Datenökosystem für die Branche eine Zukunft erhoffen, die im Gemeinsamen liegt. Mit der Plattform sollen die Akteure zu durchgängigen Wertschöpfungsketten verknüpft werden – einfach, sicher und trotzdem weiterhin unabhängig. Das gemeinsame Ziel ist ein standardisierter Datenaustausch und der Anspruch ist Datensouveränität: Wer Daten zur Verfügung stellt, behält die Kontrolle und entscheidet individuell, wer am Datenaustausch wie, wann, wo und unter welchen Bedingungen beteiligt wird.

Ein weiteren Schwerpunkt bildeten in Hannover die künftigen digitalen Produktpässe, die Transparenz bis zum Rohstoff (und möglichweise auch, wie dieser abgebaut wurde) ermöglichen. Der erste Pass – im Prinzip ein aufgeklebter QR-Code, der auf im Netz gespeicherte Daten zu Materialien und Herkünfte der betreffenden Komponente leitet – ist ein Batteriepass für Industrie- und Pkw-Akkus. Die Batterieverordnung ist die erste Maßnahme der Politik, die einen digitalen Produktpass fordert. Dieser soll dazu beitragen, Umweltbelastungen zu reduzieren. Dafür werden Hersteller verpflichtet, sämtliche Emissionen zu dokumentieren, die bei der Herstellung, Nutzung sowie der Entsorgung ihrer Produkte entstehen. Ziel ist die Zweitverwertung und Nachnutzung von großen Batterien.

Erarbeitet werden der Batteriepass und Modelle wie Catena-X stets in Industriekonsortien, auch gemeinsam mit der Forschung. Man hat verstanden, das auch die Absicherung des Wirtschaftsstandort Europa nur gemeinsam funktionieren wird. ■


# KI IN DER ANWENDUNG

## Der Nachbericht zum Publikumsgespräch

*Der Hype um künstliche Intelligenz ist groß – wo stehen wir mit diesen Technologien heute wirklich? In welchen Bereichen sind Lösungen mit Unterstützung durch Machine Learning besonders erfolgreich?*

TEXT | MARTIN SZELGRAD

Bei einem Publikumsgespräch des Report Verlags am 30. März im Bundesrechenzentrum in Wien diskutierten Expert*innen aus Wirtschaft, Forschung und Politik zum Thema »Werkzeugkiste KI« und der aktuellen Gestaltung von Wirtschaft und Verwaltung damit. Die Veranstaltung wurde von AIT, BearingPoint, BRZ und Nagarro unterstützt.

### Die Podiumsteilnehmer*innen:

- **Florian Tursky,** Staatssekretär für Digitalisierung und Telekommunikation im Bundesministerium für Finanzen
- **Andreas Trost,** Teamleiter Productmanagement AI, BRZ
- **Jasmin Lampert,** Senior Data Scientist, AIT Austrian Institute of Technology
- **Sabine Walch,** CEO von danube.ai
- **Thomas Schweiger,** KI-Enthusiast bei Nagarro
- **Martin Beck,** Head of Data Analytics & AI bei BearingPoint Österreich

Fotos zu Event

Fotos: Milena Krobath

## FLORIAN TURSKY

*Staatssekretär für Digitalisierung und Telekommunikation im Bundesministerium für Finanzen*

Welchen Nutzen werden KI-Lösungen für die Menschen bringen? Und welche Herausforderungen sehen Sie hier?

**Florian Tursky:** Wir arbeiten seit vielen Jahren an der Digitalisierung und Modernisierung des öffentlichen Dienstes in Österreich – und setzen dabei auch auf Lösungen mit künstlicher Intelligenz. Mit Angeboten wie ChatGPT haben die Bürger*innen nun die Chance, sich mit den Möglichkeiten durch KI selbst auseinanderzusetzen – das wird der gesamten Entwicklung der Technologie eine enorme Geschwindigkeit verleihen. Für mich ist es so etwas wie ein iPhone-Moment, als 2007 das Smartphone den kompletten Markt verändert hat. Künstliche Intelligenzen werden unser Leben zukünftig einfacher, schneller und bequemer machen. Das wird auch dazu führen, dass wir länger und gesünder leben, aber auch den Energieverbrauch von Technologie reduzieren müssen – an KI werden alle großen Fragen unserer Zeit adressiert. Die Digitalisierung ist ein Prozess, der weltweit stattfindet. Wir sollten jetzt die Chancen nützen, mitzuhalten und den Wohlstand der Bevölkerung in Österreich und in Europa mit Innovation zu sichern. Denn wenn wir bei Technologien wie KI nicht mithalten können, heißt das weniger Wettbewerbsfähigkeit und weniger Wertschöpfung.

Haben wir die richtigen Rahmenbedingungen für Entwicklungen dazu – und auch genügend Fachkräfte? Wie kann hier der Staat noch unterstützend wirken?

**Tursky:** Ich denke, dass wir in Österreich gut aufgestellt sind – zum Beispiel bei Anschubfinanzierungen für Start-ups durch die FFG. Bei weiteren Finanzierungsrunden ab rund einer Million Euro tun sich Jungunternehmen in Österreich schon etwas schwer. Hier müssen wir noch attraktiver werden und auch bessere Rahmenbedingungen für Venture Capital schaffen.

Der Mangel an Fachkräften und auch Arbeitskräften, auch durch den demografischen Wandel, ist wiederum ein Problem, das wir nicht nur in Europa, sondern weltweit haben. Den Highend-Bereich am IT-Arbeitsmarkt in Österreich versuchen wir mit neuen Institutionen und Initiativen, wie die neue TU für Digitalisierung und digitale Transformation in Linz, zu stärken. Wir brauchen allerdings auch in der Bevölkerung mehr Grundverständnis für Digitalisierungsthemen – etwas, das wir mit Maßnahmen im Schulterschluss mit mehreren Ministerien adressieren.

Welche Rolle wird eine Regulierung von KI spielen?

**Tursky:** Eine Regulierung, die aktuell die Europäische Union als einzige Region in der Welt gesetzlich umsetzt, betrachte ich als zentralen Faktor für den Erfolg eines KI-Marktes. Ein gut durchdachtes Regelwerk wie der »EU AI Act« ist sicherlich besser, als Innovation oder Forschung zu verbieten – wozu zuletzt in einem KI-Moratorium aufgerufen wurde. Die KI-Regulierung darf aber nicht zu einem Wettbewerbsnachteil für Europa führen. Sie muss Rechtssicherheit für Unternehmer*innen schaffen, zum Wohle der Konsument*innen. Dazu gehört auch, dass wir niemals ein Social-Scoring-System zulassen oder Konsument*innen aufgrund von Datenanalysen von Angeboten etwa einer Versicherung ausgeschlossen werden dürfen. Mit dem Reallabor-Gesetz werden wir in Europa abgesteckte Räume schaffen, damit sich Innovationen bestmöglich ausbreiten können. Denn es nützt nichts, wenn wir in Europa Musterschüler der Regulierung sind, aber uns links und rechts alle anderen überholen.

*»Ein Regelwerk wie der ›EU AI Act‹ ist besser, als Innovation oder Forschung zu verbieten«, ist Staatssekretär Florian Tursky überzeugt.*

## ANDREAS TROST

*Teamleiter Productmanagement AI, BRZ*

*Andreas Trost, BRZ: »Wir können mit KI-Hilfe Muster und komplexe Zusammenhänge in Daten entdecken.«*

Welchen Ansatz haben Sie mit KI-Lösungen für die Verwaltung?

**Andreas Trost:** Als Kompetenzzentrum für Digitalisierung sehen wir im Bundesrechenzentrum in KI eine große Chance und Innovationstreiber für die öffentliche Verwaltung. Das Einsatzfeld ist sehr breit – von der Unterstützung in der Entscheidungsfindung im Bereich der Prozessautomatisierung intern bis zu den Schnittstellen zu den Bürger*innen. Die Ziele sind stets, Effizienz und Effektivität zu steigern und Systeme zu verbessern. KI bietet nicht die Antworten auf alle Fragen der Digitalisierung, aber es gibt sehr gute Themenfelder für den Einsatz. Wir gehen verantwortungsbewusst mit dem Thema um und setzen KI unterstützend für den Menschen ein – keinesfalls werden autonom Entscheidungen getroffen. Der Mensch hat immer das letzte Wort.

Wie kann Machine Learning speziell im Public Sector unterstützen?

**Trost:** In der Betrugsbekämpfung können als Teil des Risikomanagements Unregelmäßigkeiten in Steuererklärungen, in der Betriebsführung oder auch als Teil der Forensik in beschlagnahmten Dokumenten und Daten mit Hilfe von KI gefunden werden. Mit »supervised learning« anhand von Daten aus der Vergangenheit werden Muster erkannt und komplexe Zusammenhänge entdeckt – was ein Mensch aufgrund der Komplexität übersehen würde. Mit KI werden so die Expert*innen der Betriebsprüfung und Steuerfahndung bei der Auswahl und Bearbeitung ihrer Fälle unterstützt.

Ein weiteres Beispiel aus dem Bereich der Textanalyse ist die automatisierte Anonymisierung von personenbezogenen Daten in Dokumenten aus Gerichtsentscheidungen, die im Rechtsinformationssystem des Bundes veröffentlicht werden. KI hilft auch, um Gesichter auf Fotos aus Gründen des Datenschutzes unkenntlich zu machen oder bei der Beschlagwortung von Bildern in Archiven, um zum Beispiel nach bestimmten Gebäudetypen suchen zu können. Im Bereich der Prognosen und Simulationen gibt es ebenfalls Anwendungsszenarien, zum Beispiel in der wirtschaftlichen Krisenvorsorge. Eine intelligente Prozessautomatisierung senkt den Aufwand bei Bürger*innen und innerhalb der Verwaltung bei vielen Anwendungsfällen. Ein wesentlicher Faktor für den Erfolg von KI ist die Identifikation geeigneter Use-Cases mit hohem Nutzenpotenzial und der Daten in ausreichender Qualität und Quantität, die dafür notwendig sind.

Welche Erfahrungen haben Sie bei der Operationalisierung von Machine Learning und wie stark spielen auch ethische und datenschutzrechtliche Fragestellungen eine Rolle?

**Trost:** Wir setzen uns bereits verstärkt seit einigen Jahren mit dem Thema Ethik und KI sorgfältig auseinander, beispielsweise mit einem eigenen Prüfkatalog für vertrauenswürdige KI. Mit unserem Rechenzentrum in Österreich haben wir bei der Datenhaltung und beim Betrieb von KI-Diensten einen großen Vorteil. Unsere Stärke ist es, KI-Anwendungen vom ersten Prototyp bis zum laufenden Echtbetrieb verantwortungsbewusst zu begleiten. Der Nutzen von KI entsteht vor allem im laufenden Einsatz, als Teil der Geschäftsprozesse. Das benötigt stets die Zusammenarbeit verschiedener Akteure: Datentechniker*innen, Systemtechniker*innen, Data Scientists, Fachbereich, Kund*innen-Vertreter, aber auch Business Sponsors, Rechtsabteilung und viele mehr. Nur so werden Projekte gelingen.

## JASMIN LAMPERT

*Senior Data Scientist, AIT Austrian Institute of Technology*

Was unternehmen Sie mit dem AIT in diesem Bereich?

**Jasmin Lampert:** Das Safety and Security Center ist ebenso wie alle anderen Bereiche des AIT an der Schnittstelle zwischen Forschung und Wirtschaft. In den industrienahen Projekten unseres Teams arbeiten wir oft mit Partnern aus der produzierenden Industrie zusammen. Der Produktionsbereich bietet ein klassisches Themenfeld für den Einsatz von KI und allgemein auch Data Science – etwa für eine automatische Qualitätssicherung oder auch für Analysen von Maschinendaten. Kein Mensch könnte diese Riesendatenmengen manuell durchgehen, aber aus den historischen Daten kann sehr wohl rechtzeitig bei sich abzeichnenden fehlerhaften Produktionsprozessen reagiert werden.

Auch bei Forschungsfragen rund um den Klimawandel versuchen wir, die Effekte aus Maßnahmen nicht nur für einen isolierten Bereich wie die Mobilität, sondern im Gesamtsystem zu begreifen. Welche klimabezogenen Folgen hat eine politische Regulierung etwa im Bereich Landwirtschaft auf andere Sektoren? Welche Folgen

Fotos: Milena Krobath

*Jasmin Lampert, AIT: »KI kann sehr große Datenmengen verarbeiten.«*

haben höhere Durchschnittstemperaturen im Anbau auf den Einsatz von bestimmten Feldfrüchten und letztlich auch auf die Lebensmittelpreise und die Nachfrage bei den Konsument*innen? Bei diesen Fragestellungen ist immer auch das große Bild erforderlich.

Was sind die Erwartungen an KI in Unternehmen? Was kann KI heute besser als starre Algorithmen – und was nicht?

**Lampert:** Die Erwartungen sind groß, dass eine KI einfach »out-of-the-box« etwas mit Unternehmensdaten macht, über die man ja bereits verfügt. Oft ist auf Nachfrage dann aber die Datenqualität nicht mehr so klar – oder die Daten können externen Partnern nicht einfach zur Verfügung gestellt werden. KI kann sehr große Datenmengen verarbeiten und in diesen Zusammenhänge erkennen, die komplex und nicht linear sind. Umgekehrt kann sie keine Aussagen über Ereignisse und Dinge treffen, die sie nicht vorher bereits in den Daten gesehen hat. In der Praxis gibt es bereits viele Einsatzbereiche von KI, mit denen wir schon in Berührung gekommen sind. So etwa am Smartphone, das ein Foto aufnimmt, sobald man in die Kamera lächelt. In der Medizin und Diagnostik werden auf Röntgen- und MRT-Bildern mit Machine Learning Krebsgewebe gesucht. Auch in der Pandemie wurden mit KI-Anwendungen Analysen durchgeführt, ob jemand an Corona erkrankt ist. Diese Werkzeuge im Gesundheitsbereich sind insbesondere für Entwicklungsländer spannend, in denen wenige medizinische Fachkräfte vor Ort sind.

Ein weiteres Projekt des AIT fokussiert sich auf die Erkennung von Hate Speech im Netz. Auch hier kann ein*e Redakteur*in allein nicht die riesigen Datenmengen von Texten und Videos durchforsten. Mit entsprechenden Sprachmodellen kann hier bereits viel vorgefiltert und erkannt werden. Und ich bin derzeit im Projekt AI4Trees tätig, bei dem wir verstehen wollen, wie sich Baumwachstum abhängig von den klimatischen Bedingungen auf eine Spezies heruntergebrochen entwickelt.

## SABINE WALCH

*CEO danube.ai*

Was macht danube.ai? In welchem Bereich setzen Sie AI ein und was haben die Anwender*innen davon?

**Sabine Walch:** Als AI-Unternehmen aus Österreich ist es uns wichtig, dass KI einen Mehrwert für jede*n Einzelne*n bietet. Unsere KI hilft Personen, Entscheidungen zu treffen und vor allem das perfekte Produkt zu finden. Wir begegnen im Internet einer Fülle von Möglichkeiten. Um genau das persönlich richtige Angebot zu finden, bedarf es unserer Assistenz-KI. Wir haben sie – ähnlich der Idee von Suchmaschinen – nach zweijähriger Entwicklungszeit für Produkte, Medienartikel, Entertainment und sogar für Themenstellungen im HR-Bereich gelöst. Eingesetzt wird es zum Beispiel auf Geizhals, denn kein Mensch kann Informationen aus 10.000 Smartphones durchsuchen und vergleichen. Eine Maschine übernimmt das liebend gerne.

Auf welchem Entwicklungsstand sehen Sie das KI-Thema generell?

**Walch:** Wir alle sind Zeitzeug*innen einer exponentiellen Entwicklung von KI. ChatGPT hat mit Beginn November 2022 die Technologie für die Massen aufbereitet. Selbst meine Eltern können nun eine KI-Lösung auf einfache Art über ein Eingabefeld nutzen, das einer üblichen Suchleiste gleicht. Die Nutzer*innen müssen nicht besonders technologieaffin sein und sie müssen auch nicht wissen, dass dahinter eine KI steckt. Ich erhoffe mir dadurch einen Boris-Becker-Effekt – ähnlich der Bewegung, als in den 1980er-Jahren die Menschen in die Tennisclubs gepilgert sind. Auch die Fachbereiche und die Entwicklungsabteilungen in der Wirtschaft und Verwaltung sehen jetzt die Möglichkeiten und wollen diese nutzen – oder überlegen, wie sie KI in ihren Prozessen einsetzen können.

Haben wir die richtigen Ausbildungen in Österreich dafür?

**Walch:** Die Johannes Kepler Universität in Linz war eine der ersten Hochschulen in Europa, die KI als vollständiges Studium angeboten hatte – mit den ersten Absolvent*innen im Jahr 2021. Trotzdem werden die Ausbildungsplätze in ganz Österreich bei weitem aktuell nicht die Nachfrage in der Industrie und Wirtschaft decken können. Hier ist sicherlich noch eine Entwicklung auch im Bildungsbereich gefragt. Das Thema ist jedenfalls auch eine Querschnittmaterie in vielen Bereichen. Nutzen wir jene Fachkräfte in den Unternehmen dafür, die wir haben.

*Sabine Walch, danube.ai: »Wir alle sind Zeitzeug*innen einer exponentiellen Entwicklung von KI.«*

DAS KURZVIDEO ZUM EVENT

*Thomas Schweiger, Nagarro: »Lösungen für die Unterstützung bei überlasteten Berufsfeldern.«*

## THOMAS SCHWEIGER

*KI-Enthusiast bei Nagarro*

Was muss man über diese Technologie und die Tools und Plattformen wissen? Wie sehr ist dieses Wissen auch in den Unternehmen bereits vorhanden?

**Thomas Schweiger:** Wir beobachten auch bei unseren Unternehmenskunden, dass das Thema KI immer noch mit einem gewissen Mythos behaftet ist. Viele beschäftigen sich damit, aber die Vorstellungen zum Einsatz in der Praxis und auch die Grenzen der Lösungen gehen weit auseinander.

Bei Nagarro versuchen wir jedenfalls, den Zugang zu KI menschlich zu gestalten. Die Lösungen sollen nicht Jobs einsparen, sondern zur Unterstützung bei überlasteten Berufsfeldern eingesetzt werden. Sie sollen Menschen von wiederkehrenden Tätigkeiten befreien, damit diese ihre Kernaufgaben besser erfüllen oder vielleicht auch wieder am Menschen serviceorientierter arbeiten können.

Für uns ist KI ein wichtiges Werkzeug, aber es ist nicht die Lösung für jede Problemstellung. Wir versuchen hier einen pragmatischen Zugang. Häufig können Anforderungen unserer Kund*innen auch mit traditionellen IT-Lösungen erfüllt werden. Dennoch wird es für die Zukunft wichtig sein, Wissen zu KI im eigenen Unternehmen aufzubauen. Viele Unternehmen in Österreich beschäftigen sich bereits damit, haben auch erste Prototypen initiiert, skalieren diese aber noch nicht. Natürlich kann man auch erst einmal abwarten, um dann fertige Lösungen vom Markt einzusetzen.

Wo befinden sich aus Ihrer Sicht die größten Hebel und gute Schnittstellen für die Zusammenarbeit von Mensch und Maschine?

**Schweiger:** KI kann beispielsweise den Arbeitsalltag im Software-Testing erleichtern. Wenn Tests automatisiert werden, geschieht das über Scripts, die dafür geschrieben werden. Bei voranschreitender Automatisation kommt man irgendwann an den Punkt, an dem die Bearbeitung der Tests und die Auswertung der Ergebnisse mehr Zeit beansprucht als die eigentliche Weiterentwicklung. Software-Testing beschäftigt sich dann nur noch mit sich selbst. Wir versuchen mit Machine Learning und KI-Technik diese Wartungsprozesse zu automatisieren, indem wir das Wissen von Tester*innen in Modelle gießen, um damit die Menschen von wiederkehrenden Themen in den Testanalysen zu befreien. Wenn es entsprechend richtig und positiv kommuniziert wird, lassen sich auch die Vorbehalte gegen KI-Unterstützung in Unternehmen aus dem Weg räumen.

Weitere Beispiele sind eine Anonymisierung von Maschinendaten aus sensiblen Produktionsprozessen mit Hilfe von KI oder die Optimierung von Routen in der Logistik und auch effizientere Beladungen von Lkw.

Natürlich gibt es auch Grenzen einer KI. Wenn ich ein Lager plane, Lagermanagement betreibe und dann entscheidet ein*e Mitarbeiter*in, im Supermarkt ein Regal neu anzuordnen, sind das Informationen, die ein System nicht hat. Eine KI kann lediglich innerhalb eines bestimmten Lösungsraums rechnen, der Mensch stets darüber hinaus. Den Erfolg macht dann das unterstützende Werkzeug in der Hand der menschlichen Entscheider*innen aus.

Fotos: Milena Krobath

*Martin Beck, BearingPoint: »Wir bringen die Themen KI und Daten auf den Boden der Praxis.«*


*Diskussion im Bundesrechenzentrum zu den Anwendungsmöglichkeiten von KI in der Wirtschaft, Wissenschaft und Verwaltung.*

## MARTIN BECK

*Head of Data Analytics & AI BearingPoint Österreich*

➲ Was bietet BearingPoint in diesem Bereich? Welche Projekte wurden im deutschsprachigen Raum bereits umgesetzt?

**Martin Beck:** Als Partner für Unternehmen in Europa agieren wir bei BearingPoint gesamtheitlich im Bereich Daten. Dabei setzen wir auch KI-Projekte um, wollen aber auch Organisationen befähigen, den eingeschlagenen Weg selbstständig weiterzugehen. BearingPoint arbeitet beispielsweise im öffentlichen Sektor in Deutschland an der Definition und Umsetzung einer ganzheitlichen Datenstrategie. Zusätzlich werden aktuell Projekte zur Entwicklung von schnelleren Dienstleistungen und rascheren Antwortzeiten umgesetzt, die auch Chatbots und RPA (Anm. »Robotic Prozess Automation«) nutzen. Wir implementieren und bauen Innovationszentren, sogenannte KI-Geschäftsstellen auf, um auch in der Öffentlichkeit das Thema KI und das Thema Daten zu fördern und dazu Projekte auf den Boden zu bringen.

➲ Bevor ein Unternehmen oder eine Organisation in ein KI-Projekt geht – welche Themen und Bereiche sollten gut überlegt und geregelt werden?

**Beck:** Studien zufolge schlagen 80 Prozent aller KI-Projekte fehl. Am Ende eines Projekts muss klar der Nutzen für die Anwender*innen stehen, sonst wird die Lösung nicht angewandt. Auch im Jahr 2023 brauchen Unternehmen eine Datenstrategie – das können wir nicht oft genug betonen. Welcher Mehrwert soll erzeugt werden? Wer wird die Lösung nutzen? Und was brauchen die Menschen dafür – auch hinsichtlich Ausbildungen, Skills und Organisation? Als Unterbau ist in Unternehmen unbedingt eine Data Governance oder auch KI Governance erforderlich – auch für den laufenden Betrieb, inklusive Prüfthemen und Sicherstellen von nachhaltig ethisch korrekten Prozessen.

➲ Wie gut tut sich generell die Verwaltung in Österreich damit?

**Beck:** Bei digitalen Services ist die österreichische Verwaltung Vorreiter. Ein Strafregisterauszug ist hierzulande mit wenigen Klicks online erledigt, während man in Deutschland dazu noch aufs Amt gehen muss – und das Dokument mit der Post zugeschickt wird. Den Vorsprung in Europa könnten wir aber im KI-Bereich verlieren, wenn man beispielsweise das aktuelle Budget Deutschlands für KI-Lösungen in den Bundesministerien in der Größenordnung von 350 Millionen Euro sieht.

➲ Was ist für Sie ein weitere s gutes Anwendungsbeispiel für KI?

**Beck:** Die Meldung und Begutachtung eines Wasserschadens ist oft ein langwieriger Prozess für die Versicherten ebenso wie für Versicherungsunternehmen – inklusive Termin vor Ort mit einem Sachverständigen. Wir haben gemeinsam mit einem Versicherer und einer Immobilienverwaltung eine Lösung umgesetzt, mit der über Smartphone-Fotos, Bilderkennung mit Computer Vision und der Eingabe von grundlegenden Daten – etwa zum Alter des Gebäudes – eine Schadenshöhe in Sekundenschnelle übermittelt wird. Das Ergebnis wird vom Versicherer akzeptiert, die Bearbeitungsprozesse zum Schaden werden automatisch in Gang gesetzt. ■

# Vom verschränkten Teilchen zum perfekten Material

*Es ist mehr ein Annähern, als Verstehen, spricht Alexander Glätzle von der Forschung rund um Quantentechnologien. Mit planqc will der gebürtige Tiroler von München aus Anwendungen für die Wirtschaft bauen, die eine neue Ära des Computing einleiten werden.*

TEXT | MARTIN SZELGRAD

Sie war im Vorjahr die erste Ausgründung des Standorts »Munich Quantum Valley«, um Quantentechnologie aus dem Forschungsbereich des Max-Planck-Instituts für Quantenoptik auf eine kommerzielle Ebene zu heben. In dem Unternehmen planqc setzt man auf einzelne Atome, die mit großer Präzision gekühlt, eingefangen und bearbeitet werden. »Wenn man weiß, wo sich das Atom im Raum genau befindet, kann es über einen Laser manipuliert werden – zum Beispiel, um eine logische Null oder Eins abzuspeichern«, erklärt Alexander Glätzle, Co-Founder und CEO von planqc. Er verändert mit einem hochpräzise gebündelten Lichtstrahl den Spin von Elektronen. Dreht sich das Elementarteilchen nach links, nimmt es einen Wert ein, dreht es sich nach rechts, einen anderen Wert.

*Das Gründungsteam von planqc: Sebastian Blatt (CTO), Alexander Glätzle (CEO) und Johannes Zeiher (Principal Scientist).*

## NEUER LEVEL

Die Physik herkömmlicher Leiterplatten- und Mikrochip-Technologie kommt mit den möglichen Leistungen und dem Platzbedarf an ihre Grenzen. In den vergangenen Jahren wurden unterschiedliche Technologien entdeckt, um die Disziplin Computing vielleicht für alle Zeit zu verändern. Alle Verfahren eint, Schaltkreise auf eine noch kleinere Ebene zu reduzieren, auf atomaren Level in Gitterstrukturen – Qubits genannt. In München wird seit Jahren an einem Verfahren geforscht, bei dem Atome in einem dreidimensionalen Lichtkristall gefangen und anhand der Intensität von Lichtstrahlen manipuliert werden. Strontium wird in einem »Ofen« aufgeheizt und verdampft, die Teilchen werden von einer Anfangsgeschwindigkeit von 200 Metern pro Sekunde in mehreren Schritten auf wenige Zentimeter pro Sekunde gebremst. Für jeden Rechenschritt wird der »Array« geladen, um die Atome in den Tälern des Lichtwellenrasters des Lasers – einer so genannten Stehwelle – anzuordnen. Nach dem Rechenschritt wird das Licht abgedreht und die Vakuumkammer entleert, der Prozess beginnt von neuem; vollautomatisch auf Knopfdruck, in einer Dauer von wenigen Millisekunden. Auf diese Weise werden auch künftige Quantenrechner gebaut werden und funktionieren, erklärt Glätzle.

Renommierte Forschungseinrichtungen wie das Max-Planck-Institut und ihre institutionellen Partner haben getreu ihren Statuten aktuell keine Möglichkeit, ihre Erfindungen zu kommerzialisieren – nicht einmal in gemeinsamen Projekten mit der Industrie. Glätzle will mit den planqc-Gründungspartnern Sebastian Blatt und Johannes Zeiher, die selbst in leitenden Funktionen am Max-Planck-Institut tätig sind, diese Lücke füllen und beispielsweise Fahrzeugherstellern den Zugang zu Quantensimulatoren verschaffen. »Wir tragen die Technologie in die Wirtschaft, bieten ein ›Testbed‹ und dienen auch als Plattform für weitere Entwicklungsarbeiten«, betont der Forscher, der zuvor in Oxford studiert hat. planqc agiert als eigenständiges Unternehmen, sieht seine Zukunft aber in einer engen Kooperation für die Nutzungsrech-

Fotos: Dirk Brunieki

*In München wird an den Computingtechnologien der Zukunft gebaut – mit gebündeltem Licht werden Atome in Gattern angeordnet.*

te an der Technologie – über einen Vertrag zur »Intellectual Property« (IP). Mit dem Standort Gaching ist planqc in unmittelbarer Nähe zum Münchener Insitutscampus. »Diese Synergie ist für uns extrem wichtig. Allein die Labors, die auf ein Zehntelgrad präzise klimatisiert werden können, kosten eine Riesensumme. Ein Start-up könnte das kaum auf eigene Faust stemmen«, weiß der gebürtige Tiroler.

## NAHE AN WELTSPITZE

Für die Qubits, mit denen Nullen und Einser abgespeichert werden, setzt man in München auf das Element Strontium. Es wird bereits seit Jahrzehnten in den weltweit präzisesten Atomuhren verwendet. Es ist in seinem Aufbau und Wechselwirkungen extrem stabil und kohärent. Quanteneffekte können damit für rund eine halbe Minute aufrechterhalten werden – das ist auf einer atomaren Skala vergleichsweise lange.

Der Forscher bringt ein anschauliches Beispiel, das in seiner Dimension menschlich trotzdem kaum zu fassen ist: Hätte man zwei Strontium-Atomuhren zu Beginn unseres Universums gestartet, wären sie heute – gut 14 Milliarden Jahre später – lediglich eine Sekunde außer Takt. Auch Quantensensoren, ein weiteres Feld einer wohl bald boomenden Quantenwirtschaft, werden damit gebaut werden. Zieht man benachbarte Strontium-Teilchen nur einen Millimeter auseinander, lässt sich aufgrund ihrer Sensitivität bereits ein Gravitationsunterschied messen. Damit werden sich Schwankungen im Erdmagnetfeld beispielsweise in der Ölindustrie oder in anderen Industrien messen lassen, um Lagerstätten im Boden zu orten.

Am Max-Plank-Institut wird aktuell ein Labordemonstrator in der Größe von 20 Qubits gebaut. »Die Zahl der Qubits ist aber nur ein Faktor beim Erfolg von Quantenrechnern, man muss auch auf die Qualität der Gatter achten«, erläutert Glätzle. In München wird zunächst eine »Gatter-Fidelity« von 99,5 – zwei Jahre später, 2026, eine Größe von 400 Qubits mit einer Vitalität von 99,9 – erreicht werden. »Und das wäre dann schon sehr nah an der Weltspitze«, ist der Forscher überzeugt.

## NATÜRLICH VORKOMMEND

IBM hat aktuell einen Quantencomputer vorgestellt, der 400 Qubits schafft – über die Gatterqualität gäbe es aber noch keine seriösen Aussagen. Der Forscher vermutet, dass die Qualität, die man selbst 2026 anpeilt, heute noch nicht erreicht werden kann. IBM und andere arbeiten mit einer Quantentechnologie, die auf Supraleitung und künstlichen Qubits basiert. Dabei werden makroskopische Objekte auf kritische Temperaturen heruntergekühlt. Im Phasenübergang verhalten sich Objekt und Ströme im Inneren einem Qubit-Modell ähnlich. »Bei unserer Technologie müssen wir diese Qubits nicht extra fertigen und wir arbeiten bei Zimmertemperatur. Mit Strontium haben wir auch eine Qubit-Basis, die direkt in der Natur vorkommt«, erklärt er. Die Herausforderung für das planqc-Team liegt vielmehr im Bau der Geometrie des Gatters und in der Kontrolle der Datenpunkte mittels Laserimpulsen.

Welche Leistungen können nun künftig von Quantencomputern erwartet werden? Als Quantenteilchen können Qubits verschränkte Zustände einnehmen. Es ist diese Ressource, die diese Technologie so besonders macht. Verschränkt bedeutet, Korrelation von Atomen über Raum und Zeit hinweg. Würde der Zustand von Atom A auf der Erde aufgrund einer Messung verändert werden, hätte dies augenblicklich – Physiker*innen sprechen von »instantan« – eine Auswirkung auf Atom B, beispielsweise auf dem Mars. Das Phänomen wird seit Einsteins Relativitätstheorie theoretisch diskutiert. Dass nichts schneller als Licht sein kann, hat die Verschränkung von Atomen nun widerlegt. Auch Nobelpreisträger Anton Zeilinger wurde für Forschung rund um diesen Effekt ausgezeichnet. Aber die Wissenschaft steht trotz der ersten Erkenntnisse an einem Anfang.

Ein Ergebnis aus den nächsten Jahrzehnten Forschungsarbeiten könnte ein besseres Verständnis sein, wie unser Universum aufgebaut ist. »Wenn jemand behauptet, Quantenmechanik verstanden zu haben, dann hat er sie definitiv nicht verstanden«, zitiert Alexander Glätzle den früheren MIT-Physiker Richard Feynman. »Wir Menschen tun uns damit schwer. Es fehlt die Sprache, Quantenvorgänge zu beschreiben«, gibt der Österreicher zu. Doch stünde Quantenmechanik auf einem soliden mathematischen Gebäude. »Mit Mathematik lässt sie sich beschreiben. Sie ist die Grundlage für die Quantenrevolution, die nun auch die Anwendungen bringen wird.«

Neben Verschlüsselungstechnologien und allgemeinen komplexen Simulationen, die große Rechenleistungen erfordern, ist für den planqc-CEO vor allem Materialforschung ein Gebiet, das von Quantencomputing profitieren wird. Moleküle und ihr Verhalten in unterschiedlichsten Zuständen exakt zu beschreiben – dazu sind die größten herkömmlichen Rechner noch nicht in der Lage. Mit der neuen leistungsfähigen Technologie wird es möglich sein, neue Medikamente oder Materialien wie etwa für Batterien nahezu unbegrenzt simulieren zu können. So werden ideale Lösungen möglich, perfekte Materialen.

# #COOL STUFF

TEXT | SARAH BLOOS

## STYLE-FAKTOR

Man sollte meinen, ein Laptop kann nicht viel zur eigenen Coolness beitragen. Elektronik-Pionier LG beweist uns das Gegenteil: Die neuen Notebooks der »LG gram Style«-Serie besitzen nicht nur OLED-Displays, performancestarke Intel Core i7-Prozessoren, 16 GB Arbeitsspeicher und Full-HD-Infrarot-Webcams, sondern sind auch ungemein elegant. Wer hinter dem perlmuttartig schimmernden Bildschirm (in 14 oder 16 Zoll) sitzt, ist da fast Nebensache. Ein zusätzliches Designelement ist das im schneeweißen Exterieur optisch »versteckte« Touchpad, das bei Berührung sanft aufleuchtet. Dank mindestens 72 Wh Akku-Kapazität kann man sich im Café cool an den Tisch der Wahl setzen. Ob man am Laptop auch wirklich gearbeitet hat, wird dank LG Glance niemand erfahren. Die KI-Funktion warnt Benutzer*innen vor ungewollten Schulterblicken und verblendet gegebenenfalls die Anzeige am Bildschirm.


**LG | LG gram Style | Preis (14"): 2.199 Euro**
**https://www.lg.com/de/notebooks**


## SCHLAUES FAHRRAD

Es war im Grunde nur eine Frage der Zeit: Nach klugen Autos kommen jetzt intelligente E-Bikes. Acer legt mit dem »ebii« vor: Das KI-betriebene »Smartbike« analysiert die Fahrweise und unterstützt automatisch je nach gewünschtem Assistenzlevel. Je mehr Zeit Fahrer*in und Fahrrad miteinander verbringen, desto besser wird der Algorithmus – für ein intuitives, reibungsloses Fahrerlebnis. Auch sicher darf man sich fühlen: Mit Sensoren ausgestattet erkennt die KI andere Fahrzeuge oder Hindernisse und warnt vor Kollisionen. Ist ihr*e Eigentümer*in nicht in der Nähe, verwehrt ebii Fahrraddieben die Fahrt und sperrt die Pedale, und wird das teure Rad doch eingesackt, kann man es über GPS-Signal tracken. Aber eigentlich soll ein Fahrrad ja nur transportieren und bestenfalls praktisch sein. Zum Glück kann ebii auch das: Auf eine Akkuladung (rund zweieinhalb Stunden) kommt eine Reichweite von 110 km. Dank Aluminiumrahmen ist das Rad mit 16 kg recht leicht, und dank Styroporreifen der Marke Air Fom kann es auch keinen Platten bekommen.

**Acer | Acer ebii | Preis & Verfügbarkeit: noch nicht veröffentlicht**
**https://www.acer.com/ebii**

Fotos: iHersteller

## IMMER FROSTIG

Pünktlich zum Sommeranfang hat Anker eine neue Kickstarter-Kampagne gestartet: Der »EverFrost Powered Cooler« wirbt mit dem sagenhaften Versprechen immerwährender Kühlung – leider nicht für Menschen, aber zumindest für unsere Vorräte. Die batteriebetriebene Kühlbox mit einer Leistung von 299 Wh kühlt Lebensmittel innerhalb einer halben Stunde von warmer Raumtemperatur auf null Grad herunter. Im Gegensatz zu anderen Kühlboxen braucht sie dafür aber weder Eis noch ein ständiges Ladekabel: Der Kühlbox-Akku hält bis zu 42 Stunden und kann variabel oder umweltfreundlich mit Solarpaneel aufgeladen werden. Die Box wird in drei verschiedenen Größenvarianten erhältlich sein (33, 43 und 53 Liter Fassungsvermögen), die Maxi-Größe erlaubt sogar Dual-Zone-Cooling – Gefrierschrank im einen, Kühlschrank im anderen Fach. All das, auch Temperatur und Performance, lässt sich wie so vieles heutzutage bequem per Smartphone-App steuern. Erhältlich ist der »EverFrost«-Cooler laut Kickstarter ab Juni 2023 – der Sommer kann also kommen.

**Anker | Anker EverFrost Powered Cooler | Preis (auf Kickstarter): 615 Euro**
**www.anker.com/everfrost-powered-cooler**

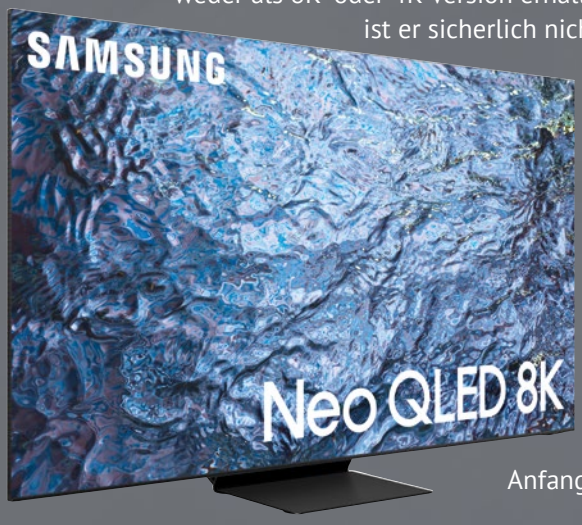
## »DU VERBRAUCHST ZU VIEL STROM!«

... Das konnte man bis dato zwar zu Partner*in oder anderen Mitbewohner*innen sagen, aber nicht beweisen. Wer harte Fakten schaffen will, greift zu Monitoring-Geräten wie der Smarten Steckdose von Eve Energy. Kombiniert mit beispielsweise einer Alexa lassen sich damit eingesteckte Lampen, Fernseher und Toaster per Sprachbefehl ein- und ausschalten – oder einfach via App ansteuern. In ebenjener App findet man außerdem einen Überblick über den Stromverbrauch, kann Zeitpläne erstellen und Geräte auch von unterwegs ausschalten, wenn man jemanden ärgern will. Sicherlich auch wichtig, wenn es um Smart Home geht: Für die Nutzung muss man sich nirgends registrieren, auch Nutzungsdaten werden nicht erhoben. Nur man selbst und die Mitbewohner*innen, die man zum Stromsparen animiert, wissen Bescheid. Aber das ist ja nur gut fürs Klima – und fürs Geldbörsel.

**Eve Energy | Smarte Steckdose | Preis: 39, 95 Euro**
**https://www.evehome.com/de/eve-energy**

## MITTEN IM GESCHEHEN

Auf der Elektronikfachmesse CES hat Samsung einige Tech-Schmankerl für 2023 angekündigt, besonders Fernseh-Fans kommen dabei auf ihre Kosten. Der Neo QLED ist bereits auf dem Markt und erfreut mit hochauflösender Bildqualität, Farbenspiel und Helligkeit in sagenhaften 8K. Durch KI-Upscaling können auf dem Infinity-Screen SDR-Inhalte wie Filme, Serien oder Spiele in HDR-Qualität geschaut werden – und zwar in Echtzeit. Zum wahren Erlebnis wird das Fernsehen durch Dolby-Atmos 360-Grad-Surround-Sound und OTS-Funktion (Object Tracking Sound), die das Publikum mitten ins Geschehen katapultieren. Der Smart-TV ist in verschiedenen Größen und entweder als 8K- oder 4K-Version erhältlich. Nur eines ist er sicherlich nicht – ein Schnäppchen. Dafür aber eine lohnende Investition in einen gelungenen Fernsehabend. Wer weniger Budget hat, findet vielleicht an der neuen OLED-Reihe von Samsung Gefallen: Sie erscheint Anfang Mai.




**Samsung | Neo QLED 8K | Preis (85"): 9.999 Euro**
**https://www.samsung.com/at/tvs/qled-tv**

# Zukunftsfit

EINE PROKRASTINATION VON RAINER SIGL

*Wer morgen vorn dabei sein will, darf nicht mit den Mitteln von gestern planen. Wer Weitsicht hat, wartet stattdessen auf die Technik von übermorgen.*

DER KANZLER WEIST MIT EINER KANTIGEN KINN-BEWEGUNG DEN WEG.

Schauen Sie, ich hab da ja auch schon schlaflose Nächte gehabt deswegen. Wegen allem. Wegen dem Klima. Wegen der Inflation. Wegen dem Pflegenotstand, der Pensionslücke, den Antibiotikaresistenzen, dem Bevölkerungswachstum und dem allem. Und neulich, wie ich so im Halbschlaf dahindämmernd im dumpfen Jammertal meiner Sorgen wandere, erscheint mir in einem Glorienschein aus Dieselgasen und Lagerhausneonröhrenlicht der Kanzler und weist mir mit einer kantigen Kinnbewegung den Weg in die Zukunft. eFuels!

## DIE AUGEN GEÖFFNET

Also, nicht dass eFuels konkret jetzt die Lösung für irgendein Problem wären. Weil, in Wirklichkeit versteht das schon ein durchschnittlich begabtes Kindergartenkind, dass es irgendwie ein Blödsinn ist, einen Faschingskrapfen auszupressen, wenn man eine Marillenmarmelade will. Allein dieser einleuchtende Vergleich müsste bei nicht von Boulevardschnodder zugegeifertem Frontallappen schon dazu führen, dass selbst der begeistertste Benzinbruder achselzuckend resigniert und kleinlaut den Verbrenner einmottet, und trotzdem hat mir diese geniale Nebelgranate die Augen geöffnet. Weil: Wieso die Probleme von morgen heute schon angehen, wenn ich sie mit der Technologie von übermorgen vielleicht gar nicht so richtig ernst nehmen muss? Dafür steht stellvertretend mein Schlachtruf, mit dem ich von nun an den Sorgen übers Morgen begegne: eFuels!

Ich sag Ihnen: Es hat mich durchzuckt wie ein Blitz und seitdem schlaf ich wie ein Baby, ich schwör. Ab jetzt mach ich mir keine Sorgen mehr über die Klimakrise, weil mein Flugauto fährt sicher mit biologisch angebautem Gänseblümchen-Hack. eFuels! Ich zermartere mir endlich nimmer den Kopf wegen Pflegebedarf im hohen Alter, weil bis dahin knuddelt mich sowieso sicher jeden Abend eine attraktive Roboterpflegekraft in den Schlaf. eFuels! Antibiotikaresistenz? Braucht keiner, in Kürze gibt's sicher eine neue Generation hyperpotenter Homöopathika, die noch weniger Wirkstoff und damit noch mehr Power haben und folglich ratzfatz vom Wimmerl am Popsch bis zum Hirntumor alles wegpotenzieren. eFuels! Sorgen wegen der Pensionslücke? Papperlapapp, bis dahin hab ich schon zig Mal im Lotto gewonnen. Ich muss nur schauen, dass ich mal spiele. Mach ich sicher noch rechtzeitig – Ehrenwort! eFuels! eFuels! eFuels!

## KEINE SORGEN MEHR

Sehen Sie, jetzt geht's mir schon viel besser. Herrlich, wenn man die Last der Zukunft auf die Zukunft verschieben kann. Ich sag Ihnen: Das hätt ich schon viel früher machen sollen!

Wie bitte? Ob ich was riech? Der Rauch? Ja, haha, ich weiß eh: Im Erdgeschoß brennt irgendwas, vermutlich die Küche. Ja, ein bissi unangenehm, oder? Wie meinen? Ob ich was dagegen machen will? Pfff, machen Sie sich mal keine Sorgen: Mir fällt sicher irgendwas ein. Morgen vermutlich. Oder übermorgen. Sie werden sehen: Auf mich ist Verlass. Ehrenwort. eFuels!

Foto: iStock

# publikumsgespräche des Report Verlag

## Infos unter:

### Wirtschaft im Klimawandel

Drängende Klimaziele und gleichzeitig der wachsende Bedarf an Energie stellen die Wirtschaft vor riesige Herausforderungen. Welche Möglichkeiten gibt es für Unternehmen, klimafreundlich und trotzdem leistbar zu bauen, zu produzieren und Dienstleistungen zu erbringen? Wo liegen noch Hürden für die Dekarbonisierung unserer Wirtschaft und Gesellschaft?

**Wann:** 9. Mai, Beginn 17:00, Dauer 90 min
**Wo:** A1 Telekom Austria, Lassallestraße 9, 1020 Wien

**Aktuelle Informationen unter www.report.at/mehr/reporttalk**


T Systems
Let's power
higher performance
RETHINK
THE
CLOUD
WIE SCHAFFEN WIR ES,
UNSERE ZUKUNFT MIT
BEGRENZTEN RESSOURCEN
NACHHALTIG ZU GESTALTEN?
Zusammen Innovationen
nachhaltig umsetzen.
Jetzt mehr erfahren:
t-systems.at