# die wirtschaft

5

2021

seit 1945 • www.die-wirtschaft.at • facebook.com/diewirtschaft


SCHWER PUNKT **SICHERHEIT**

# ES KANN JEDEN TREFFEN

Die Anzahl von Cyberattacken steigt rasant. Wer die Angreifer sind und warum KMU am meisten gefährdet sind, erklärt Oberst Walter J. Unger, Leiter der Abteilung für Cyberdefence und IKT-Sicherheit im Abwehramt des österreichischen Bundesheeres.

COVERSTORY
**WISSEN IST MACHT**
Wie Unternehmen wertvolles Know-how pflegen und schützen


Österreichische Post AG, MZ 02Z030737 M, Österr. Wirtschaftsverlag, Grünbergstr. 15, 1120 Wien.

Der Wirtschaftsverlag | BUSINESS-TO-BUSINESS COMMUNICATIONS


# Starte dein Morgen heute!

Hole dir jetzt deine Förderung zur Verwirklichung deiner Ideen und beruflichen Veränderung und trage so zu deinem eigenen sowie zum Wachstum unserer Stadt bei.

**1. Unterstützung für Ausbildung:**

- € 31,5 Millionen für Ausbildung in Sozial- und Pflegeberufen, Gastronomie, Handel und Handwerk mit dem Angebot „Jobs PLUS Ausbildung“
- Inkl. € 400,– Ausbildungsgeld pro Monat

**2. Förderung von Ideen:**

- € 1 Million für Ideen zum Thema „Future Communities“ mit dem Programm „Creatives for Vienna“
  - € 7.000,– Förderung für konkrete Projekte
  - € 5.000,– Förderung für allgemeine Ideen, die besonders wirksam und kreativ sind

**3. Förderungen für Frauen:**

- € 10 Millionen für Frauen und Wiedereinsteigerinnen
  - Professionelle Beratung
  - Bis zu € 5.000,- bei beruflicher Weiterbildung

**Gleich informieren unter coronavirus.wien.gv.at/wirtschaft**

**Stadt Wien**

**wien.gv.at/coronavirus**

# AUGEN AUF, OHREN AUF!

SCHWER PUNKT **SICHERHEIT**

Warum eigentlich eine Ausgabe, die sich dem Generalthema Sicherheit widmet? Vor allem, weil es kaum ein Thema gibt, das unseren Alltag, unser Denken, ja unsere gesamte Gesellschaftsordnung und unser Wirtschaftssystem so sehr durchdringt. Gegen alle möglichen Gefahren wollen wir uns bestmöglich absichern. Das betrifft Gesundheitsrisiken genauso wie den Straßenverkehr, das Eigenheim oder unsere IT. Wir stellen in allen möglichen Bereichen komplexe Regeln auf und zahlen jede Menge Geld, um für den Fall des Falles abgesichert zu sein. Rund 2.000 Euro gibt jeder Österreicher pro Jahr allein für Versicherungen aus.

Ein System, das sich grundsätzlich bewährt hat. Vor allem, weil es uns das gute Gefühl gibt, alles getan zu haben. Dagegen ist nichts einzuwenden. Gefahr erkannt, Gefahr gebannt. Ein Motto, das uns von klein auf begleitet. Der ORF etwa hat mit seinem Sicherheitsmaskottchen Helmi ganze Generationen dafür sensibilisiert, dass die Welt ein gefährlicher Ort ist. Völlig zu Recht. Doch in den letzten Jahren scheint der Wunsch, in allen Bereichen für Sicherheit zu sorgen, doch ein wenig auszuufern und sich zu verselbstständigen. Immer mehr Regeln, Vorschriften, Gebote und Verbote durchziehen unseren Alltag. Durchaus wohlmeinend ersonnen, um zu schützen, wer oder was auch immer gerade schutzbedürftig erscheint. Auch dagegen wäre noch nichts einzuwenden, würde man nicht damit Zug um Zug die Eigenverantwortung für einen selbst und für die Gesellschaft vom Einzelnen loslösen. Das Endergebnis wäre eine echte Vollkasko-Gesellschaft, in der niemand mehr selbst überlegen müsste, wann Vorsicht geboten ist. Noch sind wir zum Glück nicht so weit. Doch das Gefühl, in einer Welt zu leben, die immer komplexer wird, die von immer mehr Gefahren durchdrungen ist, lässt sich nicht ganz abschütteln. In Zeiten von Corona erst recht nicht. Wir zeigen in dieser Ausgabe vor allem solche Gefahren auf, gegen die es als Unternehmen zweifelsfrei sinnvoll ist, sich zu wappnen. Von der Datensicherheit bis zum Objektschutz. Und wie viel Risiko darüber hinaus jeder Einzelne zu nehmen bereit ist, bleibt reine Nervensache.

Viel Spaß beim Lesen wünscht

*Stephan Strzyzowski, Chefredakteur*

*s.strzyzowski@wirtschaftsverlag.at*




**IMPRESSUM**

**Medieninhaber, Herausgeber, Verleger, Redaktion:** Österreichischer Wirtschaftsverlag GmbH, Grünbergstraße 15/1, A-1120 Wien, T +43 1 54664 0, www.wirtschaftsverlag.at, **Geschäftsführer:** Thomas Letz, **DVR-NR.:** 0368491, **Chefredakteur:** Stephan Strzyzowski, (str), T +43 1 54664 381, E s.strzyzowski@wirtschaftsverlag.at, **Redaktionelle Mitarbeit:** Alexandra Rotter, Harald Koisser, Markus Mittermüller, Harald Fercher, Mara Leicht, Oliver Weberberger, Thomas Stubbings, Stefan Grampelhuber, Peter Martens, **Redaktionsleitung:** Stefan Böck, **Fotos:** Getty Images **Anzeigenberatung:** Erhard Witty, T+43 1 54664 283, Philipp Phillipeck, T+43 1 54664 221 **Anzeigenservice:** T +43 1 54664 444, E anzeigenservice@wirtschaftsverlag.at, **Grafik Design:** Markus Bürger (Konzept, AD), **Hersteller:** Druckerei Ferdinand Berger & Söhne GmbH, 3580 Horn, Wiener Straße 80, **Aboservice:** Aboservice Österreichischer Wirtschaftsverlag GmbH: velcom GmbH, T +43 1 54664 135, E aboservice@wirtschaftsverlag.at • www.die-wirtschaft.at • http://www.facebook.com/diewirtschaft • Aus Gründen der Textökonomie verzichten wir auf geschlechtsspezifische Formulierungen. • Die Offenlegung gemäß § 25 Mediengesetz ist unter **http://www.wirtschaftsverlag.at/offenlegung** ständig abrufbar. • **Wir tragen Verantwortung:** Wir verpacken unsere Zeitschrift nur dann in (umweltverträgliche) Folie, wenn der Postversand es aufgrund von Beilagen erfordert. Der Verlag und alle unsere Druckbetriebe sind $CO_2$-neutral. Mehr erfahren: www.wirtschaftsverlag.at/ueber-uns/csr und auf Twitter @CSR_Verlag

„Cyber-Angriffe wachsen exponentiell und sie werden immer zielgerichteter. Wir sehen allein 71 Mio. Angriffe auf das Honey Pot-System der Deutschen Telekom an einem einzelnen Tag. Viele Firmen können diese Angriffswucht alleine nicht stemmen“, so Christopher Ehmsen, Security-Experte bei T-Systems.



# Security as a Service von T-Systems – zum Schutz

*Cyberattacken bleiben von betroffenen Unternehmen durchschnittlich mehr als 200 Tage unentdeckt. Und das, obwohl die Firmen präventive Maßnahmen wie Virenscanner oder Firewalls im Einsatz hatten. Dies zeigt, dass die Erkennung und Reaktion auf komplexe Angriffe gestärkt werden muss. Es steigt jedoch nicht nur die Anzahl der Angriffe, sondern auch die Professionalität, mit der Hacker in IT-Systeme von Unternehmen eindringen und dort massiven Schaden anrichten. Ein simpler Virenschutz und klassische Firewalls bieten hierfür zu wenig Sicherheit.*

Cyber Bedrohungen nehmen laufend zu. Mit seinem Security Operations Center (SOC) bietet T-Systems ein rund um die Uhr Service an. In diesem werden aktuelle Entwicklungen und Bedrohungen im Cyberspace laufend analysiert, um bessere Lagebeurteilungen für unterschiedliche Branchen machen zu können. Eingesetzt wird eine Kombination unterschiedlicher technischer Produkte und Lösungen, um die Erkennung von IT-Sicherheitsvorfällen in den Infrastrukturen der Unternehmen zu unterstützen, Angriffe zu erkennen und bezüglich ihrer Kritikalität zu bewerten. Die jahrelange Erfahrung in hochkomplexen IT-Landschaften macht T-Systems damit zu einem starken Partner in Sachen Sicherheit. Weltweit profitieren über 1,2 Mio. gemanagte Server und Clients bereits von den Security Services von T-Systems. „Wir betrachten das Thema Cyber Security aus einer 360°-Sicht und bieten umfassende Maßnahmen zur Überprüfung bestehender IT-Infrastrukturen an, sei es durch Security Assessments, Penetration Tests oder Identity & Data Screenings“, so Christopher Ehmsen, Head of Portfoliomanagement & Solution Sales Cyber Security bei T-Systems Austria.

### Magenta Industrial Security bietet EVUs Sicherheit

Energieversorgungsunternehmen (EVUs) gehören jedenfalls immer zur kritischen Infrastruktur. Besonders im eng verwobenen Stromnetz innerhalb von Europa, bekommen auch lokale Unternehmen in Österreich und der Schweiz eine Bedeutung weit über die eigenen Landesgrenzen hinaus. Sowohl gesetzliche Vorgaben als auch die eigenen Anforderungen nach der Erfüllung von höheren Sicherheitsstandards sind für diese Unternehmen große Herausforderungen. „Wir sehen, dass sich der Aufbau eines eigenen größeren Security Teams mit einer 7x24 Abdeckung für viele EVUs schwierig gestaltet, unter anderem deshalb, weil zu wenige Fachkräfte am Markt verfügbar sind. Viele Firmen wissen nicht, dass der Angreifer längst in ihre Systeme eingedrungen ist und in aller Ruhe wichtige Dinge digital stehlen kann. Mit dem „Magenta Security Shield“ bieten wir im


# kritischer Infrastruktur

Cyber Defense Center von T-Systems, Monitoring in Echtzeit und automatische Abwehr. So sind Unternehmen wirkungsvoll geschützt", weiss Ehmsen.

### Anbindung an Cyber Defense Center und Zugriff auf lokales Security Team

Ein wichtiger Mehrwert für EVUs ist die Einbindung des T-Systems Security Teams in den Gesamtverbund der Security Spezialisten der Deutschen Telekom. Damit ist der Zugriff auf einen der größten Wissenspools an Security-Informationen spezifisch für kritische Infrastrukturen gewährleistet. „Als T-Systems Alpine beschäftigen wir in Österreich und der Schweiz ein Security-Team von über 120 Mitarbeiterinnen und Mitarbeiter. Neben mittelständischen Unternehmen, Industrieunternehmen, Finance & Insurance, sowie Kunde aus dem Public Bereich, betreuen wir auch namhafte EVUs. Unser hochspezialisiertes Team stellt von der organisatorischen Beratung, über die Konzepterstellung für unterschiedliche Themengebiete in der Security, bis hin zur effizienten Implementierung von Security-Services, flexibel gestaltbare Lösungen zur Verfügung“, so Ehmsen.

### Security Intelligence as a Service

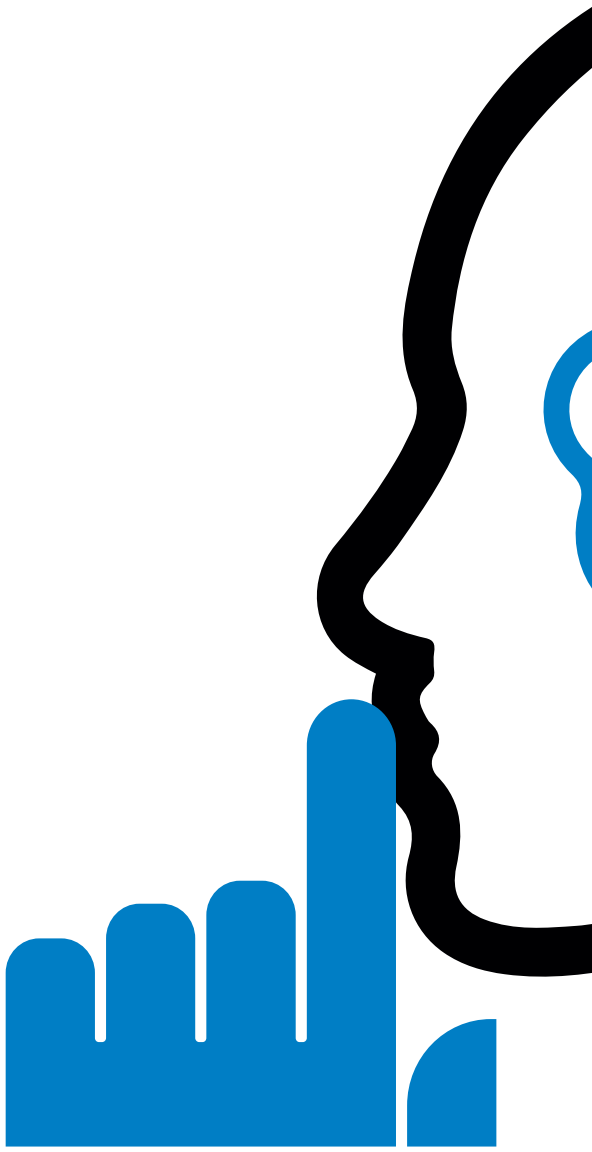
Mit Security Intelligence as a Service – kurz SIaaS – steht eine Lösung zur Verfügung, die in Österreich entwickelt wurde. Die Lösung ist aufgrund unterschiedlicher Module, die miteinander kombiniert werden können, aufgrund der guten Skalierbarkeit hoch flexibel und  für unterschiedliche Unternehmensgrößen geeignet. Natürlich passt sich die Lösung nahtlos dem Wachstum eines Unternehmens an. „Mit SIaaS schließen wir diese Lücke und verbessert im Falle von Cyberangriffen sowohl die Erkennung als auch die Reaktion darauf. SIaaS stellt die Balance zwischen präventiven, detektiven und reaktiven Maßnahmen mit Fokus auf die beiden letztgenannten her. Ziel ist es, die Zeit bis zur Erkennung von Bedrohungen wesentlich zu verkürzen und rasch mit geeigneten Gegenmaßnahmen zu antworten“, so Ehmsen. Hinter SIaaS steht eine gemanagte Plattform zur übersichtlichen Bewertung der Bedrohungslage für die gesamte IT-Infrastruktur, die eine große Anzahl an Basisleistungen umfasst.

### Sicherheit basiert auf Vertrauen

„Sicherheit ist ein Geschäft, das auf Vertrauen basiert. Wir als Sicherheitsanbieter kennt die Schwachstellen in den Kundensystemen, etwa Details in der Netzwerksegmentierung oder zum Patchmanagement in der Operational Technology (OT), die auch Angreifer interessieren würden. Dieses Vertrauen wird eher über einen persönlichen Kontakt aufgebaut, als irgendwo anonym eingekauft. Denn ein Unternehmen kann nicht endlos in IT-Security investieren“, meint Ehmsen.
Weitere Informationen: **www.t-systems.at**

**TEXT** ALEXANDRA ROTTER UND MARKUS MITTERMÜLLER

# Wissen ist Macht



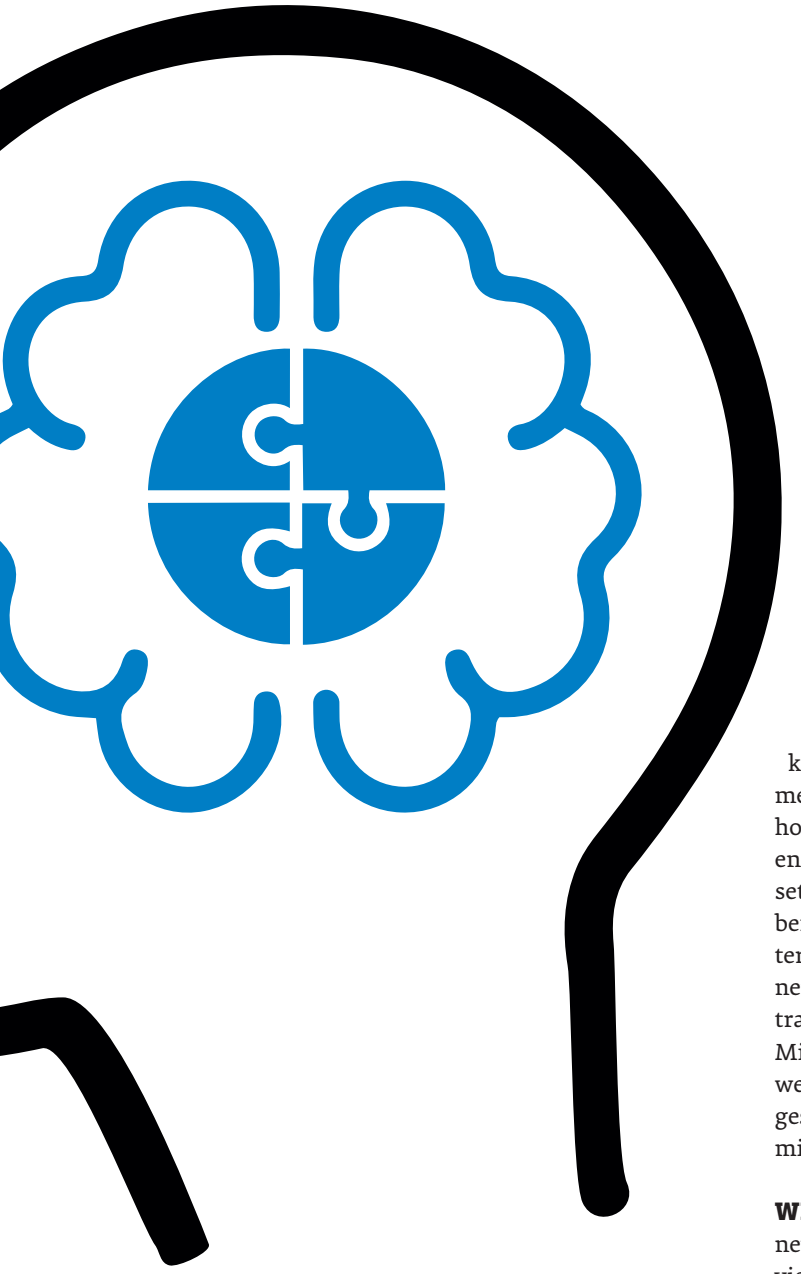
**Besondere Kenntnisse wollen gehegt, gepflegt und geschützt werden. Wissensmanagement bringt einen Wettbewerbsvorteil, wird aber noch von wenigen KMU strategisch und konsequent eingesetzt. Doch damit laufen sie Gefahr, ihren Wissensvorsprung allmählich zu verlieren.**

Wissen ist Macht. Das gilt besonders für Unternehmen, die eine führende Marktposition anstreben oder behalten wollen. Sowohl Leitbetriebe als auch KMU, die dem Wissensmanagement keine Priorität einräumen, werden es künftig schwer haben. Josef Herget, Direktor des Excellence Institutes, einem Thinktank und Forschungsinstitut in Wien, das unter anderem auf Wissensmanagement spezialisiert ist, sagt: „KMU leben vom Wissen. Und noch nie war so viel Wissen verfügbar wie jetzt." Die logische Folge für heimische Unternehmen – von denen laut KMU Forschung Austria 99,6 Prozent KMU sind – müsste daher sein, dass für sie ein goldenes Zeitalter angebrochen ist.

Doch nicht alle KMU profitieren von der Masse an vorhandenem Wissen. Es liegt schließlich nicht auf der Straße. Und selbst wenn es leicht zugänglich ist, heißt das noch nicht, dass Unternehmen einen Überblick darüber haben oder alle Mitarbeiterinnen und Mitarbeiter immer wissen, wo sie genau die Information finden, die sie brauchen. Wissen will eben gemanagt, gepflegt und geschützt werden, damit es Unternehmen in der täglichen Praxis sinnvoll einsetzen können und es ihnen einen Wettbewerbsvorteil verschafft. Viele von ihnen haben sich noch keine Strategie zurechtgelegt, wie sie mit bestehendem Wissen umgehen und neue Wissensquellen anzapfen können, und so manches wird laut Josef Herget immer noch dem Zufall überlassen: „Den Umgang mit Wissen im Unternehmen systematisch zu planen und zu evaluieren, das macht kaum jemand."

**STABSSTELLE WISSENSMANAGEMENT** Die Leitz-Gruppe, führender Hersteller von maschinengetriebenen Präzisionswerkzeugen zur zerspanenden Bearbeitung von Holz, Holzwerkstoffen, Kunststoffen und anderen Materialien, stellt eine erfreuliche Ausnahme dar. Das Unternehmen, das in Europa, Asien und Amerika produziert und seine Produkte in mehr als 150 Ländern vertreibt, beschäftigt sich seit 2005 intensiv mit Wissensmanagement und hat es sogar in einer eigenen Stabsstelle im Unternehmen verankert. Peter Merzendorfer, IT- und Konstruktionsleiter

Illu: Hiranmay Baidya, furtaev / Getty Images Bearbeitung: Markus Bürger



bei Leitz, sagt: „Wissen stellt eine wertvolle Ressource für uns dar. Wie jede Ressource muss Wissen dabei den generellen Managementprinzipien unterworfen werden. Es muss geplant, gesteuert und evaluiert werden." Unter Wissensarbeit versteht man bei Leitz, Wissen nicht nur als Ressource zu nutzen, sondern auch kontinuierlich zu hinterfragen und weiterzuentwickeln: „Lernen auf allen Ebenen ist dabei ein wesentlicher Bestandteil." Wissensmanagement verstehe man als ein „Set von Tools, das uns unterstützt, unsere Ziele besser zu erreichen, besser zusammenzuarbeiten und somit immer erfolgreicher zu werden".

Dazu hat Leitz aus der eigenen Konzernstrategie und den Zielen konkrete Fragen zum Wissensmanagement abgeleitet und in einem Self-Check zusammengefasst. Damit überprüft sich das Unternehmen jedes Jahr selbst und macht so seine Entwicklung sichtbar. Mithilfe des Self-Checks identifiziert es jene Handlungsfelder, in denen es in der Wissensarbeit effizienter werden will (z. B. bei der Organisation, Abstimmung und Meeting-Kultur), wo es unternehmenskritisches Wissen bewahren und verfügbar machen und Kompetenzen stärken will, wo es seine Marktposition und den Umsatz durch den Ausbau und das Nutzen von Wissen verbessern will und schließlich wo es Fachbereichsziele mit Wissensmanagement einfacher und besser erreichen will.

**AUS FEHLERN LERNEN** Entscheidend für erfolgreiches Wissensmanagement sind bei Leitz die stetige Ausbildung und Erfahrung der Mitarbeiterinnen und Mitarbeiter und – aus Fehlern zu lernen. Um das Wissen und den Standard im Unternehmen zu festigen und auszubauen, müssen beispielsweise nach Abschluss einer Reklamation die Erkenntnisse in sogenannte Wissensdokumente eingearbeitet werden, sodass sich Fehler nicht wiederholen. Die Dokumente, mit denen die Organisation arbeitet, entwickeln sich so ständig weiter. Zum Schutz des Wissens setzt Leitz zum einen auf Patente und IT-Infrastruktur und befragt zum anderen Expertinnen und Experten vor dem altersbedingten Berufsausstieg aus dem Unternehmen in einem Expert-Debriefing. Merzendorfer: „Bei diesem Wissenstransfer zwischen ausscheidenden Mitarbeiterinnen und Mitarbeitern und deren Nachfolgerinnen und Nachfolgern werden ihnen anhand eines Leitfadens strukturiert Fragen gestellt, um das Wissen zu externalisieren und weiterzuvermitteln bzw. in unserer Wissensdatenbank zu speichern."

**WISSENSCHAFTLICHES KNOW-HOW ANZAPFEN** Um neues Wissen von außen ins Unternehmen zu holen, setzen viele KMU auf Kooperationen mit Forschungseinrichtungen. So hat die Joanneum Research Forschungsgesellschaft, eine der größten außeruniversitären Forschungseinrichtungen Österreichs, in den vergangenen Jahren allein in der Steiermark zusammen mit mehr als hundert KMU geforscht. Spezialisiert ist Joanneum Research auf Informations- und Produktionstechnologien, Humantechnologie und Medizin sowie Gesellschaft und Nachhaltigkeit. Gemeinsam neues Wissen zu generieren ist bei den Kooperationen zentral. Silvia Russegger, Forschungsgruppenleiterin bei Joanneum Research, sagt: „Wir suchen Unternehmen, die wirklich etwas Neues und Innovatives ausprobieren und nicht nur Altes erneuern wollen." Unternehmen, die aktiv an ihrem Wissensaufbau arbeiten wollen, wird ein langer Atem abverlangt: „Die KMU sollen die Ergebnisse der Forschungen nachhaltig nutzen. Oft kommen die Ergebnisse aber nicht so schnell, wie es sich die Unternehmen wünschen." Keinesfalls sollten die Forschungsergebnisse in der Schublade verschwinden, weil nicht genug Zeit und Energie dafür vorgesehen ist. Unumgänglich ist zudem, dass die grundlegende Idee vom Unternehmen kommt. Dass Wissensgenerierung in Zusammenarbeit mit externen Forschungseinrichtungen trotz dieser Vor-

Mario Hartinger, AVL

**Wir müssen darauf achten, dass keine Informationen von einem Kunden zum anderen fließen.**

Fotos: GEOPHO/AVL

aussetzungen gut funktionieren kann, hat unter anderem das Grazer Technologieunternehmen HS-Art vorgezeigt, das mit Joanneum Research eine Software zur digitalen Filmrestaurierung entwickelt und in Folge weiter verbessert hat.

**FÖRDERUNG FÜR PROTOTYPEN** Ein finanzieller Anreiz, um auch als KMU den Einstieg in die Forschung zu schaffen, sind Förderungen wie etwa der Innovationsscheck der Österreichischen Forschungsförderungsgesellschaft (FFG). Damit können förderbare Leistungen von Forschungseinrichtungen bis zu einer Höhe von 12.500 Euro bezahlt werden. 20 Prozent des Betrags muss das geförderte Unternehmen selbst beisteuern. Silvia Russegger: „Mit diesen 10.000 Euro an Förderung können wir schon Prototypen entwickeln." Mit solchen Finanzspritzen sinkt auch die Scheu vieler KMU vor dem Einstieg in die Forschung. „Die meisten kleineren Unternehmen haben keine eigene F&E-Abteilung und wissen oft auch nicht, welche Forschungsergebnisse es bereits gibt. Daher profitieren die KMU von unserer Erfahrung in der Co-Creation", meint die Forschungsexpertin.

Bei Lithoz, einem auf 3D-Druck von Knochenersatzmaterialien und Hochleistungskeramiken spezialisierten Wiener Unternehmen, ist Wissensmanagement in der Qualitätssicherung und damit direkt unter der Geschäftsführung verankert. Mit rund 100 Mitarbeitern, Tendenz steigend, entwickelt Lithoz die Materialien und die 3D-Fertigungssysteme selbst und stellt sie her. Für das Spin-off der TU ist Wissensgenerierung sowohl inhouse als auch durch Forschungskooperationen sehr wichtig. Nach wie vor arbeitet das Unternehmen intensiv mit der TU zusammen, aber auch mit anderen Unis und Institutionen wie etwa der Montanuni Leoben, der Uni Wien und dem Fraunhofer IKT in Dresden. Gründer und CEO Johannes Homa beobachtet, dass Forschungseinrichtungen extrem vorsichtig beim Teilen von Wissen geworden sind. Auch Partnerorganisationen versuchen meist, Wissen für sich zu behalten. Homa: „Die meisten sind sehr zurückhaltend, auch wenn sie ergänzende Businessmodelle haben." Ohne Geheimhaltungsvereinbarungen könne man heute praktisch mit niemandem mehr sprechen. Homa glaubt, mit einer höheren Businessethik und dem Selbstverständnis, Informationen nur dann weiterzutragen, wenn man die Person um Erlaubnis gebeten hat, wäre das Arbeiten einfacher: „Es bedarf einer großen Anstrengung, Innovationen in den Markt zu bringen. Das würde viel besser gemeinsam und mit mehr Wissensaustausch gehen."

**KREATIVES DENKEN FÖRDERN** Gründe für Forschungskooperationen gibt es viele. Einer ist die Funktion externer Einrichtungen als Ideenschmiede: So werde kreatives Denken im Unternehmen gefördert. Außerdem sagt Homa: „Für Unternehmen ist teilweise schwer zu greifen, was Innovation bedeutet." Da helfen akademische Partner, mit denen man Forschungsfragen erarbeite und die für die Industrie einen neutraleren Zugang zur Materie schaffen. Auch der Zugang zu Forschungs-Infrastruktur, etwa zu Analysegeräten, spielt eine Rolle.

Das Sammeln und Aufbereiten von Wissen ist nie Selbstzweck, sondern muss einen Mehrwert bringen und der Wertschöpfung dienen. Dabei kann Technologie helfen: Althergebrachte Wissensspeicher werden immer öfter durch neue ersetzt. Mitarbeiter, die Information suchen, die in ihrem Unternehmen vorhanden ist, mussten bisher in der Regel Datenbanken nach Text-Dokumenten durchforsten. Immer öfter kommen jetzt laut Josef Herget Videos und Chatbots zum Einsatz – unter anderem auch in der Kundenberatung: „Auf Webseiten können zum Beispiel Chatbots eingesetzt werden, um Kunden direkt Antworten auf ihre Fragen bereitzustellen – das ist effizient und verursacht keine große Kosten." Mit Alexa und Siri werde zukünftig auch die Spracherkennung als neue Interaktionsform des Wissensmanagements noch bedeutsamer.

**KOOPERATION MIT GANZEN BRANCHEN** Gleich mit ganzen Branchen – etwa aus dem Textil-, Nahrungsmittel- oder Energiebereich – arbeitet das Austrian Institute Of Technology (AIT) zusammen. Dazu führt das Forschungsunternehmen zu spezifischen Fragen längerfristige Stakeholder-Prozesse durch, an denen unterschiedliche Unternehmen, Interessenvertretungen, Branchenorganisationen, Clustermanager, Technologieentwickler, Wissenschaftler, Nutzer etc. teilnehmen. Doris Schartinger, wissenschaftliche Mitarbeiterin am AIT, sagt: „Wir erörtern gemeinsam, welchen Bedarf es gibt, damit die Unternehmen am Markt besser bestehen können. Dadurch entsteht ein vielschichtiges Bild von Trends, Treibern und Friktionen mit sektoralem Zuschnitt und aus der Systemperspektive."

Wie wichtig externe Forschungseinrichtungen für die Wirtschaft sind, zeigt allein schon die Größe so mancher Einrichtung. So forschen etwa rund 1.400 Mitarbeiterinnen und

Mitarbeiter in ganz Österreich an verschiedenen Standorten des AIT in sieben Kernbereichen, darunter Energie, digitale Sicherheit, Gesundheit und Bioressourcen. Wie es mit künftigen Kooperationspartnern in Kontakt kommt, ist sehr unterschiedlich. Ein Anknüpfungspunkt sind Publikationen, mit denen das AIT auf seine Leistungen aufmerksam macht. Schartinger: „Darüber bauen sich Kontakte auf – oder auch bei Treffen auf Veranstaltungen."

**DAS WISSEN IM MITARBEITER** Ist die Forschung erfolgreich, sollte das neue Wissen im Idealfall nicht nur veröffentlicht, sondern auch vor Plagiaten geschützt werden. Ein klassischer Weg, Ideen zu schützen, sind Patentierungen. Ebenfalls gut geschützt – wenn auch in einem anderen Sinn – ist das sogenannte „stillschweigende Wissen". Schartinger: „Dieses Wissen ist implizit, das heißt, im Mitarbeiter vorhanden und in ihm verankert. Meist weiß niemand, dass der Mitarbeiter dieses Wissen hat. Es äußert sich durch sein Tun." Von diesem Wissen können auch andere im Unternehmen profitieren. Zugleich ist es besonders gefährdet, durch Jobwechsel oder Pensionierungen verloren zu gehen. Wie man stillschweigendes Wissen am besten schützt und nützt, dafür gibt es laut Schartinger kein Patentrezept: „Offenheit, Wertschätzung und Freiräume für Mitarbeiter sind auf jeden Fall nötig. Durch wechselnde Kooperationen und Rotationen innerhalb des Unternehmens kommen neue Leute zusammen, die ihr Wissen teilen."

Wie innerhalb von Unternehmen Wissens- und Innovationsgenerierung gefördert werden kann, macht die steirische AVL List GmbH vor, die seit 2012 Jahr für Jahr die meisten Patente in Österreich anmeldet. Das Unternehmen, das weltweit mehr als 11.500 Mitarbeiter hat, entwickelt, prüft und testet Powertrain-Antriebssysteme. Mario Hartinger, seit 2012 Patentanwalt bei AVL List, erzählt: „Beim Wissensaufbau in Unternehmen geht es unter anderem darum, Erfindungen zu generieren, zu identifizieren und zu schützen. Und das machen wir sehr systematisch." So bekommt buchstäblich jeder Mitarbeiter, der eine Idee für eine neue technische Lösung hat, Zeit,

um diese auszuarbeiten: „Wir versuchen, diese kleinen Pflänzchen, die man sich entweder systematisch erarbeitet hat oder die einem unter der Dusche einfallen, zu pflegen."

**FORSCHUNGS-PFLÄNZCHEN GIESSEN** Eine Erfindung mache am Ende immer eine Person, aber die Prozesse und Strukturen drumherum will AVL List möglichst vereinfachen. Jenen „Pflänzchen", die am vielversprechendsten aussehen, widmet AVL laut Hartinger ein Forschungsbudget. Hartinger selbst unterstützt diesen Prozess, indem er in der Patentliteratur nach ähnlichen Erfindungen sucht: „Als Patentanwalt nutze ich die öffentlichen Datenbanken der Patentämter als Informationsquellen und schaue, welche Themen es schon gibt, die wir als Absprungbasis verwenden können." Und sobald Erfindungen im Unternehmen entstehen, kümmert sich Hartinger um die Anmeldung beim Patentamt. 2020 meldete AVL List 180 Erfindungen beim Patentamt an – bei weitem die meisten Anmeldungen in Österreich: Der Zweitplatzierte, die Julius Blum GmbH, schaffte im selben Zeitraum 76 Anmeldungen.

Unternehmen, die ein Patent einreichen, gehen laut Hartinger einen Deal ein: Sie schützen ihre Idee und bekommen zeitlich begrenzt eine Monopolstellung, „müssen aber der Allgemeinheit erzählen, wie die Erfindung funktioniert, damit die Gesellschaft sie weiterentwickeln kann". Damit man allerdings nicht gleich seinen Wissensvorsprung verliert, wird eine Patentanmeldung erst 18 Monate nach der Einreichung in einer öffentlichen Datenbank publiziert. Eine in Österreich patentierte Erfindung ist übrigens nur im Inland, aber nicht weltweit geschützt. Es gilt das Territorialitätsprinzip. Hartinger: „Wenn ich jemandem die Herstellung oder Benutzung meiner Erfindung zum Beispiel in China verbieten möchte, brauche ich auch dort ein Patent." Und weil Patentanmeldungen keine günstige Angelegenheit sind, stehen für jede Patentierung wichtige betriebswirtschaftliche Überlegungen an: „In welchen Ländern will ich einen Patentschutz, und wo will ich kein Geld dafür ausgeben?"

**KMU sollen die Ergebnisse der Forschungen nachhaltig nutzen.**

Silvia Russegger, Joanneum Research

### WIE SIE IHR WISSEN IM UNTERNEHMEN SICHERN

**STRATEGIE ENTWICKELN** Welchen Stellenwert hat Wissen im Unternehmen? Darauf wird die Strategie aufgebaut, wie mit dem Wissen in Folge umgegangen wird.

**TECHNOLOGIEN NUTZEN** Textsysteme und Datenbanken werden von neuen Technologien wie Chatbots abgelöst.

**FREIRÄUME UND WERTSCHÄTZUNG GEBEN** Mitarbeiter, die ihr Wissen teilen, brauchen dafür Zeit und sollen, z. B. mittels Bonussystem, auch eine Wertschätzung erhalten.

**MENTORENPROGRAMME STARTEN** Neue Mitarbeiter bekommen einen Mentor zur Seite gestellt. So wird auch Wissen weitergegeben, das noch nirgends dokumentiert ist.

**EVALUIEREN** Hat das Wissensmanagement tatsächlich einen Mehrwert gebracht? Regelmäßiges Prüfen der Maßnahmen hilft, dass das gesammelte Wissen auch Wertschöpfung bringt.

**KOPIEREN UNTER UMSTÄNDEN ERLAUBT** Insbesondere, wenn Wissen in Kooperationen entsteht, sollten Geheimhaltungsklauseln und vertragliche Klauseln zu den Rechten selbstverständlich sein. Hartinger: „Wir arbeiten zum Beispiel auch für Rennställe. Da müssen wir extrem darauf achten, dass keine Informationen von einem Kunden zum anderen fließen." Wissen zeichne Experten aus: „Wir bei AVL entwickeln zum Beispiel für viele Firmen Batterien. Die Kunden kommen zu uns, weil wir hier schon Know-how aufgebaut haben." Insbesondere Start-ups gibt Hartinger mit auf den Weg: „Es ist wichtig, dass sie eine technische Idee oder ein Design schützen, bevor sie einen Partner suchen und ihm davon erzählen." Sonst könne es passieren, dass der potenzielle Partner die Reise allein antrete. Zwar gebe es ein Wettbewerbsrecht und es sei unlauter, jemandem eine Idee zu klauen: „Aber grundsätzlich darf ich eine Idee, von der ich eine Beschreibung höre, schon kopieren, wenn kein Schutzrecht besteht."

Wissen ist Macht. Das klingt nach einer großen Sache – und das ist es auch. Doch das sollte nicht abschrecken. Selbst große Errungenschaften beginnen oft im Kleinen, zum Beispiel bei regelmäßigen informellen Lunch-Meetings. Josef Herget rät Unternehmen etwa, mindestens einmal pro Woche Meetings zu organisieren, in denen sich Mitarbeiter aus allen Abteilungen – von der Produktion, F&E oder auch vom Außendienst – treffen und einander von den Entwicklungen in ihren Arbeitsgebieten erzählen: „In den vergangenen zehn Jahren haben wir zu viel Fokus auf die Technologie gelegt. Das Wissensmanagement lebt aber vor allem auch von den Personen, deren Fähigkeiten und ihrem Willen, dieses Wissen zu teilen". ◀

Foto: Bernhard Bergmann

# WANDEL DES BEWUSSTSEINS

**Der Mythos musste einst der Rationalität Platz machen.
Jetzt muss die Rationalität dem integralen Bewusstsein weichen.**

Mitte des 14. Jahrhunderts begann der Glaube an die Heilige Katholische Kirche zu bröckeln, auch wenn deren Macht gerade am Höhepunkt schien und durch die rund hundert Jahre zuvor von einem Papst namens Innozenz (Unschuld) ins Leben gerufene Inquisition gefestigt wurde. Die Bewusstseinsstruktur der Menschen war in einem Wandel, und dieser Wandel war eine Antwort auf die neuen Lebenssituationen.

Die völlige Preisgabe an den Mythos wurde der neuen Komplexität des Lebens nicht mehr gerecht. Die Städte waren größer geworden, der Handel internationaler, es brauchte weniger Gottesurteile und mehr Berechenbarkeit, um den Tagesablauf zu bewältigen. Um 1300 hatten Mönche die erste mechanische Uhr erfunden, noch mit dem Ziel, die Gebetszeiten exakter erfassen zu können. Doch die Uhr hatte eine teuflische Folge. Sie enthob die Menschen der Naturzeit, die durch den Tages- und Jahresrhythmus gegeben war. Anstatt „bei Sonnenaufgang" konnte man nun präzisere Verabredungen treffen. Egal, was die Sonne gerade machte, war eine Verabredung um sieben Uhr am Morgen möglich, auch wenn die Uhren noch keinen Minutenzeiger hatten und nur die Stunden anzeigten. Damit bekamen die Menschen die Zeit, die vorher ganz in Gottes Hand war, unter ihre Herrschaft.

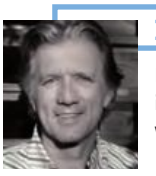
Doch wie den sich anbahnenden Wandel durchsetzen? Wie die nötige Abkehr vom blinden Glauben hin zu einer Rationalisierung großflächig verbreiten? Im Jahr 1347 kam die große Seuche. Und zwei Sommer mit Regen, Regen, Regen. Das Getreide faulte auf den Feldern, die Ernte war gering, der Tod allgegenwärtig. Die Hälfte der Bevölkerung Europas wurde hinweggerafft.

Diese dramatische und tragische Ausnahmesituation forcierte den Bruch in der Bewusstseinsstruktur. Wenn das Gottes Wille sein sollte, dann war er unverständlich. Dann musste es eine andere Möglichkeit geben, um das Leben zu meistern. Die Idee der Rationalität und Selbstmächtigkeit begann Raum zu greifen. Die Wiedergeburt des Menschen, die Renaissance, fand statt. Der Individualismus und die Anbetung des menschlichen Genies brachen an. Der Raum des Mythos zerbrach, der Raum der Ratio wurde eröffnet.

Anfang des 21. Jahrhunderts begann der Glaube an die pure Rationalität, die mit der Renaissance und dann mit der Aufklärung Raum gegriffen hatte, zu bröckeln, auch wenn die Macht des Geldes, die Idee des ewigen Wachstums und der Glaube an die Machbarkeit von allem unendlich schienen. Die Bewusstseinsstruktur der Menschen war in einem Wandel, und dieser Wandel war eine Antwort auf die neuen Lebenssituationen.

Die völlige Preisgabe an die Rationalität wurde der neuen Komplexität des Lebens nicht mehr gerecht. Der Mensch hatte die Natur unterworfen und lebenswichtige Ressourcen fast vollständig vernichtet, er hatte das Atom gespalten und das Klima verändert. Es brauchte weniger Rationalität und mehr Lebensechtheit. Die Menschheit gierte nach Sinn, Liebe und Miteinander.

Doch wie den sich anbahnenden Wandel durchsetzen? Wie die nötige Abkehr von der Rationalität hin zu einem integralen Bewusstsein großflächig durchsetzen? Im Jahr 2020 kam eine Seuche namens Corona, die die Rationalität an ihre Grenzen brachte. Sie entpuppte sich als Brandbeschleuniger der Transformation. Die Idee des All-eins-Seins begann Raum zu greifen. Die Wiedergeburt des Menschen (Renaissance 2.0) fand um ca. 2021 statt. Das Miteinander und eine Lebensweise der Liebe und Menschlichkeit brachen an. Der Philosoph Jean Gebser nannte es „das integrale Bewusstsein". Der Raum der Ratio zerbrach, der Raum der Liebe wurde eröffnet. Übrigens haben wir einen ziemlich verregneten Frühling. ◀



**DER AUTOR**

Harald Koisser schreibt philosophische Bücher und ist Herausgeber des Mutmacher-Magazins „wirks". www.wirks.at, www.koisser.at

# Es kann jeden

**INTERVIEW** STEPHAN STRZYZOWSKI

**Die Anzahl von Cyberattacken steigt rasant, und die Angriffsfläche wird aufgrund der zunehmenden Digitalisierung immer größer. Wer die Angreifer sind, warum sie auch in sehr gut geschützte Unternehmen eindringen können und warum KMU am meisten gefährdet sind, erklärt Oberst Walter J. Unger, Leiter der Abteilung für Cyberdefence und IKT-Sicherheit im Abwehramt des österreichischen Bundesheeres.**

**Befinden wir uns aktuell im Cyberkrieg?** Mit dem Vokabel sollte man sehr vorsichtig sein. Krieg bezeichnet Gewaltanwendung zwischen Staaten, um politische Ziele zu erreichen. Diese Situation haben wir aktuell im Cyberbereich nicht. Wir erleben aber das, was als hybride Kriegsführung bezeichnet wird. Dabei geht es auch um politische Ziele, aber ohne offene Gewaltanwendung. Ein Mittel sind dabei Cyberangriffe.

**Worauf zielen diese Angriffe ab?** Die Angreifer versuchen zum Beispiel Wahlen oder die öffentliche Meinung zu manipulieren. Solche Angriffe reichen aber bis zum Versuch, die Stromversorgung eines Landes lahmzulegen oder Uran-Anreicherungsmaschinen zu sabotieren. Diese Art der Angriffe läuft immer knapp unterhalb der Schwelle, wo der Angegriffene zu den Waffen greifen würde. Es ist eine verdeckte Konfliktaustragung. Dazu eignet sich diese Art der Kriegsführung sehr gut. Auch weil die Zuordnung extrem schwierig ist. Die Angreifer können ihre Identität im Netz gut verschleiern und sich verstecken. Es gibt nur wenige Fälle, wo man die Herkunft der Angriffe genau identifizieren kann. Und selbst dann kann man nur schwer nachweisen, dass der Angriff vom Staat ausgegangen ist. Erst dann bestünde völkerrechtlich Handlungsbedarf. Denn der Staat müsste solche Angriffe natürlich unterbinden. Allerdings gibt es auch Länder wie Nordkorea, die sich recht offensichtlich mittels Cybercrime-Methoden Devisen beschaffen.

**Unsere gesamte Welt wird immer stärker von Digitalisierung durchdrungen. Wird dadurch ein echter Cyberkrieg wahrscheinlicher?** Die Angriffsfläche wird jedenfalls größer. Alleine durch die Tatsache, dass unzählige Menschen ins Homeoffice gegangen sind und die Sicherheitsvorkehrungen nach wie vor zu wünschen übrig lassen. Auch mit jedem Sensor und mit jedem Gerät, das mit dem Internet verbunden wird, steigt das Risiko. 20 bis 50 Milliarden Devices sind mittlerweile mit dem Internet verbunden. Die vernetzte Heizung oder der Kühlschrank sind für den Staat nicht kritisch. Aber wenn es um Kläranalagen, Flughäfen oder Wasserkraftwerke geht, die teilweise auch über das Netz gesteuert werden, sieht die Sache anders aus.

**Wer sind die Angreifer? Was wollen sie?** Es gibt staatsnahe Angreifer, die Instrumente sind, um Macht auszuüben. Ihnen geht es um politische Ziele und nicht um Geld. Die andere Gruppe sind Cyberkriminelle mit finanziellen Interessen. Vor allem die Angriffe dieser Gruppe schießen massiv in die Höhe. Wir sehen alleine in Österreich einen Anstieg der Anzeigen um 26 Prozent im letzten Jahr. Es geht also dramatisch hinauf, und dabei ist die Dunkelziffer noch nicht berücksichtigt.

**Vermutlich geraten damit auch immer mehr Unternehmen in den Fokus?** Ja, der Kranhersteller Palfinger musste beispielsweise kürzlich Lösegeld zahlen, um wieder Zugriff auf seine Systeme zu erhalten, die von Cyberkriminellen lahmgelegt wurden. Das ist sehr bitter für so ein erfolgreiches Unternehmen. Vor allem, weil Palfinger sehr viel für die Sicherheit getan hat. Aber die Kriminellen haben den Vorteil, dass sie sich lange mit ihrem Opfer befassen können und so auch in eine wirklich gut beschütze Burg eindringen können. Das ist ein Trend, den man beobachten kann. Die Erpresser befassen sich sehr intensiv mit ihren Opfern. Und sie verlangen von großen Betrieben sehr hohe Summen.

**Halten sie wenigstens in der Regel Wort, wenn bezahlt wird?** Besonders bösartige Angreifer erpressen zuerst Geld und stellen die Daten dann trotzdem ins Netz. Immer häufiger werden auch Angriffe, bei denen Botprogramme auf Millionen Rechnern verbreitet werden, die dann den Auftrag erhalten, alle gleichzeitig auf einer Unternehmensseite Anfragen zu stellen. Das System bricht dann natürlich zusammen. Früher kamen solche Angriffe von PCs, heute sind es oft Hochleistungsserver. Die Bandbreiten werden größer.

ZUR PERSON

**WALTER J. UNGER** Oberst des Generalstabsdienstes, ist Leiter der Abteilung für Informations- und Kommunikationstechnik-Sicherheit und Cyber-Verteidigung im Abwehramt des österreichischen Bundesheeres und seit 30 Jahren im Sicherheitsbereich tätig.

Foto: Walter J. Unger

# treffen

Darum tun sich heute selbst große Provider schwer, wenn sie angegriffen werden. Dadurch haben solche Kriminelle die Unternehmen echt in der Hand.

**Gibt es im Cyberwar auch ein Wettrüsten? Und wer hat mehr Mittel zur Verfügung?** Es gibt ein Wettrüsten – absolut. Anfang der 2000er haben viele Länder erkannt, dass man etwas gegen die kriminellen Netzwerke tun kann, und sie haben offensive Cyberfähigkeiten aufgebaut. Vergleichbare Fähigkeiten haben aber auch die kriminellen Gruppen entwickelt. Sie wollen Geld und ein schönes Leben. Staaten wollen politische Macht ausüben und sich rüsten. Wer angreifbar ist, muss heute Defence-Konzepte aufbauen, die weit über technische Maßnahmen hinausgehen. Österreich hat deshalb eine umfassende Strategie für Cybersicherheit erarbeitet, die seit 2013 auf einen immer besseren Schutz der Infrastruktur abzielt.

**Wann rückt Ihre Einheit aus?** Wir kommen ins Spiel, wenn die Handlungsfähigkeit des Staates eingeschränkt ist. Beispielsweise wenn ausländische Mächte versuchen, Österreich etwas abzupressen. Letztes Jahr gab es einen Angriff auf das Außenamt, dessen Handlungsfähigkeit lahmgelegt wurde. Das Innenministerium hat uns um Unterstützung ersucht, und meine Experten haben gemeinsam mit dem Team des Innenministers erfolgreich an der Wiederherstellung der Systeme gearbeitet.

**Schlagen Sie in solchen Fällen auch mit gleichen Mitteln zurück?** Wir schießen nicht zurück. Das ist rechtlich nicht möglich. Wir dürfen aber den militärischen Eigenschutz wahren. Das Bundesheer muss ja handlungsfähig bleiben, und wir sind auch von der digitalen Infrastruktur abhängig. Zum Eigenschutz sind wir berechtigt, in besonderen Fällen auch offensive Maßnahmen zu setzen. Das heißt: Wir identifizieren den Server, von dem viele Angriffe starten, suchen dann den diplomatischen Weg, und wenn das nichts nutzt, ergreifen wir technische Lösungen. Das ist rechtlich abgedeckt.

**Unser Bundesheer gilt, was die finanzielle Ausstattung anbelangt, nicht gerade als gesegnet. Trifft das auch auf die Cyberdefence zu?** Das österreichische Bundesheer hat tatsächlich im internationalen Vergleich nur eine geringe Dotierung. Die NATO legt circa zwei Prozent des BIP für die Verteidigung fest. Wir liegen bei 0,64 Prozent. Der Cyberbereich wurde allerdings sukzessive immer wieder ausgebaut. Meine Abteilung wurde sechsmal in 15 Jahren vergrößert. Da wird also ein wenig mehr investiert.

**Weil hier die Kosten geringer sind, als wenn Panzer oder Flugzeuge angeschafft werden müssen?** Vor allem, weil die Awareness steigt. Man hat erkannt, dass auch industrielle Systeme angreifbar sind und es dadurch rasch zu wirklich kritischen Situationen kommen kann. Im Jahr 2010 konnte der Computerwurm Stuxnet sogar in physikalisch abgeschlossene Urananreicherungsanlagen eingeschleust werden. Das hat einen Wake-up-Call erzeugt. Auch in der Politik. Daraufhin kam der Auftrag, ein militärisches Computer Emergency Response Team, kurz CERT, aufzubauen. Die Strategie haben wir ernsthaft ausgearbeitet. 2013 wurde eine Strategie zur staatlichen Sicherheit erarbeitet. Darin haben wir uns auf ein hohes Sicherheitsniveau für die strategisch wichtige Infrastruktur festgelegt.

**Wie sicher ist die heimische Infrastruktur, wenn man etwa an die Stromversorgung oder die Telekommunikation denkt?** Das Kuratorium Sicheres Österreich hat kürzlich mit KPMG eine Studie dazu präsentiert. Die wesentliche Aussage: 60 Prozent der heimischen Unternehmen wissen, dass sie in den letzten zwölf Monaten angegriffen wurden. 25 Prozent wissen es nicht. Und es gibt eine Dunkelziffer. Es kann jeden treffen. Das gilt natürlich auch für Stromversorger und IKT-Unternehmen. Allerdings sind die Infrastruktur-Betreiber in der Regel besser geschützt. Auch Banken sind zum Beispiel besonders heikel und entsprechend gut vorbereitet. Nicht zuletzt, weil sie durch internationale Vorgaben dazu verpflichtet sind. Das gilt auch für die Energieversorger, die ein eigenes CERT aufgestellt haben. Auch die großen Telekom-Unternehmen tun sehr viel. Wir sehen insgesamt eine deutliche Verbesserung in allen möglichen Bereichen. 100-prozentigen Schutz gibt es aber nicht.

**Wie gut sind Österreichs KMU geschützt?** KMU sind am meisten gefährdet. Weil ihnen vielfach die Ressourcen fehlen. Es reicht nicht, einen Mitarbeiter in ein Sicherheitsseminar zu stecken. Sie stehen vor zwei wesentlichen Herausforderungen: Sie müssen die Ressourcen schaffen und dann die hohe Qualität nachhaltig sichern. Bei einem Angriff fällt es einem kleinen Betrieb zudem schwer durchzuhalten. Beim Angriff auf das Außenamt waren bis zu 30 Experten gleichzeitig tätig. In solchen Fällen muss man manchmal alles neu aufstellen. Das ist ein Riesenaufwand. Bei einem Angriff auf A1 mussten 50.000 Passwörter neu erstellt werden. In solchen Fällen wird es extrem aufwendig. Darin liegt ein Dilemma für kleine Unternehmen. Sie alle brauchen Digitaltechnik. Sonst können sie nicht reüssieren, und alle haben Daten in der Cloud und müssen mobil sein. Doch für die permanente Absicherung steht kein Personal zur Verfügung.

**Niemand ist davor gefeit, attackiert zu werden.**

> **In Österreich ist für Spione viel zu holen.**

**Wie entgeht man diesem Dilemma?** Als Unternehmen mit Hausverstand verkleinert man die Angriffsfläche durch Abkoppelung der wichtigen Systeme von unsicheren. Und man sucht sich einen Partner, der sich umfassend um die IT-Sicherheit kümmert. So wie man eine Schneeräumung, den Steuerberater oder das Facility-Management beauftragt.

**Gerade manches kleinere Unternehmen mag sich aber vielleicht denken: Ich bin zu unbedeutend, um angegriffen zu werden. Ein Irrglaube?** Das ist ein großer Denkfehler. Von dem Gedanken muss man sich schleunigst verabschieden. Der erste Angriff kommt nämlich immer von einer Maschine, die ein Programm abspult. Sie schaut im übertragenen Sinn, wo die Türen offen sind, wo keine Kamera hängt, wo kein Hund Wache hält. Die Maschine klopft Schwächen ab und liefert dem Hacker eine Liste. Niemand ist davor gefeit, attackiert zu werden. Denn auch vielen kleinen Betrieben jeweils 2.000 Euro abzupressen führt zu enormen Summen.

**Österreich ist die Heimat vieler Weltmarktführer. Sind solche Firmen ganz besonders gefährdet?** Definitiv. Und während man eine Erpressung durch Verschlüsselung der eigenen Daten sofort wahrnimmt, wird man jemanden, der Know-how und Betriebsgeheimnisse stehlen will, nicht sofort erkennen. So ein Angreifer legt alles drauf an, möglichst lange unerkannt zu bleiben und Informationen zu stehlen. Oft dauert es mehrere Monate, bis so eine Attacke erkannt wird. Solche Operationen sind sehr geschickt gemacht und durchgeplant. Die Angreifer haben nachrichtendienstliche Aufträge. Wir haben in Österreich 300 Weltmarktführer, die höchst interessant sind für alle Nachrichtendienste der Welt.

**Betrifft das jede Art von Innovation oder insbesondere Unternehmen wie zum Beispiel den Drohnenhersteller Schiebel, die Sicherheitstechnik entwickeln?** Drohnen sind ein Milliarden-Geschäft, das erst aufblüht: von der Landwirtschaft bis zum Militär und der Sicherheitspolizei. Schiebel wird also sicher gezielt von anderen Staaten attackiert. Staatliche Dienste zahlreicher Länder sind verpflichtet, Wirtschaftsspionage zu betreiben.

**Wirklich?** Es klingt natürlich sehr nach James Bond, aber Spione und Geheimagenten kosten sehr viel Geld. Wir müssen davon ausgehen, dass auch viele Diplomaten, die in Wien tätig sind, für entsprechende Nachrichtendienste arbeiten. Solche Mitarbeiter kassieren hohe Gehälter und müssen dafür etwas liefern. In Wien ist viel zu holen, weil die Stadt eine internationale Drehscheibe mit tollen Unternehmen und entscheidenden politischen Institutionen ist. Die heimische Wirtschaft ist innovativ, und auch die Forschung ist sehr gut aufgestellt. Wir gehören zu den reichsten Ländern der Welt. In Österreich ist für Spione viel zu holen. Know-how zu stehlen ist billiger, als es selbst zu entwickeln. Auf 200 Liftanlagen in China steht der Markenname Doppelmayr, aber nur ein Teil davon wurde wirklich von dem Unternehmen gebaut. Es gibt viele solcher Beispiele.

**Was ist der wichtigste Gedanke zum Thema Cybersicherheit, den Unternehmer verinnerlichen sollten?** Sicherheit muss Chefsache sein. Wer operativ für das Thema im Betrieb zuständig ist, muss direkten Zugang zum Chef haben. Der fünfzehnte Zwerg von links kann das nicht machen. Genauso wichtig: Alle im Unternehmen müssen die Spielregeln kennen. Oft wissen die Mitarbeiter nicht einmal, wer der Sicherheitsbeauftragte ist. Es braucht klare Regeln, die alle kennen. Man muss selbst oder durch eine Fachfirma ein Sicherheitskonzept erstellen und es dann leben. Es ist auch wichtig zu begreifen, dass Sicherheit kein Hemmschuh ist, sondern ein Business-Enabler, der immer wichtiger wird. Man kann damit werben, dass Daten in besten Händen sind. Das ist heute ein extrem wichtiger Punkt. Sicherheit ist kein Hindernis, sie ermöglicht vielmehr zusätzliche Geschäfte. ◀


BUCH-TIPP

**MANFRED LAPPE, WALTER J. UNGER: SICHER IM NETZ**

So schützen Sie sich vor Hackern und Betrügern

**TEXT** ALEXANDRA ROTTER

# Schwachstelle Mensch

**Der Mensch, das betonen Sicherheitsexperten unermüdlich, ist in der IT-Security das größte Risiko: Er klickt auf infizierte Anhänge, verwendet schwache Passwörter oder verschickt sensible Daten unverschlüsselt. Was heißt das für Unternehmen?**

Der Mensch ist in der IT-Sicherheit das schwächste Glied", sagt Michael Krausz, CEO der i.s.c. – information security consulting eU. Die Technik kann top aufgestellt sein: „Aber bis zu einem gewissen Grad spielt die menschliche Natur eine Rolle." Die allermeisten Angriffe auf IT-Systeme sind laut Krausz darauf zurückzuführen, dass jemand auf etwas klickt, auf das er besser nicht geklickt hätte. Das zeigt sich auch in Tests: Um herauszufinden, wie sicherheitsbewusst sich Mitarbeiter verhalten, lassen Experten wie Krausz in Unternehmen USB-Sticks oder CDs liegen. In Hinblick auf die IT-Sicherheit ist es ein No-Go, Datenträger zu verwenden, deren Herkunft man nicht kennt: „In USB-Sticks steckt ein Riesen-Bedrohungspotenzial. Daher ist es vernünftig, sein Unternehmen so abzustellen, dass keine oder höchstens verschlüsselte USB-Sticks verwendet werden." Es kann sich Schadsoftware darauf befinden, die sich automatisch installiert und es Angreifern ermöglicht, von außen auf ein System zuzugreifen, Daten zu stehlen, zu manipulieren oder die ganze IT lahmzulegen. Krausz erzählt: „Wenn auf einer CD ‚Vorstandssitzung' steht, interessiert sich keiner dafür. Wenn Sie aber ‚XXX' draufschreiben, macht das die Menschen neugierig und es gibt garantiert einen Mitarbeiter, der die CD in seinen Computer schiebt."

**VERMEINTLICH VERTRAUENSWÜRDIG** „Nicht auf jeden Quargel klicken", wie Krausz sagt, ist eine der Grundregeln, die in jedem IT-Sicherheits-Training vermittelt wird. Und trotzdem wird immer wieder auf „Quargel" geklickt. So kam es etwa dazu, dass sich ein Angreifer in den deutschen Bundestag hacken konnte. In diesem Fall war der Angriff sehr gut geplant und die E-Mail, auf deren Anhang eine Mitarbeiterin klickte, so professionell gefälscht, dass sie kaum Verdacht schöpfen konnte. Michael Krausz erzählt von einem anderen Fall, wo einer seiner Kunden einen Ransomware-Befall hatte: Die Hacker konnten die Verschlüsselungssoftware ins System schleusen, indem sie eine Bewerbung an das Sekretariat schickten. Dieses leitete die Mail an die HR-Abteilung weiter, welche die Bewerbung öffnete, weil die Mail quasi aus vertrauenswürdiger Quelle – dem Sekretariat – kam.

Doch nicht immer sind Angriffe gut gemacht – manchmal ist die Schwäche auch fehlendes Sicherheitsbewusstsein. Krausz: „Sicherheits-Technologie kann man im Sprint installieren, aber nachhaltig Awareness zu betreiben ist ein Marathon." Es könne bis zu zwei Jahre dauern, bis das Bewusstsein im Unternehmen implementiert ist. Wichtig sei nicht, dass Mitarbeiter in Trainings oder Newslettern etwas nur hören oder lesen, „sondern dass sie etwas lernen". Um das sicherzustellen, werden laut Krausz zum Beispiel Online-Tests oder auch Computerspiele, welche die Awareness trainieren, eingesetzt.

**SENSIBILITÄT SCHÄRFEN** Bei der Heinzel Group, einem Unternehmen aus der Papier- und Zellstoffindustrie, machen die Mitarbeiter einmal im Jahr eine IT-Security-Schulung. Außerdem werden immer wieder interne Phishing-Kampagnen durchgeführt, um die Awareness zu testen. Einmal wird dabei etwa ein Preisausschreiben vorgegaukelt, dann wieder steht in einer Mail, es sei ein Update nötig und man müsse dafür sein Kennwort eingeben. Barbara Potisk-Eibensteiner, CFO der Heinzel Holding GmbH, sagt: „Diese Maßnahmen sind nicht sehr aufwendig, aber sie schärfen die Sensibilität." Dabei geht es nicht darum, diejenigen, die in die Falle getappt sind, an den Pranger zu stellen, sondern gemeinsam besser zu werden. Potisk-Eibensteiner hält die Menschen für das mit Abstand größere Gefahrenpotenzial in der Cyber-Security als die Technik: „Ich glaube, die besten Firewalls helfen nicht, wenn die Sensibilität bei den Mitarbeitern fehlt." Und wie

**Die besten Firewalls helfen nicht, wenn die Sensibilität bei den Mitarbeitern fehlt.**

Barbara Potisk-Eibensteiner, Heinzel Holding

Foto: Heinzel Group Illu: Vetvector / Getty Images

leicht oder schwer ist es, das Bewusstsein im Unternehmen für IT-Sicherheit zu stärken? „Ich glaube, das ist eine Kulturfrage“, sagt Potisk-Eibensteiner. „So wie wir auf unsere Waren und Maschinen aufpassen, betrachten wir auch Informationen und Daten als hohes und wertvolles Gut.“ Nur Verbote auszusprechen hält sie für falsch. Viel eher gehe es darum, den Mitarbeitern zu erklären, warum gewisse Verhaltensweisen wie etwa die Verwendung eines USB-Sticks gefährlich sein können. Es gebe auch viel Verständnis dafür, dass der Sicherheit wegen „da und dort noch ein Passwort eingegeben werden muss“. Ein ungeschriebenes Gesetz laute: Ist man sich nicht sicher, ob man auf einen Link oder Anhang klicken oder sein Passwort eingeben soll, soll man sich an die IT wenden und nachfragen. Als Papier- und Zellstoff-Unternehmen habe man zudem die Möglichkeit, bestimmte Webseiten zu sperren: Ist es dennoch notwendig, eine dieser Seiten anzusurfen, kann die IT diese freischalten.

„Fragen, fragen, fragen“, das sollen Mitarbeiter laut Robert Lamprecht, Director im Bereich Cyber-Security beim Wirtschaftsprüfungs- und Beratungsunternehmen KPMG, wenn sie sich in einer IT-Security-Frage unsicher sind. Dabei betont er, dass sie sich nicht immer gleich an die IT-Abteilung wenden müssen: „Wir müssen eher als Gruppe denken und gemeinsam Upskilling betreiben.“ Wenn zum Beispiel ein Kollege im Rechnungswesen durch den Versuch eines CEO-Frauds attackiert wird, sollte er sich zuerst an sein Team wenden, welches durch Sicherheits-Trainings dazu befähigt wurde, den Kollegen zu helfen. Diese Fähigkeiten werden vor allem in jährlichen Schulungen aufgebaut. Lamprecht betont, wie wichtig es dabei ist, die richtige Sprache zu finden: „Die Kunst ist, das Ganze in Geschichten zu verpacken und die Mitarbeiter auf der emotionalen Ebene anzusprechen.“ Und es brauche eine überschaubare Auswahl konkreter Tipps, Tricks und Handlungsanweisungen. Übrigens: Die Ergebnisse der aktuellen KPMG-Studie „Cyber-Security in Österreich“, die Lamprecht jedes Jahr verfasst, bestätigen: Bei allen aktuellen Top-3-Angriffsmethoden – Phishing-Attacken, CEO-Fraud und Malware-Angriffen – geht es darum, die Schwachstelle Mensch auszunützen. ◀

**TEXT** ALEXANDRA ROTTER

# Gefährliche Hintertüren

**Wenn Software-Entwickler Sicherheitslücken beheben, ist die Gefahr nicht automatisch gebannt. Sind Hacker bereits tief genug in ein System vorgedrungen, können sie trotz Updates weiter ungestört ihr Unwesen treiben. Doch viele Unternehmen wissen nichts davon.**

Sicherheitslücken in Software sind fiese Bedrohungen: Denn man muss nicht erst irgendwo draufklicken oder eine Datei herunterladen, um zum Angriffsziel zu werden. Es reicht, die betroffene Software mit der Sicherheitslücke am Rechner zu haben – und schon ist man ein potenzielles Hacking-Opfer. Das ist so lange egal, solange niemand die Lücke entdeckt. Doch wenn sie Hackern bekannt ist, können sie die Schwachstellen mit sogenannten Exploits ausnützen. Die Info macht meist schnell die Runde in der Szene, sodass plötzlich viele Angreifer unterwegs sind und verschiedene Ziele attackieren. Und je länger die Softwareentwickler nichts davon erfahren, desto länger bleiben die Angreifer in den Systemen ungestört.

Zuletzt sorgte eine solche Schwachstelle im E-Mail-Programm Exchange von Microsoft, das in vielen Firmen und Behörden genutzt wird, für massenhafte Hacks. Angegriffen wurden unter anderem das Parlament in Norwegen, das deutsche Umweltbundesamt und die Bankenaufsichtsbehörde der EU. Außerdem sollen die Hacker mehr als 100.000 Server von Unternehmen übernommen haben. Allgemein sind laut Wolfgang Ebner, Präsident des Kuratoriums Sicheres Österreich (KSÖ), eher Unternehmen als Privatpersonen gefährdet, angegriffen zu werden: „Es kann natürlich auch eine gezielte Attacke auf eine Privatperson geben, aber Unternehmen sind für Angreifer viel interessanter." Der Grund ist schlicht: Dort gibt es mehr zu holen: „Kriminelle Organisationen suchen sich gut aus, ob sich ein Angriff für sie auszahlt oder nicht."

**KEIN ÖFFENTLICHER PRÜFVORGANG** Benjamin Weissmann, Leiter der Cyberforensik bei EY Österreich, erklärt, wie es in der Regel zu Softwarelücken kommt: „Jede Software ist von Menschen programmiert, und Menschen machen Fehler." Eine Software bestehe aus Abermillionen Zeilen Code: „Da den Überblick und den Fokus auf Sicherheit zu behalten ist selbst für große Entwickler-Teams eine Herkulesaufgabe." Zwar beginne sich der Security-by-Design-Ansatz durchzusetzen, was so viel heißt, dass Sicherheitsaspekte in allen Phasen und Bereichen der Programmierung grundlegend mitzubedenken sind. Bei den Microsofts und Googles dieser Welt testen auch qualitätssichernde Teams die Software durch. Doch „selbst die Großen sind überfordert davon, eine Übersicht über den Code zu behalten". Während etwa ein wissenschaftlicher Artikel in Peer-Reviews von anderen Wissenschaftlern auf Herz und Nieren geprüft wird, gebe es bei einem Großteil der Software keinen solchen öffentlichen Prüfvorgang. Weissmann weist zudem auf den „Wildwuchs bei Software" hin. So würde etwa bei Start-ups, die zum Beispiel eine App schnell herausbringen wollen, selten eine Prüfung der Sicherheitsqualität durchgeführt. Und manchmal werden Sicherheitslücken sogar absichtlich eingebaut. Weissmann kennt einen Fall, wo ein Online-Poker-Anbieter es auf diese Weise möglich machte, in die Karten der Spieler zu schauen. Auch könne es sein, dass Geheimdienstmitarbeiter in die Programmierteams eingeschleust werden und bewusst Lücken einbauen, damit User später im staatlichen Interesse spioniert und ausgespäht werden können.

**EINGEBAUTE HINTERTÜREN** Doch was tun, wenn man eine Software verwendet, von der bekannt wird, dass sie eine Sicherheitslücke hat? Meist heißt es dann in den Medien, die Sicherheitslücke sei geschlossen, und als User muss man ein Update machen. Doch selbst nach dem Update ist die Gefahr

Illu: klyaksun/GettyImages

nicht unbedingt gebannt. Denn erstens weiß man nicht, ob man bereits Opfer eines Hacks war und womöglich Daten abgezogen wurden. Und zweitens kann es sein, dass die Hacker Hintertüren eingebaut haben und so tief ins System vorgedrungen sind, dass sie, auch nachdem Sicherheitslücken geschlossen wurden, weiter ihr Unwesen treiben können. Denn laut Weissmann zielen solche Angriffe oft nicht auf die mangelhafte Software ab: „Oft ist es das Hauptziel der Hacker, so weit in ein Netzwerk vorzudringen, dass man sie, selbst wenn man sie entdeckt, nicht so leicht loswird, weil sie sich zum Beispiel schon eigene Benutzeraccounts mit administrativen Rechten angelegt haben." Betroffene Unternehmen sollten sich daher nach dem Installieren des Updates nicht zurücklehnen, sondern herausfinden, ob Angreifer im System waren – und vor allem noch sind. Wenn das der Fall ist, können sich Cyber-Forensiker wie Weissmann gezielt auf die Suche machen. Doch so eine Spurensuche kostet Geld, das Unternehmen ungern ausgeben, wenn sie subjektiv das Gefühl haben, die Gefahr sei mit dem Update ohnehin gebannt.

**PLANSPIELE FÜR DEN ERNSTFALL** Und kann man im Vorhinein etwas tun, um sich vor Exploits zu schützen? Laut Wolfgang Ebner vom KSÖ spielt zunächst die Wahl des Software-Herstellers eine Rolle: „Je ausgeprägter der Bekanntheitsgrad der Hersteller, desto eher werden sie sich mit Sicherheitsfragen beschäftigen." Auch Daten in bekannten Clouds abzuspeichern, hält Ebner für empfehlenswert, weil auch dort davon auszugehen sei, dass die Anbieter sehr hohe Sicherheitsstandards einsetzen. Software-Updates laufend zu installieren ist der nächste Tipp, denn diese Updates mit neuen Funktionen oder Designs seien in Wirklichkeit entdeckte Schwachstellen, die behoben werden, bevor sie ausgenutzt werden konnten. Außerdem empfiehlt es sich laut Ebner im Geschäftsbereich, Penetrationstests oder Krisenmanagement-Planspiele durchzuführen: „Schon KMU mit 50 Mitarbeitern aufwärts können zum Beispiel durchspielen, was im Unternehmen passiert, wenn Daten abgesaugt werden."

Bei aller Gefahr betont Wolfgang Ebner aber, dass Unternehmen nicht vor Digitalisierungsschritten wie zum Beispiel der Implementierung eines Webshops zurückschrecken sollten: „Durch die Digitalisierung passiert zwar viel, aber es ist auch sehr vieles möglich." Eine hundertprozentige Sicherheit gebe es nie, aber Risiken ließen sich minimieren. Und für den möglichen Schadensfall, der schlimmstenfalls auch richtig ins Geld gehen kann, gibt es mittlerweile auch immer mehr Cyber-Versicherungen für den Business-Bereich. ◀

**TEXT** STEFAN GRAMPELHUBER

# EINBRUCH? SICHER NICHT!

**Einbruch, Brand, Sabotage. Jedes Unternehmen hat andere Sicherheitsansprüche. Zum Glück kosten auch maßgeschneiderte Schutzkonzepte heute nicht mehr die Welt. Ein Überblick.**

F

Freitagnachmittag. Eine Drogerie in der Wiener Innenstadt. Geschäftiges Treiben. Die einzige Verkäuferin präsentiert einer Kundin Eyeliner und Wimperntusche. Eine weitere Dame wartet schon, schaut nervös auf ihre Armbanduhr. Etwas abseits stehen zwei Männer vor einem Parfum-Regal. Einer der beiden nimmt einen Flakon und steckt ihn rasch in die Tasche des anderen. Das gleiche Spiel wiederholen sie dreimal. Die Diebe verlassen das Geschäft, ohne dass der Diebstahl bemerkt wird.

Nach der monatelangen Corona-Zwangspause tummelt es sich im stationären Einzelhandel nun wieder. Gerade in den ersten Tagen nach der Öffnung im Mai strömten viele Kunden mit leuchtenden Augen und voller Vorfreude in die Geschäfte. Zusätzlich angelockt von günstigen Preisen und Aktionsangeboten. Aber mit der Kundenfrequenz steigt auch die Zahl der Ladendiebstähle. Hochsaison für Langfinger ist deshalb auch der Dezember, wenn wir unsere Weihnachtseinkäufe tätigen. Dann sind nämlich nicht nur besonders viele Menschen in den Geschäften anzutreffen, sondern es lässt sich auch die gestohlene Ware gut unter dicken Winterjacken verstecken.

Der volkswirtschaftliche Schaden von Ladendiebstahl ist beträchtlich. Laut Schätzungen der Wirtschaftskammer Österreich lässt sich dieser mit 0,55 Prozent des Bruttoumsatzes im Einzelhandel beziffern. Oder in absoluten Zahlen ausgedrückt: 430 Millionen Euro verlor Österreichs Wirtschaft durch Diebstahl im letzten „regulären“ Geschäftsjahr 2019, also im Jahr vor Ausbruch der Pandemie. „Im Handel wird nach wie vor gestohlen, was nicht niet- und nagelfest ist“, sagt Frank Horst vom Kölner Handelsforschungsinstitut EHI. Er veröffentlicht einmal jährlich eine Studie zu Inventurdifferenzen im deutschen Handel, an der über 20.000 Verkaufsstellen teilnehmen.

„Generell gilt: Was sich gut verkauft, wird auch oft geklaut“, heißt es in der Studie. So verwundert es nicht, dass sich während der Pandemie Desinfektionsmittel und Hygienepapier zu wahren Diebstahl-Rennern entwickelten. Im Modehandel führen Markenbekleidung, Jeans und Turnschuhe das Ranking. Besonders gefragtes Diebesgut in den Elektro-Geschäften sind Konsolenspiele und Smartphones. In Supermärkten sind Spirituosen und in Drogerien die eingangs erwähnten Parfums besonders beliebt. Auch die Daten und Einschätzungen einiger Betriebe aus Österreich fanden Eingang in die EHI-Studie. Schlüsselergebnisse lassen sich deshalb auf Österreich übertragen. Damit Diebstahl erst gar nicht passieren kann, investieren viele Unternehmer in die elektronische Warensicherung. Bei Textilien funktionieren diese Lösungen schon recht gut. Je kleiner die Produkte, desto schwieriger wird es aber, derartige Systeme in die Waren zu integrieren.

**GEFAHR IST NICHT GLEICH GEFAHR** Diebstahl mag im stationären Einzelhandel eine wichtige Rolle spielen, in anders ausgerichteten Unternehmen ist er kein großes Thema. Etwa im Gewerbe oder im Dienstleistungssektor. Selbst die Folgen eines nächtlichen Einbruchs, bei dem ein paar Scheine aus der Handkassa, ein Laptop und ein Drucker entwendet werden, sind hier überschaubar. Zerstört aber ein Brand einen teuren Rohstoff und muss die Arbeit in Folge mehrere Wochen lang eingestellt werden, dann droht enormer Schaden. Derlei Risiken jenseits des klassischen Einbruchs gibt es eine ganze Reihe – vom Schädlingsbefall verderblicher Güter bis zur Sabotage durch einen Konkurrenzbetrieb.

**RISIKEN DEFINIEREN UND PRIORISIEREN** Deshalb gilt es, so der Rat von Experten, für jedes Unternehmen – egal welcher Größe oder Branche – eine passgenaue Sicherheitslösung zu entwickeln. „Der erste Schritt ist eine detaillierte Gefahrenanalyse durch ein professionelles Sicherheitsunternehmen. Dabei werden alle möglichen Risiken erfasst und priori-

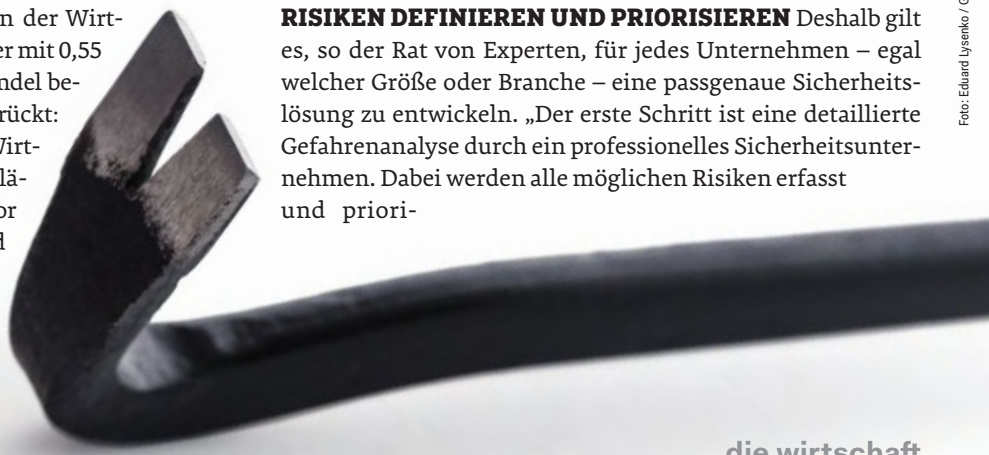


Foto: Eduard Lysenko / Getty Images

Andreas Teischl, VSÖ

**Der erste Schritt ist eine detaillierte Gefahrenanalyse.**

Foto: beigestellt

siert. Diese Analyse ist Basis für ein wirkungsvolles Schutzkonzept", sagt Andreas Teischl, Generalsekretär des Verbandes der Sicherheitsunternehmen Österreichs (VSÖ).

Darauf aufbauend, erarbeiten Fachleute ein Maßnahmenpaket, das den Betrieb entsprechend seinen Erfordernissen und Schwachstellen schützt. Dazu gehören etwa eine Alarmanlage und Videoüberwachung, aber auch Bewegungsmelder, ein Notrufsystem oder bauliche Veränderungen, die ein Eindringen unerwünschter Gäste erschweren. „Einige Unternehmen, vor allem kleinere, schrecken noch davor zurück, weil sie denken, dass die Anschaffung dieser Kontrollsysteme mit hohen Kosten verbunden ist", sagt Andreas Teischl. Aber das stimme heute nicht mehr. Es gebe mittlerweile eine Reihe von Lösungen, die exakt für KMU-Bedürfnisse entwickelt wurden und keiner großen Investitionen bedürfen.

**DIE SCHLÜSSELFRAGE KLÄREN** So gibt es zum Beispiel modular aufgebaute Systeme wie elektronische Schließanlagen, die sich besonders gut bei kleinen Einheiten einsetzen lassen. Mechanische Schlüssel werden deshalb zunehmend von der Bildfläche verschwinden und durch Transponder, Smartcards und digitale Schließzylinder ersetzt werden. Interessant für KMU sind außerdem Offline-Zutrittssysteme, die man unkompliziert zu einer Funk-Programmierung ausbauen kann. Bei Mobile-Access-Lösungen fungiert wiederum das Smartphone als digitaler Schlüssel. Und für den Brandschutz können wartungsfreie Feuerlöscher für KMU attraktiv sein. Sie werden aus verdichtetem Kunststoff gefertigt, sind leichter und korrosionsresistenter als Löschgeräte aus Stahl – und deshalb besonders langlebig. Bei der Videoüberwachung haben sich IP-basierte Systeme durchgesetzt, die mit niedrigeren Betriebskosten als analoge Geräte verbunden sind. Im Einzelhandel punkten zur Abschreckung von Ladendieben Kombinationen aus Videokamera- und Audiosystem. Weil Audiosignale durch die kamerainterne Analyse gewisser Geräusche ausgelöst werden, verkürzt sich die Reaktionszeit bei Einbruchsversuchen. Und das kann entscheidend sein, um den Täter auf frischer Tat zu schnappen und dingfest zu machen.

**HIGHTECH FÜR HOHE ANSPRÜCHE** Als große Entlastung betrachten viele Betriebe sogenannte integrierte Sicherheitslösungen. Dabei gilt es, technische Systeme mit personellen und organisatorischen Maßnahmen, etwa einem Alarmmanagement, zu kombinieren. Qualifizierte Fachkräfte übernehmen die technische Installation, man bekommt sozusagen alles aus einer Hand. Der Kunde bezahlt dann eine Monatspauschale. Natürlich gibt es auch Hightech-Systeme, deren Anschaffung mit hohen Kosten verbunden ist. Aber diese Systeme müssen dann auch besonders hohe Sicherheitsansprüche erfüllen und kommen zum Beispiel bei Juweliergeschäften oder Banken zum Einsatz. ◀

**INFOS**

**KMU FINDEN MASSGESCHNEIDERTE LÖSUNGEN**
für den Objektschutz wie Alarmanlagen und elektronische Zutrittssysteme u. a. bei diesen Anbietern:

A1 Telekom Austria: *a1.net/gebaeudesicherheit*
Dormakaba Austria: *dormakaba.com/at-de*
Kapsch Security Solutions: *kapsch.net*
Labor Strauss Sicherheitsanlagenbau: *laborstrauss.com*
G4S Security Systems: *g4s.com*
ÖWD Security Systems: *owd.at/sicherheitstechnik*
PKE Electronics GmbH: *pke.at*
Siemens Österreich Sicherheitstechnik: *siemens.com/sicherheit*

**TEXT** MARA LEICHT

# Nachhaltig agieren, Firma schützen

**Nachhaltigkeit begann klein im Risikomanagement. Mittlerweile ist sie um viele Dimensionen reicher geworden. Doch nach wie vor schützt sie Unternehmen vor Ungemach – wenn sie wirklich gelebt wird.**

Zur Jahrtausendwende war Nachhaltigkeit ein Thema für Philanthropen. Umwelt, Soziales und interne Transparenz interessierten nur Gutmenschen oder Bluffer, hieß es. Erst 2010 schaffte die Nachhaltigkeit über das Risikomanagement Einzug in die Köpfe der Entscheider. Wir erinnern uns: Die Finanzkrise provozierte jede Menge regulatorischer und Compliance-Vorgaben. Gebot der Stunde war es, blitzartig zu lernen, langfristig statt in schnellem Profit zu denken. Auf einmal war nachhaltig zu wirtschaften ein probates Mittel, künftigen Unbill vom Unternehmen fernzuhalten. Erst um 2016 poppte dann bei mehr und mehr Betrieben die große Erkenntnis auf: Da stecken ja Chancen drinnen!

So kurzweilig klingt es, wenn der Kölner Strategieprofessor René Schmidpeter das Aufblühen des einstigen Nischenthemas beschreibt. Schmidpeter, Mitgestalter mehrerer Thinktanks und Gründer der M3trix GmbH, gilt als Vordenker auf diesem Gebiet. Zwar dachten die meisten Familienunternehmen schon immer in Generationen, so manche andere aber nicht: „Früher sagte man, zuerst muss ich Geld verdienen, dann schaue ich, wie viel Nachhaltigkeit ich mir leisten kann. Dieser Trade-off löst sich gerade auf."

Ihrem Sprungbrett Risikomanagement bleibt das Thema treu. „Strategisch nachhaltige Geschäftsmodelle haben einen höheren risikoadjustierenden ROI", sagt Schmidpeter, jetzt ganz Professor. Haupttreiber sind – nein, nicht die Gesetzgeber, sondern die Investoren. „Sie suchen Investments, die beides sind: profitabel und nachhaltig." Nach manchem Totalverlust wegen des Klimawandels, disruptiver Innovationen, des Preisverfalls „alter" Technologien oder wegen eines bösen Shitstorms sitzt vielen der Schreck in den Knochen. „Deshalb verlagern sie ihr Geld in nachhaltige Geschäftsmodelle. Nachhaltigkeit ist nicht mehr diskutabel."

**MARKT NOCH LANGE NICHT GESÄTTIGT** Das spiegelt sich auch in der Welt der großen Konzerne. Dort lösen neuerdings „Impact"-Reports die früheren Nachhaltigkeitsberichte ab, die oft ein wenig nach Greenwashing rochen. Schmidpeter genießt auch Impact-Reports mit Vorsicht: „Sie bedeuten nicht, dass Tesla, Nike oder Shell tatsächlich nachhaltig sind. Sie sagen nur, dass sie die neue Logik implementiert haben."

Gerade das ist für Unternehmen schwierig, solange alle Aufmerksamkeit dem Kerngeschäft gilt. „Unternehmenslenker müssen den Blick darüber hinaus heben und das neue Denken in alle Unternehmensbereiche integrieren." Je schneller, desto besser: „Wir sehen das bei allen großen Transformationen: Der First-Mover-Advantage ist sehr stark." Und, als Ansporn: „Der Markt ist noch lange nicht gesättigt."

Dieses Momentum bestätigt auch Karin Steppan, Sonderbeauftragte Nachhaltigkeit & CSR bei der Raiffeisenlandesbank NÖ-Wien: „Früher hat man Nachhaltigkeit als eine stra-

**Investoren suchen Investments, die profitabel und nachhaltig sind.**

Rene Schmidpeter, Nachhaltigkeitsexperte

Foto: M3trix Illu: lemono / Getty Images

tegische Option gesehen – kann man, muss man aber nicht. Jetzt muss man." Sie empfiehlt, in zwei Richtungen denken: Was macht die Umwelt/das Umfeld mit meinem Unternehmen? Und was macht mein Unternehmen mit der Umwelt/dem Umfeld? Bei Ersterem sollte der Obstbauer über neue Obstsorten nachdenken, wenn schon wieder der Frühlingsfrost seine Blüte zerstört. Bei Zweiterem muss der Glasverarbeiter schweren Herzens den generationenalten Familienbetrieb verlegen, wenn der nahe Bach seinen Wasserverbrauch nicht mehr stillen kann. Oder kann er mit neuen Technologien Wasser sparen? Das Schwierigste, sagt Steppan, ist, sich von Geschäftsbereichen oder -modellen zu trennen, denen man sich lange und mit Erfolg widmete. Im Vergleich dazu sei es für Geschäftsführer nur Daily Business, eine neue, sparsamere Maschine anzuschaffen. An die Moral gehe es wiederum, wenn ein Produzent herausfindet, dass es einer seiner Zulieferer mit dem Arbeitsrecht nicht so genau nahm: „Dann muss er sich auch mit der Frage auseinandersetzen, wie wichtig ihm das selbst ist."

Und welches Risiko es birgt. Womit wir wieder beim Risikomanagement sind. Unternehmer stehen vor etlichen Risikokategorien, doch Steppan beruhigt: „In Österreich gibt es viele Instrumente und Stellen, an die man sich wenden kann." Hier sind die häufigsten Risiken und Steppans bevorzugte Anlaufstellen dafür. Über allen thront für sie – natürlich – die Hausbank:

- Technologische Risiken. Klassisches Beispiel: Ein Planenhersteller will aus Umweltschutzgründen weg vom Kunststoff – „Bei einer Kooperation mit einer universitären Einrichtung oder einem Kompetenzzentrum hilft ihm die For-

**KEINE CHANCE OHNE RISIKO** Risiken sind nichts anderes als positive oder negative Abweichungen vom Gesamtplan. Das Risikomanagement ermittelt Gefahrenbandbreiten, um Abweichungen und ihre Folgen einzugrenzen und eine Entscheidungsbasis zu liefern. Vergangenheitsbezogene Daten helfen dabei nur bedingt, weil Risiken immer spontaner, disruptiver und unvorhersehbarer werden. Deshalb arbeiten Risikomanager mit Trendlandschaften, dynamischen Risk-Maps, Szenarienplanung (Best Case / Worst Case) und IT-gestützter Simulation.

**ABGRENZUNG ZUM CONTROLLING** Im Unterschied zu diesem Gesamtansatz liefert das Controlling Punktprognosen, wenn es etwa für eine Investition die zu erwartende Rendite mit zu erwartenden Kosten vergleicht. Beide Disziplinen haben ihre Berechtigung und sollten Hand in Hand arbeiten.

**EIN PAAR NÜTZLICHE BEGRIFFE** Bruttorisiko meint das Schadensausmaß, wenn man „es einfach laufen lässt": ein Risiko zwar identifiziert, aber keine Präventivmaßnahmen setzt. Nettorisiko bezeichnet das Restrisiko, das nach Einsatz aller Maßnahmen bleibt.

**DAS RISIKOINVENTAR** ist eine Liste der wichtigsten Gefahren. Sie dient als Basis für die monetäre Bewertung und Gegenmaßnahmen.

**DIE KENNZAHL VALUE AT RISK** quantifiziert den theoretischen Höchstschaden, der bei einer vorgegebenen Wahrscheinlichkeit nicht überschritten wird.

**RISIKOARTEN UND BEISPIELE**

- Umwelt- und Klimarisiken: Klimawandel, Ressourcenknappheit
- Politische Risiken: Unruhen, Exportembargos
- Regulatorische Risiken: Gesetzesänderungen, Umweltauflagen
- Sozio-kulturelle Risiken: demografische Veränderungen, verändertes Verbraucherverhalten
- Technologische Risiken: disruptive Technologien, Digitalisierung, Preisverfall konventioneller Technologien
- Strategische Risiken: Marktveränderungen, Produktportfolio, Standort
- Operative Risiken: Produktionskapazitäten, Maschinenausfälle, menschliches Versagen
- Finanzielle Risiken: Bonität, Liquiditätsengpässe, Wechselkurse, Kreditzinsen, Rohstoffpreise
- Personelle Risiken: Fachkräftemangel, Fluktuation
- IT-Risiken: Hacker, Viren, Trojaner, Serverausfälle

**PHASEN DES RISIKOMANAGEMENTS**

**1. Risikoidentifikation:** Die meisten Unternehmen hanteln sich entlang der Wertschöpfungskette und identifizieren Risiken anhand von Ursache und Herkunft (z. B. IT, Einkauf, Personal). Eine andere Option ist, ihre Wirkung auf Unternehmensziele oder -bereiche zu errechnen (z. B. Ertrag, Liquidität, Kapital).

**2. Risikobeurteilung:** Die in- und externen Risiken finden ihren Niederschlag in der Risk-Map, wo ihnen Eintrittswahrscheinlichkeiten zugeordnet werden. Schwachstelle: Letztere sind willkürliche Annahmen, die auch Interdependenzen nicht berücksichtigen.

**3. Risikosteuerung:** An der Ursache anzusetzen heißt, das Auftreten des Risikos möglichst zu verhindern. Dann müssten riskante Projekte abgeblasen werden, was auch die Chancen killt, die in ihnen stecken. Unternehmerischer ist es, Risiken zu minimieren. Interne Maßnahmen dafür sind Frühwarnsysteme, Notfallpläne, Risikostreuung und das Setzen von Limits. Externe Klassiker sind Abwälzen (Versicherungen) und Verlagern des Risikos auf Dritte, etwa auf Kunden, Partner (z. B. Joint Venture) und Lieferanten (z. B. Rahmenvereinbarungen mit Ersatzlieferanten). Faustregeln: Nur operative Risiken lassen sich versichern, strategische nicht. Und finanzwirtschaftliche Risiken lassen sich etwa mit Anleihen oder Derivaten abfedern.

**4. Risikoüberwachung:** Tritt der Fall des Falles ein, kontrolliert der Risikomanager das Umsetzen der geplanten Maßnahmen und passt sie ggf. an. Vorausschauend prüft er regelmäßig, ob sich Rahmenbedingungen und Eintrittswahrscheinlichkeiten ändern.

Trotz seiner überlebenswichtigen Bedeutung wird das Risikomanagement oft stiefmütterlich behandelt. Schon klar, es zahlt wenig zum operativen Erfolg ein. Auch scheint es mit seiner pessimistisch-vorsichtigen Grundhaltung zu bremsen. Deshalb sollte es hierarchisch möglichst hoch angesiedelt sein, am besten auf C-Level, um die nötige Rückendeckung zu haben. Sein wahrer Wert zeigt sich erst im Fall der Katastrophe, wenn dank seiner Vorarbeit Schäden rasch und schmerzarm abgewendet werden können. Oder wenn sie gar nicht erst eintreten – dann kassiert garantiert der CEO die Lorbeeren.

schungsförderungsgesellschaft (FFG), die Entwicklungsrisiken mit Haftungen und Zuschüssen abzufedern." Geht es um IT-Risiken und das Schreckgespenst Hackerangriff, ist das wie jedes Projekt anzugehen: mit einem kompetenten IT-Partner und einem guten Konzept.

- Marktrisiken: Donald Trumps Handelsrestriktionen ärgerten auch so manchen heimischen Produzenten. Für Steppan „eine Rechenaufgabe, ob sich der Export in ein bestimmtes Land noch rentiert. Oder ob ich andere Zielländer brauche."
- Reputationsrisiken: Ein Shitstorm lässt sich nie ganz verhindern, aber man kann sich wappnen. Indem man erstens wieder von außen nach innen denkt. Beispiel: Was tun, wenn ein Zulieferer als Umwelt- oder Sozialsünder enttarnt wird? Präventiv helfen hier vertragliche Standards, im Fall des Falles das Bekenntnis zu prompter Wiedergutmachung. Die zweite Denkrichtung ist wieder von innen nach außen. Beispiel: Was tun, wenn ein gedankenloser Mitarbeiter die Firma in die Schlagzeilen bringt? Steppan: „Das fällt unter Good Governance. Ich muss meine Werte und Regeln niederschreiben und allen zur Kenntnis gebracht haben."
- Politische und rechtliche Risiken: In Österreich ist das für die meisten Unternehmen kein Thema. Anders im Ausland. Als Absicherung stehen – neben der Hausbank und dem Anwalt des Vertrauens – die Garantieinstrumente der Kontrollbank und die Informationsleistung der Kammern offen: „Auch Information sichert gegen Risiko ab."

All das durchzudenken ist Aufgabe des Risikomanagements und – eine Ebene darüber – der Geschäftsführung. Leider wird das Thema in vielen, vor allem sehr kleinen oder jungen Unternehmen stiefmütterlich behandelt. Bis es eben kracht. Damit es erst gar nicht so weit kommt, gibt es oberhalb noch einen kurzen Crashkurs. ◀






bmf.gv.at/ecommerce

# Es sind auch die kleinen Dinge, die zählen

## Fairness für den österreichischen Handel

Bundesministerium
Finanzen

Ab 1. Juli 2021 werden alle Online-Bestellungen ab dem 1. Cent gleich besteuert – egal, woher die Produkte kommen. So wird die heimische Wirtschaft geschützt.

Alle Informationen auf **bmf.gv.at/ecommerce**
oder unter **050 233 729**

**TEXT** MARA LEICHT

# Rechtsvertretung nach Maß

**Eine Großkanzlei, um alles abzudecken? Ein Haus- und Hofjurist, der die Firma wie seine Westentasche kennt? Oder eine schnelle KI? Unternehmen können ihr juristisches Sicherheitsnetz auf verschiedene Arten knüpfen.**

Ein Lebensmittelproduzent erfährt aus den Medien, dass eine Charge seine Produktes durch Glassplitter verunreinigt war und Konsumenten schon eine Sammelklage vorbereiten. Ein Mitarbeiter hat versucht, einen Beamten zu schmieren. Ein Schlüsselkunde ist insolvent. Oder das eigene Unternehmen ist nahe dran, es zu werden. Wenn es im Business haarig wird, ist guter Rat teuer. Die meisten Unternehmen, selbst sehr kleine, haben einen Hausanwalt, oft seit dem ersten Tag ihres Bestehens. Doch der stößt bei Spezialfällen schnell an seine Grenzen. Wie sich wappnen?

„Eine Aufgabe für das Risikomanagement", sagt Clemens Grossmayer, CMS-Partner und Rechtsanwalt für Gesellschaftsrecht. „Das Risikoprofil des Unternehmens durchgehen, was alles passieren kann, und sich Reaktionen überlegen, bevor der Fall des Falles eintritt." Doch einen Risikomanager muss man sich erst einmal leisten können. Und der Geschäftsführer steckt zu tief im Kerngeschäft. Also vorausschauend eine Großkanzlei engagieren, die für alle Eventualitäten Spezialisten an Bord hat? Damit schläft es sich tatsächlich besser. Allerdings: Je größer und je internationaler die Kanzlei, desto höher ihre Overheadkosten. Die weltbekannte Marke, die fancy Locations und die drei Models an der Rezeption müssen bezahlt werden.

Manche Unternehmen finden ihren Königsweg in einer überschaubar großen Anwaltsboutique mit zehn bis 20 Rechtsanwälten, die unterschiedliche Fachgebiete abdecken. Hier sind die Overheads erträglich, was sich in erfreulichen Stundensätzen unter 200 Euro niederschlägt. Einen klingenden Markennamen darf man sich aber nicht erwarten.

**DIE JAGD NACH DEM SPEZIALISTEN** Eine andere Option ist, sich für jede Eventualität einen Spezialisten zu suchen. Die Idee könnte von einem Einkaufschef stammen: viele Rahmenvereinbarungen, dafür muss man sich im Ernstfall nicht mit Honorarverhandlungen aufhalten. Praktikabel ist das nur dann, wenn eine gewisse Gefahrenneigung oder ein voraussichtlicher Beratungsbedarf absehbar ist, meint Gesellschafts- und Unternehmensrechtanwalt Christian Vitali. Er selbst lebt in der Kanzlei Tanos Vitali Zupancic eine Kooperation dreier selbstständiger Rechtsanwälte, die einander ergänzen. Von einer umfassenden Vorabvereinbarung hält er wenig: „Das ufert aus. Würde man sich viele Spezialisten in petto halten, nach dem Motto, ‚Wenn mal was ist, darf ich Sie dann anrufen?' – da sagt ohnehin kein Anwalt Nein." Auch weil sich schon ein Grund findet, im Ernstfall mit Verweis auf die Komplexität des Falles die Stundensätze hinaufzuargumentieren. Die Kanzlei des langjährigen Vertrauens ist hier kulanter.

CMS-Partner Grossmayer zieht die Analogie zum praktischen Arzt: „Soweit er kann, wird er weiterhelfen. Und sonst etwa an den Internisten, den Augenarzt oder den Neurologen verweisen." Eine Idee, der auch Vitali zustimmt: „Ein Allgemeinjurist kennt sicher jemanden, der speziell weiterhilft. Das ist Vertrauenssache." Ob diese Variante dann auch kostengünstiger ist, darauf will Vitali sich nicht festlegen. „Es gibt Einzelkämpfer mit Stundensätzen, da legt man die Ohren an." Jedenfalls sollte man sich solche Honorarnoten ge-

**Unternehmen sollten sich Reaktionen überlegen, bevor der Fall des Falles eintritt.**

Clemens Grossmayer, CMS

nau anschauen. Finden sich darauf auffallend hohe Recherchekosten, ist Nachfragen angesagt: Ein Experte für ein bestimmtes Rechtsgebiet sollte seine Expertise auch ohne langes Nachschlagen abrufen können. Eine andere gern genutzte Möglichkeit, wenn der Hausanwalt ein Fachgebiet nicht abdeckt: Er übernimmt die Causa dennoch zu seinen üblichen Konditionen und substituiert das fremde Fachgebiet an einen Kollegen. Den bezahlt er selbst. Wer sich seine Professionals lieber selbst sucht, wird in der Datenbank der Rechtsanwaltskammer sicher fündig. Ein Angebot ist schnell eingeholt. Oder eine kostenlose Erstberatung in Anspruch genommen. Die Wiener Rechtsanwaltskammer bietet das etwa gegen Voranmeldung. Allerdings: Große Probleme löst man in solchen maximal 15 Minuten sicher nicht.

**GO DIGITAL!** Es gibt auch vielversprechende Legal-Tech-Unternehmen. Nicht nur für die Anwaltssuche. Das Vorlagenportal (www.vorlagenportal.at) erspart im Arbeitsrecht so manchen vom Anwalt aufgesetzten Vertrag. Wer ein anderes Fachgebiet benötigt oder es doch lieber persönlich mag, gibt auf der Anwaltsplattform Advocado seine Frage ein und wird innerhalb von zwei Stunden von einem passenden der 550 Anwälte der Plattform kontaktiert. Die Stärke von Advocado ist ihr gutes Matching. Doch was wäre, wenn eine KI schon konkrete Rechtsauskünfte vorbereitet und ein passender Anwalt sie nur finalisiert? Das müsste kostengünstig für den einen und ressourcenschonend für den anderen sein, dachte sich incaseof.law-Gründer Max Kindler. Kindler verdiente sich seine ersten Sporen als Konzernanwalt bei AT&S und den ÖBB und leitete zuletzt die Rechtsabteilung von Rail Cargo. Vor Unternehmensjuristen hat er höchsten Respekt. „Ihre Rolle ist wie die des Consigliere in ‚Der Pate': Als Ratgeber bei jedem Gespräch dabei und Marlon Brando hört auf ihn." Übertragen auf KMU: Jede Handlung eines Geschäftsführers hat juristische Implikationen, die sein General Counsel – diese Bezeichnung gefällt Kindler besser als Hausjurist – im Auge behält. Hand aufs Herz, wie viele Geschäftsführer haben das Gesellschaftsrecht gelesen? Kindler bringt ein Beispiel, wie tückisch es ist: „Die meisten GmbH-Geschäftsführer denken, ihre Haftung ist auf 35.000 Euro begrenzt. Das stimmt nur, solange sie alles richtig machen." Hält aber etwa ein Lieferant die Lieferfrist nicht ein und macht der Geschäftsführer die dafür vertraglich vorgesehene Strafe nicht geltend, hat er schon ein strafrechtliches Delikt begangen: „Untreue. Er hat das Vermögen der Gesellschaft geschädigt." Ein Hausjurist wüsste das. Doch wie viele KMU können sich schon sein Jahressalär leisten? Kindler nahm sich deswegen die gängigsten Anwendungsfälle einer GmbH vor und standardisierte sie mit KI-Unterstützung. Ganz obenauf zwei Tools für automatisierte Mahnklagen (aus Gläubigersicht) und deren Abwendung (Forderungsabwehr aus Schuldnersicht). Wer nicht über das Justizportal gehen will, findet bei Kindlers incaseof.law eine elegante und kostengünstige Alternative. Für Forderungen unter 5.000 Euro braucht es keine anwaltliche Vertretung. Das System erstellt anhand der Fakten eine Mahnklage. Den Gläubiger kostet das nichts, nur der Schuldner muss je nach Forderungshöhe zehn bis 20 Prozent Pauschale zahlen. Übersteigt die Forderung 5.000 Euro, schaltet sich ein Anwalt aus dem Netzwerk dazu. Vier Wochen nach der Zustellung entsteht automatisch ein Exekutionstitel. Findet der Schuldner die Forderung ungerechtfertigt, kann er sie auf symmetrischem Weg abwehren und automatisiert Einspruch erheben. Dann wird ein ordentlicher Zivilprozess eingeleitet. Für Juni plant Kindler neue Features. Ein Vertragstool soll Vertragsentwürfe zuerst von einer KI, dann von einem menschlichen Juristen gegenchecken. Ein Ausschreibungstool wird auch kleineren KMU ermöglichen, an großen Ausschreibungen teilzunehmen. Ein Finanzunterlagentool macht dem Kreditschutzverband Konkurrenz, prüft die eigene Zahlungsfähigkeit und schlägt Sanierungsverfahren mit und ohne Eigenverwaltung oder Konkurs vor. Und wenn bisher nichts passt: Für alle übrigen Beratungsanlässe matcht auch dieser Algorithmus mit passenden Anwälten. ◀

Foto: Michael Sazel Illu: the-lightwriter / Getty Images

**TEXT** THOMAS STUBBINGS

# Zur Sicherheit verpflichtet

**Weil Cyberangriffe auch die Gesellschaft an neuralgischen Punkten treffen, greift der Staat mit immer mehr Vorschriften regulierend ein. Welche Entwicklungen es hier international gibt und was die einzelnen Verordnungen und Auflagen für Unternehmen bedeuten.**

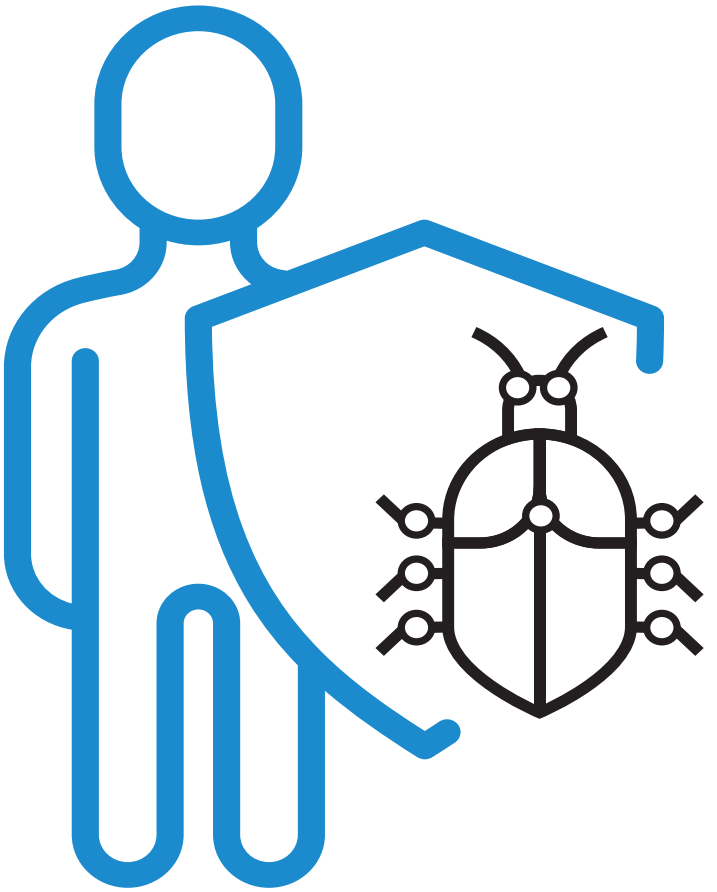
Unternehmen werden immer häufiger Opfer von Cyberbetrug und tragen Verluste davon. Abhilfe soll Cybersecurity schaffen. Die Maßnahmen dürfen allerdings nicht damit enden, Betriebe vor Verschlüsselungstrojanern oder vereinzelten Datenschutzverletzungen zu bewahren. Wenn Sicherheitslücken nämlich die kritische Infrastruktur beeinträchtigen, erhält die Bedeutung von Cybersecurity eine gesellschaftliche Dimension. Cyberangriffe, die die Gesellschaft an neuralgischen Punkten treffen, erweitern den Kreis der Geschädigten weit über das direkt betroffene Unternehmen hinaus. Energieversorger, die ihre Kunden nicht mehr mit Strom oder Gas beliefern können, Banken, die kein Bargeld ausgeben können, Krankenhäuser, deren Patienten aufgrund nicht funktionierender Infrastruktur sterben: All diese Szenarien infolge von Cyberangriffen wurden bereits Realität. Vor diesem Hintergrund erachten es Gesetzgeber zunehmend für notwendig, Cybersecurity aus dem ausschließlichen Verantwortungsbereich der betroffenen Unternehmen und Einrichtungen zu holen. Regierungen setzen sich zunehmend mit den Risiken im Netz auseinander, die weit über die Bedrohung einzelner Betriebe hinausgehen und der Regulierung bedürfen.

**WIE DIE EU CYBERSECURITY REGELT** Als Folge dieser Überlegungen entstand die erste EU-Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-Richtlinie), die im August 2016 in Kraft trat. Diese Richtlinie verpflichtet Unternehmen der kritischen Infrastruktur dazu, eine Reihe an Sicherheitsauflagen im Internet zu erfüllen: Zum einen sind angemessene, dem Stand der Technik entsprechende Sicherheitsmaßnahmen zu treffen, zum anderen müssen gravierende Sicherheitsvorfälle an eine staatliche Behörde gemeldet werden. Im internationalen Vergleich kam diese EU-Initiative verhältnismäßig spät. In den USA gibt es schon seit langem entsprechende Gesetze, die Gesundheitsorganisationen, Finanzdienstleistern und Bundesbehörden den Schutz ihrer Systeme und ihnen anvertrauter Informationen vorschreiben.

**VERORDNUNGEN WERDEN ERWEITERT** Diese Gesetze und Verordnungen sind auf bestimmte kritische Bereiche beschränkt: Banken, den Gesundheitssektor, Telekommunikation etc. Die immer ausgeklügelteren Cyberangriffe der letzten Jahre haben jedoch gezeigt, dass es zu kurz greift, Cybersicherheit ausschließlich den Führungsetagen systemrelevanter Betriebe zu überantworten. Auch andere Sektoren werden immer öfter zum Ziel von Angriffen. Zudem sind kleine und mittlere Unternehmen das Rückgrat jeder Volkswirtschaft. Mit dem Schutz des digitalen Binnenmarkts als erklärtem Hauptziel der Cybersecurity-Strategie der Europäischen Union vor Augen wurde klar, dass Cyberhygiene auch auf die digitalen Sektoren ausgeweitet werden muss. Etwa bei Online-Marktplätzen, auf denen Unternehmen ihre Produkte und Dienste online zur Verfügung stellen können, Cloud-Computing-Diensten sowie Suchmaschinen.

Die von der ursprünglichen NIS-Richtlinie umfassten Bereiche werden daher bei der nächsten Überarbeitung des Gesetzestextes um Sektoren und Dienstleister ergänzt werden, ohne die gesellschaftliche und wirtschaftliche Schlüsselaktivitäten im Binnenmarkt nicht erbracht werden können. Diese Ausweitung und Harmonisierung der Zielgruppen werden den Geltungsbereich der europäischen Netzwerk- und Informationssicherheitsrichtlinie deutlich vergrößern. Im Zuge der Überarbeitung werden auch Sicherheitsauflagen konkretisiert und ausgeweitet: Betroffene Einrichtungen werden dazu verpflichtet, angemessene und verhältnismäßige technische und organisatorische Maßnahmen gegen die Bedrohung der Sicherheit ihrer Netzwerke und Informationssysteme zu ergreifen, die dem neuesten Stand der Technik entsprechen und auf das spezifische Risiko zugeschnitten sind. Ziel ist das Propagieren von Mindestsicherheitsstandards in einem weiten Teil unserer auf Informationssicherheit basierenden Gesellschaft, um widerstandsfähigere Ökosysteme sowohl auf nationaler als auch auf europäischer Ebene zu schaffen. In der Pflicht sind dabei nicht nur große Konzerne. Bezüglich der Größe der betroffenen Unternehmen spricht der Entwurf auch von mittleren Unternehmen, also Betrieben mit mehr als 50 Mitarbeitern und einem Umsatz von mehr als zehn Millionen Euro. Alle Unternehmen, die diesen Kriterien entsprechen, müssen sich an die Vorgaben der NIS-Richtlinie halten, also entsprechende Cybersecurity-Mindeststandards einhalten und Meldepflichten von Vorfällen nachkommen.

**TENDENZ ZU STÄRKERER STANDARDISIERUNG** Die Achillesferse der digitalen Sicherheit stellen nach wie vor Sicherheitsmängel bei Produkten und Dienstleistungen dar.



Sicherheitslücken dieser Art erleichtern es Cyberkriminellen, ihrem illegalen Handwerk nachzugehen. Vor diesem Hintergrund verabschiedete die Europäische Kommission 2019 den Rechtsakt zur Cybersicherheit, mit welchem erstmals ein EU-weiter Rahmen für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen geschaffen wurde. Zudem erteilt der Rechtsakt der EU-Cybersicherheitsagentur ENISA ein dauerhaftes Mandat für die Ausarbeitung eines möglichen europäischen Schemas für die Cybersicherheitszertifizierung, in welchem die Bedingungen für die zukünftige Zertifizierung von Produkten, Dienstleistungen und Prozessen auf drei Vertrauenswürdigkeitsstufen festgelegt werden sollen. Derzeit sind diese Zertifizierungen noch freiwillig, die Kommission hat jedoch bereits ihre Absicht bekundet, in Zukunft ein verpflichtendes Regime zur Förderung von Sicherheitsmindeststandards anzustreben.

**UNTERNEHMEN IN DER PFLICHT** Generell lässt sich ein Trend, Cybersecurity-Auflagen durch entsprechende Gesetze und Verordnungen verpflichtend zu machen und dabei den Kreis betroffener Unternehmen zu erweitern, beobachten. Auch wenn Cybersecurity und Resilienz vor dem Hintergrund der potenziell gravierenden Auswirkungen von Cyberangriffen ein wichtiges Anliegen für jeden Betrieb sein sollten, der Technologien einsetzt, ist vorauszusehen, dass es in diesem Bereich in Zukunft weniger Wahlmöglichkeit geben wird. Verordnungen und Auflagen werden in absehbarer Zeit auch in weiteren Branchen und Sektoren Einzug halten und auch KMU direkt oder im Rahmen der Lieferketten von Betreibern wesentlicher Dienste zu entsprechenden Vorkehrungen verpflichten. Wer das Thema Cybersecurity bisher noch nicht am Radar hatte, ist also gut beraten, dies schleunigst zu ändern. ◀

Illu: Alexey Blogoodf, Vadim Sazhniev / Getty Images Foto: beigestellt

### MIT VIER SCHRITTEN BESSER GEWAPPNET

**CYBER-EXPERTEN INS UNTERNEHMEN HOLEN** Entweder eine interne Abteilung aufbauen oder externe Berater holen. Wichtig: Cybersecurity muss als strategisches Thema der Unternehmensführung implementiert werden.

**BASIS-SICHERHEIT HERSTELLEN** Firewalls, Monitoringsysteme und auch tiefergehende Cyber-Technologien für Mailsysteme und sensible Bereiche aufsetzen. Regelmäßige Updates und Schutz vor Schadsoftware gewährleisten. Sicheres Passwort- und Berechtigungsmanagement und Zwei-Faktor-Authentifizierung hinterlegen. Berechtigungsmanagement und Schutz vor Schadsoftware einführen.

**CYBERSECURITY-KULTUR ETABLIEREN** Eine Onlineschulung pro Jahr für alle MitarbeiterInnen reicht nicht. Cybersecurity muss Teil der täglichen Kultur und des Joballtags sein und regelmäßig in Meetings thematisiert werden.

**NOTFALLPLANUNG UND RESILIENZKONZEPT** Analysieren, wo die größten Risiken und Schadensszenarien liegen und diese antizipieren: Schaffen präventiver und reaktiver Maßnahmen für den Fall der Fälle.


**DER AUTOR**

Thomas Stubbings ist CEO der CTS Cyber Trust Services und Global Executive MBA Alumnus der WU Executive Academy.

**TEXT** MARKUS MITTERMÜLLER

# Cloud – Wie Daten sicher bleiben

**Die Auslagerung von Daten in externe Rechenzentren kann zum Risiko werden. Ob sie in den USA oder in Europa gespeichert werden, ist dabei eine der entscheidenden Fragen.**

Zwischen zwei und vier Milliarden Euro – so viel will Microsoft in den kommenden Jahren in Österreich investieren. Mit dem Geld sollen Datencenter für Cloud-Anwendungen wie Office 365 errichtet werden. Microsoft reagiert damit offensichtlich auf eine Frage, die sich auch viele KMU stellen: Wo liegen eigentlich meine Daten, wenn ich eine Cloud nutze? „Die Antwort ist: Wir wissen es nicht. Denn Microsoft hält sich bei dieser Frage sehr bedeckt. Mit den geplanten Rechenzentren will der Konzern die Daten hier in Österreich halten", sagt Christian Büll, Leiter des Departments für Informationstechnologie an der FH Burgenland. Denn die Speicherung von Daten in Ländern außerhalb der EU wird zum echten Datenschutzrisiko. Viele KMU vertrauen dennoch den großen Cloud-Anbietern wie Google, Amazon und Microsoft, da die Nutzung meist einfach und die Tools bereits bekannt sind. Doch eine vorschnelle Entscheidung bei Cloud-Lösungen kann auch zum negativen Bumerang werden. Wie sicher sind die verschiedenen Cloud-Anbieter, und worauf muss ein KMU achten, wenn es sich für die Auslagerung von Daten und Nutzung von externer Software entscheidet?

Dass kein KMU diesen Fragen ausweichen kann, zeigen auch folgende Zahlen. 38 Prozent der österreichischen Unternehmen nutzen laut Statistik Austria Cloud-Services. Damit hat sich die Nutzung dieser IT-Infrastruktur im Vergleich zu 2014 verdreifacht. Speziell kleine und mittelgroße Unternehmen weisen eine hohe Steigerungsrate auf. Diese liegt zwischen knapp 190 und 260 Prozent.

**SOFTWARE AUS DER STECKDOSE** Warum diese externe IT-Lösung immer attraktiver wird, hat viele Gründe. „Ein eigenes Rechenzentrum verursacht fixe Kosten, ich benötige eigene Hardware und auch IT-Mitarbeiter. Mit einer Cloud habe ich höhere Flexibilität und zahle nur die Leistung, die ich auch beziehe", sagt Alexander Bruckner, Public-Cloud-Sales-Experte bei T-Systems Austria. Auch die Servicegeschwindigkeit ist ein Vorteil. Kurzfristig höherer Bedarf kann via Cloud sofort abgedeckt werden, neue Applikationen stehen auf Abruf zur Verfügung. „Die Software kommt quasi aus der Steckdose und ich als Unternehmer muss mich sonst um nichts mehr kümmern", ergänzt Büll.

Doch so einfach die Anwendungen im digitalen Alltag sind, so komplex kann die Auswahl des passenden Cloud-Anbieters werden. „Der ‚Weg in die Cloud' ist, genauso wie die Digitalisierung selbst, nicht als Selbstzweck zu verstehen, sondern muss immer letztendlich der Wertschöpfung dienen", erklärt dazu Maha Sounble, Chief Information Security Officer an der Wirtschaftsuniversität Wien. Daher ist es unumgänglich, eine eigene Cloud-Strategie zu haben. „Die Cloud ist nicht aufhaltbar. Sich vor ihr zu verschließen ist daher nicht zielführend. Um für sich den richtigen Weg in

**Die Cloud ist nicht aufhaltbar.**

Maha Sounble, WU Wien

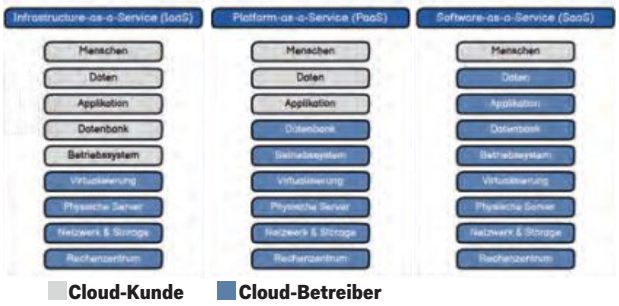
die Cloud zu finden, sollte vorher überlegt werden, wohin die Reise gehen soll und was dafür benötigt wird – und dieser Plan stellt dann die Strategie dar", meint Sounble.

Ein großer Irrtum, den viele KMU dabei begehen, ist die Cloud auf ein IT-Thema zu reduzieren. Denn bei der Auswahl von Cloud-Services gehe es laut der WU-Expertin um die Gestaltung von Arbeitsweisen und Arbeitsabläufen, nicht in erster Linie um IT. Ein Fehler wäre auch zu glauben, die Verantwortung an den Cloud-Betreiber abtreten zu können. „Die Cloud-Nutzung entbindet das Unternehmen nicht von der Pflicht, für den Schutz der Daten zu sorgen. Diese Pflicht beginnt bereits bei der Auswahl eines Cloud-Anbieters, wo auch Rechtskonformität und Informationssicherheit Entscheidungskriterien darstellen", erklärt die WU-Expertin.

**EUROPA VS. USA** Warum es so relevant ist, ob die Daten in Europa oder den USA gespeichert werden, liegt an einem Urteil des Europäischen Gerichtshofs (EuGH). Dieser hat das EU-US Privacy Shield, welches die datenschutzrechtliche Übermittlung personenbezogener Daten von der EU in die USA geregelt hat, für ungültig erklärt. Die Begründung des Gerichts: Das Gesetz bietet keine Garantien, die den strengen Ansprüchen der Datenschutzgrundverordnung (DSGVO) genügen würden. Damit kann in der US-Cloud solange keine Rechtskonformität gemäß DSGVO gewährleistet werden, bis ein neuer Gesetzesentwurf vorliegt. „Damit befinden wir uns derzeit in einem rechtsfreien Raum. Alle Mechanismen der DSGVO, wie das Recht auf Löschen von Daten oder das Recht auf Auskunft, greifen hier nicht", erklärt Büll.

Wie findet man also Anbieter österreichischer Cloud-Lösungen mit einem Speicherort der Daten im Inland – oder zumindest in der EU? Eine Möglichkeit ist, dem Gütesiegel „Austrian Cloud" zu vertrauen. Im Rahmen dieser Initiative der Wirtschaftskammer können sich heimische Cloud-Dienstleister für das Gütesiegel qualifizieren, indem sie rund 90 Fragen beantworten. Neben dem Speicherort Österreich sind für das Gütesiegel auch Faktoren wie Datenschutz, Sicherheit, rechtliche Konformität oder die technische Infrastruktur relevant. >

Foto: www.interfoto.at Illu: polygraphus / Getty Images




### DREI HAUPTKATEGORIEN VON CLOUD-DIENSTEN

**INFRASTRUCTURE AS A SERVICE** Dieses Modell stellt grundlegende IT-Ressourcen wie Rechenleistung, Speicher oder Netzwerkkapazitäten zur Verfügung. Der Anwender hat dabei die Kontrolle über Betriebssysteme und Anwendungen, er muss die Infrastruktur selbst aus den benötigten Recheninstanzen und Speichern zusammenstellen.

**PLATFORM AS A SERVICE** Dabei werden Programmiermodell und Entwicklerwerkzeuge bereitgestellt, um Cloud-basierte Anwendungen zu erstellen und auszuführen.

**SOFTWARE AS A SERVICE** Der Provider stellt bei diesem Service seine eigenen Anwendungen für die Benutzer zur Verfügung.

**ALTERNATIVE ZU US-GIGANTEN** Eine Alternative zu den US-Giganten wird derzeit auf europäischer Ebene vorangetrieben. Auf Initiative der deutschen und französischen Regierungen wurde das Projekt GAIA-X ins Leben gerufen. Ziel ist eine sichere und vernetzte europäische Dateninfrastruktur. A1 Digital, einer der führenden heimischen Cloud-Service-Provider sowie Spezialist in Sachen IoT, Machine-Learning und Cybersecurity, unterstützt dieses Projekt von Beginn an. „Mit dieser Dateninfrastruktur bekommen die Nutzer Sicherheit hinsichtlich Transparenz und Datenschutz", erklärt Markus Fleischer, Head of Strategy & Business Development bei A1 Digital. Mit Exoscale bietet das Unternehmen bereits jetzt ein DSGVO-konformes Cloud-Portfolio aus Europa an. „Unsere Rechenzentren liegen in Deutschland, der Schweiz, Österreich und Bulgarien. Damit liegt die Datensouveränität in der Hand der Unternehmer", so Fleischer.

Grundsätzlich rät Fleischer den Unternehmen zu einer Multi-Cloud-Strategie: „Dabei trenne ich kritische von nichtkritischen Daten und entscheide selbst, wo welche Daten gesichert werden. Damit bin ich nicht abhängig von einem Cloud-Anbieter."

**WIE KOMME ICH RAUS?** Apropos Abhängigkeit. Diese kann auch entstehen, wenn ein Unternehmen seine Daten im Rechenzentrum eines Cloud-Anbieters mit einer bestimmten Technologie gespeichert hat. Will man den Anbieter wechseln, kommt oft die böse Überraschung. „Oft ist es schwer, wieder aus der Cloud herauszukommen. Diese Frage wird meist unterschätzt und sollte von jedem KMU bereits vor der Wahl des Anbieters geklärt sein", meint Markus Fleischer. Im Fachjargon wird diese Abhängigkeit als Vendor Lock-in bezeichnet. Denn auch wenn viele Software-Tools und Services vom Cloud-Anbieter zur Verfügung gestellt werden: Die grundsätzliche Verantwortung für die Daten bleibt weiterhin beim KMU. „Ich kann nicht die Daten in die Cloud schicken und glauben, der Betreiber kümmert sich nun um alles. Für die Datensicherheit und das Backup ist das KMU weiterhin selbst verantwortlich", sagt Bruckner.

**RISIKOFAKTOR MENSCH** Trotz digitalen Fortschritts gilt immer noch: Die Sicherheit steht und fällt mit den Menschen. „95 Prozent aller erfolgreichen Cyberangriffe starten mit einer Phishing-Mail an einen Mitarbeiter", erklärt Sounble. Sie rät daher dazu, im eigenen Sicherheitskonzept auch immer die menschliche Komponente zu berücksichtigen. Dazu gehört eine gelebte Sicherheitskultur im Unternehmen sowie eine regelmäßige Schulung der Mitarbeiter.

Ein zusätzlicher Nutzen, den die Unternehmen aus der Cloud in Zukunft immer mehr ziehen werden, ist laut Fleischer die Innovation: „Diese wird im Verbund von Unternehmen stattfinden. Als KMU kann ich Daten mit den verschiedensten Partnern tauschen und diese für die weitere Entwicklung meiner Produkte und Services einsetzen." ◀

### MODELLE DES HOSTINGS

**PUBLIC CLOUD** Ein Pool aus virtuellen Ressourcen, der über eine Self-Service-Schnittstelle automatisch für mehrere Kunden bereitgestellt wird. Wie zum Beispiel Amazon Web Services oder Google Cloud. „Der Vorteil ist, dass diese Cloud mit einer Anmeldung über Kreditkarte schnell und frei verfügbar ist und viele Services bietet", erklärt Bruckner.

**PRIVATE CLOUD** Wird nicht für die Allgemeinheit, sondern nur für ausgewählte Benutzer über das Internet oder ein privates internes Netzwerk bereitgestellt. „Hier weiß der Kunde im Gegensatz zur Public Cloud, wo genau die Daten und Systeme liegen", so der T-Systems-Austria-Experte.

**HYBRID CLOUD** Eine gemischte Rechen-, Speicher- und Serviceumgebung, die aus einer lokalen Infrastruktur, privaten Cloud-Diensten und einer öffentlichen Cloud besteht.

### SICHERHEIT DER CLOUD-ANBIETER:

**ZERTIFIZIERUNGEN** nach internationalen oder europäischen Standards gelten als Nachweis für das Sicherheitsmanagement der Cloud-Anbieter. Häufige Zertifizierungen sind ISO/IEC 27001 oder ISO/IEC 27018.

Wer sicherstellen will, dass seine Daten in Österreich bleiben, kann auf das Gütesiegel „Austrian Cloud" achten. Die Liste der Anbieter findet man unter *www.staraudit.org/austriancloud/*

# Wenn‘s so leicht wär‘...

WKO
WIRTSCHAFTSKAMMER WIEN
Immobilien- und Vermögenstreuhänder

... dann könnte jeder meinen Job machen. Vertrauen Sie bei Verkauf, Vermietung und Verwaltung von Immobilien den ExpertInnen.

**Wir wissen, worauf es ankommt.**

Was Immobilienmakler, Verwalter & Bauträger für Sie tun, erfahren Sie unter

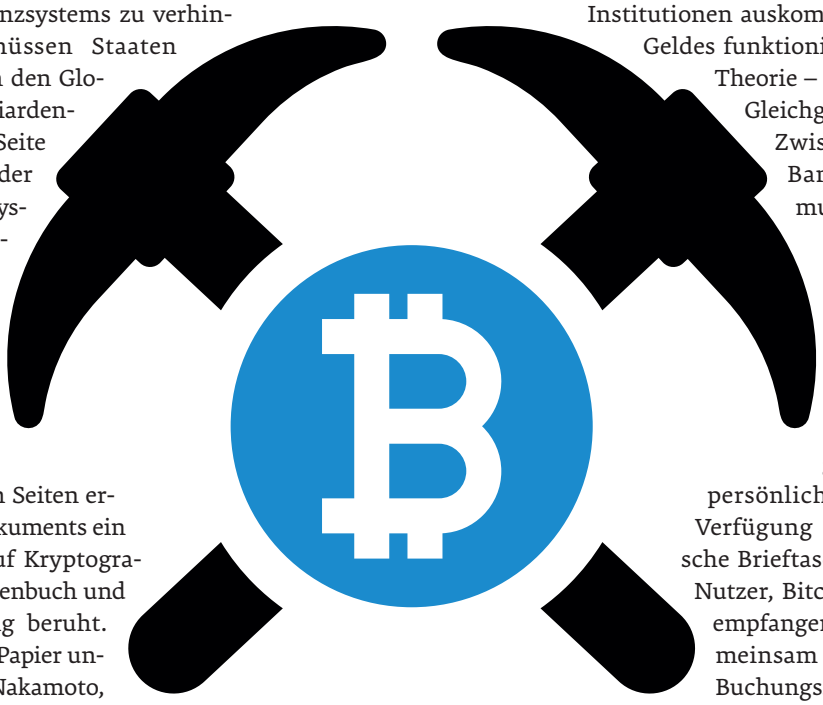
**www.IMMY.at**

**TEXT** HARALD FERCHER

# Geld, das keine Banken braucht

**Vertrauen ist die Grundlage jedes Finanzsystems. Just als jenes Vertrauen 2008 gewaltig ins Schleudern geriet, tauchte mit Bitcoin erstmals eine alternative Lösung auf. Doch wie vertrauenswürdig sind Kryptowährungen? Acht Fragen und Antworten.**

Oktober 2008: Die Finanzwelt steht kopf. Nach der Pleite von Lehman Brothers herrscht Panik. Börsenkurse krachen wie die warmen Kaisersemmeln. Um einen Kollaps des Finanzsystems zu verhindern, müssen Staaten rund um den Globus den Banken mit milliardenschweren Garantien zur Seite springen. Das Vertrauen der Menschen in das Finanzsystem ist in seinen Grundfesten erschüttert. Genau zu diesem Zeitpunkt taucht erstmals ein Papier auf, in dem das Konzept eines Peer-to-Peer funktionierenden elektronischen Cash-Systems beschrieben wird. Auf neun Seiten erklärt der Verfasser des Dokuments ein Austauschsystem, das auf Kryptographie samt digitalem Kassenbuch und dezentraler Buchführung beruht. Veröffentlicht wurde das Papier unter dem Namen Satoshi Nakamoto, ein Pseudonym, wie sich bald herausstellen sollte. Bis heute rätseln Hundertschaften von Kryptologen, Sprachwissenschaftlern und anderen detektivisch veranlagten Menschen, wer sich hinter dem mittlerweile mythenumrankten Namen tatsächlich verbirgt. Das von ihm verfasste Papier gilt heute als „Gründungsurkunde" von Bitcoin.



**WARUM ÜBERHAUPT BITCOIN?** Dazu ein Zitat von Nakamoto, welches mittlerweile zum Standardrepertoire jedes Vortragenden zum Thema Bitcoin gehört: „Das Kernproblem konventioneller Währungen ist das Ausmaß an Vertrauen, das nötig ist, damit sie funktionieren. Der Zentralbank muss vertraut werden, dass sie die Währung nicht entwertet, doch die Geschichte des Fiatgeldes ist voll von Verrat an diesem Vertrauen. Banken muss vertraut werden, dass sie unser Geld aufbewahren und es elektronisch transferieren, doch sie verleihen es in Wellen von Kreditblasen mit einem kleinen Bruchteil an Deckung. Wir müssen den Banken unsere Privatsphäre anvertrauen und darauf vertrauen, dass sie Identitätsdieben nicht die Möglichkeit geben, unsere Konten leerzuräumen. Ihre massiven Zusatzkosten machen Micropayments unmöglich." Sprich, das „moderne Geld" beruht auf dem Vertrauen in für die Geldwirtschaft zentrale Institutionen wie National- bzw. Zentralbanken oder Geschäftsbanken. Demgegenüber steht das Bitcoin-Konzept, das ohne zentrale Institutionen auskommt. Der Austausch des Geldes funktioniert – zumindest in der Theorie – Peer-to-Peer, also unter Gleichgestellten, ohne dass ein Zwischenhändler wie eine Bank beauftragt werden muss.

**WIE FUNKTIONIERT BITCOIN?** Für den einzelnen Nutzer ist Bitcoin nicht viel mehr als eine App oder ein Computerprogramm, welches ein persönliches Bitcoin-Wallet zur Verfügung stellt. Diese elektronische Brieftasche ermöglicht es dem Nutzer, Bitcoins zu senden und zu empfangen. Dahinter steht ein gemeinsam genutztes öffentliches Buchungssystem, die sogenannte Blockchain. In dieser Blockchain wird jede bestätigte Transaktion gespeichert. Neue Transaktionen werden nur durchgeführt, wenn der vom Wallet errechnete Kontostand gedeckt und sichergestellt ist, dass die versendeten Bitcoins tatsächlich dem Sender gehören. Die Wallets enthalten einen geheimen Datenblock (privater Schlüssel oder Seed genannt), der verwendet wird, um eine Transaktion zu signieren. Die Signatur verhindert, dass Transaktionen im Nachhinein verändert werden können.

**WAS IST BITCOIN-MINING?** Wird eine Transaktion bzw. Überweisung von Bitcoins in Gang gesetzt, so wird diese über das Netzwerk verbreitet und innerhalb von zehn bis 20 Mi-

Illu: Hiranmay Baidya / Getty Images

nuten beginnt die Bestätigung durch das Netzwerk mithilfe eines Prozesses, der Mining genannt wird. Dabei führen im Netzwerk vorhandene Computer mathematische Berechnungen durch, die die Bitcoin-Transaktion bestätigen bzw. die Sicherheit erhöhen sollen. Als Belohnung für diese Dienste können Bitcoin-Miner Transaktionsgebühren für die von ihren Rechnern bestätigten Transaktionen erhalten und neu geschaffene Bitcoins sammeln. Die Belohnungen werden je nach geleisteter Rechenarbeit aufgeteilt.

**MIT BITCOINS AUCH WAREN DES ALLTAGS KAUFEN?** Ja, es gibt eine ganze Reihe von (zumeist Online-)Händlern, die Bitcoins oder andere Kryptowährungen als Zahlungsmittel akzeptieren. Manche von ihnen gewähren sogar ein Skonto, wenn die Waren mit einer Kryptowährung bezahlt werden. Abrufen kann man Händler, die Kryptowährungen akzeptieren, über spezialisierte Suchmaschinen wie etwa spendabit. Dort finden sich u. a. Onlineshops wie Sugartrends, die es sich – laut Eigenbeschreibung – zur Aufgabe gemacht haben, lokale Geschäfte mit speziellen Produkten einem internationalen Publikum online zu präsentieren. Einziges Problem: Angesichts der „Wechselkurs-Schwankungen" zwischen Bitcoin und z. B. dem Euro empfiehlt es sich nicht unbedingt, Bitcoins zum Einkaufen zu verwenden. Dazu ein kleines Rechenbeispiel: Angenommen, Sie hätten am ersten Februar 2021 eine Halskette im Gegenwert von 140 Euro in Bitcoins bezahlt, dann hätten Sie an diesem Tag 0,00503 Bitcoins transferieren müssen. Am 6. Mai hätten ihre ausgegebenen Bitcoins einen Gegenwert von 235,10 Euro. Aus Sicht des Käufers ein schlechtes Geschäft. Womit wir auch schon bei der nächsten Frage wären.

**WESHALB SCHWANKT DER BITCOIN-KURS?** Dafür gibt es gleich mehrere Gründe. Einerseits neigen Anleger dazu in Krisenzeiten – wie jetzt in der Corona-Pandemie –, ihre Depots breiter aufzustellen. So mancher wird dabei – wohl auch angezogen von der starken Entwicklung – einen Teil seines Geldes in Bitcoins investiert haben. Die Ankündigung von Tesla, Bitcoins als Zahlungsmittel zu akzeptieren und selbst in die Währung investieren zu wollen, tat ein Übriges. Dazu kommt, dass Bitcoins und andere Kryptowährungen über diverse Krypto-Börsen wie Bitpanda heute deutlich einfacher zu handeln sind. Auch die Diskussion über die Möglichkeit von digitalen Währungen, die durch Notenbanken ausgegeben werden, zeigt, dass die Blockchain-Technologie von der Finanzwelt zunehmend ernst genommen wird. Zusätzlich gibt es mittlerweile eine Menge an Finanzprodukten (Zertifikate, Futures) etc., die auf Bitcoin begeben werden und für die Spekulation geeignet sind. Last, but not least sorgt die Bitcoin-Konstruktion selbst dafür, dass der Wert steigt. Die Anzahl der Bitcoins ist nämlich endlich – sprich auf 21 Millionen begrenzt. Derzeit sind Schätzungen zufolge bereits an die 18,6 Millionen im Umlauf.

**IST BITCOIN SICHER?** Zugegeben, eine schwer zu beantwortende Frage. Wie im realen Leben gilt auch für die virtuelle Währung, dass wohl nichts absolut sicher ist. Dennoch: Die hinter Bitcoin stehende Technologie Blockchain ist trotzdem die wohl sicherste Technologie, die es derzeit gibt. Hacker haben es bisher noch nie geschafft, die Blockchain zu knacken. Obwohl es sicher Tausende gibt, die es probiert haben. Die Belohnung wäre jedenfalls immens. Ein Hacker, dem es gelingt, in die Blockchain einzudringen bzw. diese zu verfälschen, müsste nur vorher Bitcoin am Markt shorten. Wenn der Markt merkt, dass die Technologie geknackt wurde, verliert er das Vertrauen, der Bitcoin-Kurs sinkt gegen null, und der Hacker sammelt seine Millionen ein. Bei den bisher bekanntgewordenen Hacks im Zusammenhang mit Bitcoin, die weltweit für Aufregung sorgten, gelang es den Hackern nicht, die Blockchain zu knacken, sondern lediglich das Sicherheitssystem, das die Schlüssel von Kunden vor einem unerlaubten Zugriff schützen sollte. So wie ein Bankräuber Bargeld mitnimmt, konnten die Hacker Bitcoins einfach auf ein anderes Konto transferieren.

**GIBT ES NOCH ANDERE KRYPTOWÄHRUNGEN?** Es gibt mittlerweile Hunderte, und es werden mehr. Das liegt daran, dass prinzipiell jeder mit dem entsprechenden Know-how Kryptowährungen auf Basis der Blockchain-Technologie kreieren kann. Er muss nur einen oder mehrere Counterparts finden, die bereit sind, mit der Kryptowährung zu handeln oder sie als Zahlungsart zu akzeptieren. ◀

**TEXT** STEPHAN STRZYZOWSKI

# Wie Schwarzgeld sauber wird

**Kriminelle nützen ausgefeilte Methoden, um ihre illegalen Einkünfte an den Behörden vorbeizuschleusen. Um welche enormen Summen es geht, können die TU Wien und die Utrecht School of Economics nun mit einfachen Modellen ermitteln.**

Geldwäsche ist ein Problem, das die ganze Welt umfasst. Einnahmen aus kriminellen Handlungen wie Drogenhandel oder Korruption werden häufig über Ländergrenzen und mehrere Stationen verschoben, bis ihre Herkunft nicht mehr nachvollziehbar und das ursprünglich kriminelle Geld weißgewaschen ist. Doch um welche Summen geht es ingesamt? Die TU Wien und die Utrecht School of Economics haben in einem gemeinsamen Projekt analysiert, wie sich das Volumen dunkler Finanzströme abschätzen lässt, und festgestellt: Mit relativ einfachen, von der Physik inspirierten statistischen Modellen lassen sich Schwarzgeld-Ströme erstaunlich gut beschreiben.

**AUF SPURENSUCHE** Dass niemand präzise und vor allem vollständige Daten über Schwarzgeld-Ströme kennen kann, ist klar. Das heißt aber nicht, dass man völlig im Dunklen tappt. Prof. Michael Getzner leitet am Institut für Raumplanung der TU Wien den Forschungsbereich Finanzwissenschaft und Infrastrukturpolitik. Um internationale Geldwäsche mathematisch beschreiben zu können, schloss er sich mit dem Team von Prof. Brigitte Unger aus Utrecht zusammen. Die Finanzwissenschaftlerin gilt als europaweit anerkannte Expertin für die Ökonomie der Geldwäsche. „Unser Team hatte die Möglichkeit, Daten der niederländischen Steuerbehörden über Geldwäsche-Verdachtsfälle zu analysieren", sagt Michael Getzner. Daraus erhält man zwar noch keinen zuverlässigen Eindruck über weltweite Schwarzgeld-Ströme, aber zumindest ein gutes Bild illegaler Transaktionen, an denen niederländische Partner beteiligt sind.

„Auf Basis dieser Daten wurde ein statistisches Modell entwickelt, das beschreibt, von welchen Parametern die Schwarzgeld-Flüsse abhängen", erklärt Prof. Getzner. „Man kann sich dabei von der Physik inspirieren lassen: Interessanterweise haben Geldwäsche-Ströme einiges mit der Gravitation gemeinsam." Die Gravitationskraft zwischen zwei Planeten wächst mit ihrer Masse, und sie nimmt mit dem Quadrat des Abstands ab. Ähnlich verhält es sich auch bei der Geldwäsche: Je größer eine Volkswirtschaft, umso größer die Geldströme. Aber auch das Volumen an Geldwäsche-Transaktionen nimmt in Näherung mit dem Quadrat des Abstands ab. Das mag auf den ersten Blick überraschend wirken – schließlich ist es in einer globalisierten Welt kein großer Aufwand, Geldsummen über große Distanzen zu überweisen. „Gerade bei kriminellen Tätigkeiten spielen Abstand beziehungsweise Nähe aber doch eine wichtige Rolle", erklärt Michael Getzner. Denn: „Geldwäsche braucht persönliche Kontakte, direkte Kommunikation und kriminelle Netzwerke, die räumlich nahe beieinander liegen – daher ist es nicht verwunderlich, auch hier auf ein Abstandsgesetz zu stoßen."

**WIE GELDWÄSCHE FUNKTIONIERT** Geldwäsche ist für die Straftäter deshalb von so wesentlicher Bedeutung, da sie dazu dient, die illegal erworbenen Vermögenswerte dem Zugriff der Behörden zu entziehen. Zu diesem Zweck wird das Schwarzgeld durch eine Reihe möglichst unauffälliger und meist komplexer Transaktionen im Kreis geschickt. Diese Vorgehensweise soll es den Behörden erschweren, die illegale Herkunft der Vermögenswerte zu erkennen. Am Ende dieses Prozesses kann das weißgewaschene Vermögen wieder in den legalen Wirtschaftskreislauf überführt werden. Der Clou ist allerdings, dass Geldwäsche eben nicht ohne ein entsprechendes Netzwerk funktioniert. Dieses Netzwerk enthält verschiedene Stationen, von denen aus Gelder überwiesen werden, wo sie geparkt und weiterverwendet werden können. Zudem benötigt das System auch Unternehmen, die ein legitimes Geschäftsmodell haben. Darüber hinaus spielen auch Steuerberater, Notare und Rechtsanwälte eine Rolle. Nicht selten ohne Kenntnis der kriminellen Anteile der mitunter komplexen Firmenkonstruktionen. Eine beliebte Möglichkeit, um illegales Geld in den legalen Wirtschaftskreislauf zu übersetzen, ist zum Beispiel der Kauf und Verkauf von Immobilien. Ein Krimineller kann etwa eine Immobilie kaufen, die einen Wert von vier Millionen Euro aufweist. Doch er bezahlt für diese Immobilie offiziell nur zwei Millionen und lässt dem Verkäufer die weiteren zwei Millionen in bar und unregistriert zukommen. Danach hält der Kriminelle die Immobilie für einige Jahre und investiert vielleicht sogar in die Renovierung. Der Verkaufswert der Immobilie steigt, sodass er sie nach einiger Zeit legal für 4,5 Millionen Euro am Markt verkaufen kann. Er hat somit einen offiziellen Profit von 2,5

Millionen gemacht, den er nun legal besitzt und versteuert.

**KOMPLEXES SYSTEM, VIELE PARAMETER** Ob nun das Geld dafür ursprünglich aus einer legalen Quelle stammt oder ob es sich um Drogengeld handelt, ist nur schwer herauszufinden. Vor allem setzen Verbrecher gerne auf eine Mischung aus Zahlungen aus legalen Quellen und kriminellem Geld. „Geldwäsche ist ein komplexes System, das darauf aufbaut, dass man es nicht entdeckt", erklärt Getzner. Entsprechend viele Parameter hat sein Team berücksichtigt. Etwa die Bemühungen der Staaten zur Umsetzung von Anti-Geldwäsche-Richtlinien, die gemeinsame Sprache, aber auch kulturelle Nähe. So kamen die Forscher zu einem statistischen Modell, mit dem sich die aus den Niederlanden bekannten Daten bemerkenswert gut abbilden lassen. „Kein statistisches Modell beschreibt die Wirklichkeit perfekt, aber im Rahmen der in der Ökonomie üblichen Unschärfen können wir die bekannten Daten mit wenigen ausgewählten Parametern erstaunlich gut beschreiben", sagt Getzner. Deshalb lässt sich das Modell auch auf andere Staaten extrapolieren, über die man weniger Information hat als über die Niederlande. So gelangte das Team schließlich zu einer groben Abschätzung über die Geldwäschesummen auf der ganzen Welt, aber auch für Österreich. Das globale Gesamtvolumen an Schwarzgeld haben die Wissenschaftler konservativ auf 2,3 Billionen US-Dollar im Jahr geschätzt. Die Höhe des heimischen kriminellen Geldes beziffert der Forscher mit rund 2,5 Milliarden Dollar. „Beim Geldvolumen, gemessen am Bruttoinlandsprodukt, das einen kriminellen Ursprung direkt im Land hat, scheint Österreich knapp unter dem OECD-Durchschnitt zu liegen. Dafür wird durch Österreich etwas mehr Schwarzgeld durchgeschleust als im OECD-Durchschnitt", sagt Prof. Getzner.

Aus derartigen statistischen Modellen und den Daten können schlussendlich Behörden Aufschlüsse über unentdeckte Transaktionen und über die Wirksamkeit von Anti-Geldwäsche-Maßnahmen ziehen. Eine wesentliche Rolle, um illegalen Transaktionen auf die Schliche zu kommen, spielen wenig überraschend die Banken.

**SEHR VERDÄCHTIG!** Entsprechend wichtig waren für die Analyse sogenannte „verdächtige Transaktionen", die bei den Instituten aufscheinen. Im Fokus stehen insbesondere Transaktionen, die unter Berücksichtigung der normalen Geschäftstätigkeit des Kunden ungewöhnlich, sehr umfangreich sind oder keinen finanziellen oder rechtmäßigen Zweck haben. Wann Transaktionen als verdächtig eingestuft werden müssen, ist oft erst im Kontext der Zeit erkennbar. Denn die Kriminellen bauen ihre Systeme mitunter langsam auf. Zunächst werden beispielsweise nur kleine Überweisungen getätigt. Alle Dokumente liegen vor, alles scheint seine Richtigkeit zu haben. Dann werden langsam Frequenz und Beträge erhöht, und irgendwann wird die Bank stutzig. Eine bestimmte Transaktion tanzt vielleicht aus der Reihe und muss als verdächtig eingestuft und gemeldet werden. Dann versucht man nachzuvollziehen, welche Zahlungen bislang getätigt wurden. Bei dieser Analyse erweisen sich häufig viele einzelne Transaktionen, die zunächst nicht verdächtig gewirkt haben, doch als auffällig. Selbst dann ist es allerdings nicht ganz einfach, den Kriminellen auf die Spur zu kommen, da Behörden verschiedener Länder aktiv werden müssen. Aufgrund der hohen Summen, die dem Fiskus durch das Phänomen entgehen und natürlich auch, um Verbrechern das Handwerk zu legen, steigt das Engagement vieler Staaten. Entsprechend groß war das Interesse der niederländischen Behörden an den Erkenntnissen der Forscher. Aber auch in Österreich besteht bereits Kontakt zu Finanzministerium und Bundeskriminalamt. Denn was die Analyse zweifelsfrei ergeben hat: Staaten können der Geldwäsche durch strenge Regulatorien und permanente Aufsicht wirksam entgegenwirken. Egal, wie einfallsreich die Verbrecher auch sind. ◀

**WIE GELDWÄSCHE FUNKTIONIERT**

**PLATZIERUNG** Zunächst werden rechtswidrig erworbene Vermögenswerte in den Finanz- oder Wirtschaftskreislauf über Banken oder andere Institutionen eingeschleust.

**HERKUNFTSVERSCHLEIERUNG** Im zweiten Schritt werden diverse hintereinandergeschaltete Handlungen gesetzt, um eine Nachvollziehbarkeit der kriminellen Herkunft der Vermögenswerte zu verunmöglichen.

**INTEGRATION** Zuletzt erfolgt die Über- bzw. Rückführung der auf diese Weise „legal" erscheinenden Vermögenswerte in den legalen Finanz- oder Wirtschaftskreislauf.

**TEXT** PETER MARTENS

# WENN DAS LICHT AUSGEHT

**Anfang des Jahres ist Europa nur knapp an einem großflächigen Stromausfall vorbeigeschrammt. Ein solcher Blackout kann alle Systeme bis hin zur Wasserversorgung lahmlegen. Österreichs Stromwirtschaft hat die Gefahr abgewehrt. Doch es gibt tatsächlich einige Gründe, beunruhigt zu sein.**

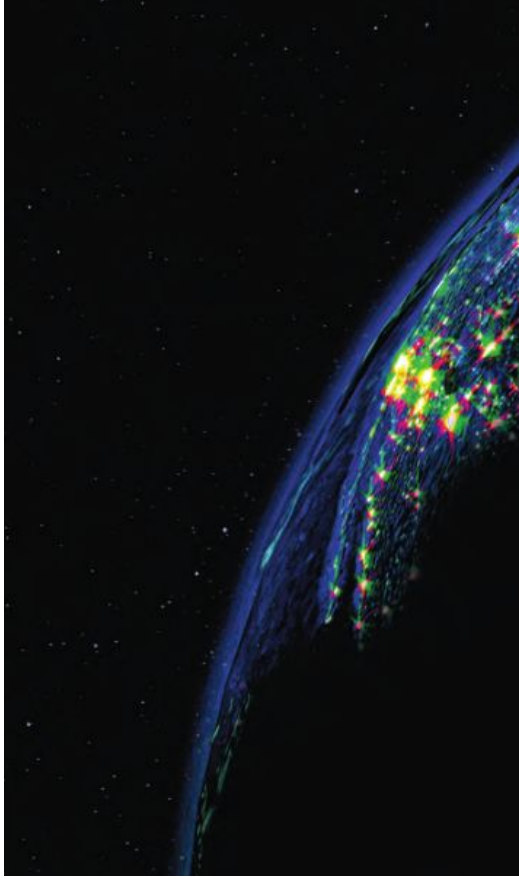


Foto: Getty Images

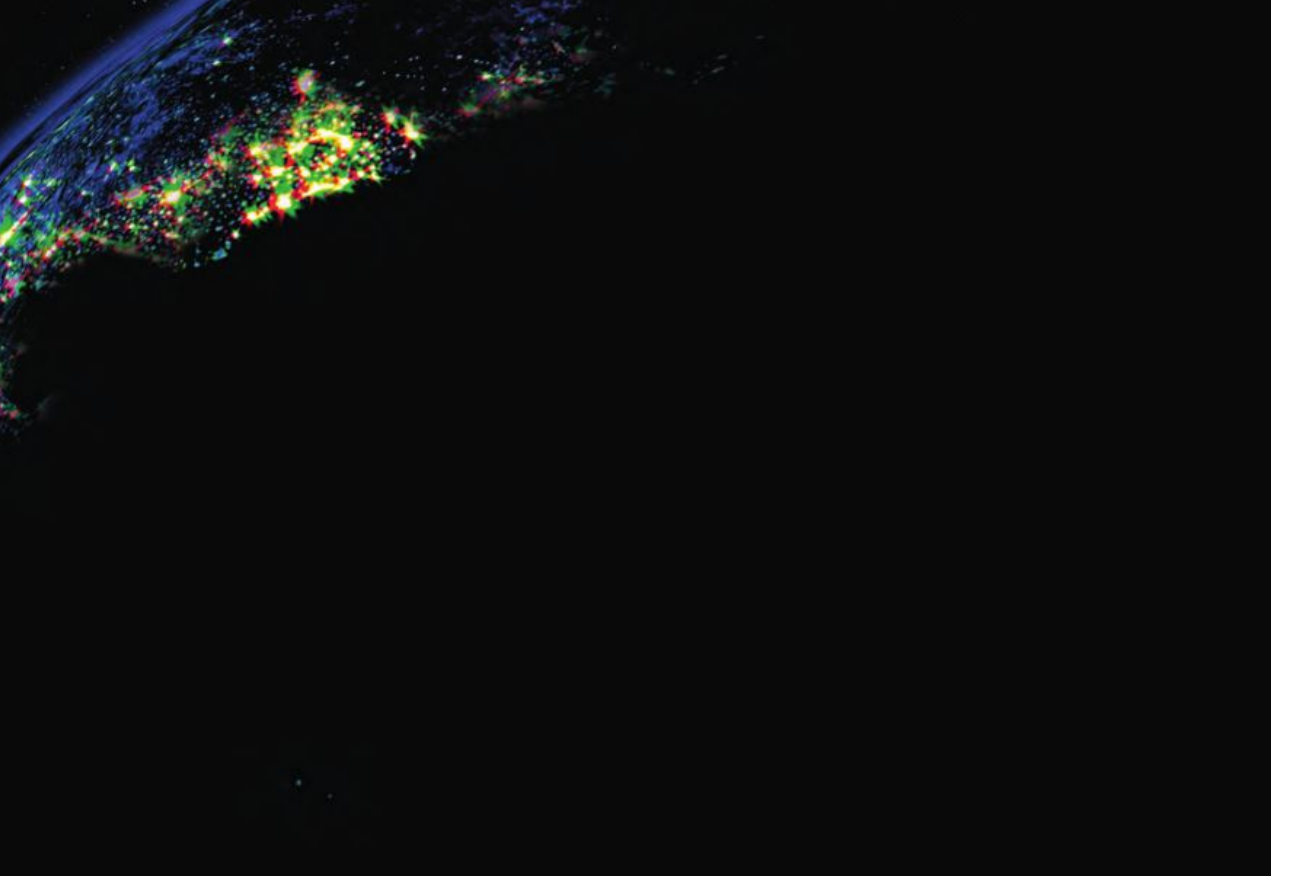
D

Die Schlagzeilen zur Energiewirtschaft bestimmen in diesem Jahr genau zwei Themen. Das eine Thema diktiert die Politik: Es ist der im Regierungsprogramm vorgesehene Ausbau der Erneuerbaren. Ihre Kapazität soll in Österreich bis 2030 um die gigantische Menge von 27 Terawattstunden steigen. Das zweite Thema ist die Gefahr eines Blackouts. Gemeint ist damit eine länger andauernde Störung der Stromversorgung, die ganze Landstriche oder sogar Europa betreffen kann. Weil das Stromnetz für die Gesellschaft wie ein Nervensystem ist, blockiert ein Blackout auch alle Verkehrsströme, die Produktion, die gesamte Kommunikation, den Betrieb von Spitälern und auch die Wasserversorgung. Dieses Thema, so scheint es, hat nichts mit dem Ausbau der Erneuerbaren zu tun. Und diktiert wird es, so scheint es ebenfalls, nicht von der Politik, sondern von der Wirklichkeit, nämlich von einer Störung der Stromnetze quer durch Europa am 8. Jänner.

Allerdings hängen die Themen Blackout und Erneuerbare sehr wohl direkt miteinander zusammen. So sagt Verbund-Konzernchef Michael Strugl: „Die Dekarbonisierung des Energiesystems ist gut und richtig. Mit dem Ausbau der Erneuerbaren ist aber die Vulnerabilität größer geworden. Die Anforderungen an unsere Netze, Kraftwerke und Speicher wachsen. Gleichzeitig schwinden unsere gesicherten Kapazitäten." Ein Blackout, so Strugl weiter, würde in Österreich Kosten von 1,18 Mrd. Euro pro Tag verursachen. Das wäre ungleich mehr als die Kosten, die ein weitreichender Lockdown verursacht.

**BLACKOUT KOMMT BINNEN FÜNF JAHREN** Klar ist, dass die verstärkte öffentliche Thematisierung dieser Gefahr Teilen der Energiewirtschaft nützt. Etwa den Netzbetreibern. Sie wollen und müssen ihre Netze immer weiter ausbauen, um mit den ständig steigenden Kapazitäten der schwankenden Erneuerbaren Schritt zu halten. Wenn sie nun immer wieder auf das Thema Blackout verweisen, erleichtern sie sich selbst sowohl die Argumentation für den Ausbau der Netze als auch Fragen zur Finanzierung. Klar ist aber auch, dass diese Gefahr real ist und dass sie offenbar wächst. Das belegen die Einschätzungen völlig unbeteiligter Akteure, in Österreich etwa des Zivilschutzverbandes und des Bundesheeres. So schreibt das Bundesheer in der „Sicherheitspolitischen Jahresvorschau 2021", die Gefahr eines Blackouts sei „das größte Risiko für eine nächste Systemkrise in Österreich". Dieses Risiko sei noch höher als jenes eines breiten Cyberangriffs, einer unkontrollierten Massenmigration oder eines kriegerischen Konfliktes mit österreichischer Beteiligung. Besonders beachtlich ist folgende Einschätzung der Armee: „Mit einem Blackout ist binnen der nächsten fünf Jahre zu rechnen."

**WAS AM 8. JÄNNER PASSIERT IST** Tatsächlich ist Europa am Nachmittag des 8. Jänner 2021 knapp an einem Blackout vorbeigeschrammt. Laut Analyse von Entso-E, dem Verband europäischer Netzbetreiber, hat es an diesem Tag ungewöhnlich hohe Stromflüsse vom Südosten in den Westen Europas gegeben. Um 14:04 Uhr fiel im Umspannwerk Ernestinovo in Kroatien eine Kupplung aus. Die Stromflüsse verlagerten sich auf benachbarte Leitungen, überlasteten diese, in der Region fielen 14 Stromleitungen aus. 30 Sekunden später spaltete sich das europäische Stromnetz in zwei „Inseln": eine im Südosten mit einer zu hohen Frequenz und eine im Westen inklusive Österreich mit einer Unterversorgung. In Österreich sprangen beim Übertragungsnetzbetreiber APG unter Vertrag stehende Wasserkraftwerke ein, aber auch thermi-



sche Kraftwerke und große Batteriespeicher. In Frankreich und Italien schalteten Netzbetreiber große Industriekunden ab, um das Netz zu stabilisieren. Zusätzlich schaufelten auch skandinavische und sogar britische Kraftwerksbetreiber große Strommengen ins Netz. Um 15:07 Uhr erreichte das Netz wieder die notwendige Frequenz von 50,0 Hertz. Die beiden „Inseln" waren wieder synchronisiert.

**INSTABILITÄT DES SYSTEMS STEIGT** Dieser Tag habe die Stabilität der Systeme in Europa bewiesen, betont Entso-E in seiner Analyse. Auch sei es kein Blackout, sondern lediglich ein „Frequenzabfall" gewesen, denn bis zu einem weiträumigen Stromausfall hätten noch mehrere Eskalationsstufen gefehlt. Auch streichen sowohl Entso-E als auch die heimische APG heraus, dass nicht die Erneuerbaren der Auslöser für die Störung waren. Allerdings waren die „neuen Erneuerbaren" Windkraft und Photovoltaik auch nicht an der Gegensteuerung beteiligt. Und Daten der APG zeigen, wie aufwendig die Stabilisierung der Netze inzwischen ist. Weil die stark schwankende Stromproduktion der Erneuerbaren wächst, muss die APG inzwischen fast täglich stabilisierend eingreifen. Dieses „Redispatch" kostete im Jahr 2001 noch 1,7 Mio. Euro. Im Vorjahr musste die APG dafür knapp 134 Mio. Euro an Kraftwerksbetreiber überweisen. Geld, das am Ende von Betrieben und Konsumenten zu zahlen ist. Tendenz heuer weiter steigend. Ein zentraler Aspekt zum Thema Blackout steht allerdings eher im Hintergrund: Heute können nur thermische Kraftwerke, Atomkraftwerke und hierzulande auch die Wasserkraft sichere Kapazitäten und damit Stabilität im Netz bieten. Mit Erneuerbaren lässt sich das Netz nur über Speicher stabil halten, doch die einzigen heute im industriellen Maßstab verfügbaren Anlagen sind Pumpspeicher, und deren Kapazitäten sind begrenzt. Wasserstoff ist hier zwar ein großer Hoffnungsträger, doch diese Speichertechnologie steckt noch in den Kinderschuhen. Auch übers Jahr gesehen ist das Wasserkraftland Österreich nach Zahlen der APG und des heimischen Bilanzgruppenkoordinators APCS von September bis April ein Stromimporteur. Bis zu ein Drittel des heimischen Stromverbrauchs produzieren dann Gaskraftwerke, Atomkraftwerke und Kohlekraftwerke im Ausland. Das Problem: Heimische thermische Kapazitäten sinken jedes Jahr, weil Gaskraftwerke immer unwirtschaftlicher werden. Gleichzeitig steigt Deutschland 2022 aus der Atomkraft aus und plant auch den Ausstieg aus der Kohlekraft. Damit kommen auch auf Österreich weitere Schwierigkeiten zu.

**BEWUSSTSEIN SCHAFFEN** Der beste Schutz gegen einen Blackout seien jedoch schnell startende, sogenannte „schwarzstartfähige" Kraftwerke, betonte als Reaktion auf den 8. Jänner Martin Graf, Vorstand der Energie Steiermark. Das können sowohl Wasserkraftwerke als auch Gaskraftwerke sein – deren Betrieb jedoch sichergestellt werden müsse, so Graf weiter. Gleichzeitig hat die Energie Steiermark eine vielbeachtete Kooperation mit dem steirischen Zivilschutzverband vereinbart. Das zentrale Ziel: Betriebe, Menschen und vor allem die Gemeinden und Bürgermeister auf den Fall des Falles vorzubereiten. Auch Verbund-Konzernchef Michael Strugl betont, dass es sehr wichtig sei, ein entsprechendes Bewusstsein in der Öffentlichkeit zu schaffen. Und mehr noch: die Energiewirtschaft die nötigen Investitionen tätigen zu lassen, damit Österreichs Stromversorgung weiterhin zu den besten der Welt gehört. ◀

**TEXT** OLIVER WEBERBERGER


Mercedes EQC

# SIND WIR SCHON DA?

**Der Sommer steht vor der Tür, Urlaubsreisen an die Obere Adria scheint nichts im Wege zu stehen. Für die Besitzer eines Elektroautos haben sich die Prioritäten freilich geändert. Wo sich einst alles um Kofferraumvolumen und Unterhaltungsprogramme für die Kinder gedreht hat, kreisen heute die Gedanken um die Frage, wie man bis zum Urlaubsziel gelangt. Ein Wegweiser.**

Kurz gesagt, das Wichtigste ist Vorbereitung. Das schmeckt jetzt nicht so recht nach Sonne, Strand und Meer, ist aber zwingend notwendig, um die heilige Dreifaltigkeit des Sommerurlaubes möglichst entspannt zu erreichen. Gott sei Dank ist man dabei nicht auf sich alleine gestellt. Neben diversen Anwendungen im App-Store seiner Wahl sind quasi alle E-Autos mit einem ganzen Sammelsurium an digitalen Hilfen ausgestattet. Das bringt uns auch gleich zum ersten, etwas banal klingenden Punkt.

**KENNE DEIN AUTO** Nicht im Sinne von „Suchen und Finden" in vollen Parkgaragen. Es geht vielmehr um das Wissen um die Kompetenzen des eigenen Stromers. Moderne und mit großen Akkus ausgestattete Elektrofahrzeuge verfügen über respektable Reichweiten. Rund 500 Kilometer sind keine Seltenheit mehr. Der Haken daran, die laut WLTP genormten Angaben sind so realitätsfern wie die Privatsphäre am Strand von Lignano. Das gilt erst recht für ein voll besetztes Auto samt Gepäck, denn jedes zusätzliche Kilogramm nagt weiter an der Reichweite. Vom Schauraum direkt Richtung Süden zu starten empfiehlt sich nur für Abenteuerlustige mit abgeschlossenem Survivaltraining. Besser wäre es, einen Testlauf unter urlaubsähnlichen Umständen zu starten, im Idealfall mit einem ähnlichen Streckenprofil. Einfach um zu erkennen, wie gnadenlos Autobahnetappen die Akkus leer saugen und wie sehr Rekuperation dagegen hilft. Was uns direkt zum nächsten Tipp bringt.

**MACHE DEN WEG ZUM ZIEL** Der Drang, möglichst rasch seine Destination zu erreichen, ist verständlich, verträgt sich mit E-Mobilität aber nur marginal. Warum also nicht aus der Not eine Tugend machen und quasi „ein bisserl ins Land einischaun". Das Klischee vom schönen Österreich mit seinen Bergen und Seen ist nämlich gar keines. Schon klar, für manche gehören Staus, Tunnelsperren und meterhohe Lärmschutzwände zum Urlaubsfeeling einfach dazu. Dabei gäbe es eine Unmenge an Sehenswürdigkeiten auf dem Weg gen

Süden. Warum nicht eine oder mehrere solche einbauen? Warum nicht gleich einen Tag früher losfahren und eine Übernachtung entlang des Weges einplanen? Es gäbe viel zu entdecken, und so ganz nebenbei lässt sich das E-Auto ohne Zeitdruck laden. Es gäbe nur Folgendes zu beachten.

**PLANEN UND ANMELDEN** Es ist ein wenig wie bei der Henne und dem Ei. Zuerst Route planen und dann Ladestationen checken? Oder umgekehrt? Dank der mittlerweile guten Ladeinfrastruktur sowohl hierzulande als auch im Bereich der Oberen Adria ist beides möglich. Sowohl die Navigationssysteme der Hersteller als auch diverse Apps sind hier verlässliche Hilfen, geben Auskunft über Anzahl der Ladeanschlüsse und Ladeleistungen. Pauschal gesagt, finden sich entlang der Hauptverkehrsrouten mehr und stärkere E-Tankstellen, man wird aber auch bei einem Ausflug ins Hinterland nicht verhungern. Falls doch, bieten praktisch alle Hersteller im Rahmen ihrer Garantien Mobilitätsservices an. Das reicht von kostenlosem Transport zur nächsten Ladestation bis zu einer mobilen Aufladung vor Ort. Praktisch ist das Horrorszenario „leerer Akku" kaum vorstellbar, zumindest nicht, wenn man sich bei allen infrage kommenden Anbietern rechtzeitig registriert hat. Die schnellste freie Ladestation bringt wenig, wenn mangels Berechtigung gar nicht geladen werden darf.

**ALSO ALLES EITEL WONNE?** Im Prinzip ja, wobei manches in einem gewissen Graubereich bleibt. So lassen sich die Kosten für die Ladezyklen angesichts eines Tarifdschungels nur schwer kalkulieren. Und in Ermangelung einer Urlaubssaison 2020 fehlen Erfahrungswerte hinsichtlich Auslastung der Ladestationen an den klassischen Reisedestinationen. Ein kleiner Rest an Nervenkitzel bleibt demnach, was bei einem Badeurlaub an der Oberen Adria ja eine nette Abwechslung ist. ◀

**Tesla Model 3**

**VW ID4 Pro Performance**

**BMW iX3**

AB IN DEN URLAUB MIT

**TESLA MODEL 3** Tesla ist und bleibt in Sachen E-Mobilität der Vorreiter, das Model 3 ein Verkaufsschlager. Nicht nur die Reichweiten sind beeindruckend, auch das dichte Netz an Superchargern macht Tesla-Fahrern das Leben leicht. REICHWEITE: 614 Kilometer, ab 54.990 Euro.

**VW ID4 PRO PERFORMANCE** Mit der ID-Familie kommt massiv Bewegung in den Markt der Elektroautos. Der ID4 ist die logische Konsequenz für alle, bei denen E-Mobilität nicht an der Stadtgrenze endet. Gilt in der Form übrigens auch für Skoda und seinen Enyaq iV.
REICHWEITE: 522 Kilometer, ab 43.970 Euro.

**BMW IX3** Mit dem iX3 macht BMW in Sachen E-Mobilität ernst. Basis ist der aktuelle X3, also eines der besten SUV am Markt. Fahrdynamisch ist der iX3 ein echter BMW, Premium at its best versteht sich sowieso von selber.
REICHWEITE: 458 Kilometer, ab 66.950 Euro.

**MERCEDES EQC** Der EQC ist in vielerlei Hinsicht ein klassischer Mercedes. Perfekte Verarbeitung und ein elegantes Interieur umschmeicheln die Insassen, die lautlose Kraft des Elektromotors unterstreicht den Highend-Anspruch des EQC noch. REICHWEITE: 450 Kilometer, ab 75.500 Euro.

# LET'S TALK ABOUT HACKS, BABY

**Hacker tauschen sich rege aus und kommen so zusammen schneller voran. Wenn das auch von Cyberattacken betroffene Unternehmen tun und über Gegenmaßnahmen und Best Practices sprechen, werden auch sie gemeinsam stärker.**

Schritt halten mit der Hacker-Szene – das wünschen sich Unternehmen, um sich vor Datendiebstahl, Erpressung und Systemstörungen zu schützen. Nicht einfach. Schließlich tauschen sich Hacker rege über Angriffsmethoden, Verwundbarkeiten und Sicherheitslücken aus. Da braucht es als Gegengewicht auch eine intensive Kommunikation aufseiten der Unternehmen. Wenn sie über ihre Schwierigkeiten sprechen, hilft das ihnen selbst und anderen. Doch ist das nicht unangenehm? Dazu die gute Nachricht: Man muss nicht immer gleich das große Scheinwerferlicht auf sich richten. Es gibt Möglichkeiten, sich informell auszutauschen. Es sind mittlerweile sogenannte Trust-Circles entstanden – vertrauenswürdige Kreise, in denen ein diskreter Austausch über den Umgang mit Cyberangriffen stattfindet.

„Gemeinsam als Community sind wir besser aufgestellt und können schneller reagieren", sagt die Informatik-Professorin Maria Leitner, die an der Uni Wien und am Austrian Institute of Technology (AIT) forscht und lehrt. Gerade bei größeren Sicherheitslücken, die viele Organisationen betroffen haben, habe sich gezeigt, dass es sinnvoll war, den Austausch zu suchen, denn meist kamen aus der Community wichtige Hinweise zur Problemlösung. Beim AIT setzt man sich unter anderem genau mit der Frage auseinander, wie Unternehmen sich über Software-Schwachstellen austauschen können. Ist eine Firma von einer Softwarelücke betroffen, sind es wahrscheinlich auch andere – und kommunizieren die Betroffenen darüber, können sie einander helfen, indem sie zum Beispiel darüber reden, welche Spuren die Angreifer in ihren Systemen hinterlassen haben und ob es schon Patches gibt, mit denen die Sicherheitslücken wieder geschlossen werden können. Leitner weist darauf hin, dass es eigene Websites gibt, auf denen sogenannte Common Vulnerabilities and Exposures (CVEs) inklusive hilfreichen Hinweisen und gegebenenfalls Lösungen beschrieben sind.

Wer noch Hemmungen hat, über die eigene Betroffenheit zu sprechen, kann diese also getrost ablegen. Und das scheint in der Pandemie auch schon vielfach passiert zu sein. Maria Leitner erzählt, die Pandemie habe insbesondere bei KMU zu einem stärkeren Interesse an Cybersicherheit und zu mehr Austausch geführt. So wurden nicht nur viele unternehmensinterne Security-Operation-Center etabliert, sondern auch branchenspezifische Computer-Emergency-Response-Teams gegründet. Gerade in Österreich gibt es Leitner zufolge eine „großartige Community", die sich über IT-Sicherheit austauscht. Als eine nationale Anlaufstelle nennt sie das Computer-Emergency-Response-Team CERT.at, das unter anderem insbesondere für KMU proaktiv Warnungen, Alerts und Tipps herausgibt, aber auch informellen Austausch ermöglicht. Eine erste Notfallhilfe bietet zudem die WKO mit ihrer Cyber-Security-Hotline an, die 24 Stunden am Tag und sieben Tage die Woche erreichbar ist. Auch die Website it-safe.at der WKO ist eine gute Plattform, um sich über aktuelle Betrugsmeldungen und Cybersicherheit, Datenschutz oder auch Förderungen von IT- und Cybersicherheits-Maßnahmen zu informieren.

Also: Überlassen Sie nicht den Angreifern das Privileg des Austausches, durch den alle zusammen schneller vorankommen! Nutzen auch Sie die Gelegenheit, über IT-Angriffe, Gegenmaßnahmen und Best Practices zu sprechen und stellen Sie die Verteidigung auf breitere Füße. ◀

**DIE AUTORIN**

Alexandra Rotter berichtet von aktuellen Cyberwar-Schauplätzen, über Angreifer und deren Strategien, Schäden sowie Rettungs- und Schutzmaßnahmen.

# ELEKTRISIEREND!

ŠKODA
SIMPLY CLEVER

## Der ŠKODA SUPERB iV

## Der ŠKODA OCTAVIA iV

Die beiden Plug-in-Hybrid Modelle vereinen durch die Kombination des elektrischen und benzinbetriebenen Antriebssystems das Beste zweier Welten. So können Sie auf Ihren lokalen Wegen rein elektrisch unterwegs sein. Die serienmäßige Standklimatisierung ermöglicht es Ihnen beispielsweise vor der Abfahrt, ferngesteuert mittels MyŠKODA App, die für Sie perfekte Innenraumtemperatur im Fahrzeug einzustellen. Details bei Ihrem ŠKODA Betrieb.

**Sparen Sie mit dem E-Mobilitätsbonus bis zu 1.500,– Euro und fragen Sie nach der attraktiven ŠKODA Wirtschaftsförderung.**

Symbolfoto. Stand 03.05.2021. Alle angegebenen Preise sind unverb., nicht kart. Richtpreise inkl. NoVA und 20% MwSt. Gültig ab Kaufvertrag-/Antragsdatum 01.04.2021 bis 30.06.2021 bzw. solange der Vorrat reicht. Der E-Mobilitätsbonus (Unternehmer: 1.200,– I Privatkunde: 1.500,– Euro) wird vom Listenpreis des Neuwagens abgezogen und kann pro Kauf nur einmal in Anspruch genommen werden – solange der Vorrat reicht (keine Barablöse möglich). Ausgenommen sind Sonderkalkulationen für Flottenkunden und Behörden.

Stromverbrauch: 14,1–18,1 kWh/100 km. Verbrauch: 1,0–1,8 l/100 km. $CO_2$-Emissionen: 22–40 g/km.

iV

skoda.at facebook.com/skoda.at youtube.com/skodaAT instagram.com/skodaAT