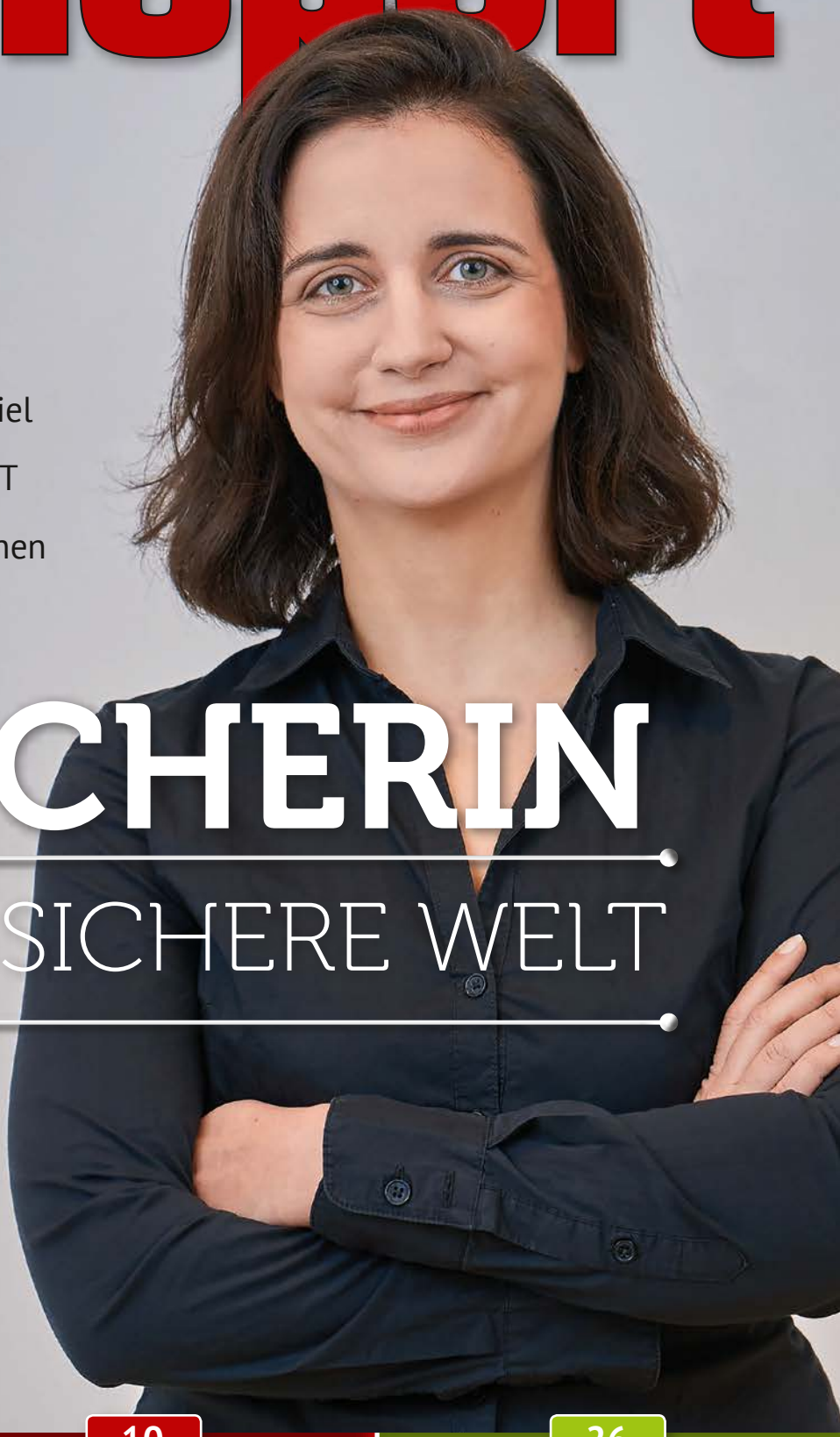
WWW.REPORT.AT DAS MAGAZIN FÜR WISSEN, TECHNIK UND VORSPRUNG

telekom +it

Report

Ausgabe 05 | 2021



20

Johanna Ullrich hat sich das Ziel gesetzt, Ingenieurwesen und IT für die Sicherheit von physischen Systemen zu verbinden.

FORSCHERIN

FÜR EINE SICHERE WELT

P. b. b. Verlagspostamt 1170 Wien, Vertriebskennzahl 02 Z030627M, Preis: EUR 4,–

publikumsgespräche des Report Verlag

Infos unter:

DIE ÖFFENTLICHE DISKUSSIONSREIHE ZU WIRTSCHAFTS- UND FACHTHEMEN, DIE DIE BRANCHE AKTUELL BEWEGEN.

DER BESUCH IST KOSTENLOS.

#REPORTTALK

»KI – vertrauenswürdig und transparent in der Praxis«

Automatisierte Geschäftsprozesse, Machine-Learning und Entscheidungshilfen für die Sachbearbeiter*innen finden zunehmend Einzug in Unternehmen und Behörden – mit weitreichenden Folgen für Kund*innen und Bürger*innen. Doch welche Kriterien zeichnen vertrauenswürdige Systeme eigentlich aus? Wie können Anwendungen hinsichtlich Transparenz und Fairness getestet werden? Die Report-Publikumsdiskussion zur Ethik von Algorithmen, Optimierungsbedarf und der Herausforderung für unsere Gesellschaft und unseren Wirtschaftsstandort.

Wann: 18. Novenber 2021, 16:00 bis 17:15 Uhr
Wo: via Zoom

EDiTORIAL

MARTIN
SZELGRAD
Chefredakteur

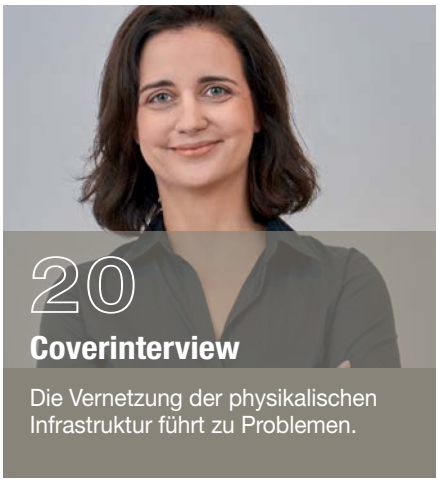
Unterschätzte Gefahren überall

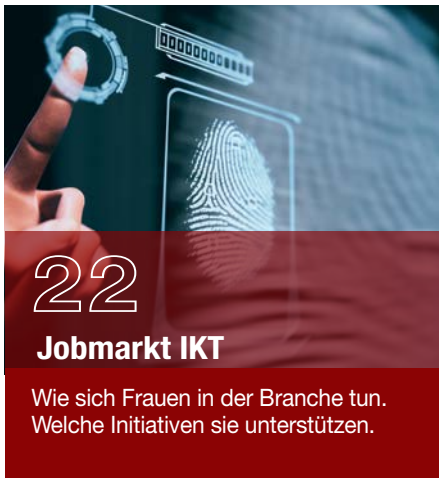
Ganze 58 % aller Cyberattacken von staatlichen Akteuren, die Microsoft im vergangenen Jahr registriert hat, stammten aus Russland. Die Angriffe der russischen Hackergruppen werden dabei immer effektiver: So stieg die Rate erfolgreich kompromittierter Systeme von 21 % im vergangenen Jahr auf 32 % im Jahr 2021, kommt die aktuelle Studie »Digital Defense Report« zum Schluss. Staaten setzen zunehmend auf Cyberangriffe, um ihre politischen Ziele zu erreichen. Dabei geht es längst um mehr als Spionage. Die Angriffe zielen ab auf die Zerstörung und Störung von staatlichen Systemen sowie wirtschaftlichen Profit, heißt es.

Und Cybercrime hat sich von einer aufstrebenden Branche zu einem ausgereiften kriminellen Wirtschaftszweig entwickelt, haben auch die Diskutant*innen einer Podiumsrunde des Report Verlags im Oktober bestätigt (Seite 10). Wer als Unternehmer*in heute noch glaubt, er werde uninteressant für Attacken bleiben, irrt gewaltig. Bei der jüngsten Ransomwarewelle Ende August in Oberösterreich hatte es auch Kindergärten, Arztpraxen und ein Blutlabor getroffen. »Wir müssen in Österreich endlich aufwachen«, appelliert Jürgen Weiss, Geschäftsführer von ARES Cyber Intelligence.

Weiss wünscht sich eine Plattform für den Austausch von Informationen und Erfahrungen auch für kleinere und mittlere Unternehmen, ähnlich wie es bereits die Branchen-CERTs für etwa die Verwaltung und Energiewirtschaft gibt. Leider ist es bei Maßnahmen für die Informationssicherheit ähnlich, wie manche immer noch mit Corona umgehen: Solange nichts Drastisches in meiner unmittelbaren Umgebung passiert – oder es auch mich selbst trifft – neige ich dazu, die Gefahr zu unterschätzen. Doch wir könnten nicht falscher liegen.

telekom+it Report
das magazin für wissen, technik und vorsprung





<< IMPRESSUM

Herausgeber: Alfons Flatscher [flatscher@report.at] **Chefredaktion:** Martin Szelgrad [szelgrad@report.at] **Redaktion:** Sarah Bloos [bloos@report.at], Angela Heissenberger [heissenberger@report.at] **AutorInnen:** Tobias Tretzmüller, Michael Xie, Katharina Bisset, Rüdiger Linhart, Karin Legat, Gebhard Borck, Rainer Sigl **Lektorat:** Johannes Fiebich **Layout und Produktion:** Anita Troger, Report Media LLC **Druck:** Styria **Vertrieb:** Post AG **Verlagsleitung:** Gerda Platzer [platzer@report.at] **Anzeigen:** Bernhard Schojer [schojer@report.at] **Medieninhaber:** Report Verlag GmbH & Co KG, Lienfeldergasse 58/3, 1160 Wien, **Telefon:** +43 1 90 299 0, **Einzelpreis:** 4 Euro **Jahresabonnement:** 40 Euro **Aboservice:** + 43 1 90 299 0
E-Mail: office@report.at Website: www.report.at

Inside

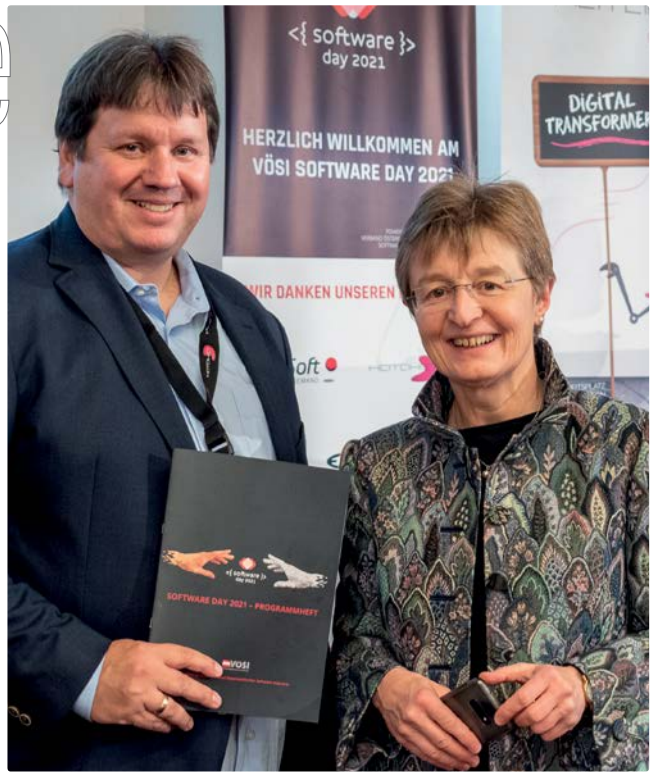
Digitale Barrierefreiheit

Die Wirtschaftsuniversität Wien wurde mit dem Zertifikat für digitale Barrierefreiheit im Web (WACA) in Bronze ausgezeichnet.

Rund 320.000 Personen in Österreich, 4 % der Bevölkerung, sind stark seheingeschränkt. Darauf gilt es auch bei der Gestaltung von Webauftritten Rücksicht zu nehmen. Aufgrund unterschiedlicher Zielgruppen – von Studierenden über Forscher*innen, Mitarbeitende bis hin zur breiten Öffentlichkeit –, und der Darstellung verschiedenster Informationen, ist der Webauftritt der WU komplex und beinhaltet viele Unterseiten. Schon bei der kompletten Neugestaltung der Website 2016 wurde auf Barrierefreiheit geachtet und laufend an der Verbesserung dieser gearbeitet. Durch diese Anpassungen wurde die Bedienungsfreundlichkeit der Website adaptiert. Unterstützt wurde die

Zertifikatsverleihung mit Vertreter*innen der WU durch Werner Rosenberger (Mitte).

WU von den Agenturen Plan2Net und Fonda. Nun unterzog sich die WU einem umfassenden Audit. Zertifiziert wurde nach den Web Content Accessibility Guidelines (WCAG-2.1, Konformität AA). »Aufgrund der Größe und Komplexität der Website der WU ist das Bronze Zertifikat eine sehr beachtliche Leistung und vorbildhaft gerade für weitere Universitäten«, sagt WACA-Projektleiter Werner Rosenberger.



Peter Lieber, VÖSI, mit Gerti Kappel, TU Wien: »Man muss verstehen, warum und wie ein KI-System Entscheidungen trifft oder etwas macht.«

KI für intelligente Unternehmen

Rund 160 Besucher erlebten beim »Software Day« Top-Forscher*innen und Vorträge von zahlreichen Expert*innen zum Thema Künstliche Intelligenz.

Software ist heute überall angekommen, künstliche Intelligenz ist am besten Wege dazu. Jetzt geht es darum, den Praxisbezug von KI auf den Boden zu bekommen«, sagte Peter Lieber, Präsident des Verbands Österreichischer Software Industrie (VÖSI), bei der Begrüßung des Software Day, der in der Wirtschaftskammer Österreich Ende September stattfand. »AI oder IA – und die Rolle der Universitäten«, fragte dazu Gerti Kappel, Dekanin für Informatik der TU Wien in ihrer Eingangs-Keynote – um gleich konkret auf aktuelle KI-Ansätze einzugehen. KI bedeute heute vor allem den Umgang mit großen Datenmengen, wichtig sei aber hier die Frage der »Explainability« und Transparenz.

»Deep Learning – the Key to Enable AI« – zu diesem Thema hielt KI-Forschungs-Pionier Sepp Hochreiter, Leiter des Instituts für Machine Learning der Uni Linz und Leiter des AI Labs am LIT, die zweite Keynote. Hochreiter zeigte auf, wie Google, Apple oder Audi aktuell auf Deep Learning und Know-how aus Linz setzen – und damit bereits jede Menge Geld verdient haben. Basis dafür ist die von Hochreiter bereits Anfang der neunziger Jahre entwickelte LSTM (Long Short-Term Memory) Technologie. Hochreiters Credo: »Wenn KI klug eingesetzt wird, kann man in den Unternehmen die Produktivität und Effizienz massiv steigern und sehr viel herausholen.«

Überschattet war der Fachtag vom plötzlichen Tod von InfraSoft-Geschäftsführer Peter Fleischmann ein Woche zuvor. »Er war ein Mann mit Handschlagqualität, ein Sir in der Softwareindustrie. Wir sind tief betroffen von diesem sehr schmerzlichen Verlust«, betont Peter Lieber. ■

die besten sager

»Man kann nicht schützen, was man nicht kennt. Vielen österreichische Unternehmen haben enorme Schwierigkeiten dabei, ihre Risiken durch Dritte – wie Lieferanten – im eigenen Umfeld zu erkennen«,

warnt Georg Beham, Cybersecurity & Privacy Leader bei PwC Österreich, dass Angreifer immer das schwächste Glied in einer Kette auswählen, um Unternehmen lahm zu legen.

»Wir sind keine Insel der Seligen, sondern Teil des globalen Cyberspace. Daher rate ich allen Unternehmen – auf gut österreichisch – nicht zu jammern, sondern anzupacken«

meint Jimmy Heschl, Head of Digital Security Red Bull, im Rahmen einer Branchenbefragung von PwC.

»Unsere Gesellschaft befindet sich an einem nie dagewesenen Wendepunkt: Ein Zurück in die Welt, die wir einmal kannten, gibt es nicht mehr und der Wandel nimmt immer weiter Fahrt auf«,

ist Vivek Mahajan, Chief Technology Officer Fujitsu, überzeugt, mit Technologie viele der aktuellen Herausforderungen meistern zu können.

Fotos: Jacqueline Godany, WU

köpfe des monats

Wechsel

Roland Ledinger löst Markus Kaiser als neuen Geschäftsführer des Bundesrechenzentrums ab. Er war bereits im Bundeskanzleramt, im Bundesministerium für Digitalisierung und Wirtschaftsstandort sowie zuletzt als Digitalisierungsbeauftragter im Burgenland tätig.

Bereichsleitung

Karin Wegscheider übernimmt die Leitung für Product Management im Bundesrechenzentrum. Sie verantwortet die Entwicklung und den Betrieb von Anwendungen und Services des BRZ.

Geschäftsführer

Marco Porak wurde zum Geschäftsführer IBM Österreich ernannt. Er folgt auf Patricia Neumann, die zum Data, AI & Automation Sales Leader IBM Europe, Middle East and Africa ernannt wurde.

Vertrieb Public

Thomas Fahler hat die landesweite Vertriebsleitung für den Geschäftsbereich Public Sector im Bechtle IT-Systemhaus Österreich übernommen. Er unterstützt die Weiterentwicklung des Geschäfts mit öffentlichen Auftraggebern.

HR-Expertin

Karin Szakal ist neue Senior Recruiting Specialist bei InfraSoft. Sie steht IT-Bewerber*innen und Kund*innen als Ansprechpartnerin zur Verfügung.

Finanzchef

Michel Grandchamp hat die Rolle des Vice President Finance und Controlling bei T-Systems Alpine übernommen.

Regionsleitung

in der neugeschaffenen Rolle als Regional Director für die Schweiz und Österreich wird Lindsay Keim Sales und Service für Citrix in den Ländern verantworten. Wolfgang Mayer verantwortet als Country Manager weiterhin Österreich.

Fotos: Andy Wenzel, BRZ/Christian Renezede, Bechtle, IBM, T-Systems Alpine, Citrix

kommentar

Open Source und »Copyleft«

Open-Source-Software hat sich in der IT-Branche mehr als etabliert und begegnet uns im Alltag in vielen Facetten. Was bei Weiterentwicklungen dazu rechtlich zu beachten ist.

Ein Kommentar von Tobias Tretzmüller

»Open-Source- und proprietäre Software sollten keine strukturelle Einheit bilden.«

Tobias Tretzmüller
Rechtsanwalt
Schwerpunktthemen IT-Vertragsrecht, Urheberrecht und Lizenzrecht, Datenschutzrecht, IT-Sicherheit und IT-Litigation

Schätzungen zufolge besteht proprietäre Standard- und Individualsoftware aus bis zu 98 % Fremdkomponenten. Nach Erhebungen des Scantool-Anbieters Synopsys basiert durchschnittlich über 57 % einer Codebasis auf Open-Source-Software. Die wirtschaftliche und rechtliche Bedeutung von Open-Source-Software ist daher hoch. Doch was hat es mit dem Copyleft-Effekt auf sich? Diese Klausel soll sicherstellen, dass Weiterentwicklungen der Software unter denselben Bedingungen der Lizenz wieder freigegeben werden. Damit birgt der Copyleft-Effekt ein erhebliches Risiko für die (eigene) proprietäre Software.

Der Copyleft-Effekt ist insofern problematisch, weil regelmäßig der Quellcode der von Open Source Software abgeleiteten Softwareelemente offengelegt werden muss. Die Open-Source-Lizenzbedingungen springen gleichsam auf die proprietäre Software über. Man spricht in diesem Zusammenhang anschaulich auch vom »viralen Effekt«. Die Open-Source-Software »infiziert« also die proprietäre Software. Das Heiligtum eines jeden Softwareunternehmens, der Quellcode, muss damit offengelegt werden. Für Entwickler von proprietärer Software besteht diese Gefahr insbesondere dann, wenn Bibliothek-Dateien (Plugins) auf Basis von Open-Source-Lizenzen in die proprietäre Software integriert werden – was häufig der Fall ist.

>> Copyleft ist nicht gleich Copyleft <<

Je nachdem, wie »aggressiv« der Copyleft-Effekt in den einzelnen Lizenzbestimmungen formuliert wird, wird differenziert zwischen einem »starken Copyleft«, einem (normalen) »Copyleft« und »Permissive Lizenzen«. Dazu zwei Beispiele zur besseren Veranschaulichung. Die aktuell am weitest verbreitete Lizenz ist die GNU General Public License: »You must cause any work…that in whole or in part contains or is derived from the (open source) program…to be licensed as a whole…under the terms of this license«.

Hingegen sehen die Lizenzen BSD Copyright License und MIT License gar keine diesbezüglichen Verpflichtungen vor (womit sie als Permissive Lizenzen zu qualifizieren sind). Dies macht die Nutzung lizenzrechtlich deutlich unkomplizierter als bei Copyleft-Software. Wenn man weiß, dass 57 % des weltweit programmierten Codes auf Open-Source-Lizenzen beruht und die GNU General Public License, Version 2, die am häufigsten eingesetzte Open-Source-Lizenz ist, wird deutlich, welche »Gefahr« Open-Source-Software für proprietäre Software begründet.

>> »Derived or not derived« <<

Die springende Frage in diesem Zusammenhang ist, wann liegt eine (von Open-Source-Software) abgeleitete Software »derived work« vor? Auch wenn Vertreter der Free Software Foundation und mit ihr das LG Berlin davon ausgehen, dass fast jede Art der Verknüpfung von proprietärer Software mit Copyleft-Open-Source-Software einen viralen Effekt auslösen soll, erscheint eine differenzierende Betrachtung geboten. Folgende Prüfungsschritte sind in diesem Zusammenhang zu empfehlen:

- Prüfung anhand formeller Kriterien: Sind die eigenen Entwicklungen von den Open-Source-Code-Elementen separat abgrenzbar? Wird dies bejaht, spricht dies gegen ein abgeleitetes Werk und somit gegen den Copyleft-Effekt.
- Prüfung anhand kommerzieller Kriterien: Wie wird die Software nach außen auf dem Markt vertrieben? Eine »einheitliche« Vermarktung spricht eher für ein »derived work« und somit für den Copyleft-Effekt. Die Eigenständigkeit liegt dann nicht vor, wenn die proprietäre Software mit der Open-Source-Software als »Teil eines Ganzen« verbreitet wird.
- Prüfung anhand funktioneller Kriterien: Sind die einzelnen Elemente jeweils für sich eigenständig nutzbar? Wenn also die proprietäre Software ohne die OS-Elemente nicht genutzt werden kann, spricht dies für ein abgeleitetes Werk und für den Copyleft-Effekt.

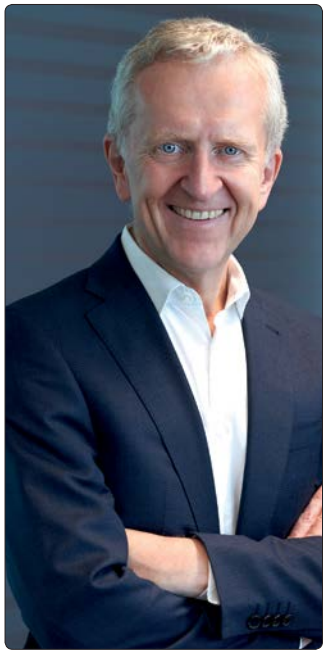
>> Handlungsempfehlung <<

Zur Vermeidung des viralen Effekts ist es erforderlich, dass die proprietäre Software unabhängig und formal von der OS-Software abgegrenzt werden kann und sowohl OS-Software als auch die proprietäre Software keine strukturelle Einheit bilden. Auf diese Abgrenzung ist sowohl während der Entwicklung als auch im Vertrieb der Software zu achten. Vertraglich sollte darauf geachtet werden, dass das Softwareunternehmen hinsichtlich der OS-Bibliotheken nicht der direkte Vertragspartner des Kunden wird. In diesem Fall würde das Softwareunternehmen für einen Mangel in den OS-Elementen haften. ■

Foto: iStock, TRetzmüller

Unternehmen als Ökosystem behandeln

Auf der »Fujitsu ActivateNow 2021« wurde erörtert, wie sich Unternehmen nachhaltig fit für die Zukunft aufstellen können – und wie Technologieunternehmen hierbei unterstützen.



Rupert Lehner, Fujitsu: »In der Zwischenzeit hat sich die Erkenntnis durchgesetzt, wie wichtig Cloud-Dienste sind und dass wir alle davon profitieren.«

Wie können aktuelle Herausforderungen bewältigt, wie die Welt nachhaltiger gestaltet werden? Welche Potenziale bietet Technologien, geschäftliche und gesellschaftliche Ziele in Einklang zu bringen? Resilienter zu werden und dabei auch Unternehmen mit Hilfe der passenden IT-Basis als Grundlage für effiziente Prozesse und Abläufe in Organisationen nach innen und nach außen neu zu formen, stand im Fokus der Konferenz »Fujitsu ActivateNow 2021« im Oktober.

»Fujitsu will seine Kunden bei der Entwicklung und Implementierung von Strategien unterstützten, die in den kommenden Jahren zur Umsetzung von Digitalisierungsprojekten benötigt werden. Dafür wollen wir Nachhaltigkeit an erste Stelle setzen, resilienter werden, ein Leben ohne Grenzen ermöglichen, Unternehmen als Ökosystem behandeln und vertrauenswürdige Automatisierung schaffen«, bestätigt Rupert Lehner, Corporate Executive Officer und Head of Central und Eastern Europe & Products Europe. »Insbesondere die Digitalisierung trägt dazu bei, dass die Innovationszyklen immer kürzer werden. Die Digitalisierung schafft neue Möglichkeiten, die von Unternehmen und Behörden aufgegriffen werden müssen. Agilität und Flexibilität spielen eine wichtige Rolle, um Geschäftsprozesse komplett neu zu denken.«

Das Technologieunternehmen will nun mit der globalen Marke »Fujitsu Uvance« Mehrwert in unterschiedlichen Einsatzgebieten für Technik liefern – bei »Nachhaltige Produktion«, »Verbrauchererlebnis«, »Gesundes Leben« und »Vertrauenswürdige Gesellschaft«, ebenso wie zu den horizontalen Themen »Digital Shifts«, »Business Applications« und »Hybrid IT«. ■

Fotos: Fujitsu

facts

10-fach

Daten von FortiGuard Labs zeigen, dass die durchschnittliche wöchentliche Aktivität von Ransomware-Bedrohungen im Juni 2021 weltweit mehr als zehnmal so hoch war wie vor einem Jahr.

Quelle: »FortiGuard Labs Global Threat Landscape Report«, Fortinet

0,05 %

beträgt in etwa die Wahrscheinlichkeit des Überführens und der Verurteilung eines Cyberkriminellen in den USA – ein Wert, der in anderen Ländern vermutlich noch niedriger ist.

Quelle: World Economic Forum

7 von 10

österreichischen Unternehmen (73 %) planen für das Jahr 2022 einen wesentlichen Anstieg ihrer Investitionen im Bereich Cybersecurity. Die Hälfte der Unternehmen kalkuliert dabei eine Erhöhung der Budgets von mehr als 10 % zum Vorjahr ein und liegt damit weit über dem globalen Durchschnitt (26%).

Quelle: »Global Digital Trust Insights Survey 2022«, PwC

35 %

der heimischen Unternehmen geben an, dass sie das Risiko von Datenschutzverletzungen durch Dritte systematisch erheben und über ein gutes Verständnis der vorhandenen Risiken verfügen. Bei Technologieanbietern oder IoT-Spezialisten haben lediglich 17% ein angemessenes Verständnis für diese Risiken.

Quelle: »Global Digital Trust Insights Survey 2022«, PwC

98 %

der Befragten weltweit wünschen sich eine Verbesserung der öffentlichen Sicherheit durch den Einsatz moderner Technologien. 75 % der Befragten geben an, dass sie Sicherheitsbehörden bei der Verwendung ihrer persönlichen Daten vertrauen, wenn sie wissen, wie diese genutzt werden.

Quelle: »Consensus for Change«, Motorola Solutions

Fotos: iStock

5

Prozesse haben 71 % der Unternehmen in Deutschland, Österreich und der Schweiz mindestens automatisiert. Robotic-Process-Automation (RPA) ist im Jahr 2021 bei sogar 76 % der Firmen über die reine Pilotphase hinausgekommen und nun Teil des Geschäftsalltags.

Quelle: »Robotic Process Automation 2021«, IDG Research, UiPath war.

-6,7 %

Österreichs Wirtschaft verzeichnete im Pandemiejahr 2020 einen historischen Rückgang der Wirtschaftsleistung um 6,7 %, der den Einbruch des Jahres 2009 (-3,8 %) im Zuge der globalen Wirtschafts- und Finanzkrise deutlich übertraf. Im Vergleich mit Handel oder Tourismus weit weniger betroffen war der Sektor Information und Kommunikation mit nur -2,0 %.

Quelle: Statistik Austria

1/2

der Menschen (50 %) fühlen sich online nicht ausreichend privat, ein knappes Drittel (31 %) fühlt sich nicht sicher – Frauen sind davon stärker betroffen als Männer. 46 % Frauen geben an, bereits einmal von einem Hack ihres Social-Media-Kontos betroffen gewesen zu sein, verglichen zu 37 % männlichen Betroffenen. Für die Studie wurden 5.000 Teilnehmer*innen in den USA, UK und Deutschland befragt.

Quelle: »Demographics of Cybercrime«, Malwarebytes

Cybersecurity für alle Fälle

Wenn PCs und Server lahmgelegt werden, kostet das nicht nur Geld und Reputation – es gefährdet den Fortbestand von Unternehmen. Am 13. Oktober diskutierten Expert*innen in einem Gespräch des Report zu Ausfallsicherheit, warum Virenscanner und Firewalls längst nicht mehr ausreichen, und auf welche Herausforderungen Organisationen bei der Absicherung ihres IT-Fundaments treffen.

Von Martin Szelgrad

Ronke Babajide, VMware: »Es braucht klare Regeln, wer worauf zugreifen darf.«

Report: Welchen Aufwand sollten Unternehmen und Organisation bei Absicherungsmaßnahmen betreiben? Welche »Levels« der Sicherheit, welche Features sind aus Ihrer Sicht unbedingt notwendig?

Ronke Babajide, VMware: Ich bin seit etwas mehr als 25 Jahren in der IT und habe die ganze Reise von einer Zeit, in der man sich noch wenig Gedanken um Viren, Trojaner und Sicherheitslücken gemacht hatte, in eine Welt der »Evasive Threats«, also schwer zu entdeckender Malware, persönlich miterlebt. Auch bei VMware beschäftigen wir uns stark mit Security.

Es gibt Themen, die man allen Unternehmen ans Herz legen kann. Zunächst sollten Organisationen vom implizierten Vertrauensmodell, wo jeder Zugriff auf alles hat, zu einem expliziten Sicherheitsmodell übergehen. Es braucht im Sinne von »Zero Trust« klare Regeln, wer auf welche Dinge zugreifen darf. Ein Vertrauensmodell beinhaltet auch ein professionelles Gerätemanagement mit entsprechenden Autorisierungen und Authentifizierung aller Nutzer*innen.

Einen weiteren Schritt, den man für die IT-Sicherheit setzen sollte, ist eine Segmentierung des Netzwerks. Im Falle eines erfolgreichen Eindringlings kann so der sogenannte »Blast Radius« der betroffenen Systeme möglichst klein gehalten werden. Gerade in der Pandemie und bei den vielen Menschen im Homeoffice haben wir wieder gesehen, dass das klassische Modell der Perimeter-Sicherheit mit Firewall nicht ausreichend ist. Unternehmen benötigen darüber hinaus eine fortgeschrittenere Absicherung mit signaturbasierten Intrusion-Detection- (IDS) und Intrusion-Prevention-Systemen (IPS). Ein noch höherer Level wäre dann eine Unterstützung durch KI- und Machine-Learning-Systeme für Verhaltensanalysen und auch Visualisierungen von Bedrohungen. Gleichzeitig befürchte ich, dass die meisten Unternehmen mit dieser Fülle an Möglichkeiten und Themen in der Security überfordert sind. Diese haben in der Regel ja andere Geschäftsmodelle als den Betrieb von IT.

Report: IT-Sicherheit – ist das also etwas, das man auslagern sollte? Inwieweit ist das eine Frage der Unternehmensgröße?

Babajide: Es kann nicht die Hauptaufgabe eines Unternehmens sein, sich mit Security auseinander zu setzen und die Hälfte seines IT-Budgets dahingehend zu investieren. Große haben dieses Problem nicht so: Sie haben ihre eigenen Security-Operation-Center und prinzipiell auch die Ressourcen dazu. Beim Mittelstand und bei kleineren Unternehmen geht der Trend eher zur Auslagerung an Spezialisten. Diese betreiben dann

Die Diskutant*innen

- RONKE BABAJIDE ist als Lead Solution Engineer Security bei VMware für die Bereiche Network Detection and Response zuständig.
- NICOLAI CZINK ist Leiter Strategie und Transformation bei Bacher Systems. Er begleitet Unternehmen bei Sicherheitsfragen in hybriden IT-Infrastrukturen.
- HELMUT HÖDL ist Product and Technology Director bei NTS Netzwerk Telekom Service AG und hat den Aufbau des Geschäftsfeldes »Defense« mitgestaltet.
- JÜRGEN WEISS ist CEO und Gründer von ARES Cyber Intelligence und Sprecher der IT Security Experts Group der WKOÖ.
- MARIO ZIMMERMANN ist Country Manager Austria von Veeam Software und auf die Verfügbarkeit von IT und »Business Continuity« von Unternehmen spezialisiert.
- ANDREA KOLBERGER hat die Leitung der Stabsstelle Informationssicherheit und Datenschutz bei der Anton Bruckner Privatuniversität in Linz inne.

die Cybersicherheit für ihre Kunden. Es betreibt ja auch nicht jedes Unternehmen mit Fahrzeugen eine eigene Autowerkstätte.

Das Thema Sicherheit muss dennoch auch in der eigenen Organisation aktiv angesprochen werden. Ein wichtiger Punkt ist die Schulung der User. Regelmäßige Securitytrainings sollten ein fixer Bestand der Unternehmenssicherheit sein.

Ich bin überzeugt, dass wir nicht die kleineren Unternehmen mit diesen Herausforderungen allein lassen dürfen. Ich würde mir auch auf öffentlicher Seite Response-Teams oder ähnliche Ressourcen wünschen, die die Wirtschaft in Sicherheitsfragen unterstützen.

Report: Welche Herausforderungen sehen Sie bei Kunden bezüglich IT-Sicherheit?

Nicolai Czink, Bacher Systems: Unternehmen müssen oft erst ein Bewusstsein für die aktuelle Bedrohungslage entwickeln. Die Frage hier ist nicht, ob etwas passiert, sondern wann es passiert. Man braucht auch nicht zu glauben, dass man in einem für Angreifer uninteressanten Wirtschaftsbereich tätig sei. So ist bei den jüngsten Schadensfällen in Österreich plötzlich auch eine Molkerei angegriffen worden und deren komplette Lieferkette zum Stillstand gekommen.

Bewusstsein für die Gefahren bedeutet aber auch, den Faktor Mensch zu beachten, der ungewollt in den meisten Fällen die Schwachstelle ist, die die Angreifer ausnutzen.

Eine Basisabsicherung, von der Netzwerksegmentierung bis hin zum Endgerät, ist jedenfalls unbedingt erforderlich. Aufbauend auf den genutzten Services im Data Center und in der Cloud sind dann weitere Schutzmaßnahmen zu treffen, wie SaaS- und IaaS-Security bis hin zum »Cloud Security Posture Management«, das Transparenz in der Cloud schafft und Security-Policies einheitlich durchsetzt. Gut ein Drittel unserer 100 Mitarbeiter*innen sind in Sachen IT-Security bei den Unternehmenskunden tätig, um diese umfassend gegen Gefahren abzusichern. Dabei arbeiten wir unter anderem mit den Technologien von Check Point, weil sie keine Sicherheitskompromisse eingehen; so gewährleisten sie innovativ und nachhaltig einen umfassenden Schutz.

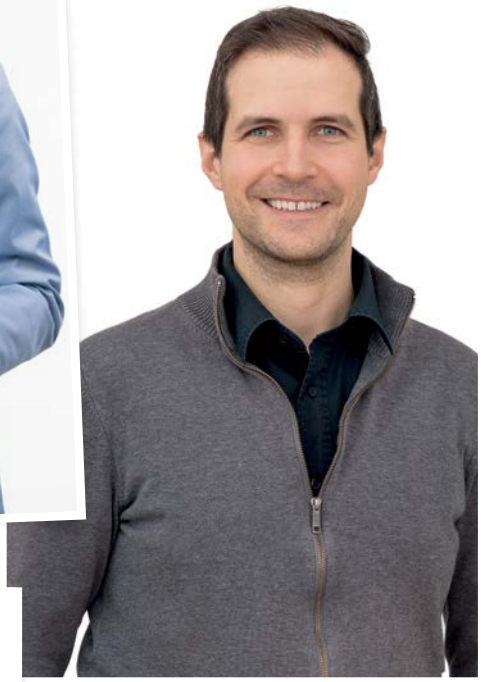
Neben der Absicherung vor möglichen Attacken, braucht es auch Vorkehrungen, wenn etwas passiert – mit einem »Security Information and Event Management«, über Detection-and-Response bis hin zu guten Backup- und Restore-Prozessen.

Auch muss man sich im Klaren sein, dass sich Angreifer ständig weiterentwickeln. Wir leben in einer agilen Welt, in der man mit Security-Maßnahmen nicht zu einem bestimmten Zeitpunkt fertig ist, sondern diese weitertreibt, verändert und ständig anpasst. Wir beschreiten mit unseren Kunden genau diesen Weg als Partner für sichere hybride Infrastrukturen.

Report: Was hat Covid hinsichtlich Cybersicherheit bedeutet?

Czink: Das verteilte Arbeiten – auch mit dem Arbeitsplatz zuhause – bedeutet das weitere Auflösen der alten Unternehmensgrenzen in der IT. Wir alle wollen Informationen und Anwendungen von überall zugänglich haben. Damit ist die IT zunehmend in der Cloud verteilt. Nun reicht es nicht mehr aus, einen hohen Zaun ums Haus zu bauen. Der neue Perimeter ist die Identität, deren Schutz nun im Vordergrund steht. Außerdem wird die Absicherung der Endgeräte mithilfe von neuen KI-basierten Technologien – Schlagwort EDR/XDR – besonders wichtig, um Gefahren zu erkennen und automatisiert darauf zu reagieren. ▶

Nicolai Czink, Bacher Systems (li.): »Bewusstsein für die aktuelle Bedrohungslage entwickeln.«



Helmut Hödl, NTS (re.): »Es geht immer darum, Angriffsflächen klein zu halten und zu dezimieren.«

Es stellt sich die Frage, ob kleinere Unternehmen ihre IT-Sicherheit selbst auf Dauer schaffen.

Report: Was darf denn IT-Sicherheit kosten? Welchen Anteil am IT-Budget würden Sie Unternehmen empfehlen?

Helmut Hödl, NTS: Eine generelle Empfehlung ist schwierig, da es immer vom Sicherheitsbewusstsein und den Anforderungen bei einem Unternehmen und der jeweiligen Industrie abhängt. Welche schutzwürdigen Daten habe ich? Wo sind sie gelagert? Wie sehen Unternehmensprozesse dazu aus? Das alles sind Basisfragen, bei denen es letztlich darum geht, Angriffsflächen klein zu halten und zu dezimieren.

Die Grundlage für IT-Sicherheit ist das Segmentieren, das saubere und gründliche Konfigurieren der Policies auf den Edge- und Data-Center-Firewalls, Investitionen in die Endpoint-Security. Ich sehe diese Aufgaben voranging, bevor man sich den großen Sicherheitssystemen, wie etwa einem »Security Information and Event Management« annimmt. Auch Vulnerability-Scans, um das Inventar in der IT zu erfassen und Schwachstellen zu erkennen, sind weitere mögliche Maßnahmen als Add-on. Prinzipiell aber sollten vorher die grundlegenden Dinge in der Netzwerk- und auch Perimeter-Firewall sauber erledigt werden.

Es stellt sich schon die Frage, ob das vor allem kleinere Unternehmen selbst auf Dauer schaffen. Schon allein das Consulting und eine Planung von solchen Infrastrukturen ist relativ komplex – von der Implementierung und dem laufenden Betrieb sprechen wir hier noch gar nicht. Wir unterstützen Unternehmen hierbei.

Report: Wie schaut der Arbeitsmarkt im Bereich Cybersicherheit aktuell aus? Haben wir genügend Fachleute in Österreich?

Hödl: Wir haben in unserem Defense-Team jene Analysten, die sich um Vorfälle kümmern, Situationen bewerten, Daten sicherstellen und auch den zeitlichen Ablauf von Attacken und den Malware-Befall prüfen. Doch allgemein haben wir derzeit definitiv zu wenige Expertinnen und Experten am Arbeitsmarkt. Ich denke, die FHs und Unis könnten zehnmal mehr Absolventinnen und Absolventen hervorbringen – die Unternehmen hätten dann wahrscheinlich gerade genug Personal im Bereich IT-Security. Dieser Mangel spricht für Partnerschaften mit Unternehmen, die diese personellen Ressourcen und die Expertisen als Kerngeschäft haben.

Wir bilden auch selbst aus und versuchen unseren Beitrag zu leisten. NTS hat sieben Standorte in Österreich, fünf Niederlassungen in Deutschland und eine in Südtirol. Es lohnt ein Blick auf die Job-Ecke auf unserer Website: Auch wir suchen und könnten vor allem im Securitybereich viele Leute einstellen.

Report: Welchen Zugang zum Thema Cybersecurity haben Sie bei ARES Cyber Intelligence? Was erleben Sie in der Praxis bei Unternehmen?

Jürgen Weiss, ARES Cyber Intelligence: Wir sind kein IT-Dienstleister, der Netzwerksicherheit und Firewalls betreibt, sondern auf Cybersecurity im IT-Umfeld und in der OT, der physischen Technik (Anm. »Operational Technology«), fokussiert. Bei den Herausforderungen im Social Engineering sollten wir nicht immer nur von externen Angreifern sprechen – eine unberechenbare Gefahr ist der »Insider Threat«. Bei großen Hacks von Ransomware-Gruppen wie LockBit wurden unter anderem IT-Administratoren für deren Zugangsdaten bezahlt. In solchen Fällen ist man als Unternehmen machtlos, selbst wenn man Unmengen in die IT-Sicherheit investiert hat.

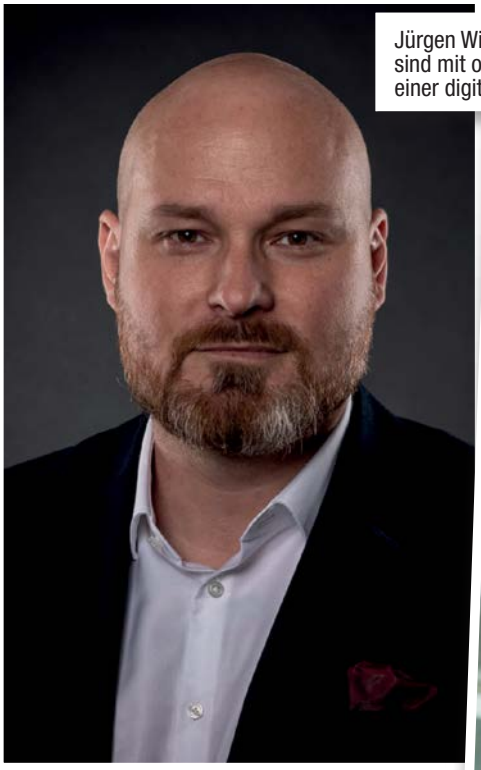
Viele Unternehmen agieren zum Teil grob fahrlässig und das betrifft nicht nur die Endkunden direkt. Wenn wir IT-Systeme prüfen, kann es schon vorkommen das wir bei IT-Dienstleistern sehen, dass diese einen dauerhaften VPN-Tunnel fürs Backup 24/7 zu ihren Kunden hin offen haben oder im schlimmsten Fall das gleiche Passwort für alle Admin-Accounts nutzen.

Alles up to date zu halten, immer auf dem neuesten Stand der Technik zu sein, ist heute die Aufgabe jeder IT-Mannschaft und auch jedes Geschäftsführers. Denn er kann dafür auch privat haftbar gemacht werden, abgesehen von rechtlichen Komponenten, die auch bei Cyberversicherungen schlagend werden.

Report: Sie haben als Sicherheitsdienstleister jüngst bei einer großen Ransomware-Attacke Unternehmen in Oberösterreich unterstützt. Was hat man aus diesen Vorfällen gelernt?

Weiss: Wir hatten Ende August an einem Samstag eine telefonische Anfrage eines Unternehmenskunden, der von der Ransomware-Gruppe BlackMatter attackiert worden war. Unser Krisenmanagement und Incident-Response-Team wurden alarmiert und wir mussten rasch alternative Kommunikationskanäle erstellen und uns ein Lagebild verschaffen. Unser Forensik-Team ist rund um die Uhr verfügbar. Das betroffene Unternehmen hätte ansonsten sehr rasch einen großen

Fotos: Georg Wilke, photoworkers



Jürgen Wiess, ARES: »Unternehmen sind mit organisierter Kriminalität, einer digitalen Mafia konfrontiert.«

Mario Zimmermann, Veeam: »Unternehmen müssen für den Fall des Falles vorsorgen.«

materiellen Schaden erlitten, da es aufgrund der Digitalisierung bereits sehr viel via IoT überwacht und monitort. Deshalb konnten wir im allerersten Schritt einen sehr großen Schaden minimieren, der für den Betroffenen eine Existenzbedrohung gewesen wäre.

Am Sonntag um neun Uhr früh kam dann die erste Ernüchterung, mit plötzlich 34 betroffenen Unternehmen. Hinsichtlich Ist-Analysen, Lagebild und Maßnahmenplänen ist das eine gewaltige Herausforderung, die wir in dieser Art auch noch nicht kannten. Zu diesem Zeitpunkt war es wichtig, den Betroffenen die notwendige Unterstützung zu bieten, aufzuklären und über weitere Schritte zu informieren.

Wir gehen im Krisenmanagement synchron mit verteilten Aufgaben in den Teams vor und gehen gleichzeitig in die Verhandlungsführung, um einfach einmal Zeit zu gewinnen. Die übliche Arbeitsweise ist, die Einsatzprotokolle auch mit den Behörden zu teilen, die bereits am Sonntag von uns direkt informiert wurden. Trotz einer Informationssperre, die mit allen Betroffenen abgestimmt war, dürften Informationen an Medien weitergegeben worden sein – die Betroffenen wurden plötzlich von Journalisten kontaktiert. Durch diesen Vertrauensverlust wurde dann unsere Verhandlungsführung zurückgeworfen, am 2. September ist dann die erste Morddrohung via verschlüsselter E-Mail gegen mich abgesetzt worden.

Das alles sind Dinge, die zeigen: Wir müssen uns in Österreich endlich bewusst werden, dass wir es nicht mit 17-jährigen Script-Kiddies zu tun haben. Hier ist die organisierte Kriminalität, eine digitale Mafia am Werk. Das ist kein Spaß mehr. Jeder, der hier meint, selbst das Problem lösen zu müssen, macht einen großen Fehler.

Den Betroffenen – unter anderem ein Kindergarten, mehrere Gesundheitseinrichtungen inklusive einem Blutlabor und einige Steuerberater – wurde mit der völligen Zerstörung ihrer Daten gedroht.

Report: Was kann man bei einer Ransomware-Attacke als Unternehmen noch tun? Gibt es andere Möglichkeiten, als auf die Lösegeldforderung einzugehen?

Weiss: Die gibt es definitiv. Das Schlüsselwort ist Backup, egal in welcher Variante. In diesem Fall war leider der IT-Dienstleister das Epizentrum des Angriffs, dies wurde durch diverse Schwachstellen der Hersteller begleitet. Wenn es dann keine aktuellen Backups gibt, die verwertbar sind, dann haben Betroffene die Wahl aus drei Möglichkeiten: Konkurs anmelden, die Daten zu entschlüsseln und wiederherzustellen oder Lösegeld zu bezahlen. Alle drei Varianten bedeuten zwischen sieben und 14 Tage Stillstand beziehungsweise Handlungsunfähigkeit. Denn selbst mit dem richtigen Schlüssel funktioniert ein Wiederherstellen von IT-Systemen nicht einfach auf Knopfdruck. Was diesen Unternehmen ebenfalls nicht erspart bleibt, ist das Aufsetzen einer neuen IT-Infrastruktur – man nimmt die alte, kompromittierte definitiv nicht mehr in Betrieb.

Letztlich hatte bei einigen auch Glück eine Rolle gespielt – man hatte selbst zusätzliche Backups gemacht oder wichtige Datensätze waren lokal auf einem Laptop gespeichert, die gerade nicht im Netzwerk gewesen sind. Heute, gut sechs Wochen nach dem Incident, konnten wir einen Großteil der Daten und IT-Systeme wiederherstellen.

Report: Wie viele der Kunden haben Lösegeld gezahlt?

Weiss: Kein einziger. Wir haben es hier mit kleineren und mittleren Unternehmen zu tun. Generell müssen die Faktoren »Cost of Deal« und »Cost of no Deal« abgewogen werden. Üblicherweise betragen die Forderungen den 52. Teil eines Jahresumsatzes – denn die IT steht auf jeden Fall eine Woche still.

Report: Allen Sicherheitsvorkehrungen zum Trotz – am Ende des Tages zählt offenbar vor allem, ob es in Unternehmen Backups gibt.

Mario Zimmermann, Veeam Software: Die Realität zeigt deutlich, dass Unternehmen für den Fall des Falles vorsorgen müssen. Wie ist man als Unternehmen auf Ausfälle vorbereitet und wie aktuell sind meine Backup- und Restore-Möglichkeiten? Auf welche Datenätze kann ich zurückgreifen und wie lange dauert es bis zur Wiederherstellung? Ich kann bestätigen, dass die meisten Unternehmen nicht die IT als Kernbusiness haben – aber alle sind auf IT angewiesen. Ohne IT und ohne Daten existieren Unternehmen heute nicht mehr. Die Abhängigkeit ist enorm und dadurch wird man angreifbar. Zudem werden die IT-Systeme immer komplexer, wenn Daten in ▶

Ohne IT und ohne Daten existieren Unternehmen heute nicht mehr – alle sind darauf angewiesen.

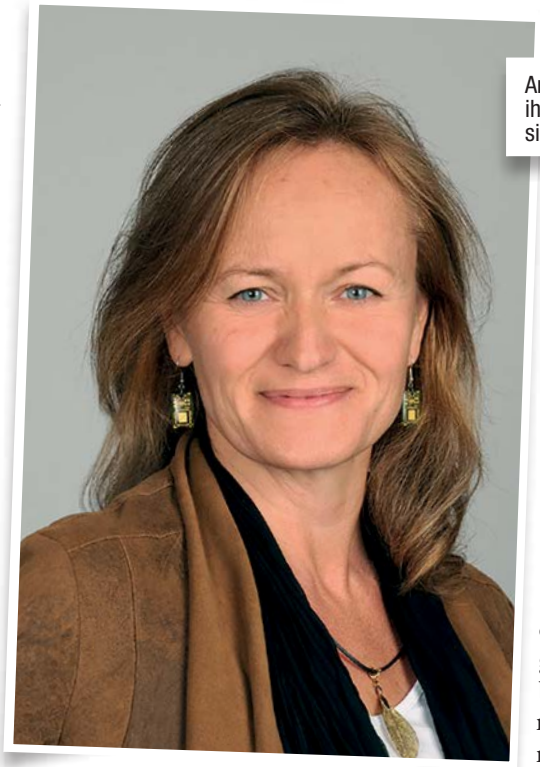
Fotos: Veeam, ARES

verschiedenen Cloudumgebungen gespeichert liegen und auch dort entsprechend gesichert werden.

Report: Welche Empfehlungen geben Sie Unternehmen hinsichtlich Sicherungen und Backups – insbesondere, wenn vielleicht sogar Eindringlinge bereits unbemerkt in einem Netzwerk sind?

Zimmermann: Je kürzer die Abstände der Backups, desto besser. Das Wissen um den Patient Null – wann ein Unternehmen infiltriert worden ist – ist auf jeden Fall wichtig. Ebenso sollte es auch Backups von Daten in der Cloud, etwa bei Microsoft 365, geben.

Meine Empfehlung: Überlegen Sie sich gut, von welchen Datenträgern Sie Sicherungen benötigen und führen Sie diese durch – und legen Sie am besten die Backups bei einem österreichischen IT-Anbieter ihres Vertrauens ab. Auf gehärteten Systemen in einem Rechenzentrum – »immutable« genannt – können Manipulationen durch Verschlüsselungen gar nicht greifen. So lässt sich sicherstellen, dass Sicherheitskopien sauber bleiben. Früher hatte man diese auch physisch getrennt auf Bandlaufwerken gespeichert. Heute ist das in der Cloud mit Technologien wie »S3 Object Lock« genauso möglich.



Andrea Kolberger: »Nutzer*innen mit ihrem Wissen dort abholen, wo sie sind.«

Der Mensch ist ein großer und wichtiger Baustein in der gesamten Security-Kette.

Am besten man hält sich in Sachen Backup an die 3-2-1-1-0-Regel: Es sollten 3 Kopien der Daten vorhanden sein, auf 2 verschiedenen Medien, mit 1 Kopie außerhalb des Standorts, mit 1 Kopie, die offline, air-gapped oder unveränderlich ist und es sollten 0 Fehler mit SureBackup-Wiederherstellungsüberprüfung vorliegen.

Aber Achtung, auch physische Desaster wie etwa ein Hochwasser oder Feuer können eine Gefahr für die IT und damit den Fortbestand von Unternehmen werden.

Report: Welche Herausforderungen sehen Sie bei der Umsetzung von Sicherheitsmaßnahmen im Alltag Ihrer Organisation?

Andrea Kolberger, Anton Bruckner Privatuniversität: Auch wenn wir die künstlerische und künstlerisch-pädagogische Ausbildung von Studierenden und Hochbegabten in den Bereichen Tanz, Musik und Schauspiel im Fokus haben, haben wir, so wie jede Organisation, IKT-Systeme für die Verwaltung und Lehre im Einsatz. Es gibt im Hochschulbereich zudem besondere gesetzliche Vorgaben, wie beispielsweise 80 Jahre Mindestaufbewahrungsdauer von Beurteilungen. Hier braucht es Überlegungen, wie in diesem Zeitraum die Informationssicherheit – insbesondere Verfügbarkeit, Integrität und Vertraulichkeit – gewährleistet werden kann.

Die Universitätsangehörigen sind technisch sehr unterschiedlich erfahren. Zum einen sind die Aufgaben in der Verwaltung mit anderen Organisationen vergleichbar, mit entsprechendem Wissen und Know-how bei den Nutzer*innen. Bei unseren Lehrenden liegt naturgemäß die Expertise in der bildenden, künstlerischen Exzellenz, mit unterschiedlich tiefgehendem technischem Know-how oder Zugang zur Informationssicherheit. Schließlich gibt es noch die große Gruppe der Studierenden, die unsere Infrastruktur nutzen und damit ein potenzielles Einfallstor bzw. einen Angriffsvektor auf die IT darstellen können.

Die Herausforderung ist in diesen durchaus konträr fokussierten Welten – Musik und darstellende Kunst einerseits und Security und Datenschutz andererseits – ein gegenseitiges Verständnis herbeizuführen. Auf welche Sicherheitsmerkmale sollte man im E-Mail-Verkehr achten und worauf sollte ich besser nicht klicken? An welchen Orten kann ich Daten dauerhaft sicher speichern? Wir haben die Herausforderung, unsere unterschiedlichen Zielgruppen passend anzusprechen und sie bei diesen Themen mitzunehmen. Meine Aufgabe ist es, Awareness-Programme, aber natürlich auch Richtlinien dazu entsprechend aufzubereiten und zu kommunizieren.

Neben all den technischen Vorkehrungen, ist der Mensch für mich nach wie vor ein sehr großer und wichtiger Baustein in der gesamten Security-Kette. Ich wünsche mir, dass unsere Nutzer*innen praktisch zur »Human Firewall« werden – allgemein gesellschaftlich betrachtet müssen Security und Datenschutz zu einer gewissen »Grundhygiene« werden, beginnend mit dem Sperren des Bildschirms beim Verlassen eines Raums oder der regelmäßigen Änderung von Passwörtern. Das sind völlig einfache Basisdinge, die dennoch im Gesamtgefüge der Informationssicherheit von Organisationen essenziell sind.

Für die Verwaltung heißt das zudem, einen Notfallplan mit Kontaktdaten zu Sicherheitsexpert*innen, IT-Dienstleister*innen, Forensik oder Behörden vorab auszuarbeiten – für den Fall, dass auch uns eine Attacke trifft. Auch wenn wir wahrscheinlich nicht vorrangiges Angriffsziel sind: ausschließen würde ich es unter keinen Umständen. ■

Eventvideo
youtu.be/Vmge23ULjGw

Fotos: Lackner-Strauss

Wie 5G die Netzwerksicherheit prägen wird

Angesichts der steigenden Zahl von IoT-Geräten, erhöhter Mobilität, Cloud-Implementierungen und einem immer größer werdenden Netzwerkrand müssen Sicherheit und Networking vereint werden, um gegen die Bedrohungslandschaft gewappnet zu bleiben.

Ein Kommentar von Michael Xie, Fortinet

»Funkstandard als Gamechanger für die Sicherheit«

Michael Xie
Founder
President und CTO,
Fortinet

Seit langem werden Unternehmen vor den Gefahren eines kleinteiligen Security-Ansatzes gewarnt, weil dadurch Sicherheitslücken entstehen können. Auch wurden nach dem Aufkommen von Covid-19 Arbeitsplätze nach nur wenig Vorlaufzeit auf eine Remote-Struktur umgestellt. Infolgedessen wurden Netzwerke, die sich ohnehin in einem bedenklichen Zustand befanden, in Größe und Umfang noch weiter ausgedehnt, um die Geschäftskontinuität aufrechtzuerhalten. Die entstandene Notwendigkeit einer sehr schnellen Expansion ließ viele Unternehmen die Sicherheit vernachlässigen. Mit dem Einzug des neuen Funkstandards 5G entstehen darüber hinaus zusätzliche Sicherheitsherausforderungen. Dabei sind sich viele nicht bewusst, wie unvorbereitet sie auf die weiteren Entwicklungen sind, die auf sie zukommen.

5G weist eine geringe Bandbreite auf und liegt in der Regel unter sechs Gigahertz. Dies steht in einem starken Gegensatz zu dem, was sich in der Praxis abzeichnet. Neue Smartphones können bereits 5G-Bandbreite mit Leistungsstufen von mehr als 24 Gigahertz nutzen. Dadurch werden sich die Anforderungen an die Netzwerkleistung am Edge sowohl für Geräte als auch für Anwendungen grundlegend ändern. Zusätzlich werden entsprechende Sicherheitsinfrastrukturen erforderlich, um das neue Leistungsniveau zu kontrollieren und zu verwalten.

Es wird bereits davon ausgegangen, dass das neue 5G sämtliche Bereiche von der Fertigung über Energienetze bis hin zu autonomen Fahrzeugen und Konsumgütern antreiben wird. Unternehmen, die sich nicht vorausschauend auf diese Umstellung vorbereiten, werden mit Latenzproblemen und stark beeinträchtigten Benutzererfahrungen konfrontiert werden und somit letztlich den Anschluss verlieren.

>> 5G-Security jetzt angehen <<

Die Anforderungen an Netzwerke, insbesondere am Netzwerk-Edge, werden erheblich steigen. Die erhöhte Komplexität führt dabei zeitgleich zu wachsenden Security-Anforderungen. Doch Sicherheit für das Netzwerk nur nachträglich zu ergänzen, kann zu Bottlenecks führen. Entscheidend ist das Finden eines Weges, der Netzwerkkapazitäten auf sichere Weise erhöht, ohne dabei die Benutzerfreundlichkeit zu beeinträchtigen.

Um die durch 5G entstehenden Herausforderungen zu meistern, stehen zwei Ansätze zur Diskussion. Der erste Ansatz besteht darin, Sicherheit auf der 5G-Netzwerkbetreiberebene zu implementieren. Der zweite konzentriert sich auf Edge-Security, da 5G am Netzwerkrand entweder als Backup-Verbindung oder zunehmend auch als primäre Verbindung genutzt wird. Unabhängig von der Herangehensweise wird der Edge-Bereich von KI gestützte sowie ASIC-beschleunigte (Anm. anwendungsspezifische integrierte Schaltung) Leistung erfordern.

Grundsätzlich wird der Cloud-Edge ein neues Level an hochoptimierter Sicherheit verlangen, selbst wenn 5G nicht als Priorität eingestuft wird. Komplexe hybride Netzwerke erstrecken sich inzwischen über eine Vielzahl von Clouds und Rechenzentren und erfordern zur Bewältigung dieser Belastung mehr virtuelle Geräte und Firewalls. Während 5G Transaktionen und Anwendungen beschleunigen wird, eröffnet es auch die Möglichkeit, schnellere Cyber-Attacken auszuführen. Ein ordnungsgemäßes Management erfordert dabei eine Einheitlichkeit der Sicherheitsrichtlinien und der Bereitstellungsstrategie.

>> Zeit zur Vorbereitung ist reif <<

Nun ist die Gewährleistung der Leistungs- und Sicherheitsanforderungen von 5G für jedes zukunftsfähige Unternehmen entscheidend. Viele Unternehmen sind derzeit nicht in der Lage, diese Voraussetzungen zu erfüllen. Hinzu kommt, dass aufgrund vorheriger Strategien mit Fokus auf Best-of-Breed-Geräte viele Unternehmen über ein veraltetes Security-Setup verfügen, das aus einem hochkomplexen Flickenteppich von zunehmend schwer zu verwaltenden Infrastrukturen besteht.

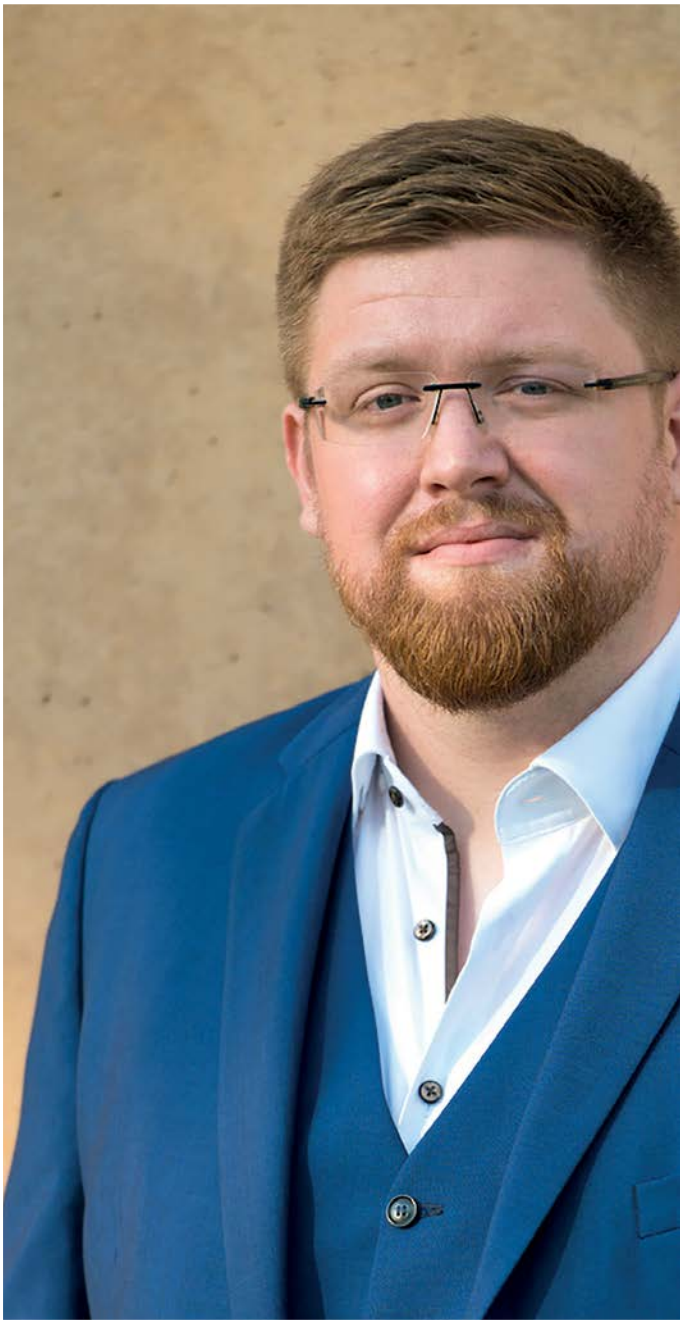
Für Unternehmen ist es jetzt an der Zeit, kohärente und umfassende Sicherheitsstrategien für 5G-Netzwerke umzusetzen. Dabei müssen sie schnell vorgehen, denn die Anforderungen einer Welt mit 5G werden stetig wachsen – und 6G ist weniger als ein Jahrzehnt entfernt. ■

Fotos: iStock, Fortinet

»Die Zahl der Vorfälle nimmt zu«

Niklas Keller, Head of Cyber Defense Center (CDC) und Teamleiter des neuen CDC-Teams im Bechtle IT-Systemhaus Österreich, über Geschäftsmodelle im Darknet, Engagement in der Sicherheit und die Notwendigkeit zur Automatisierung.

Von Martin Szelgrad



Niklas Keller ist IT-Sicherheitsexperte bei Bechtle und berät Unternehmen zu Cyberdefense-Strategien und Lösungen für die Absicherung von IT- und OT-Netzen.

Report: Welche aktuellen Herausforderungen sehen Sie im Bereich Cybersicherheit in Unternehmen?

Niklas Keller: Ransomware ist nach den jüngsten Attacken auf österreichische Unternehmen sicherlich das große Thema derzeit. Hier steckt ein klares Business-Modell dahinter. Ein Teil der Kriminellen hat sich auf das Programmieren und Bauen von Ransomware-Tools spezialisiert, während sich andere um den Vertrieb im Darknet kümmern. Wir sehen mittlerweile sogar Benchmark-Tests zur Vergleichbarkeit der verschiedenen Anbieter, die offenlegen, wie schnell eine Verschlüsselungssoftware arbeitet. Die Interessenten bekommen im Darknet eine bis ins kleinste Detail beschriebene, fixfertige Anleitung, die auch ohne technische Grundkenntnisse ausführbar ist. Sie liefert Hinweise, wie die Infrastruktur vorbereitet werden muss oder auch Tipps, wie Angreifer sich vor einer Verfolgung durch Behörden schützen können.

Report: Welche Angriffsmethoden sind da zu sehen?

Keller: Es werden sogenannte »Living off the Land«-Techniken eingesetzt, die vorhandene Schutzmaßnahmen umgehen und nicht als Gefahr erkannt werden. Angreifer nutzen Administratorbefehle, die über eine Powershell oder die Eingabeaufforderung CMD abgesetzt werden. Präventive Sicherheitslösungen, die mit Signaturen und Next-Generation-Technologien arbeiten, können das Ausführen solcher Kommandos nicht verhindern und greifen demnach nicht. Die einzigen Technologien, die aktuell für diese Art der Angriffe gerüstet sind, sind »Endpoint Detection and Response«-Lösungen.

Das Ziel der Angreifer ist in der Regel der Diebstahl von Identitäten. Wir kennen aber auch Vorfälle, denen kein initialer Hacker-Angriff vorausging, sondern ein verantwortlicher Administrator Zugangsdaten verkauft hat.

Report: Nun werden oftmals die einfacheren Nutzer*innen als schwächstes Glied in der Sicherheitskette betrachtet. Sind diese nicht eher kompromittierbar als die Kolleg*innen aus der IT?

Keller: Es gibt unterschiedliche Metho-

LIVING OFF THE LAND. »Von Angreifern werden Standardtools verwendet, mit denen Administratoren tagtäglich arbeiten.«

Foto: Bechtle

den, um in ein Unternehmen einzudringen. Die gängigste Praxis sind Phishing-Mails mit Links oder Attachements, die über eingebettete Scripts eine Schadsoftware aktivieren und einen Client infiltrieren. Der nächste Schritt ist das dauerhafte Einnisten im System und ein Ausforschen des jeweiligen Netzwerks. Die Angreifer sammeln Informationen und stellen dem Administrator mit einem eigens produzierten Fehler eine Falle. Mit einem Anruf beim Administrator gibt dieser dann seine Identitäten preis. Der Täter fängt sie ab, um sich damit selbst im Netzwerk zu bewegen.

Eine weitere, seit März bekannte Methode ist der Angriff auf Exchange Server durch den Hafnium-Exploit. Dabei werden Schwachstellen in lokal betriebenen und über das Internet erreichbaren Services aktiv ausgenutzt. Hafnium betraf Anfang des Jahres alle Unternehmen mit Exchange Servern. Microsoft reagierte mit einem Patch und unser Bechtle-Team empfahl ergänzend Verbesserungen der Architektur und realisierte diese auf Wunsch.

Wir gehen davon aus, dass es rund um Hafnium noch weitere Angriffe geben wird.

Report: Ist der Exchange Service damit weiterhin unsicher?

Keller: Nein, das ist er nicht. Vorsicht ist aber prinzipiell geboten. Software wird von Menschen entwickelt, Fehler und Schwachstellen sind also nicht grundsätzlich auszuschließen. Auch deshalb gibt es rund um Penetration Testing und Bug Bounty Hunting eine wachsende Community, die potenzielle Schwachstellen sucht und beheben will.

Wir empfehlen IT-Verantwortlichen in Unternehmen, sich nicht nur auf Patches und Bugfixes zu verlassen, sondern die gesamte Architektur im Blick zu haben. So können sie das Angriffspotenzial minimieren und mögliche Auswirkungen abschwächen.

Report: Welche Schwerpunkte setzen Sie im Cyber Defense Center bei Bechtle?

Keller: Mit unserem Cyber Defense Center verfolgen wir einen ganzheitlichen Ansatz: Prävention, Detektion und Reaktion. Dabei gibt es zwei Möglichkeiten zum Aufbau eines »Security Operation Centers«, kurz »SOC«. Der konventionelle Security-Incidence-and-Event-Management-Ansatz oder der Next-Generation-SOC-Ansatz, der mit einem sehr hohen Automatisierungsgrad bei der Analyse und der Fehlerbehebung arbeitet. Zusätzlich bieten wir passgenaue Managed Services an. Dazu zählen etwa »Endpoint Detection and Response«, »Network Detection and Response«,« Security Orchestration Automation and Response« und »Security Incidence and Event Management (SIEM)«.

Report: Was kann man sich unter dieser Automatisierung vorstellen?

Keller: Wir platzieren unsere Sensorik an signifikanten Punkten im Unternehmen, meist auf Endgeräten, aber auch im Netzwerk. Die gesammelten Informationen werden automatisiert mit Logikregeln ausgewertet. Je nach Bedrohung werden dann Gegenmaßnahmen eingeleitet. Auf Basis dieser Logiken können auch Verhalten beschrieben werden, um Living-off-the-Land-Techniken zu erkennen, die ansonsten durch das Sicherheitsnetzwerk rutschen würden.

Das ist ein Ansatz, der parallel zu herkömmlichen Maßnahmen und Technologien der Administratoren läuft, die weiter ihren eigentlichen Aufgaben nachgehen. Es bleibt festzuhalten, dass Security-Verantwortliche ohne Automatisierung schnell ans Limit des Machbaren kommen.

Report: Wie sieht es derzeit am Arbeitsmarkt in der IT-Sicherheit aus?

Keller: IT-Fachkräfte sind generell stark nachgefragt – auch im Bereich Security. Daher setzen wir verstärkt auf die Ausbildung eigener Fachleute. Das fängt bei unseren Lehrangeboten an und reicht bis hin zu dualen Studienmöglichkeiten. Aber auch mit Quereinsteiger*innen haben wir gute Erfahrungen gemacht. Bechtle bietet mit flexiblen Arbeitszeitmodellen sowie der Möglichkeit, auch aus dem Homeoffice zu arbeiten, ein attraktives Umfeld in einer zukunftsstarken Branche.

Report: Wie lange dauert die Ausbildung, bis Sie jemanden einsetzen können?

Keller: Wir rechnen hier Minimum mit sechs Monaten Einarbeitungszeit. Interessierten Kolleginnen und Kollegen bieten wir die Möglichkeit, dass sie sich über ergänzende Zertifizierungen schnell weiterentwickeln können.

Report: Steigen die Sicherheitsvorfälle in den Unternehmen – und auch die Awareness für Sicherheitsmaßnahmen?

Keller: Die Zahl der Vorfälle hat auf jeden Fall zugenommen. Unsere Kunden wissen, dass ihr Geschäftserfolg an einer funktionierenden IT hängt. Diese Erkenntnis wirkt sich auch positiv auf die Budgets für IT-Sicherheit aus.

Es ist im Prinzip wie bei einem Auto: Ich entscheide mich für ein bestimmtes Modell mit dem gewünschten Motor. Letztlich entscheiden danach aber regelmäßige Services und Inspektionen, ob, wie und wie lange das Auto läuft. ■

EINSATZ VON RESSOURCEN. »Auch bei einem Auto entscheide ich mich für ein bestimmtes Modell mit dem gewünschten Motor. Aber regelmäßige Services und Inspektionen entscheiden, ob, wie und wie lange das Auto läuft.«

kommentar

Data Breach – der Notfall im Datenschutz

Was ist ein Datenvorfall oder Data Breach? Welche Meldepflichten oder rechtliche Folgen daraus entstehen können, beantwortet in einem Kommentar Rechtsanwältin Katharina Bisset.

»Eine Meldung an die DSB muss bei einem Vorfall immer gemacht werden.«

Katharina Bisset
Rechtsanwältin und Co-Founder von Nerds of Law
Sie hat sich auf Gebiete mit technischem Hintergrund spezialisiert, wie IT-, E-Commerce, IP, Datenschutz- und Medienrecht.

Ein Datenvorfall liegt vor, wenn es ein Risiko für die (datenschutzrechtlichen) Rechte von Betroffenen gibt. Was bedeutet das? Daten werden von Unberechtigten erhalten, Daten werden gelöscht. Es kann aber auch der Verlust der Verfügbarkeit ein Datenvorfall sein. Klassische Beispiele können Ransomware-Attacken, Cyberangriffe, bei denen Daten abgegriffen werden, Verlust oder Diebstahl von unverschlüsselten Datenträgern sein, aber auch, wenn ein Newsletter mit sensiblen Inhalten an Empfänger in »An:« gesendet wird statt in »BCC:«.

>> Wer muss einen Datenvorfall melden? <<

Der datenschutzrechtlich Verantwortliche ist verpflichtet, Datenvorfälle zu melden. Bedient man sich Dienstleistern (Auftragsverarbeitern) und geschieht der Datenvorfall dort, muss der Dienstleister den Verantwortlichen Informieren.

>> Was muss an wen gemeldet werden? <<

Es gibt mehrere Meldepflichten – einerseits an die Datenschutzbehörde, andererseits an die Betroffenen, und falls man diese nicht herausfinden kann, kann man die Informationen über den Datenvorfall auch publizieren.

Die Meldung an die Datenschutzbehörde muss bei einem Datenvorfall immer gemacht werden, und dies binnen 72 Stunden ab Kenntnis des Datenvorfalls. Dadurch kann es gerade an Wochenenden zu einem großen Zeitdruck kommen.

An Betroffene muss man den Datenvorfall zusätzlich zur Datenschutzbehörde nur melden, wenn es zu einem hohen Risiko für die Rechte und Freiheiten der Betroffenen kommt. Wenn ein Datenvorfall überhaupt kein Risiko für Betroffene darstellt, und es keine Meldeverpflichtung gibt, muss dieser trotzdem dokumentiert werden.

Die Meldung muss unter anderem folgende Punkte beinhalten – ein Formular gibt es auch auf der Webseite der Datenschutzbehörde:

- Was ist passiert?
- Wer ist betroffen und wie hoch ist ungefähr die Anzahl der Betroffenen?
- Welche Datenkategorien sind betroffen?
- Wann war der Vorfall und wann wurde dieser bekannt?
- Was sind die wahrscheinlichen Folgen?
- Welche Maßnahmen wurden getroffen?

>> Was sind die Konsequenzen? <<

Bei Nicht- oder Spätmeldung eines Datenvorfalls kann es zu Strafen kommen. Darüber hinaus kann es auch zu einem amtswegigen Audit durch die Datenschutzbehörde kommen, insbesondere in Fällen, wenn der Datenvorfall ein Zeichen für größere strukturelle Probleme ist.

Im Idealfall stellt die Datenschutzbehörde das Verfahren ein, insbesondere wenn sie der Meinung ist, es liege kein Datenvorfall vor, oder die Auswirkungen vom Verantwortlichen angemessen behandelt und minimiert wurden.

>> Wie beugt man dem Datenvorfall vor? <<

Die wichtigsten Vorbeugemaßnahmen sind natürlich technischer Natur. Sichere Systeme, verschlüsselte Inhalte und geschulte Mitarbeiter*innen sind hier zentral. Es gibt aber auch einen starken rechtlich-organisatorischen Aspekt. Mitarbeiter*innen muss bewusst sein, dass alle Vorfälle gemeldet werden. Hierfür müssen Prozesse und allenfalls Notfallsnummern respektive E-Mail-Adressen im Unternehmen eingerichtet werden, um die Situation möglichst schnell beurteilen zu können.

Beispielsweise können technische Vorfälle an die IT gemeldet werden – es muss aber dort klar sein, ob etwas ein Datenvorfall sein kann, und wen man fragt. Gibt es Datenschutzbeauftragte, sind diese die zentrale Kommunikationsstelle. Je nach Größe des Unternehmens und des Vorfalls, kann der Datenvorfall-Notfallsplan bis hin zu einer Strategie für die Krisenkommunikation gehen.

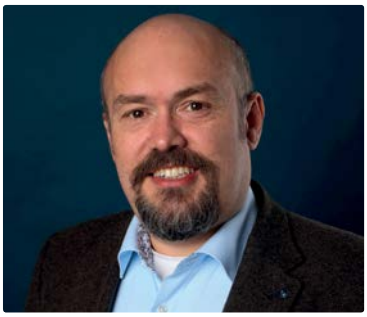
Die wichtigsten Punkte sind jedenfalls, dass die verantwortlichen Mitarbeiter*innen wissen, an wen sie sich wenden können – sowohl intern als auch extern. Weiters muss eine Analyse, ob ein Datenvorfall vorliegt, so schnell wie möglich geschehen. Und nicht zu vergessen: festgelegte Abläufe und Kommunikationsprozesse für den Datenvorfall. ■

Fotos: iStock, Wolfgang Lehner

»Schutz vor Cyberkrisen vordringlich«

Gerade jetzt, da noch immer viele Unternehmen keine sicheren IT-Konzepte für ihre Homeoffice-Lösungen eingeführt haben, besteht akuter Handlungsbedarf.

Ein Kommentar von Rüdiger Linhart, Wirtschaftskammer Wien



»Empfehle die Hotline 0800 888 133 für den Ernstfall.«

Rüdiger Linhart
Berufsgruppensprecher IT
Fachgruppe UBIT der Wirtschaftskammer Wien

Kurz vor der Bundestagswahl in Deutschland hat die EU schwere Vorwürfe gegen Russland erhoben: Mittels Cyberattacken würden Daten abgegriffen, um gezielt Falschinformationen zu streuen. Aber nicht nur auf staatlicher Ebene in Deutschland und um Falschinformationen zu verbreiten, auch in Österreich werden Cyberkriminelle immer umtriebiger – ob zuletzt in Salzburg, Oberösterreich oder auch Wien. Betroffen davon sind fast alle: Einrichtungen der öffentlichen Verwaltung, große und namhafte Betriebe, aber auch kleine und mittlere Unternehmen sowie Privatpersonen.

Besorgniserregend ist, dass die Anzahl und Intensität der Vorfälle kontinuierlich steigt, wie die Cyberkriminalitätsstatistik des BMI belegt: Alleine bei Angriffen im engeren Sinne, also auf Daten oder Computersysteme unter Verwendung der Informations- und Kommunikationstechnik, wurde gegenüber dem Vorjahr ein enormes Plus um fast 70 % mit 12.914 Deliktsfällen (2019: 7.622) verzeichnet. Fakt ist: Cyberkriminelle scheuen nicht mehr länger davor zurück, vor allem kleine und mittlere Unternehmen ins Visier zu nehmen.

>> Lösegeld erpressen <<

Worauf es die Kriminellen abgesehen haben? In erster Linie geht es nicht darum, Betriebsgeheimnisse zu stehlen oder Daten zu entwenden. Meist handelt es sich um ein »Flächenbombardement« mit dem Ziel, Unternehmen zur Kasse zu bitten. Im Austausch für durch Trojaner verschlüsselte Firmendaten wird Lösegeld, meist in der digitalen Währung Bitcoin, gefordert, um wieder Zugriff auf die eigenen Computersysteme zu erlangen. Allerdings nehmen die Cyberkriminellen dabei bewusst in Kauf, dass das betroffene Unternehmen wirtschaftlich ins Wanken gerät und es zu weiteren Kollateralschäden, etwa bei Lieferanten, kommt.

Wie sollten sich betroffene Unternehmen im Ernstfall verhalten? Der Aufforderung zur Zahlung von Lösegeld sollte üblicherweise nicht nachgekommen und die weitere Vorgehensweise mit Experten und nach eingehender Analyse abgestimmt werden. Denn es ist nicht auszuschließen, dass die Erpresser trotz Überweisung teilweise beträchtlicher Geldbeträge ihr Versprechen nicht einhalten und den Zugriff auf verschlüsselte Daten oder Computersysteme tatsächlich wiederherstellen. Zudem sollte jedweder Vorfall umgehend gemeldet werden. Das ist insbesondere deswegen vordringlich, um den Aktionsradius der Übeltäter einzuschränken und damit die entsprechenden Behörden oder Kontaktstellen aktiv werden und die Ermittlungen aufnehmen können.

>> Vorsorge ist besser als Nachsicht <<

In Österreich ist man mit Nachdruck bestrebt, das vernetzte Alarmsystem gegen Cyberangriffe und die Koordination auf operativer Ebene weiter zu verbessern. Wichtige Bausteine bei der Bekämpfung und zum Schutz vor Cyberbedrohungen sind insbesondere das nationale Cybersicherheitszentrum, das nationale Cyber Security Operation Center oder das Cyber Rapid Response Team. Um etwaigen Cyberkrisen besser vorzubeugen und das Zusammenspiel aller Einrichtungen weiter zu optimieren, steht aktuell ein neuer gesetzlicher Rahmen zur Diskussion.

Unmittelbar müssen Unternehmen und Organisationen jedoch vor allem selbst die Initiative ergreifen und den eigenen Sicherheitsstatus verbessern. Es gibt viele ausgezeichnete heimische Anbieter und Dienstleister, die beratend zur Seite stehen, um die IT-Infrastruktur möglichst sicher aufzusetzen. Gerade jetzt, da noch immer viele Unternehmen keine sicheren IT-Konzepte für ihre Homeoffice-Lösungen eingeführt haben, besteht akuter Handlungsbedarf. Tritt ein Ernstfall ein, dann bietet die Wirtschaftskammer Wien mit der kostenlosen Cybersecurity-Hotline für Unternehmer eine verlässliche Anlaufstelle: Die Hotline ist unter 0800 888 133 erreichbar – 24 Stunden am Tag, sieben Tage die Woche. ■

Fotos: iStock, Ruediger Linhart

»Allzu einfach darf man es Angreifern nicht machen«

Johanna Ullrich ist Forscherin bei SBA Research und hat sich das Ziel gesetzt, physische Systeme zu sichern und Konzepte aus dem Ingenieurwesen mit jenen aus der IT-Security zu verbinden.

Von Martin Szelgrad

Report: Was sind Ihre Forschungsbereiche bei SBA Research?

Johanna Ullrich: Auch wenn ich eine HTL für Informationstechnologie besucht habe, war es dann eher untypisch für den Bereich Security, dass ich nicht Informatik oder Mathematik studiert habe, sondern Elektrotechnik. Über verschiedene Wege habe ich dann SBA Research kennengelernt und hier Praktika gemacht. 2013 war mir mit meinem elektrotechnischen Wissen dann schon klar, dass die Verbindung aus IT und physischen Systemen zu einem Pferdefuß wird. Damals hatte man begonnen, sich vermehrt mit Themen wie Fernwartung, die ja auch sehr praktisch ist, zu beschäftigen.

In der IT haben wir es innerhalb von mehreren Jahrzehnten geschafft, IT-Systeme halbwegs sicher zu machen. Die Systeme werden von Informatiker*innen gebaut und auch von Informatiker*innen abgesichert. In dieser Berufsgruppe spricht man die gleiche Sprache. Wenn aber Anlagen von Expert*innen aus der Elektrotechnik, Verfahrenstechnik und aus dem Maschinenbau geplant und gebaut werden, wird oft nicht erkannt, welche Einfallstore mit den Verbindungen nach außen geöffnet werden.

Heute sieht man, wie die Vernetzung der physikalischen Infrastruktur – Stromnetze, Fahrzeuge, Medizintechnik und Produktionsanlagen – zu Problemen führt. Auf einmal sehen wir dort Angreifer, die wir auch in der IT kennen. Mit einem großen Unterschied: Wenn eine Bank oder eine Versicherung angegriffen wird, ist Geld weg. Das ist unangenehm, aber es geht um keine körperlichen Verletzungen oder gar

Zu Person und Unternehmen

■ JOHANNA ULLRICH ist »Key Researcher« beim COMET-Zentrum SBA Research in Wien. Sie leitet die Forschungsgruppe »Networks and Critical Infrastructures Security« und wurde bereits mehrfach ausgezeichnet, darunter mit der Promotio Sub Auspiciis Praesidentis und dem Forschungspreis der Dr. Maria Schaumayer Stiftung.

■ SBA RESEARCH ist mit mehr als 100 Mitarbeiter*innen das größte Forschungszentrum Österreichs, das sich exklusiv mit Informationssicherheit beschäftigt. Neben Forschungsaktivitäten unterstützt SBA Research Unternehmen mit Cybersecurity-Trainings, bei der Planung und Durchführung von Penetration-Tests, dem Umsetzen von Datenschutz-Managementsystem und auch bei der Softwaresicherheit in der Entwicklung.

Menschenleben. In der Industrie dagegen können Sicherheitsvorfälle Maschinen zerstören und Menschen gefährden. Ich möchte mit meiner Forschung erreichen, dass eine Brücke geschlagen wird und die verschiedenen Fachdisziplinen zusammenkommen. So sollen Geräte und Anlagen sicherer werden.

Report: Wo steht die Industrie derzeit, was die Sicherheit ihrer Systeme betrifft?

Ullrich: Es wird graduell besser, man hat aber auch sehr unterschiedliche Herausforderungen – angefangen bei einer im Vergleich zur IT sehr langen Lebensdauer von physischen Artefakten. Handys und Laptops sind zwei bis vier Jahre in Gebrauch, ein Auto vielleicht zehn bis 15 Jahre, ein Flugzeug 30 Jahre, im Stromnetz reden wir schon von 50 bis 60 Jahren Lebensdauer oder noch mehr. Wenn dann die Security laufend Updates benötigt, klaffen diese Welten auseinander.

Dann haben wir eine Herausforderung zwischen Safety und Security. Beim Bau eines Flugzeugs oder eines Zugs wird mit Zertifikaten sichergestellt, dass durch den Gebrauch und Betrieb keine Menschen gefährdet sind. Wenn nun permanent Updates eingespielt werden, ändert das diese Systeme – und eine neue Zertifizierung müsste her. Das ist aber kaum durchführbar, denn sie sind aufwändig, teuer und personalintensiv. Hier sehe ich noch keine Lösung, wie etwa einen Stand der Technik. Der herkömmlichen IT gleich, werden auch in physischen Systemen Maßnahmen, beispielsweise zu Perimeter-Sicherheit gesetzt – aber eine durchgehende Verknüpfung ist eine der offenen Forschungsfragen.

Report: Könnte man der Komplexität von langlebigen Systemen hinsichtlich Sicherheitszertifizierung nicht auf einer abstrakteren Ebene – mit Modellen – begegnen?

Ullrich: Diese Idee gibt es schon, ebenso wie die Trennung in einen inneren, zertifizierten Systemkern und außen leichter änderbare Teile. Eine weitere Herausforderung ist – und das sehen wir in der Forschung aktuell in den Stromnetzen – die Angreifbarkeit von Infrastruktur über smarte, vernetzte Geräte. Ein Hersteller eines smarten Kühlschranks hat nicht unmittelbar die Motivation, sein Produkt zu sichern. Der Stromnetzbetreiber wiederum hat keine Möglichkeit auf die Technik im Haushalt zuzugreifen.

Report: Wenn wir von der Sicherheit von Geräten im Smart Home sprechen – hier braucht es wohl eine systemübergreifende Zusammenarbeit von Herstellern? Was steht dem im Weg?

Ullrich: IoT-Devices sollen möglichst wenig kosten. Jeder Cent Einsparung in der Herstellung ist ein Erfolg. Da bleibt Security natürlich auf der Strecke. Security hat den Sexappeal einer Versicherung: möglichst wenig Kosten oder Aufwand und man ist froh, wenn man sie nicht braucht.

Report: Gibt es in dieser Betrachtung und auch beim Wissen um die Gefahren eine Trennung in Business- und in Consumer-Welt?

Ullrich: Die Business-Welt nimmt das natürlich ernster, aber im Prinzip sitzen wir alle in einem Boot. Für ein Stromnetz werden unsichere Consumer-Geräte zum Problem, wenn diese in Summe ein gewisses Potenzial an Last haben. Wenn das in einer Attacke erreicht wird, kommt es zu Störungen bis zum Ausfall des Netzes – Stichwort Blackout.

Der einzelne Kühlschrank wird keinen Schaden anrichten können. Wenn aber viele andere Haushalte das gleiche Gerät besitzen, kann ein Hack schwerwiegende Folgen haben. Wir brauchen Security auf allen Leveln – auf Seite der Hersteller ebenso wie bei den Nutzer*innen, die etwa sichere Passwörter setzen. Dazu braucht es auch Regulatorien sowie Sanktionen, wenn hier etwas missachtet wird.

Auch wenn es Techniker*innen nicht gerne hören: Sicherheit ist nicht nur etwas Technisches, sondern vor allem auch etwas Organisatorisches. Viele aus der Technik finden Sicherheitsthemen in den Medien zum Beispiel auch gar nicht so spannend, weil die realen Angriffe meistens nicht ausgeklügelt sind und über einfache Wege erfolgen. Man ist dann vielleicht auch sehr tief in der Materie drinnen und sorgt für komplexe Angriffsvektoren vor, während es eigentlich ganz wo anders hapert – und dort die einfachsten Dinge nicht beachtet werden.

Report: An welchen konkreten Projekten für die Industriesicherheit arbeiten Sie bei SBA Research?

Ullrich: Ein Projekt im Automotive-Bereich hatte Sensoren in Prüfständen zum Thema, die drahtlos betrieben werden sollten – die Verkabelung des Prüflings sollte aus Effizienzgründen gespart werden. Autohersteller sind bei der Abhörsicherheit von Funkverbindungen aber sehr sensibel – die Konkurrenz könnte Daten stehlen oder auch manipulieren. Wir haben mit einem Protokoll einer anderen Universität gearbeitet und einen Beitrag geleistet, um die Prüfstände sicherer zu machen und Sicherheitsfeatures zu implementieren.

Aber eigentlich ist ein nachträgliches Sichern nicht der optimale Ansatz. Besser wäre, die Sicherheit gleich von Anfang an mitzudenken. Ein »Security by Design« ist immer effizienter, schlanker und dadurch auch weniger fehleranfällig oder liefert weniger Angriffsfläche. Ich gehen davon aus, dass es langfristig auch günstiger ist.

> DER EINZELNE **KÜHLSCHRANK WIRD KEINEN** SCHADEN ANRICHTEN KÖNNEN. WENN ABER VIELE HAUSHALTE DAS GLEICHE GERÄT BESITZEN, KANN EIN HACK SCHWERWIEGENDE FOLGEN HABEN.

Report: Wie sollten Bestandssysteme abgesichert werden, die nicht nach dem Prinzip »Security by Design« gebaut worden sind?

Ullrich: Bis man etwas Sinnvolleres findet, sollte man diese Systeme abkapseln und möglichst gut vor Angreifern verstecken – bis man sie durch bessere Systeme möglichst ablöst. Aber im Prinzip gilt das auch für die IT, in der man Netzwerke und Geräte trotz Sicherheitsfeatures an Bord auch mit einer Firewall und verschiedenen Intrusion-Detection-Lösungen schützt. In der Industrie mit teilweise noch offeneren Systemen brauchen wir dringend mehrere »Lines of Defence«.

Allzu einfach darf man es Angreifern nicht machen. Es ist wie bei Fahrradschlössern. Das absolut sichere Schloss gibt es nicht. Aber Sie gewinnen viel, wenn Sie den Aufwand des Knackens mit zum Beispiel mehreren Schlössern erhöhen. Auch in der IT-Sicherheit gibt es eine Ökonomie bei Angriffen: Wenn zu viel Zeit, Computing-Ressourcen und Aufwand im Vergleich zum erwarteten Ergebnis gebraucht wird, wird es uninteressant. Unternehmen müssen ihr Risiko bewerten und entscheiden, welchen Sicherheitsaufwand sie betreiben wollen. ■

Foto: SBA Reserch

Weiblicher Fingerprint in der IKT

Von Karin Legat

Vielfalt und Chancengleichheit stellen einen wichtigen Anker der modernen Unternehmensstrategie dar. In der Informations- und Kommunikationstechnik (IKT) hat sich das noch nicht flächendeckend durchgesetzt. Die letzten beiden Jahre haben allerdings positive Veränderungen für Frauen am IT-Arbeitsmarkt gebracht.

Fotos: iStock, T-Systems

Für Nicole Berlakovich ist der Aufbau von Frauennetzwerken innerhalb des Unternehmens entscheidend. »T-Systems hat dazu zwei Programme: FEM-T ist eine Plattform von Frauen im Berufsleben, die Diversity-Strategy ist eine Kampagne zur Realisierung von mehr Vielfalt, nicht nur bei Gender.« Eine große Hilfe sieht Berlakovich, die an der FH Wirtschaftsrecht studiert hat, einige Jahre in der Personalberatung tätig war und seit 2018 als HR Business Partnerin fungiert, in der Präsenz von Frauen in leitenden Funktionen. »Sie leben vor, dass die Karriere im technischen Bereich für Frauen möglich ist und stärken das Selbstbewusstsein der nachfolgenden Generationen.« Mit Gertrud Hierzer als Mitglied der Geschäftsführung setzt T-Systems diesen Wunsch um.

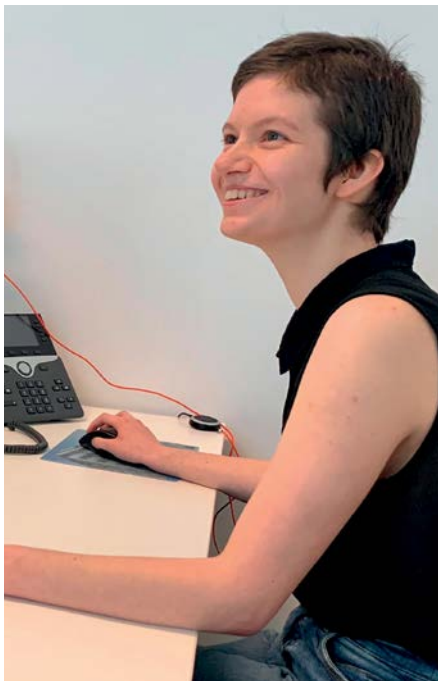
Der Anteil von Frauen in spezifischen IKT-Berufen liegt unter zehn Prozent.

IKT besteht nicht nur aus Programmieren, sie bietet vielseitige und kreative Jobs«, stellt Christine Wahlmüller-Schiller, Initiatorin und Mitbegründerin von WOMENinICT, fest. »Ich bin seit mehr als 20 Jahren in der Informations- und Kommunikationstechnologie tätig. Vielfach wird sie nur mit Mathematik verbunden, IKT erfordert aber vor allem logisches Denken, das können Mädchen ebenso wie Burschen.« Sie umfasst die Kommunikation über die Problemlösung und Weiterentwicklung bestehender Technologien und gerade hier beweisen Frauen ihre Stärke.

»Sie haben mehr soziale Kompetenzen, können besser auf die jeweiligen Gesprächspartner eingehen«, meint Wilfried Seyruck, Geschäftsführer der Programmierfabrik und Präsident der Österreichischen Computer Gesellschaft.

Für Katharina Bechtloff, HR-Managerin im Bechtle IT-Systemhaus Österreich, braucht es vor allem Wissen über technische Berufe. »Wir haben die Erfahrung gemacht, dass sich mehr Frauen für eine Karriere in der Technik entscheiden, wenn sie eine genaue Vorstellung davon haben, wie technische Berufe konkret ausgestaltet sind.« Bechtle unterstützt daher Initiativen wie den Töchtertag, berufspraktische Tage für Schülerinnen und begleitet Technikerinnen bei Berufsorientierungsevents.

Auch Wahlmüller-Schiller fordert mehr Engagement in der frühen Bildungsphase. Es müsse bereits in der Volksschule gestartet, Lehrerinnen für die IKT begeistert werden. Der Bildungsfokus ist eine der zentralen Forderungen von WOMENinICT. In einer Umfrage hat sich die Mehrheit der Befragten dafür ausgesprochen, dass Schülerinnen wie Schüler zumindest ein bis zwei Jahre verpflichtend programmieren lernen sollen. Gleichzeitig wird eine spielerische Vermittlung von informatischem Grundwissen, »Computational Thinking«, schon für die Volksschule vorgeschlagen. Mädchen müssen bereits mit 12 bis 13 Jahren für die IKT gewonnen werden, denn in diesem Alter fallen wesentliche Schritte der Weiterbildung und damit der künftigen Karriere. Ausprobieren muss die Devise sein. Events wie »Girls TECH UP« zeigen Einblicke in die Branche, es wird gebastelt, inspiriert und ausprobiert.



Marlene Thallinger ist ein Trainee der ersten Stunde in der Programmierfabrik mit Sitz in Oberösterreich.

>> Frau an der Spitze <<

»Frauen sind bereit für die IKT«, kommt eine klare Aussage von Wilfried Seyruck.

Mankos in der IKT

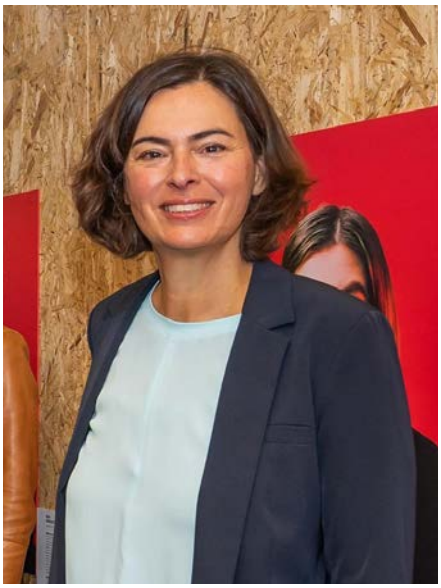
Der Grund für den geringen Frauenanteil in IKT-Berufen wird oft zurückgeführt auf

- fehlende Frühförderung in der Schule
- negative Einstellung im sozialen Umfeld gegenüber Frauen in der Technik
- fehlende Gleichstellung in den Unternehmen (Gender-Pay-Gap und Übergehung bei Beförderungen)
- Mangel an weiblichen Rolemodels in IKT-Berufen.

Um weibliche Fachkräfte zu gewinnen, braucht es laut Katharina Bechtloff attraktive Angebote wie flexible Arbeitszeiten, Homeoffice-Möglichkeiten, Programme für Wiedereinsteigerinnen oder die Möglichkeit zum dualen Studium. »So haben wir bei Bechtle den Frauenanteil seit 2018 mehr als verdoppelt«, betont sie und berichtet von guten Erfahrungen mit Quereinsteigerinnen. Gerade für diese Menschen sei Weiterbildung entscheidend – die Bechtle Akademie hilft. Erfolgreich laufen auch Mentoring-Programme. »Immer mehr Technikerinnen stehen selbst als Mentorinnen neuen Teammitgliedern zur Seite«, berichtet Bechtloff, die selbst nach einem BWL-Studium an der WU Wien und Auslandssemestern in Großbritannien und den USA seit 2019 als HR-Managerin im Bechtle IT-Systemhaus Österreich arbeitet, sich der Aus- und Weiterbildung des Mitarbeiter*innenstabs widmet sowie Berufspraktika von Schüler*innen aus HTLs, Fachhochschulen und Universitäten ermöglicht.

Für die Förderung von Chancengleichheit und Diversität sind Frauen an der Unternehmensspitze hilfreich.

In seinem eigenen Unternehmen, der Programmierfabrik, liegt der Frauenanteil in der Technik bereits bei 40 %. »Wir sind erfolgreich beim Akquirieren von Frauen, weil gut die Hälfte der Teamleiter weiblich ist.« Besonders in diesen Teams gebe es Soft Skills, die Männer nicht so mitbringen.



Silvia Angelo, ÖBB Infrastruktur: »Große Chance für mehr Frauen in der IKT.«

>> ÖBB Infrastruktur <<

Die Kampagne #joboffenSIEve ist einer von mehreren Schritten der ÖBB zur Förderung von Frauen. Deutlich sichtbar war sie durch die Baustellengalerie mit fotokünstlerischen Porträts von Technikerinnen bei der Haltestelle Wien Matzleinsdorfer Platz. In persönlichen Steckbriefen erzählten die Protagonistinnen von ihrem Werdegang, ihrer Motivation, in ehemals männlich dominierten Berufen Fuß zu fassen, und welche Vorbilder auf dem Weg zum Traumjob geholfen haben.

Silvia Angelo, Vorständin ÖBB Infrastruktur, sieht eine große Chance für mehr Frauen in der IKT in der zunehmenden Digitalisierung. Innerhalb der letzten Jahre wurden die Lehrberufe E-Commerce-Kauffrau/-mann und Applikationsentwicklung und Coding etabliert. Die Ausbildungszentren der ÖBB wurden mit 3D-Druck- und VR-Technologie aufgerüstet.

»Die Berufsanforderungen ändern sich und wir können immer vielfältigere Jobs anbieten, die auch für Frauen attraktiv sind«, betont Angelo. Vielfalt bildet bei den ÖBB ein Leitmotiv. Noch liegt der Anteil der weiblichen Beschäftigten bei zehn Prozent, bis 2026 soll er auf 17 Prozent steigen. Dazu gibt es eine »Diversity Charta«. Im Fokus

Christine Wahlmüller-Schiller, VÖSI: »Haltung gegenüber Frauen in der IKT ist mittlerweile offener.«

Medien- und Technikexpertin

■ DER WEG VON CHRISTINE WAHLMÜLLER-SCHILLER in die IKT ist außergewöhnlich. »Ich habe Publizistik, Spanisch, Geschichte und Internationale BWL an der Universität Wien und der London School of Media studiert. Mein Wunsch war, Wissenschafts- oder Auslandsjournalistin zu werden.« Durch den engen Kontakt zu IKT-Kunden in einer PR-Agentur hat sie sich dann autodidaktisch das notwendige Technikwissen angeeignet. Mittlerweile ist Wahlmüller-Schiller mehr als 20 Jahre in der IKT-Branche tätig. »Die Haltung gegenüber Frauen in der IKT ist heute offener, aber nicht selbstverständlich.« Im Februar 2020 hat sie mit anderen Frauen WOMENinICT als Initiative und Netzwerk im Verband Österreichischer Software Industrie (VÖSI) gestartet.

Fotos: Bechtle, ÖBB/Michael Fritscher, timeline/Rudi Handl

Duale Akademie

TRAINEE-PROGRAMM
ca. 70 % der Ausbildung

- Ausbildungsvertrag und Vollzeitanstellung bei Duale-Akademie-Partnerunternehmen
- Trainee-Programm in verschiedenen Unternehmensbereichen
- Mentor*in als Ansprechpartner*in in der Ausbildung & Fachexpert*in bei der Erstellung des Zukunftsprojekts
- Betriebsspezifisch werden zusätzlich modernste Ergänzungen und Vertiefungen organisiert

FACHTHEORIE
ca. 20 % der Ausbildung

- Vermittlung der Fachtheorie durch Duale-Akademie-Kompetenzzentren in den Berufsschulen
- Ausgewählte Module in englischer Sprache – in Kooperation mit der Fachhochschule Oberösterreich

ZUKUNFTSKOMPETENZEN
ca. 10 % der Ausbildung

SOZIAL- UND SELBSTKOMPETENZ
Teammanagement, Kommunikation & Präsentationstechniken, Zielorientierung & Kontrolle, Zeitmanagement & Arbeitsorganisation, Kund*innenorientierung & Qualitätsmanagement, Leadership-Management

INNOVATIONS- UND DIGITALE KOMPETENZ
ECDL-eLearning-Module, Office Refreshing, IT-Security, Social Media & Digitalisierung

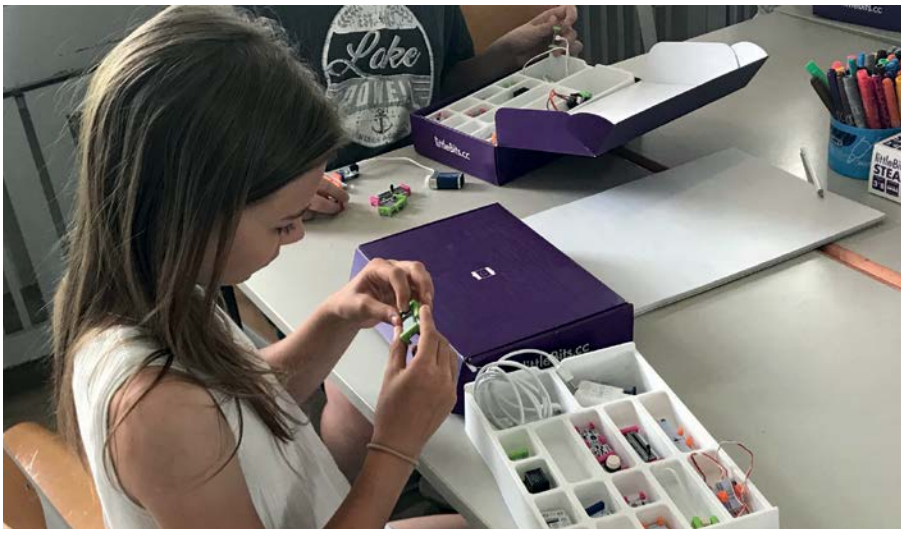
INTERNATIONALE KOMPETENZ
Cambridge-Business-English, Intercultural Competence, Auslandspraktikum

Die WK Oberösterreich hat 2018 die Duale Akademie als betriebsnahe Alternative zum Studium konzipiert. »Die Hälfte der Studierenden schließen ihr Studium nicht ab. Im MINT-Bereich ist es noch gravierender«, erklärt WKOÖ-Präsidentin Doris Hummer. Die Teilnehmer*innen erhalten 70 % der Ausbildung im Betrieb, 20 % in der Berufsschule und 10 % Zukunftskompetenzen bei Bildungspartnern der dualen Akademie, wie dem WIFI oder Fachhochschulen. Auch ein Auslandsaufenthalt ist vorgesehen. Das Konzept wird im Herbst 2022 mit vier Berufsbildern auf ganz Österreich ausgedehnt: Mechatronik, Applikationsentwicklung/Coding, Elektrotechnik und Speditionskaufmann/-frau. IT-Systemtechnik startet später.

steht der Frauenanteil bei Neuaufnahmen, der Lehrlingsausbildung sowie bei Weiterbildungsprogrammen, der Nachbesetzung von Führungspositionen und in Aufsichtsräten. Mit der ÖBB-Gleichstellungspolicy 2011 wird dem Anspruch von Vereinbarkeit von Beruf und Privatleben entsprochen, Aufklärung bietet die Kampagne #joboffenSIEve. Daneben setzen die ÖBB auf Maßnahmen wie Karriereworkshops, Netzwerkveranstaltungen bis hin zu Weiterbildungsangeboten im Bereich »Gender and Diversity Management« und Cross-Mentoring-Programme.

>> Ausbildung gegen Mangel <<

»Der Fachkräftemangel ist unsere größte Wachstumsbremse, daher nutzen wir die Duale Akademie, um selbst einen Teil der benötigten Fachkräfte auszubilden«, erklärt Programmierfabrik-Geschäftsführer Seyruck. AHS-Absolvent*innen, an die sich das Angebot der Dualen Akademie vor allem richtet, sind bestens geeignet für eine IT-Ausbildung, weil sie gute Englischkenntnisse mitbringen und in der Lage sind, rasch Wissen zu akquirieren. Mittlerweile arbeiten acht Trainees im Unternehmen. ■



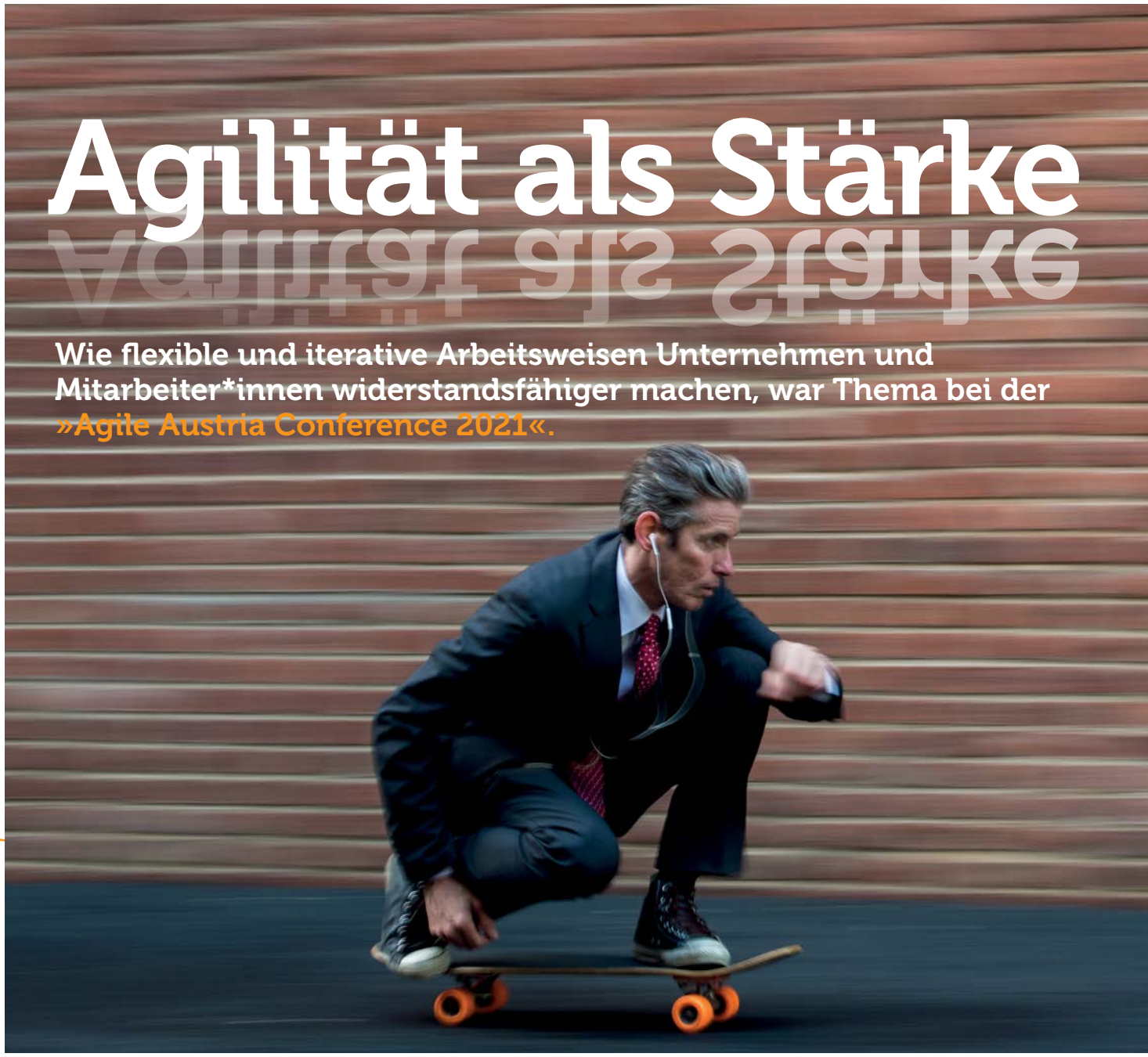
IKT wird in den Schulen noch viel zu wenig vermittelt. Jedes Kind, egal ob Bub oder Mädchen, sollte in der Schule IKT-Fähigkeiten erwerben. Hilfreich wären eigene Mädchengruppen im IKT-Unterricht, denn rein unter Mädchen traut sich jede Einzelne mehr.

Initiativen für ein Plus an Frauen in der IT

■ PROJEKTE ZUR STÄRKUNG der technischen Interessen und Fähigkeiten bei jungen Frauen und Mädchen gibt es bereits einige, darunter Kompass, FiT, Girl's Day, LET'S TECH, meine TECHNIK, zimd, MiT, Mit Mut, OVE fem, Women in Technology, Re-Ment, Roberta und Sprungbrett. »Praxisnahe Einblicke können viel dazu beitragen, dass mehr Schülerinnen die Technik als spannendes Berufsfeld für sich entdecken. Vor allem dann, wenn es gelingt, ihnen die Vorteile einer solchen Berufswahl näherzubringen und ihre Neugierde geweckt wird«, beurteilt Katharina Bechtloff den Girl's Day. Die ÖBB sind auch mit Unternehmensbesuchen im Rahmen des Töchtertags oder der Kooperation mit dem Österreichischen Frauenlauf aktiv.

Agilität als Stärke

Wie flexible und iterative Arbeitsweisen Unternehmen und Mitarbeiter*innen widerstandsfähiger machen, war Thema bei der »Agile Austria Conference 2021«.



Sohrab Salimi, *Gründer und CEO Scrum Academy*

Report: Vor welchen Herausforderungen stehen Unternehmen hinsichtlich Führung und Arbeitsweisen in den kommenden Jahren?

Sohrab Salimi: Wenn ich Führungskräften die Frage stelle, ob sie ihre Teams systematisch führen und entwickeln, bekomme ich in aller Regel ein »Nein« als Antwort. Auf die Folgefrage, welche Modelle sie nutzen, kommt in der Regel nur »Teambuilding«.

Warum sind so wenige Führungskräfte bis hin zu Topmanager*innen nicht in der Lage, Teams, die den Grundstein für jeden Erfolg bilden, systematisch zu entwickeln? Die meisten kleinen und mittelständischen Unternehmen haben keinerlei Weiterbildungsprogramme für Führungskräfte. Die großen Unternehmen verfügen zwar über solche Programme, diese sind aber in aller Regel so altmodisch, dass man sie am besten komplett ignoriert. Und selbst wenn Unternehmen vernünftige Leadership-Programme haben, werden die Erkenntnisse aus diesen Programmen kaum umgesetzt. Zwar durchlaufen Unternehmen häufig Jahr für Jahr irgendwelche Change-Initiativen, jedoch verlaufen die meisten dieser Veränderungen im Sand. Häufig geht es bei Change-Projekten auch nur darum, versteckt Mitarbeiter*innen zu entlassen und vor allem ältere Mitarbeiter*innen loszuwerden.

Den Topmanager*innen, die sich selbst häufig als Macher*innen inszenieren, fehlt es in aller Regel an Mut und Durchsetzungsfähigkeit. Es ist erschreckend, wie wenige Aufsichtsrät*innen – mit Ausnahmen der Betriebsrät*innen – und Führungskräfte eine Verantwortung gegenüber den Mitarbeiter*innen empfinden. Sofern wir Wohlstand für die künftigen Generationen sichern und ausbauen möchten, braucht es vor allem ein Umdenken im Hinblick auf Führung. Dieses Umdenken – ähnlich groß wie die Kopernikanische Wende – bedeutet vor allem, dass sich Unternehmen für alle

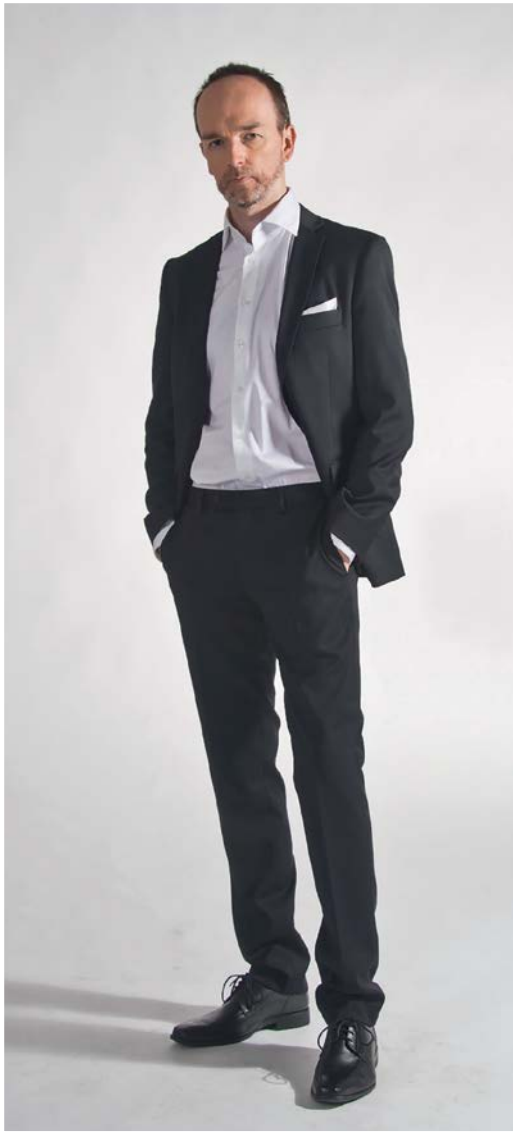
Bereits die Events 2017, 2018 und 2019 waren ein überwältigender Erfolg und lockten mehr als 250 nationale sowie internationale Besucher*innen nach Graz. Nach der Covid-bedingten Absage 2020 fand die »Agile Austria Conference 2021« nun Mitte Oktober in Form einer Onlinekonferenz statt. Neben den Keynote-Sprechern Sigi Kaltenecker und Sohrab Salimi wurde zahlreichen Vertreter*innen von österreichischen und internationalen Unternehmen wie Raiffeisen, Dynatrace, Erste Bank, willhaben, Magenta Telekom oder Österreichische Post eine Bühne geboten. Sie stellten das Thema Agilität unter vielseitigen Gesichtspunkten in ihren Organisationen vor. Der Reinerlös der Konferenz in einer Höhe von 8000 Euro ist der Schülerwohngruppe Graz von SOS Kinderdorf zugutegekommen.

Wir haben Organisatoren und Sprecher der »Agile Austria Conference 2021« zu ihrer Einschätzung der Chancen und Herausforderungen rund um das Thema Agilität befragt – und warum agile Organisationen resilienter bei Marktveränderungen sind.

Wolfgang Richter,
Agile CEO JIPP.IT

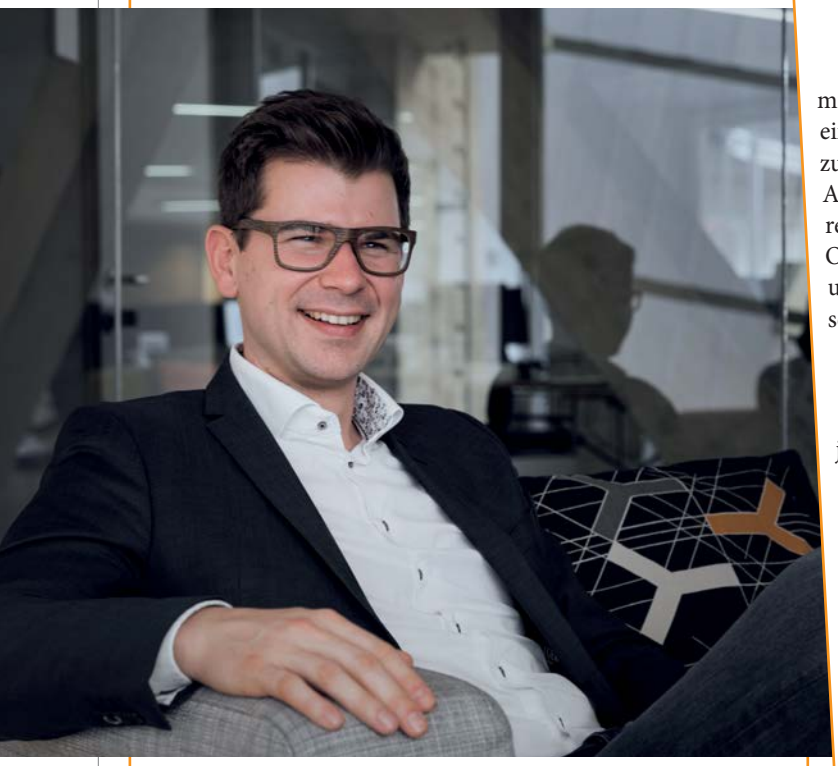
Report: Warum sehen Sie Agilität als Stärke?

Wolfgang Richter: Unsere Welt und damit der Markt verändert sich immer schneller. Unternehmen aus allen Branchen verpassen viele Gelegenheiten, unter anderem weil Unsicherheiten und eine Vielzahl an Optionen Schockstarre auslösen können. Agilität ist für mich die Fähigkeit, auf Veränderungen zeitnah reagieren zu können, und der Mut zu reagieren, um das Beste aus einer Situation herausholen zu können. Dadurch ist langfristiger Erfolg möglich.



Stakeholder und nicht nur für die Shareholder verantwortlich fühlen. Wir müssen auch wieder mehr Innovation in den Vordergrund stellen.

Dieser Wandel wird uns alle – jedes Unternehmen und jede Person – Kraft, Zeit und Ressourcen kosten. Die daraus resultierende Veränderung kann dann aber nicht ohne Weiteres von Wettbewerbern kopiert werden. Daher bin ich überzeugt, dass diese Herausforderung für Unternehmen auch die größte Chance für nachhaltiges Wachstum und Erfolg aller Stakeholder sein kann. Man muss diese Chance nur ergreifen.



Christoph Platzer,
CEO von Parkside Interactive

Report: Was macht eine agile Organisation aus?

Christoph Platzer: Agilität ist etwas Lebendiges, Dynamisches – das sind gelebte Werte und Prinzipien innerhalb einer Gruppe. Eine Organisation muss nicht in allen Teilen zu 100 Prozent agil sein, um als agil zu gelten. Der Grad der Agilität sollte dabei so gewählt werden, dass er für die Erreichung der Ziele der Gruppe ideal ist. Genauso wie eine Organisation nicht gleich agil ist, weil sie agile Prozesse und Praktiken einsetzt. Agile Prozesse sollten nur die Konsequenz einer intrinsischen Agilität sein.

Report: Warum sehen Sie Agilität als Stärke?

Platzer: Als Dienstleister mit unterschiedlichsten Projekten und Kund*innen können wir uns durch die agile Arbeitsweise bestmöglich auf den Kunden einstellen. Gleichzeitig stellt agiles Arbeiten einen Rahmen dar, innerhalb dessen wir uns gemeinsam mit dem Kunden bewegen können. Das schafft Sicherheit und klare Erwartungen an die Zusammenarbeit und legt somit den Grundstein für erfolgreiche Projekte.

Report: Warum und wie können aus Ihrer Sicht flexible und iterative Arbeitsweisen mein Unternehmen und die Mitarbeiter*innen widerstandsfähiger machen?

Platzer: Iteratives Vorgehen allein macht die Mitarbeiter*innen noch nicht per se widerstandsfähiger. Unserer Erfahrung nach nimmt diese Vorgangsweise aber Stress und Druck aus den Projekten und entlastet so die Mitarbeiter*innen: Indem die einzelnen Iterationen entsprechend geplant sind, dass sowohl das Sprint-Ziel als auch das Gesamtziel des Projekts erreicht werden können.

Report: Vor welchen Herausforderungen stehen Unternehmen hinsichtlich Führung und Arbeitsweisen in den kommenden Jahren?

Platzer: Für Unternehmen, die bisher klassisch geführt wurden und eine agile Transformation anstreben, wird es darum gehen, ein neues Verständnis von Führung in allen Ebenen zu etablieren. Prinzipien wie verteilte Führung werden so auf das Unternehmen anzupassen sein, dass durch diese mehr Klarheit bezüglich Verantwortungen von einzelnen Rollen entsteht. Gleichzeitig müssen Themen wie Selbstverantwortung und Selbstorganisation im Unternehmen gelernt werden, damit die entsprechenden Mitarbeiter*innen eigenständig Entscheidungen für ihre Teams treffen können. Das braucht explizite Unterstützung und auch eine aktive Fehlerkultur.

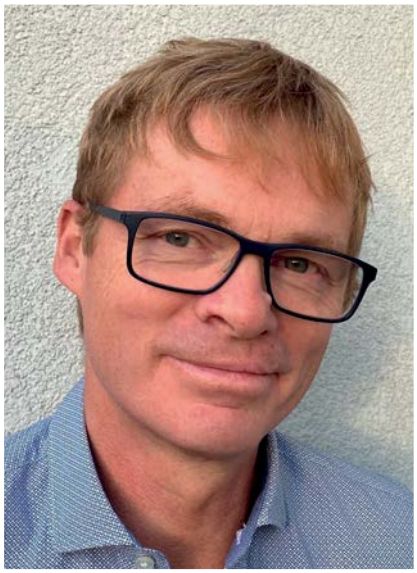
Report: Wo kann eine agile Vorgehensweise beim Finden von Innovationen unterstützen?

Platzer: Agil meint in diesem Zusammenhang vor allem das Fail-Fast-Prinzip, bei dem sich viele der agilen Werte und Prinzipien widerspiegeln. Dabei geht es darum, schnell und effizient ein gewisses Ziel zu erreichen. Innovationen haben ebenfalls immer etwas mit einem mehr oder weniger hohen Grad an Ungewissheit, mit hoher Geschwindigkeit, Anpassungsfähigkeit und Wettbewerb zu tun. Für solche Voraussetzungen ist eine agile Vorgehensweise prädestiniert.

Sigi Kaltenecker,
Managing Director Loop Organisationsberatung

Report: Was assoziieren Sie mit dem Schlagwort Agilität?

Sigi Kaltenecker: Spontan geantwortet bedeutet Agilität, besonders beweglich zu sein. Agile Organisationen sind fähig, schnell auf veränderte Anforderungen zu reagieren und neue Angebote rasch umzusetzen. Ich sehe agile Organisationen in einem Wettbewerbsvorteil – auch, weil dadurch attraktivere Arbeitsbedingungen für Mitarbeiter*innen entstehen können. Prinzipiell ist dadurch Unternehmen eine höhere Anpassungs- und Veränderungskompetenz gegeben – was ich gerade während Covid beobachtet habe.



Report: Wo kann eine agile Vorgangsweise beim Finden von Innovationen unterstützen?

Kaltenecker: Eine Unterstützung sehe ich durch den kreativen Freiraum, der durch die Selbstorganisation innerhalb bewegungsfreundlicher Rahmenbedingungen geboten wird – etwa bei einer Verteilung von Entscheidungsautorität. Ein weiterer positiver Effekt entsteht durch die Fähigkeit, Innovationen rasch umsetzen zu können – Stichwort »Lean Startup« und »Minimal Viable Product«.

Fotos: BearingPoint, Loop, Parkside Interactive, Apus

Gerhard Hammer, *CEO von APUS Software*

Report: Was bedeutet für Sie eine agile Organisation?

Gerhard Hammer: Mit Agilität verbinden wir schnelle, flexible Adaption an neue und sich ständig ändernde Anforderungen – an uns und an unsere Kund*innen. Eine agile Organisation lässt von ihrer Struktur her diese Adaption zu und fördert sie. Im Fall von APUS zeigt sich das beispielsweise in einer flachen Hierarchie, einer guten Fehlerkultur und dem Bewusstsein, dass eine agile Organisation ständig lernt und sich weiterentwickelt. Sie ist fest verankert und gleichzeitig flexibel. Dadurch kann sie mit Störimpulsen gut umgehen, sich selbst wieder aufrichten und gestärkt weitermachen.

Report: Warum und wie können aus Ihrer Sicht iterative Arbeitsweisen Unternehmen widerstandsfähiger machen?

Hammer: Iterative Arbeitsweisen ermöglichen, Fehler früh zu erkennen und diese Erkenntnisse unmittelbar in die nächsten Schritte einfließen zu lassen. Dadurch wird in jedem Iterationsschritt das Ergebnis besser – besonders auch qualitativ. Das allein bringt schon eine gewisse Widerstandsfähigkeit mit sich. Fehler bringen uns nicht aus der Ruhe, sondern sind Möglichkeiten, zu lernen und nachhaltig Verbesserungen zu schaffen.

Durch Flexibilität gelingt es uns, mit Hindernissen und Störungen im Projektverlauf oder im Unternehmensalltag besser umzugehen. Wir überprüfen Planungen ständig und passen sie an, lassen neue Marktgegebenheiten in unsere strategischen Überlegungen miteinfließen. Die Teamverantwortung wird jeden einzelnen Tag gestärkt. Unsere Mitarbeiter*innen sollen nicht alleine große Last auf ihren Schultern tragen – durch die Verteilung von Kenntnissen und Wissen wachsen wir gemeinsam.

Report: Welche Herausforderungen sehen Sie für Unternehmen?

Hammer: Mit dem Klimawandel und den in dessen Fahrwasser gewachsenen sozialen Krisen werden nur jene Unternehmen überleben, die widerstandsfähig sind. Diese bestehen aber aus ihren Mitgliedern und allen ihren Stakeholder*innen – sowie deren Beziehungen. Agile Vorgehensweisen stärken diese Beziehungen nachhaltig. Das ist nicht Freunderlwirtschaft und Postenschacher, sondern rücksichtsvolles und wahrhaft nachhaltiges Beziehungs- und Projektmanagement.

Andreas Mitter, Partner,
Head of Agile Advisory BearingPoint

Report: Wofür steht eine agile Organisation für Sie?

Andreas Mitter: Agilität heißt für uns Wandelbarkeit: Wir möchten auf Veränderungen für unsere Mitarbeiter*innen und Kund*innen reagieren können. Eine agile Organisation beobachtet, lernt und adaptiert auch ohne große bürokratische Hemmnisse.

Report: Sie sehen Agilität ebenfalls als Stärke?

Mitter: Agilität stärkt vor allem die Menschen in einer Organisation. Oftmals wird Agilität mit dem Einsatz von Methoden und Rahmenwerken wie Scrum oder Kanban gleichgesetzt, aber es geht viel mehr um das Zusammenarbeiten von Menschen an einer konkreten Vision und einem gemeinsamen »Purpose«.

Durch das Fördern und Fordern von Fähigkeiten und die Ermöglichung, Prozesse und Produkte mitzugestalten, erleben wir sehr oft, dass die individuellen Stärken von Personen in Teams zu einer gesamtheitlichen Stärke der Organisation werden. Es gibt keine pauschale Antwort, wieso Agilität gleichzusetzen ist mit Stärke, aber durch die Werte und Prinzipien stärkt Agilität den Weg hin zu einer menschenzentrierteren Organisation, die durch die individuellen Stärken der Menschen innerhalb dieser einzigartig wird.

Report: Vor welchen Herausforderungen stehen Unternehmen hinsichtlich Führung und Arbeitsweisen in den kommenden Jahren?

Mitter: Das Führungsverhalten muss empathischer, offener und transparenter werden. Es muss zu einer Führungskultur kommen, die es als Stärke sieht, nicht alles Wissen im Management zu vereinen. Weniger »Command and Control«, mehr »Trust and Value«. Auch jüngere Menschen wollen Flexibilität, mehr Menschlichkeit, eine sinnvolle Arbeit und die Freiheit, mitgestalten zu können. Lange Planungsvorhaben und risikoscheue Entwicklung werden dazu führen, dass bestehende Marktführer von kleineren, flexibleren und agileren Unternehmen vom Podest vertrieben werden.

Report: Wo kann eine agile Vorgangsweise beim Finden von Innovationen unterstützen?

Mitter: Agile Arbeitsweisen lassen mehr kreativen Freiraum zu, in dem man empathisch und neugierig auf die Bedürfnisse von Menschen eingehen kann. Oft wird Innovation als etwas Brandneues missverstanden. Letztlich ist Innovation das Produkt von Gelegenheit und Notwendigkeit – und wenn man in kleineren iterativen Zyklen arbeitet, dann ist es viel leichter, diese Gelegenheiten auch zu erkennen. Organisationen sind gut beraten, ihren Mitarbeiter*innen entsprechende Frei- und Gestaltungsräume einzuräumen, ansonsten kann Innovation nicht stattfinden. Man sollte künftig mehr Wert darauf legen, zuerst Prototypen statt fertige Produkte zu entwickeln und diese danach sehr eng mit dem Kunden weiterzuentwickeln.

Kostentreiber bei der ERP-Einführung:

Vorsicht Falle!

Bei der Wahl eines ERP-Anbieters spielen die Kosten eine wesentliche Rolle – sowohl in der Projektphase als auch für den laufenden Betrieb. Denn hier lauern einige Kostenfallen – und das hat oft gar nicht so viel mit der Funktionalität an sich zu tun. Der Software-Hersteller proALPHA hat einige »Klassiker« gesammelt und erklärt, wie sie sich umgehen lassen.

>> Prototyp schlägt Wasserfall <<

Schon die Projektmethodik hat ihre Tücken. Beim klassischen Wasserfall-Projektansatz aus Anforderungsdefinition, Entwurf und Implementierung bekommen User erst relativ spät das von ihnen am grünen Tisch spezifizierte System live zu sehen. Statt langer Konzeptionsphasen sollten Unternehmen daher auf das viel schnellere Prototypen-Verfahren setzen. So sehen die Anwender*innen schon früh, wie ihre zukünftige Arbeitsumgebung aussehen wird. Fehler lassen sich früher aufspüren, Änderungswünsche schneller berücksichtigen.

>> Auf Integrität achten <<

Idealtypische Abläufe sind von Anfang bis Ende bereits durchdacht und anhand von »Process Templates« vorgezeichnet. So fokussiert sich das Projektteam auf das Wesentliche, nämlich die Abweichungen vom Standard. Die Implementierung kommt dadurch schneller voran. Im Idealfall stellt der ERP-Anbieter auch schon für jeden Prozess durchgängig digitale Lösungen bereit, so dass keine weitere Software nötig ist. Das spart auch Lizenzkosten für Drittsoftware.

>> Flexibel bleiben, ohne die Software zu verbiegen <<

Heute führt der Weg zum maßgeschneiderten System nicht mehr durch das lange, tiefe Tal des »Customizing«. ERP-Systeme, die schon im Standard viele branchenspezifische Extras mitbringen und zudem umfassende Konfigurationsmöglichkeiten bieten, machen Sonderprogrammierungen weitgehend überflüssig. Deshalb ist ein Anbieter, der sich auf einige Kernbranchen fokussiert und diese Funktionalität richtig gut abdeckt, besser als ein Softwarehersteller, der alles so ein bisschen kann. Hier schlägt klar der Spezialist den Generalisten.

>> Integration: einen Bus nutzen <<

Es beginnt ganz harmlos mit dem Satz: Diese Software binden wir einfach an, da programmieren wir schnell eine Schnittstelle. Die bitteren Konsequenzen dieses Vorgehens zeigen sich oft erst Jahre später: Niemand kennt sich mehr mit den vielen Sonderlocken aus. Änderungen werden zum russischen Roulette. Spätestens wenn es darum geht, mehrere Systeme, IoT-Geräte oder Anwendungen ans ERP-System anzudocken, lohnt sich eine Middleware mit einem Enterprise Service Bus. Einmal aufgesetzt, lassen sich weitere Systeme schneller und einfacher anbinden. Die so standardisierten Schnittstellen reduzieren nicht nur die Abhängigkeit von einzelnen Dienstleistern. Weil der Automatisierungsgrad steigt, sinken zudem die Prozesskosten.

>> Aufwand nicht unterschätzen <<

Überspannen Prozesse mehrere Geschäftsbereiche, Länder oder Tochterunternehmen wird es schnell knifflig. Unterschiedliche Vorschriften und Währungen machen Intercompany-Prozesse zu einer besonderen Herausforderung. Das kann zu hohen Anpassungskosten führen – oder einem Wildwuchs unterschiedlicher ERP-Systeme je Land. Diese schmerzliche Erfahrung lässt sich vermeiden, wenn Mittelständler bereits bei der Ausschreibung darauf achten, dass die ERP-Software die nötigen Landesversionen mitbringt.

>> Mit Modulen wachsen <<

Das Gros der ERP-Verantwortlichen verbindet monolithische Warenwirtschaftssysteme vor allem mit einem Wort: teuer. Modulare Systeme bieten dagegen den großen Vorteil, dass nur für die genutzte Funktionalität Kosten anfallen. Und dennoch dürfen sich die Unternehmen sicher sein: Der Hersteller investiert in die Entwicklung des Gesamtsystems. Wollen sie später weitere Module ergänzen, steht ihnen eine Software auf dem letzten Stand zur Verfügung.

>> Möglichst viel selber machen <<

Low Code, besser noch No Code, sind die Buzzwords der Stunde. Formulare designen, Auswertungen individualisieren, Intercompany-Prozesse einrichten, Stammdaten replizieren – all das ist heute mit wenig bis gar keinem Entwicklungsaufwand machbar. Umfassenden Konfigurationsmöglichkeiten sei Dank. Natürlich ist »Do it yourself« nicht jedermanns Geschmack, viele übergeben diese Arbeiten lieber einem Consultant. Aber wer selbst Hand anlegen will, sollte es können.

>> Beraterleistung: Vor-Ort-Zeiten reduzieren <<

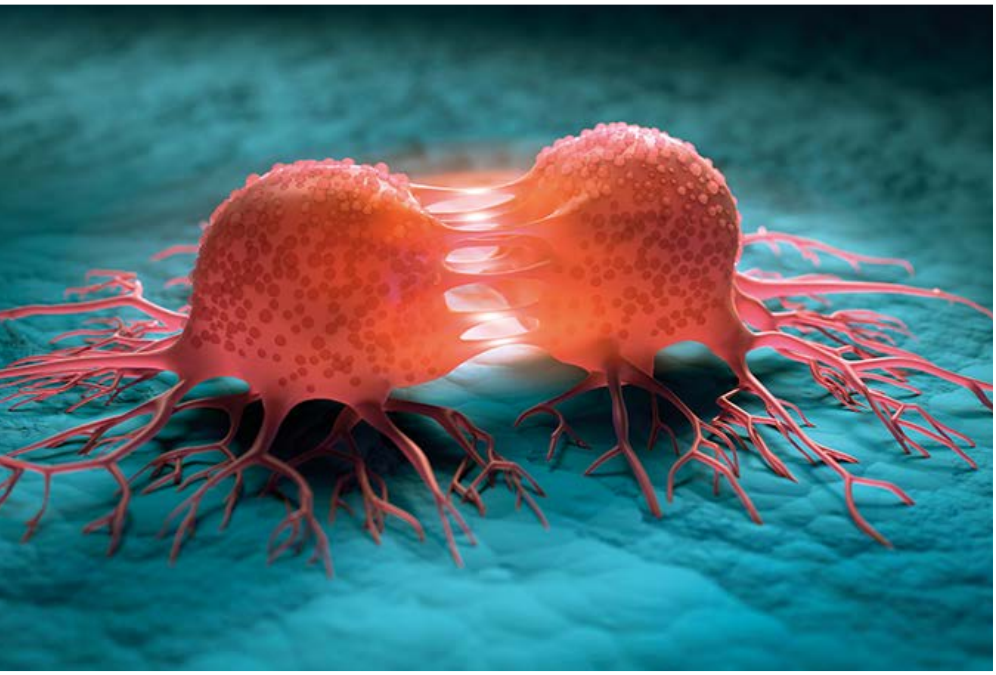
Früher musste für jede Kleinigkeit, jede Anpassung ein*e Berater*in vor Ort kommen. Hatte der ERP-Hersteller gerade einen Personalengpass, konnte das schon mal Tage oder Wochen dauern. Heute lässt sich via Remote-Zugriff bereits einiges aus der Distanz übernehmen. Das spart Reisekosten. proALPHA etwa hat sich etwas Neues einfallen lassen: Remote Consulting. Statt auf den Beraterbesuch vor Ort zu warten, erhalten Anwender*innen schnelle und professionelle Hilfe zu Fragen und Aufgaben ihres Tagesgeschäfts – sei es in Form von fest definierten Paketen oder individueller Unterstützung. ■

Fotos: iStock

Forschungsschiene Biomed-Technik

Vor 50 Jahren fand Österreichs Biomedizinische Technik ihren Anfang an der Technischen Universität in Graz und legte den Grundstein für eine erfolgreiche Forschungsgeschichte.

Von Karin Legat



Mit dem ersten Krebszellmodell konnten Forschende der TU Graz ein essentielles Werkzeug für die moderne Krebsforschung und Medikamentenentwicklung auf den Weg bringen.

Erstmals ist es gelungen, einen robotischen Arm rein durch Gedanken in Echtzeit zu steuern.

Als Wahlfach im Bereich Elektrotechnik startete 1970 eines der erfolgreichsten Lehr- und Forschungsgebiete der TU Graz: die Biomedizinische Technik. Die Arbeitsgruppe BCI-Forschung – eine Teildisziplin der biomedizinischen Technik – rund um Gernot Müller-Putz zählt heute zu den führenden europäischen Forschungsgruppen auf dem Gebiet der computergestützten Interpretation von Hirnströmen und ihrer Übersetzung in elektronische Impulse für Prothesen, Roboterarme und Kommunikationsprogramme. Neue Anwendungen der biomedizinischen Technik entwickelt auch der Fachbereich Biomedical Engineering Building.

>> BCI-Forschung <<

Der Mensch denkt, die Maschine lenkt. So lässt sich stark vereinfacht das Prinzip des »Brain Computer Interface (BCI)« beschreiben. Mittels einer Elektrodenhaube werden hirnelektrische Signale nicht-invasiv, dh ohne Operation, von der Schädeloberfläche aus gemessen und mittels EEG aufgezeichnet. Im jüngst abgeschlossenen ERC-Consolidator Grant-Projekt (Anm. des European Research Council) »Feel your Reach« ist es gelungen, einen Roboterarm rein durch Gedanken in Echtzeit zu steuern, wie gewohnt nicht-invasiv mittels EEG-Haube. Möglich wurde das durch das Dekodieren kontinuierlicher Bewegungsintention aus den Hirnsignalen. »Wesentlich hierbei ist der Beitrag der Augen«, informiert Gruppenleiter Gernot Müller-Putz. Die Sehinformationen tragen dazu bei, die Bewegungsintention zu erfassen. Ein weiteres BCI erkennt und korrigiert nicht erwünschte Bewegungen des Roboterarms. Durch Vibrationsgeber an der Haut werden die Bewegungen zudem fühlbar.

>> Krebszelle <<

Computermodelle zählen seit Jahren zu den Standardwerkzeugen in der biomedizinischen Grundlagenforschung. Unter Mitwirkung der Medizinischen Universität Graz und des Memorial Sloan Kettering Cancer Center in New York ist es Forscher*innen der TU Graz gelungen, das weltweit erste Krebszellmodell zu erarbeiten und damit ein essentielles Werkzeug für die moderne Krebsforschung und Medikamentenentwicklung auf den Weg zu bringen.

Bislang fokussierten digitale Zellmodelle auf erregbare Zellen wie Nerven- oder Herzmuskelzellen. Das Team rund um Christian Baumgartner, Leiter des Instituts für Health Care Engineering an der TU Graz, legte das Augenmerk nun erstmals auf die spezifischen elektrophysiologischen Eigenschaften nicht-erregbarer Krebszellen. Das Computermodell simuliert die zyklischen Veränderungen des Membranpotenzials einer Krebszelle am Beispiel des menschlichen Lungenadenokarzinoms und eröffnet damit neue Wege in der Krebsforschung.

»In einer bestimmten Zellzyklusphase lassen sich Krebszellen quasi einfrieren. Mittels Computermodellen können diese Mechanismen simuliert werden«, sieht Baumgartner das erste digitale Krebszellmodell als den Beginn umfassender Forschungen. Weitere experimentelle und messtechnische Validierungen sind geplant. ■

Am Institut für Computergrafik und Vision entwickeln Forscher*innen Methoden des maschinellen Lernens, um Bilder aus der Computertomographie und Magnetresonanztomographie zu verarbeiten.

Fotos: peterschreiber.media/AdobeStock, Baustädter/TU Graz

Steffen Lange ist Country Leader Salesforce Austria.

»Datenhaltung muss vertrauensvoll und sicher funktionieren«

Steffen Lange verantwortet seit April das Österreichgeschäft von Salesforce – als überhaupt erster Geschäftsleiter, der von dem CRM- und SaaS-Pionier dezidiert für den heimischen Markt eingesetzt wird.

Report: Welche Herausforderungen sehen Sie bei Unternehmen aktuell, warum diese auf Cloud-CRM-Lösungen wie Salesforce setzen?

Steffen Lange: In den letzten eineinhalb Jahren hat sich die Welt extrem verändert. Krisen wie die Pandemie aber auch die Klimakrise dringen auf unsere Gesellschaft und die Wirtschaft ein. Wir sehen wachsende Ungleichheiten und einen angespannten Arbeitsmarkt – in weiterer Folge auch eine Vertrauenskrise in der Gesellschaft ebenso wie im Zusammenspiel von Kund*innen und Unternehmen. Nun ist Vertrauen das wichtigste Gut in der Wirtschaft. Langfristig ist Wirtschaftserfolg nur möglich, wenn sich Unternehmen stark in Richtung Kund*innen ausrichten. Sie sollten also ihr Geschäft weniger aus Sicht ihrer Produkte, sondern serviceorientierter an den Kundenbedürfnissen ausrichten.

Durch die steigenden technologischen Möglichkeiten ergeben sich gleichermaßen Chancen und Herausforderungen. Wir sprechen hier vom »digitalen Imperativ«: Unternehmen sollen die digitalen Möglichkeiten als Chance begreifen, um ihr Geschäft wieder neu ausrichten zu können. Unser Vorteil ist, dass wir seit über 20 Jahren den Markt mitgestalten und viele konkrete Beispiele für erfolgreiche digitale Transformationsthemen bringen. Diese Verlässlichkeit und das Vertrauen, das uns in diesem langen Zeitraum erbracht worden ist, sehen wir auch fix als Unternehmenswert in unserer Rolle als »Trusted Advisor« verankert.

Report: Was können Sie Kunden sagen, die aus Datenschutzgründen ihre Daten in Europa gespeichert lassen wollen?

Lange: Wir nehmen als Cloud-Anbieter dieses Thema sehr ernst und übererfüllen die rechtlichen Vorgaben sogar. Wir bietet eine Datenhaltung innerhalb der EU an und haben dazu auch verschiedene Ankündigungen in den letzten Wochen gemacht. Eine Datenhaltung muss natürlich vertrauensvoll und sicher funktionieren – sowohl für Unternehmen als auch für ihre Kunden. Man sollte aber auch drauf achten, wie Cloud-Kunden mit deren Kundendaten arbeiten. Da fehlt oft die Transparenz, wenn Unternehmen mit »Spray and Pray«-Ansatz personenbezogene Daten ohne Einwilligungen verarbeiten.

Report: Haben Sie Unternehmen in Österreich, denen die Wahlmöglichkeit des Datenspeicherorts wichtig ist?

Lange: Absolut. Dem begegnen wir immer wieder.

Report: Welchen Einfluss hat die Änderung in Richtung hybride Arbeitsplätze generell auf Business-Software?

Lange: Abgesehen davon, dass wir durch die Pandemie keineswegs in eine neue Arbeitsplatz-Situation gekommen sind – hybride Arbeitsmodelle sind seit langer Zeit fest bei uns verankert, unsere Zusammenarbeit intern ist stark von Vertrauen geprägt – sehen wir dadurch auch neue Chancen. In der Nutzung auch unserer eigenen Technologien reden wir vom sogenannten »digitalen

Lernplattform

■ FÜR DIE QUALIFIZIERUNG in Salesforce-bezogenen Berufen stellt Salesforce die kostenlose Online-Lernplattform Trailhead bereit, mit deren Hilfe sich weltweit bereits 3,6 Millionen Menschen mit den entsprechenden Nachweisen weiterqualifiziert haben. Ein Schwerpunkt der Bildungsinhalte liegt auf neu konzipierten Rollen in Marketing, Vertrieb und Design.

Info: trailhead.salesforce.com/de

Fotos: Salesforce

Headquarter« als Arbeitsort. Unternehmen sollten sich bei den Anforderungen unserer Zeit auch ihre internen Unternehmensprozesse anschauen, schließlich bedeuten Webkonferenzen und Homeoffice allein noch keine nachhaltige Veränderung. Auch mit den Kund*innen sollte digital interagiert werden. Es gilt, alle technologischen Möglichkeiten zu nutzen und für Eventualitäten gewappnet zu sein.

Report: Wie ist Salesforce in Österreich personell aufgestellt? Wen adressieren Sie speziell?

Lange: Während wir im österreichischen Markt in der Vergangenheit eher reaktiv tätig waren, wachsen wir jetzt nach einem starken Vorjahr nun rasant. Wir stellen jeden Monat weitere Mitarbeiter*innen ein. Dementsprechend macht es Spaß, das verantworten zu dürfen.

Salesforce kommt ursprünglich aus dem Markt für kleinere und mittlere Unternehmen – im Mittelstand sind wir eigentlich groß geworden. Dementsprechend ist unsere Kundenbasis auch in Österreich in diesen Segmenten am ausgeprägtesten.

Es ist bei den Unternehmen generell auch in der Pandemie die Investitionsbereitschaft nicht zurückgegangen. Laut einem aktuellen »Small and Medium Business Trend Report« von Salesforce werden 31 % der Investitionen in Marketing-Technologien gesteckt, knapp vor Kundenservice mit 29 %. Es ist deutlich erkennbar, dass auch aus Sicht der Unternehmer*innen die Kund*innen in den Vordergrund rücken müssen. Zusätzlich stellen wir unsere Software gemeinnützigen Organisationen kostenfrei zu Verfügung. Wir wollen auch wieder an die Gesellschaft zurückgegeben.

Report: Sie bieten eine Lernplattform als Service an. Was wollen Sie damit erreichen?

Lange: Wir sind überzeugt, dass die Vermittlung von digitalen Fertigkeiten und Stärken nicht allein staatliche Organisationen verantworten müssen. Als Vorreiter der Digitalisierung sehen wir uns in einer gesellschaftlichen Verpflichtung. Einer IDC-Studie zufolge werden bis zum Jahr 2026 voraussichtlich 11.000 neue Arbeitsplätze rund um Salesforce, seinen Partnerfirmen und Kunden in Österreich entstehen. 2026 werden gut 18.000 Menschen in Salesforce-bezogenen Jobs arbeiten. Das bedingt auch, dass die Anforderungen an die digitalen Skills der Beschäftigten kontinuierlich steigen werden.

Ich kann herzlich dazu aufrufen, diese kostenfreie Möglichkeit der Weiterbildung zu nutzen. ■

ERP und CRM – Neues von Anbietern, Konferenzen und Projekten

>> Schritt nach Österreich <<

Der Cloud-ERP-Pionie myfactory wurde vor rund 20 Jahren gegründet. Nun kündigt das Unternehmen eine erste Niederlassung am Standort Österreich an, um seine Aktivitäten, insbesondere im Channel, weiter zu forcieren. Noch gesucht wird ein*e Standortleiter*in. Auch offen ist der genaue Ort der Niederlassung, der Standort Wien wird allerdings präferiert.

Aktuell vertreibt myfactory seine Lösungen in Österreich über fünf Partner. Der Vertrieb erfolgt ausschließlich indirekt. Ein Ziel der neuen Niederlassung ist die Gewinnung zusätzlicher Partner und der Aufbau von myfactory.Centern in allen österreichischen Ballungszentren. Bei den myfactory.Centern handelt es sich um ein Partnermodell.

>> Künstliche Intelligenz und ERP <<

ERP-Systeme sind Basis für die Digitalisierung von Unternehmen. Das zeigte sich bei der Fachtagung ERP Future 2021 am 21. September. Mehr als 100 Anwender*innen, Entscheidungsträger*innen und Lösungsanbieter aus der Region DACH und Italien informierten sich bei der virtuellen Tagung über Entwicklungen und Innovationen auf dem Gebiet der Enterprise-Software-Landschaften, den Zusammenhang mit künstlicher Intelligenz und welche Rolle ERP-Systeme für Unternehmen in Zeiten der Pandemie spielen.

Seit mittlerweile zwölf Jahren wird die Fachtagung ERP Future vom Institut für Strategisches Management, Marketing und Tourismus der Universität Innsbruck in Zusammenarbeit mit Christoph Weiss als unabhängige Plattform für Anwender und Entscheidungsträger organisiert. Veranstaltungspartner der Online-Tagung heuer war die Fachhochschule Vorarlberg. Aussteller waren All for One Austria, Asseco Solutions, CMC Unique Solutions, IFS Deutschland, ISTOS, Kreuzbauer IT, proALPHA, proTask Consulting, PSI Automotive & Industry Austria, schrempp edv, SIS Consulting sowie Xentral ERP Software.

>> Künstliche Intelligenz und CRM <<

Salesforce hat den Marktstart von neuen KI-gestützten Workflows und Contact-Center-Innovationen in seiner Service Cloud angekündigt. Diese sollen den Kontakt und die Zusammenarbeit zwischen Service-Mitarbeiter*innen und Kund*innen vereinfachen. In die Customer-360-Plattform integrierte Workflows lassen Kundenbedürfnisse »vorhersehen«, weiterzuleiten und lösen – manchmal sogar, bevor Kund*innen überhaupt wissen, dass ein Problem besteht, heißt es. Darüber hinaus bieten neue digitale Contact-Center-Innovationen für Video, Chat, Voice und »Workforce Engagement« Erleichterungen für Anwender*innen und Serviceteams gleichermaßen.

Da die Kundenanfragen zunehmen und viele Unternehmen personelle Engpässe zu bewältigen haben, mussten bereits 78 % der Verbraucher*innen ein Unternehmen mehrfach kontaktieren, um ein einziges Anliegen zu klären. Um dies zu verhindern sind Serviceteams auf Plattformen angewiesen, die wiederholende und weniger anspruchsvolle Aufgaben automatisieren.

>> Mehr Kundennähe <<

Mit dem Ziel, näher an die Prozesse seiner Industriekunden heranzurücken, treibt der deutsche Werkzeug- und Maschinenbauers WBE die Digitalisierung der Entwicklungs- und Fertigungsprozesse mit Hilfe des »mesonic WinLine ERP«-Systems voran.

Schon beim Import der Kundenbestellung in die WinLine werden automatisierte Prozesse ausgelöst: Zunächst liest die Software aus den übermittelten Stücklisten des Kunden die erforderlichen Produktionsmaterialien heraus und erstellt automatisch einen Bestellvorschlag für fehlende Teile bei den Lieferanten. Parallel dazu werden bereits die Ressourcen und einzelnen Arbeitsschritte für die Produktion zugeordnet. Hierfür wird das tief in die WinLine integrierte Modul »M-Prozesse« des mesonic-Systemhauspartners S&S Software und Service GmbH genutzt. Die beiden Systeme synchronisieren automatisch alle Datenstände und geben jederzeit aktuell Auskunft über Lager- und Produktionsbestände. Sämtliche Abläufe – vom Wareneingang über das Lager, zum Veredler und zurück sowie der Warenausgang zum Kunden – werden ebenfalls in der Unternehmenssoftware erfasst, dokumentiert und mit den notwendigen Begleitbelegen für den Kunden versehen. Damit verfügt WBE über den gesamten Produktionsprozess hinweg über eine durchgängige digitale Dokumentation aller Warenflüsse und Tätigkeiten. ■

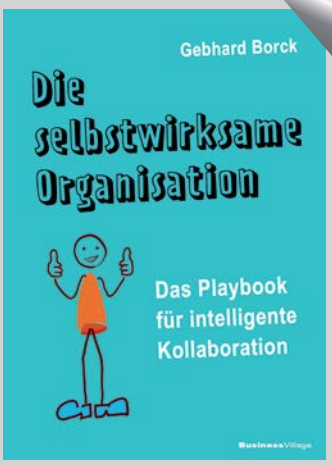
Der Vier-Tage-Woche-Betrug

Von Gebhard Borck

Alle sind aus dem Häuschen – Eine Studie aus Island zeigt, dass der herbeigesehnten Vier-Tage-Woche nichts mehr im Wege steht. Doch was machen wir mit der gewonnenen Freizeit? Das Versprechen, das sich hinter der Vier-Tage-Woche verbirgt, zeigt das eigentliche Dilemma der Arbeitswelt.

Diesen Sommer hat eine Studie zur Vier-Tage-Woche aus Island mit dem Titel »Going Public: Iceland's journey to a shorter working week« die Runde in den Medien gemacht. Das einhellige Urteil: Eine viertägige Arbeitswoche ist besser für die Menschen und die Wirtschaft. Die Onlinezeitung Perspective Daily fragt in einem Artikel zum Thema: Wäre die Vier-Tage-Woche eine gute Lösung für Dich? Drei Antworten stehen zur Wahl: »ja«, »nein«, »ich arbeite bereits vier Tage«. Die erste Option bekommt aktuell 74 %, die zweite 6 % und die dritte 18 % der abgegebenen Stimmen. Ich gehöre zur Minderheit, die mit »nein« abstimmten. Denn ich halte das durchgeführte Experiment für einen Betrug gegenüber den Arbeitnehmer*innen.

BUCHTIPP



DIE SELBSTWIRKSAME ORGANISATION
Gebhard Borck
Das Playbook für intelligente Kollaboration
1. Auflage BusinessVillage 2020
296 Seiten
ISBN 978-3-86980-486-6
Preis: 29,95 Euro

www.businessvillage.de/presse-1067

Fotos: iStock, beigestellt

Studie: Es fehlt das Vertrauen

DIE ERGEBNISSE EINER STUDIE von Ricoh Europe zeigen, dass nur 35 % der Arbeitgeber ihren Mitarbeiter*innen beim Remote Working uneingeschränkt vertrauen. 39 % sind der Ansicht, im Homeoffice werde nicht so engagiert oder effektiv gearbeitet wie im Büro. Im Rahmen der von Opinion Matters durchgeführten Studie wurden 1.500 europäische Führungskräfte aus Unternehmen aller Größen befragt. Zu einem Zeitpunkt, an dem viele Unternehmen eine – zumindest teilweise – Rückkehr an den Arbeitsplatz erwägt hatten, sind diese Ergebnisse ein Hinweis darauf, dass mit der Pandemie das Vertrauen ins Homeoffice geschwächt wurde. Aber trotz ihrer Bedenken und des schwindenden Vertrauens berichten nur 19 % der Arbeitgeber von einem Rückgang der Produktivität seit der Umstellung auf Remote Working. Darüber hinaus sind 57 % der Ansicht, dass Investitionen in flexible Arbeitstechnologien für Recruiting und Bindung von Talenten unerlässlich sind. 42 % der Führungskräfte berichten, dass ihre Teams aufgrund von Sorgen hinsichtlich Gesundheit und Sicherheit Bedenken haben, bei Aufhebung der Beschränkungen ins Büro zurückzukehren. Sollten diese Bedenken nicht berücksichtigt werden, könnte dies nicht nur die Arbeitsmoral beeinträchtigen, sondern auch zum Verlust wesentlicher Leistungsträger führen, heißt es.

>> Der große Betrug <<

Viele der Digitalisierer in der Wirtschaft machen ihren Kunden diese, durchaus derbe Ansage zu Beginn des Vorhabens: »Eines muss ihnen klar sein, wenn sie heute einen Scheißprozess haben und den digitalisieren, haben sie einfach einen scheißdigitalen Prozess.« Genauso geht es mir mit der Glorifizierung einer reduzierten Arbeitswoche. Wenn wir die Verkürzung von schlechten Arbeitsbedingungen glorifizieren, hat sich an den Umständen ja nichts verändert. Wie die Studie aus Island aufzeigt stimmt das auch. Denn im Kern erreichte die Reduktion der Arbeitszeit vor allem, dass die Menschen ihre unbefriedigende Arbeit besser aushalten können. Das gelingt, indem sie mehr Zeit haben, ihren Frust zu kompensieren.

Der Autor der Studie, Jack Kellam, sagt dazu im Zeit-Interview: »Die Probanden konnten über die Zeit, in der sie nun weniger arbeiten mussten, selbst bestimmen. Es ist egal, ob jemand in dieser Zeit vor dem Computer sitzt und zockt oder im Wald spazieren geht.« Was laut Kellam die Menschen zufrieden macht, ist Selbstbestimmung. Das unterstreicht er mit der Aussage: »Wichtig ist vor allem, dass die Teilnehmerinnen und Teilnehmer ein hohes Maß an Selbstständigkeit bei der Gestaltung ihrer Arbeitszeit hatten.«

>> Worum es wirklich geht <<

Plakativ bietet die Studie eine Verringerung der Arbeitswoche als Lösung an. Doch bei genauem Hinschauen zeigt sich etwas anderes. Menschen fehlt Selbstwirksamkeit im Arbeiten. Wir wollen Einfluss nehmen. Wir wollen mitgestalten. Wir wollen dreizehn gerade sein lassen. Die Art, wie heute die allermeisten Firmen organisiert sind, verhindert bei der weiten Mehrheit der Angestellten genau das. Und zwar systematisiert. Deshalb braucht es mehr als die Verbesserung der bestehenden Strukturen. Wir sind bereit für einen Systemwechsel. Wir brauchen ein adaptives Organisationsdesign, das selbständiges Gestalten durch die Mitarbeitenden professionalisiert. Herkömmliche Organisationsstrukturen sind kaum an diese Anforderungen angepasst. Formal festgezurrte Befehls- und Kontrollstrukturen vereiteln die Fähigkeit von Menschen, sich selbstverwaltet an verändernde wirtschaftliche, technologische und Marktbedingungen anzupassen.

Soll die eigene Organisation adaptiv werden, fordert das deshalb vor allem die traditionellen Führungsgewohnheiten heraus. Für den Erfolg gilt es, die Silos zu verlassen. Und mehr noch. Niemand kann sich weiter auf vorgebende Planungen einlassen. Denn bis sie aufgehen, ist längst eine andere Lösung nötig. In dieser Gemengelage heißt es, Autonomie zuzulassen. Doch nur die, die schlussendlich auch im Sinne der Organisation handelt. Das gelingt durch drei zentrale Wirkungsmechanismen:

1. Verteilung von Führungsaufgaben/ -verantwortung in die gesamte Firma, anstatt sie auf formale Rollen zu begrenzen.
2. Übergang von Management zu Selbstverwaltung
3. Transfer hin zu funktionsübergreifenden autonomen Teams

Bei Firmen, die diesen Weg konsequent gehen, kommt heraus, dass für viele die Vier-Tage-Woche oder sogar noch geringere Arbeitszeiten bei vollem Lohnausgleich kein Thema sind. Es geht ja keineswegs darum, wie lange jemand arbeitet. Es kommt darauf an, welche Wirkung sie/er mit seiner Arbeit erzielt. Das gilt im Übrigen für die Unternehmer*innen genauso wie für ihre Angestellten. So betonen die Eigentümer der Teledata IT-Lösungen GmbH, Peter Wassmuth und Robin Aigner, die mit ihrer Firma diesen Weg erfolgreich gehen: »Einer unserer größten Erfolge ist, dass wir keine fünfzig oder sechzig Stunden Woche mehr haben, sondern mit dreißig bis vierzig wunderbar hin kommen.« Bei kununu liest sich die Reaktion eines Mitarbeitenden auf die adaptiven Arbeitsbedingungen in der Teledata so: »Einfach schön, wenn man sich Sonntags auf Montags freut«.

Und so frage ich: Sollten wir uns wirklich weiterhin mit Vier-Tage-Wochen als Heilsversprechen betrügen, wenn es in unserer Gestaltungsmacht liegt, sinnvoll zusammen zu arbeiten? Ich weiß: Wir können das besser! ■

DER AUTOR

GEBHARD BORCK ist »Transformations-Katalysator«. Mit aus der Praxis erprobten Denkwerkzeugen löst er konkrete, drängende Probleme. Und Borck ist mehr als ein Berater: Anstatt Luftschlösser zu bauen, deckt er auf, spricht Tacheles. Er ist Speaker, Bestsellerautor, Sparringpartner und gilt als Erfinder echter Fairness in der Wirtschaft.

www.gebhardborck.de

HR-TOOL

Management von »Skills«

Workday unterstützt Unternehmen bei der Einführung von detaillierten Personalstrategien.

Workday HCM ist ein einheitliches System, das die Daten aller Mitarbeitenden sicher zusammenführt – einschließlich Skills – und diese als Teil einer vernetzten »Talent Experience« zur Verfügung stellt. Unter anderem werden die Bereiche Weiterentwicklung, Rekrutierung und Performance abgedeckt. Die Skills Cloud, die in Workday HCM enthalten ist, aktualisiert sich dynamisch über die gesamte »Employee Journey« hinweg, um die Entwicklung neuer Skills abzubilden und Unternehmen bei der kontinuierlichen Weiterentwicklung von Skill-basierten Personalstrategien zu unterstützen. Dazu gehört auch die Möglichkeit, in Echtzeit auf Daten zu vorhandenen wie auch fehlenden Skills zuzugreifen. Auf diese Weise können Unternehmen besser auf geschäftliche Anforderungen reagieren und ihrer Belegschaft eine einheitliche Talent Experience bieten. »Unternehmen konzentrieren sich mehr denn je auf den Einsatz Skill-basierter Personalstrategien, um die Bindung, Einstellung, Rekrutierung und das Engagement der Mitarbeitenden zu verbessern«, sagt David Somers, Group General Manager, Office of the Chief HR Officer, Workday. »Unsere Skills Cloud bietet die Grundlage, um unseren Kunden dabei zu helfen, eine Strategie für den Umgang mit Skills zu entwickeln und ihren Weg zu einer agileren Belegschaft zu unterstützen.« Workday liefert zusätzlich Einblicke mittels Dashboards, die auch vergangene – aber verlorene – Skills dokumentieren. ■

Der millionste VX25 Schaltschrank ist im Werk Rittershausen vergoldet vom Band gelaufen – Muhammet Akin, Mitarbeiter in der Montage.

Millionster Schaltschrank

2021 ist für Rittal ein Jubiläumsjahr im dreifachen Sinn. Das Unternehmen feiert seinen 60. Geburtstag, den 75. Geburtstag seines Inhabers Friedhelm Loh und auch den VX25.

Am 16. August rollte der millionste Schaltschrank vom Band im Werk Rittershausen, Deutschland. Inhaber und Management würdigten die Leistung der Belegschaft genau dort, wo der VX25 jeden Tag gefertigt wird: inmitten der Produktion. Drei Jahre nach der Markteinführung, kommt der VX25 bei Industrie- und IT-Kunden in der ganzen Welt zum Einsatz: zum Beispiel in Fertigungsstraßen aller namhafter Automobilhersteller, in Windenergieanlagen an entlegensten Orten, auf Kreuzfahrtschiffen oder in Rechenzentren von IT-Giganten wie Facebook und Amazon.

»Das ist nur mit Ihrer Unterstützung wirklich gelungen. Dafür danke ich Ihnen sehr. Wir sind Weltmarktführer in Technologie immer gewesen und haben mit dem VX25 Schaltschrank ein neues Zeichen im Markt gesetzt. Wir haben unsere Kunden damit komplett überrascht. Damit zeigen wir seit vier Produkt-Generationen Exzellenz im Schaltschrankbau«, sagte Prof. Friedhelm Loh den anwesenden Mitarbeiter*innen.

Mittlerweile fertigt das Unternehmen nicht nur in Rittershausen, sondern in eigenen Werken auch in China, Indien, England, Brasilien und den USA. »Wir produzieren weltweit mehrere Tausend Großschränke pro Tag.« Viele, auch die großen Elektrokonzerne, hätten es versucht, aber ohne Erfolg. Eine der großen Stärken von Rittal sieht der Inhaber darin, immer wieder Wege gegen den allgemeinen Trend und den Trends voraus gegangen zu sein – zum Beispiel durch Erweiterung des Portfolios vom Schaltschrank hin zum System mit Kühltechnik und Stromverteilung bis hin zur IT-Infrastruktur. Dies müsse auch in Zukunft so bleiben. ■

KONFERENZ

CO2-Einsparung durch effiziente IT

Digitalisierung und Klimaschutz waren die zentralen Themen einer Digitalveranstaltung in Karlsruhe im Oktober.

Entwickelt sich ein neuer »Business Imperativ« als wirtschaftliche Notwendigkeit, der die unternehmerische Verantwortung und das Erreichen der Klimaschutzziele mit handfesten wirtschaftlichen Erfordernissen zusammenführt? Im Rahmen des »CDR Summit« (Anm. »Corporate Digital Responsibility«) wurde am 21. und 22. Oktober dieses Thema in einer Digitalveranstaltung der TechnologieRegion Karlsruhe für ein breiteres Publikum zugänglich gemacht. Technologieunternehmen wie etwa

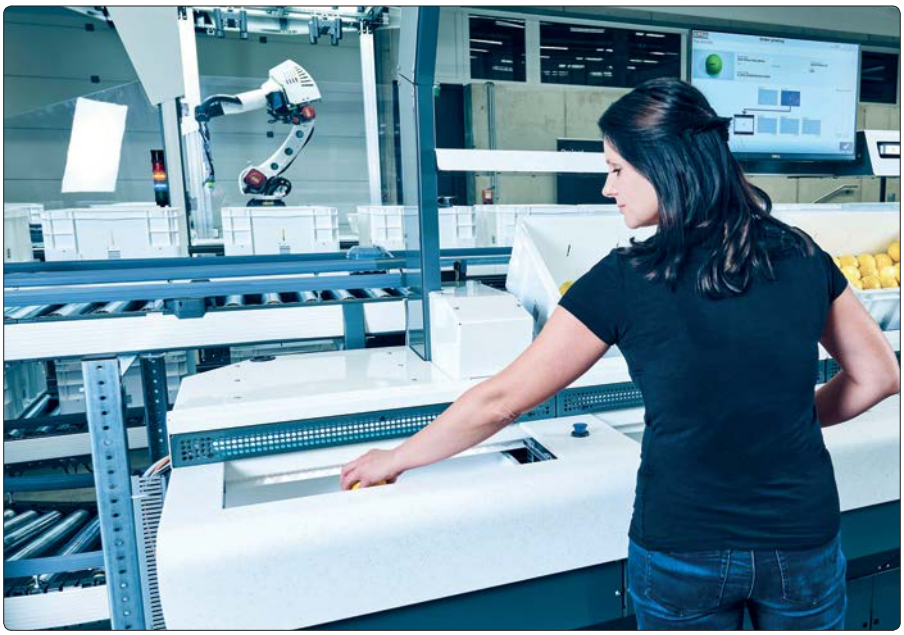
Klimaschutz ohne Digitalisierung wird nicht funktionieren. Gleichzeitig stellt die Digitalisierung selbst eine Klima-Herausforderung dar.

Cisco haben bereits »Net Zero Emission Goals« als weltweites Unternehmensziel angekündigt. Damit sollen die komplette Wertschöpfungskette und der Einsatz eigener Produkte und Lösungen bei Kunden emissionsfrei gestaltet werden. Unterstützt wurde der CDR Summit Digital durch Bechtle. Ebenfalls an Bord waren Apple, Cisco, Dell, Dropbox, Ecosia, Greendeal Company, HP IBM, Kyocera, Limebird, Panasonic, PlanA, T.P.I. Trippe und Partner, sowie WiseWay. ■

Fotos: Rittal

Wegweiser für Knapp AG

Der Lagerlogistik-Spezialist Knapp AG in Hart bei Graz wird die neue SAP-Business-Prozessmanagement-Suite Signavio zum Einsatz bringen. Unterstützt wird das Unternehmen vom Wiener SAP-Berater CNT, der als langjähriger Implementierungspartner und Lösungsprovider die Gesamtkoordination übernimmt.



Mit Unterstützung durch CNT wird der Lagerlogistik-Spezialist Knapp AG in Hart bei Graz die neue Prozessmanagement-Suite Signavio (zu deutsch: Wegweiser) zum Einsatz bringen.

Die cloud-basierte Managementsoftware zur Modellierung von Geschäftsprozessen wurde von einem Spin-off des Hasso Plattner Instituts entwickelt und ist seit Jänner 2021 zentraler Part des digitalen Transformationsangebots von SAP. Konkret geht es um eine All-in-One-Plattform, die Kunden bei ihrem digitalen Wandel durch Live Insights unterstützt, insbesondere bei jenen Kernprozessen, die sie Tag für Tag ausführen.

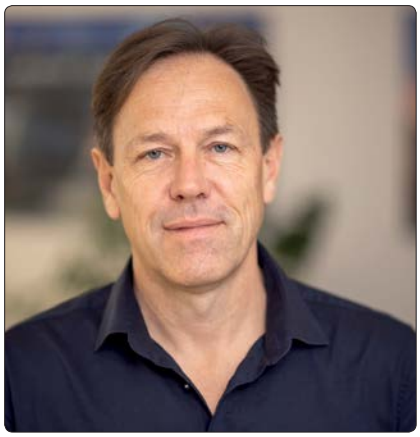
Signavio bietet eine ganz neue Qualität der Digitalisierung - und das integriert in die SAP-Welt. Prozesse in einer einzigen Plattform zu modellieren, optimieren und auszuführen, das kann bisher keine andere Business Prozess Management Lösung. »Hier werden moderne Technologien wie Prozess- und Entscheidungsmanagement, Process Mining und Customer Journey Mapping kombiniert – eine tolle Ergänzung des bestehenden SAP-Portfolios«, wie CNT-Partner Gerald Rossmann bestätigt.

»Nach einer Initialisierungsphase gemeinsam mit Signavio wird CNT das Grunddesign mit Knapp festlegen und bis Jahresende einen möglichst umfassenden Anforderungskatalog erarbeiten und definieren, um die Umsetzungsphase 2022 effizient zu gestalten«, sagt Rossmann. Zunächst werden die Kernprozesse im Headquarter unter die Lupe genommen, danach folgen die transnationalen Prozesse und Zusammenhänge. ■

Start von SASE-Plattform

Flexible und sichere Fernzugriffsfunktionen bei verringerten Latenzzeiten mit Point-to-Cloud-Konnektivität.

Der Cloud-Sicherheitsspezialist Barracuda hat den Marktstart einer cloud-nativen SASE-Plattform angekündigt, die ermöglicht, den Zugriff auf Daten von jedem Gerät aus immer und überall zu kontrollieren. Um SASE-Konvergenz zu erreichen, vereint die Plattform Barracudas Technologien Secure SD-WAN, Firewall-as-a-Service, Zero Trust Network Access und Secure Web Gateway. Sie ermöglicht Securityservices auf den Cloud-Hubs der Kunden, zusätzlich zu der Möglichkeit, sie direkt auf den Geräten vor Ort auszuführen »Auf diese Weise besteht neben einer räumlichen Nähe zwischen dem Netzwerkzugang und dem Standort der Assets der Vorteil einer globalen Public-Cloud-Architektur«, erklärt Klaus Gheri, General Manager Network Security bei Barracuda Networks. »Secure Access Service Edge (SASE)« ist ein Architekturkonzept, das WAN-Services und Security-Funktionen kombiniert cloudbasiert bereitstellt. ■



Klaus Gheri, Barracuda: »Wenn Unternehmen ihre Ressourcen in die Public Cloud verlagern, ist es sinnvoll, SASE-Angebote in Betracht zu ziehen, die cloud-nativ sind.«

AXIANS UND FORTINET

Advanced Partner

Durch einen konsequenten Aufbau von Know-how und Ressourcen erreichte Axians ICT Austria den Status »Fortinet Advanced Partner«. Der IT-Dienstleister ist einer der bestzertifizierten Fortinet-Partner in Österreich, das Serviceportfolio rund um Fortinet wurde sukzessive erweitert und wird flächendeckend angeboten. »Die innovativen und weltweit erfolgreichen Angebote von Fortinet ergänzen unser Security-Portfolio ideal und ermöglichen uns, unseren Kunden ein breiteres Spektrum an Security-Lösungen sowie neue Services anbieten zu können«, so Martin Egger, Business Unit Leiter Network & Cyber Security bei Axians ICT Austria. Dominik Wendl, Fortinet Channel Account Manager, betont zum neuen Partner-Status von Axians ICT Austria: »Expertise und Engagement sind die Eckpfeiler unseres Partnerprogramms. Wir schätzen daher die erfolgreiche Weiterentwicklung von Axians ICT Austria. Gemeinsam sind wir starke Partner für unsere österreichischen Kunden – wir haben für aktuelle Bedrohungen die passenden Technologien und Services.« ■

Fotos: Knapp AG, Barracuda

Mein Office

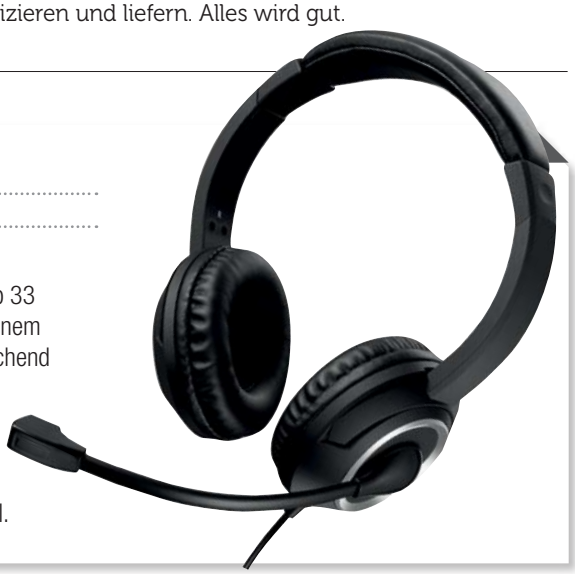
Praktische Werkzeuge fürs Wirtschaften

Wir sind Getriebene von Input und Output. Wir haben die passenden Tools. Wir können noch schneller aufnehmen, kommunizieren und liefern. Alles wird gut.

Im Test: robust und praktisch

Preis 32,99 Euro

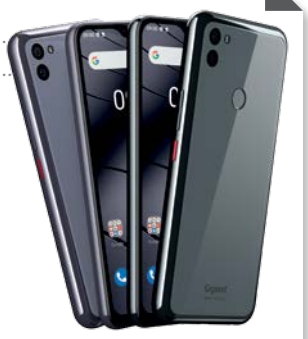
Der Hersteller Sandberg hat mit dem »USB Chat Headset« ein einfaches, aber in der Qualität überzeugendes Headset für die Arbeit am Computer im Sortiment. Für knapp 33 Euro (inkl. MwSt.) bekommen Nutzer*innen ein hervorragendes Kopfhörerset – mit einem angenehm fest sitzenden, aber drehbaren Mikrofonarm – das auch halbwegs ausreichend Bass-Frequenzen beim Abspielen von Videos und Musik wiedergibt. Im Report-Test hat das Gerät unseren Erwartungen entsprochen: Im Preis-Leistungsverhältnis schneidet es aufgrund der Tonqualität, der Polsterung der Hörmuscheln und der Robustheit besser ab, also so viele andere Office-Headsets. Ebenfalls positiv sind die Länge des USB-Kabels von 1,8 m sowie eine Lautstärkeregelung direkt am Kabel.



Flaggschiff GS5

Preis: 299 Euro

Doppelt so viel interner Speicher, ein energiesparender Prozessor, ein leistungsstarker Wechsel-Akku, eine Kamera, die alles Bisherige toppt – das ist das neue Smartphone GS5 von Gigaset. Mit 48 Megapixel bietet es die dreifache Auflösung der Kamera des Vorgängers GS4.



Cloud Print Service

Preis: flexibel, je nach Aufkommen

Der Service »Konica Minolta Cloud Print« wird in einem deutschen Rechenzentrum gehostet und ist nach ISO 27001:27017 zertifiziert. Wie es funktioniert Wird der Druckjob abgeschickt, befindet sich das Dokument in der Cloud. Sobald es im gewünschten Multifunktionssystem angekommen ist, kann es ausgedruckt werden.

Hoher Durchsatz

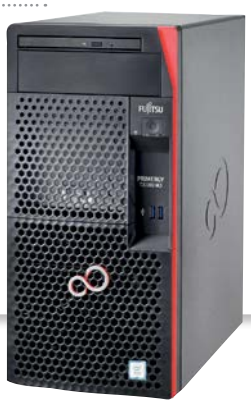
Preis: abhängig von der Konfiguration

Neue Exadata X9M-Plattformen von Oracle beschleunigen die Online-Transaktionsverarbeitung mit mehr als 70 % höheren IOPs-Raten und I/O-Latenzen von unter 19 Mikrosekunden. Sie können den analytischen SQL-Durchsatz sowie die Geschwindigkeit von Workloads für maschinelles Lernen um bis zu 87 % erhöhen.

Zertifiziert für Windows Server

Preis: abhängig von Spezifikation und Region

Fujitsu PRIMERGY Server sind jetzt für Windows Server 2022 zertifiziert. Das Betriebssystem bietet erweiterte Multi-Layer-Schutzfunktionen und ermöglicht sicheres Remote-Arbeiten. Die Fujitsu-Microsoft-Kombination soll neben dem höheren Sicherheitsniveau mehr Flexibilität sowie eine höhere Produktivität bieten.



Fotos: iStock, Sandberg, Gigaset, Konica Minolta, Oracle, Fujitsu

VON RAINER SIGL

Kopfweh durch Social Media. Die Algorithmen, die entscheiden, was an wen ausgespielt wird, sind seit Jahren auf Krawall gebürstet.

Morbus TikTok

Am gesellschaftlichen Nutzen von Social Media scheiden sich die Geister. Facebook, Twitter, Instagram, TikTok & Co könnten aber auch Ihre Gesundheit gefährden.

Was Twitter- Bonmots angeht, ist das eines der besseren: »Fox News und Facebook haben unseren Eltern das angetan, was die geglaubt hätten, dass Videospiele uns antun würden.« Da ist was dran. Während der behauptete Zusammenhang von Videospielen und realer Gewalttätigkeit von zahlreichen Studien ins Reich der Vorurteile verbannt wurde, wird der düstere Befund in Sachen Social Media immer konkreter: Social Media radikalisiert die Gesellschaft und sorgt für Spaltung und Konflikte bis hin zur Gewalt. Kein Corona-Leugner, kein Verschwörungstheoretiker, der nicht mehr oder weniger durch die Rutsche im Internet zu seinen Überzeugungen gekommen wäre.

Und das nicht zufällig, sondern mit voller Absicht und Unterstützung der Plattformen: Kontroverse, Hass und starke emotionale Themen sorgen für lange Verweildauer auf YouTube, Facebook & Co, die wiederum bringt Werbemilliarden. Die Algorithmen, die entscheiden, was an wen ausgespielt wird, sind seit Jahren auf Krawall gebürstet. Zornige Nutzer bleiben länger. Der aktuelle Skandal um Facebooks diesbezügliche Praktiken belegt nur, was seit Jahren allgemein bekannt war und – auch an dieser Stelle – berichtet wurde. Zu diesen gesellschaftliche Fliehkräfte anheizenden Schattenseiten sozialer Medien kommt nun eine weitere, ganz konkret physische Bedrohung der oft jugendlichen Nutzerinnen und Nutzer sozialer Medien hinzu. Wie gleich in zwei Studien dokumentiert wurde, ist der Ausbruch einer sozial ansteckenden Verhaltensstörung bei einer global verteilten Gruppe von Jugendlichen wohl direkt auf deren Social-Media-Konsum zurückzuführen. Nach dem Anschauen von TikTok- und Youtube-Videos entwickelten die Patienten innerhalb weniger Tage Tourette-artige Symptome, wie sie im konsumierten Content zu sehen waren. Die Ärzte schlagen für dieses neuen Phänomen den Term »Mass Social Media-Induced Illness« vor.

Social Media radikalisiert die Gesellschaft und sorgt für Spaltung und Konflikte.

>> Angesteckt im Netz? <<

Es mag wie ein dummer Witz klingen, ist aber ernst gemeint: Jugendliche sehen auf TikTok und YouTube Videos von Menschen mit Tourette-Symptomen und erkranken zumindest kurzfristig selbst an der seltenen neurologischen Zwangsstörung, die mit Bewegungstics und unfreiwilligen Schreien und Schimpfwörtern einhergeht. Die Betroffenen leiden ebenso wie die Angehörigen unter der Stigmatisierung durch diese Beeinträchtigung. In manchen Fällen ist eine langwierige Therapie nötig, um die Symptome wieder verschwinden zu lassen, bei anderen legt sich das bestürzende Verhalten innerhalb weniger Stunden wieder.

Kann man sich via TikTok und YouTube mit krankhaften, motorischen und vokalen Tics anstecken? Was nach wilden Vorurteilen medienskeptischer Großeltern klingt, hat reale Grundlagen. Ein aktueller Artikel im renommierten British Medical Journal, der unter anderem auf Fälle in den USA, Neuseeland und Deutschland bezug nimmt, scheint dies zu bestätigen. Die Forscher verweisen dabei auch auf historische Fälle von »Massenhysterien«, am berühmtesten darunter wohl die »Tanzkrankheit« im Europa des 14. und 15. Jahrhunderts. Gerade bei jüngeren Menschen dürfte das Auftreten solcher »sozial ansteckender Verhaltensstörungen« ohne eindeutige körperliche Grundlage auch mit den mentalen Belastungen durch die Coronapandemie einhergehen.

Ein Grund mehr, sein Sozialleben wieder vermehrt in die reale Welt zurückzuverlagern. ■

Fotos: iStock

Gewinner*innen gesucht

Jetzt einreichen für den Wirtschaftspreis »eAward 2022«!

eAWARD

Sie haben viel Zeit und Energie in Ihr Produkt, Ihre Dienstleistung oder in ein Kundenprojekt gesteckt? Nutzen Sie den »eAward 2022«, um den Mehrwert für Ihre Zielgruppen einer breiten Öffentlichkeit vorzustellen!

Der »eAward« zeichnet Projekte mit IT-Bezug aus und wird für den Raum DACH verliehen.

Mehr unter: award.report.at

Report Verlag
Magazine | Bücher | Publishing | New Media

powered by

BRZ BearingPoint DIO Data Intelligence Offensive MP2 IT-SOLUTIONS NTT

ÖGV ÖSTERREICHISCHER GEWERBEVEREIN SPARX SERVICES CENTRAL EUROPE T-Systems VÖSI