www.itbusiness.ch Fractal Verlag GmbH Ausgabe 1/2023 CHF 10.–

itbusiness

Das Schweizer Fachmagazin für ICT

Mit KI zum intelligenten ERP-System

Cybergefahren im Jahr 2023 – grösser denn je!

Transformation der Arbeitswelt

HSLU Hochschule Luzern

Jetzt informieren
hslu.ch/
data-intelligence

Applied Data Intelligence

Big Data und Künstliche Intelligenz erfolgreich einsetzen

MAS Business Intelligence
MAS Data Management & Ecosystems
CAS Applied Robotics
CAS Artificial Intelligence Management for Business Value
CAS Business Intelligence & Analytics
CAS Data Engineering and Applied Data Science
CAS Digital Analytics in Marketing
CAS Machine Learning

Liebe Leserinnen und Leser

In den vergangenen Jahren haben sich die Bedrohungen durch Cyberangriffe vervielfacht. Gerade grosse Unternehmen und staatliche Einrichtungen sind beliebte Ziele geworden. Dabei hat sich die Qualität der Angriffe erheblich verändert. Es sind nicht mehr einfach nur noch Viren und Trojaner, die eingeschleust werden. Die Angreifer nutzen mittlerweile auch das Darknet als Marktplatz und verkaufen Zugänge an den Meistbietenden. Unternehmen tun also gut daran, sich auf die neue Art der Bedrohungen einzustellen und aufzurüsten. Ab Seite 6 lesen Sie, worauf Sie achten müssen.
Unabhängig von den Bedrohungen bleibt die Datensicherung wichtig und somit ein regelmässiges Backup. Die Möglichkeiten sind mittlerweile so vielfältig, dass man sich bewusster damit auseinandersetzen muss, wo und wie man sensible Daten aufbewahren und sicherstellen möchte. Früher hatte man einfach Bänder, heute die Cloud. Doch stellt sich die Frage: Ist die Cloud wirklich die sicherste und beste Lösung? Ab Seite 14 finden wir es heraus.
Wer hat Angst vor künstlicher Intelligenz? ERP-Systeme bestimmt nicht. Im Gegenteil: Dank der KI werden sie intelligenter. Die Nachfrage ist derzeit noch zurückhaltend. Jedoch prophezeit eine IDC-Studie, dass die Nutzungsrate von KI in den kommenden 24 Monaten rasant steigen wird. Welche Vorteile eine KI in ERP-Systemen bringen kann, entnehmen Sie ab Seite 18.
Hybride Autos sind jedem von uns ein Begriff, aber Hybrid Work hat sich erst seit Einzug der Digitalisierung aufgrund der Pandemie zu einem neuen Begriff des Arbeitsmarkts entwickelt. Aber was heisst das Zauberwort Digitalisierung konkret, was genau sind die Auswirkungen auf die Gestaltung der Arbeitsplätze und Jobprofile? Lesen Sie dazu ab Seite 22.
Um dem Fachkräftemangel entgegenzuwirken, werden laufend neue Berufslehren ins Leben gerufen. Diesen Sommer werden die ersten Lernenden in die neue Berufslehre «Entwickler/in digitales Business EFZ» starten. Dabei sind qualifizierte Lehrbeauftragte unerlässlich, denn sie sind mitunter dafür verantwortlich, Berufslehren mitaufzubauen. Im Interview ab Seite 28 erzählt Angela Munz, weshalb sie vom Potenzial dieses Berufs überzeugt ist und was ihr daran besonders gefällt.
Nun wünsche ich Ihnen viele interessante Erkenntnisse beim Lesen dieser Ausgabe und einen schönen Frühling.

Herzlichst Ihre

Petra De Meo

Inhalt

SECURITY

Homeoffice: Massnahmen für Datenschutz und Datensicherheit

HYBRID WORK

Neugestaltung der Arbeitsplätze verändert die Jobprofile

BACKUP & DISASTER RECOVERY

Backup und Recovery in Zeiten von Ransomware

AUSBILDUNG/ WEITERBILDUNG

«Sie sind Brückenbauer zwischen den verschiedensten Anspruchsgruppen»

Cybersecurity-Test für KMU

Vor rund zwei Jahren lancierte der Wirtschaftsverband Suissedigital einen Cybersecurity-Test, der die Öffentlichkeit für die Gefahren des Cyberraums sensibilisiert. In Ergänzung dazu wurde nun ein Test entwickelt, der spezifisch an die Bedürfnisse von kleinen und mittleren Unternehmen angepasst ist. Der neue Test ist ab sofort online verfügbar. Immer mehr Aspekte des Geschäftslebens finden digital statt. Dies gilt gerade auch für kleine und mittlere Unternehmen (KMU), die dank der Digitalisierung ihre Prozesse effizienter gestalten und potenzielle Kunden leichter erreichen und binden können. Gleichzeitig steigt damit für die KMU das Risiko, Opfer von Cyberkriminalität zu werden. Aus diesem Grund hat der Wirtschaftsverband Suissedigital seinen vor rund zwei Jahren lancierten und für die breite Öffentlichkeit bestimmten Cybersecurity-Test mit einem weiteren Online-Test ergänzt, der KMU eine Selbsteinstufung und im Laufe der Zeit einen Vergleich mit anderen KMU ermöglicht. Der neue Test, der auch Nichtmitgliedern offen steht, ist ab sofort online auf Deutsch, Französisch und Englisch verfügbar.
https://control.forthub.io

Engagierte ICT-Lehrbetriebe und Berufsbildner/innen gesucht

ICT-Lehrbetriebe aus der ganzen Schweiz können sich bis zum 31. Mai 2023 für den ICT Education & Training Award bewerben. Mit dem Preis zeichnet ICT-Berufsbildung Schweiz Organisationen aus, die sich überdurchschnittlich für den Berufsnachwuchs im Bereich der Informations- und Kommunikationstechnologie (ICT) einsetzen. Zudem können herausragende ICT-Berufsbildner/innen für den Special Prize nominiert werden. Die Gewinner/innen werden am 25. Oktober 2023 an der ICT Award Night in Bern verkündet. Neu haben die drei besten Lehrbetriebe zudem die Chance, am Digital Economy Award von swissICT mit dem ICT Education Excellence Award ausgezeichnet zu werden.
www.ict-berufsbildung.ch

Frauen in der Cybersicherheit gezielt fördern

Weltweit sind nur 24 Prozent aller Angestellten im Bereich Cybersicherheit Frauen. Gleichzeitig bleibt der Fachkräftemangel hoch und Cyberangriffe nehmen zu. Vor diesem Hintergrund unterstreicht Fortinet, dass Organisationen mehr unternehmen müssen, um Frauen zu gewinnen und zu halten. Inklusion muss Priorität haben, Führungskräfte angemessen geschult und ein offener Dialog geschaffen werden. Unternehmen können für Frauen im Bereich Cybersicherheit gezielt Möglichkeiten schaffen mit der Entwicklung von Schulungs- und Weiterbildungsangeboten, Praktikumsangeboten und der Implementierung von Mentoring-Programmen.
www.fortinet.com/de

Gründung der Swiss Metaverse Association

Gemeinsam für ein innovatives und weltweit führendes Schweizer Metaverse-Ökosystem: 47 Partner aus Wirtschaft, Wissenschaft und Verwaltung gründen die Swiss Metaverse Association. Sie wollen zusammen lernen, Ideen austauschen, Proof of Concepts erstellen und sich für günstige Rahmenbedingungen einsetzen, damit die Schweiz als Zukunftsstandort für Metaverse zu den weltweit besten gehört. Das Ziel dieses jüngst in Bern gegründeten Vereins ist es, ein breit abgestütztes Metaverse-Ökosystem zu schaffen und sich für attraktive Rahmenbedingungen in der Schweiz einzusetzen, so dass neue Geschäftsmodelle, Firmen und Arbeitsplätze entstehen können. Präsidiert wird die Swiss Metaverse Association (kurz: Metassociation) von Tina Balzli, Partner und Leiterin der Fintech & Blockchain Abteilung bei CMS Schweiz, und Alexandra Hofer, Senior Consultant bei furrerhugi. «Mit diesem Verein schaffen wir wichtige Grundlagen, um die Schweiz als innovativen und zukunftsgerichteten Standort zu positionieren, der Metaverse-Projekte ermöglicht. Als Verein vernetzen wir die relevanten Akteure, initiieren Projekte und fördern den Dialog und die Aufklärung», sagt die Co-Präsidentin Tina Balzli.
www.metassociation.ch

IT-Probleme kosten Mitarbeitende Produktivität

Die neue Studie der Unisys Corporation «From Surviving to Thriving in Hybrid Work» (Vom Überleben zum Gedeihen in der hybriden Arbeitswelt), die in Zusammenarbeit mit dem Forschungsunternehmen HFS Research durchgeführt wurde, liefert einen Fahrplan für Arbeitgeber, um die Produktivität und das Engagement ihrer Mitarbeiter zu steigern. Der Bericht zeigt: Zugang zu erstklassiger Technologie wird weiterhin ein entscheidender Faktor für das Mitarbeiterengagement und ihre Leistung sein. 62 Prozent der befragten Mitarbeiter gaben an, dass der Zugang zu Technologie ein sehr motivierender Faktor für ihre Arbeitsleistung ist. Der Bericht zeigt jedoch auch, dass die Art und Weise, wie Unternehmen Technologielösungen einführen und kontinuierlich unterstützen, für Mitarbeiter eine Herausforderung darstellt: Fast die Hälfte (49 Prozent) der Arbeitnehmer schätzt, dass sie wöchentlich zwischen einer und fünf Stunden an Arbeitsproduktivität verlieren, weil sie sich mit IT-Problemen beschäftigen. Dennoch messen 42 Prozent der Arbeitgeber den Produktivitätsverlust aufgrund von IT-Problemen nicht. Mitarbeiter wollen dazu beitragen, die IT-Erfahrung zu verbessern.
www.unisys.com

Cyberbedrohungen 2023

Bedrohungen aus dem Internet bleiben, doch die Schwerpunkte ändern sich meist jährlich. Cyberkriminelle werden zunehmend Medien nutzen, um Unternehmen und staatliche Einrichtungen zu erpressen. Und im Darknet werden zudem Zugänge zu bereits kompromittierten Unternehmen angeboten.

Niels Gründel

Im vergangenen Jahr hat die Mehrzahl der Grossunternehmen einen Zuwachs an Cyberangriffen verzeichnet. Die Angriffe sind nicht nur ein Risiko für die eigenen Daten, sondern auch für den Ruf eines Unternehmens. Darauf scheinen die Angreifer zunehmend zu setzen. Experten prognostizieren für dieses Jahr, dass Cyberkriminelle gezielt Medien nutzen werden, um grosse Unternehmen und staatliche Einrichtungen zu erpressen. Dabei müssen nicht alle Datenlecks, über die berichtet wird, tatsächlich bestehen. Gerade weniger erfolgreiche Kriminelle werden behaupten, ein Unternehmen gehackt zu haben, da es dem genannten Unternehmen schadet und für Aufmerksamkeit sorgt. Im Darknet lassen sich immer häufiger Zugänge zu bereits kompromittierten Unternehmen erwerben und auch die Beliebtheit von Malware-as-a-Service (MaaS) sowie Angriffe über die Cloud dürften im Fokus künftiger Angriffe stehen. Ransomware-Akteure berichten in ihren Blogs zunehmend über erfolgreiche Hackerangriffe auf Unternehmen. Während Cyberkriminelle sich früher direkt an die Betroffenen wandten, um ein Lösegeld zu erpressen, schreiben sie häufiger in Blogs über die Sicherheitsverletzung und zeigen dort einen Countdown für die Veröffentlichung der durchgesickerten Daten an. Es ist naheliegend, dass sich dieser Trend voraussichtlich auch in diesem Jahr fortsetzen wird. Die Cyberkriminellen scheinen dabei in jedem Fall zu gewinnen, unabhängig davon, ob das betroffene Unternehmen zahlt oder nicht. Die Daten werden häufig versteigert und das Schlussgebot kann durchaus das geforderte Lösegeld übersteigen. Neben Angriffen auf Unternehmen werden Cyberattacken weiterhin für das gezielte Abgreifen persönlicher Daten gefahren. Öffentlich verfügbare E-Mail-Adressen können für Phishing und Social Engineering genutzt werden. Dies hat einerseits unmittelbaren Einfluss auf die Privatsphäre, andererseits kann dies ebenso die Sicherheit von

Unternehmen gefährden, wenn berufliche E-Mail-Adressen für Registrierungsprozesse an Websites von Drittanbietern genutzt werden.

Automatisierung der Angriffe steigt

Ransomware-Angriffe sollen durch Malware-as-a-Service-Tools insgesamt immer ähnlicher und die Angriffe dürften zudem immer komplexer werden, sodass automatisierte Systeme allein nicht mehr ausreichen, um eine umfassende Sicherheit für das eigene Unternehmen zu gewährleisten. Cyberkriminelle werden zunehmend künstliche Intelligenz (KI) einsetzen. Andererseits wird sie auch dabei helfen, entsprechende Angriffe abzuwehren, indem verdächtige Verhaltensmuster besser erkannt werden. Aktuell wird eine Vielzahl verdächtiger Aktivitäten festgestellt und führt zu einer hohen Zahl Fehlalarmen, sodass das zuständige Personal häufig überfordert ist. Ein weiterer Fokus wird auf die Cloud-Technologie gerichtet, da sie allein durch ihre Bedeutung für viele Unternehmen ein lohnendes Angriffsziel darstellt. Vor allem geopolitisch motivierte Angriffe auf die Cybersicherheit werden zur steigenden Gefahr. Insbesondere Russlands Angriff auf die Ukraine zeigt, dass Kriegsführung heute hybrid und die Risiken geopolitisch motivierter Cyberangriffe real sind. Im Jahr 2023 stehen in mehr als 70 Ländern Wahlen an, die häufig von staatlich unterstützten oder geduldeten Akteuren angegriffen werden. Ebenso real sind Cyberangriffe gegen kritische nationale Infrastrukturen. Wenn das Licht ausgeht oder das Gas abgestellt wird, werden wohl die wenigsten Menschen in Erwägung ziehen, dass dies auf eine Verletzung der industriellen Cybersicherheit zurückzuführen sein könnte. Aber auch die Operational Technology (OT) ist ein neues Schlachtfeld für Cyberangriffe. Die Systeme, die Fabriken und zivile Infrastrukturen – einschliesslich Kraftwerke und Staudämme – steuern und automatisieren, werden zur Zielscheibe. Eines ist sicher: Unternehmen sind zunehmend gezwungen, sich entsprechend schnell den Änderungen der Sicherheitslage anzupassen. Dennoch kann keine Organisation je zu 100 Prozent sicher sein. Ebenso wenig ist es möglich, Bedrohungen oder Cyberkriminelle zu kontrollieren. Aber jedes Unternehmen kann Prioritäten setzen und in geeignete Sicherheitsmassnahmen investieren, um möglichst gut vorbereitet zu sein und auf Vorfälle unmittelbar reagieren zu können. Es wird nicht immer möglich sein, Angreifer im Vorfeld zu stoppen. Daher ist es wichtig, Vorfälle unmittelbar zu untersuchen und direkt darauf reagieren zu können. Ein Angriff muss in jedem Fall in seiner Wirkung begrenzt werden.

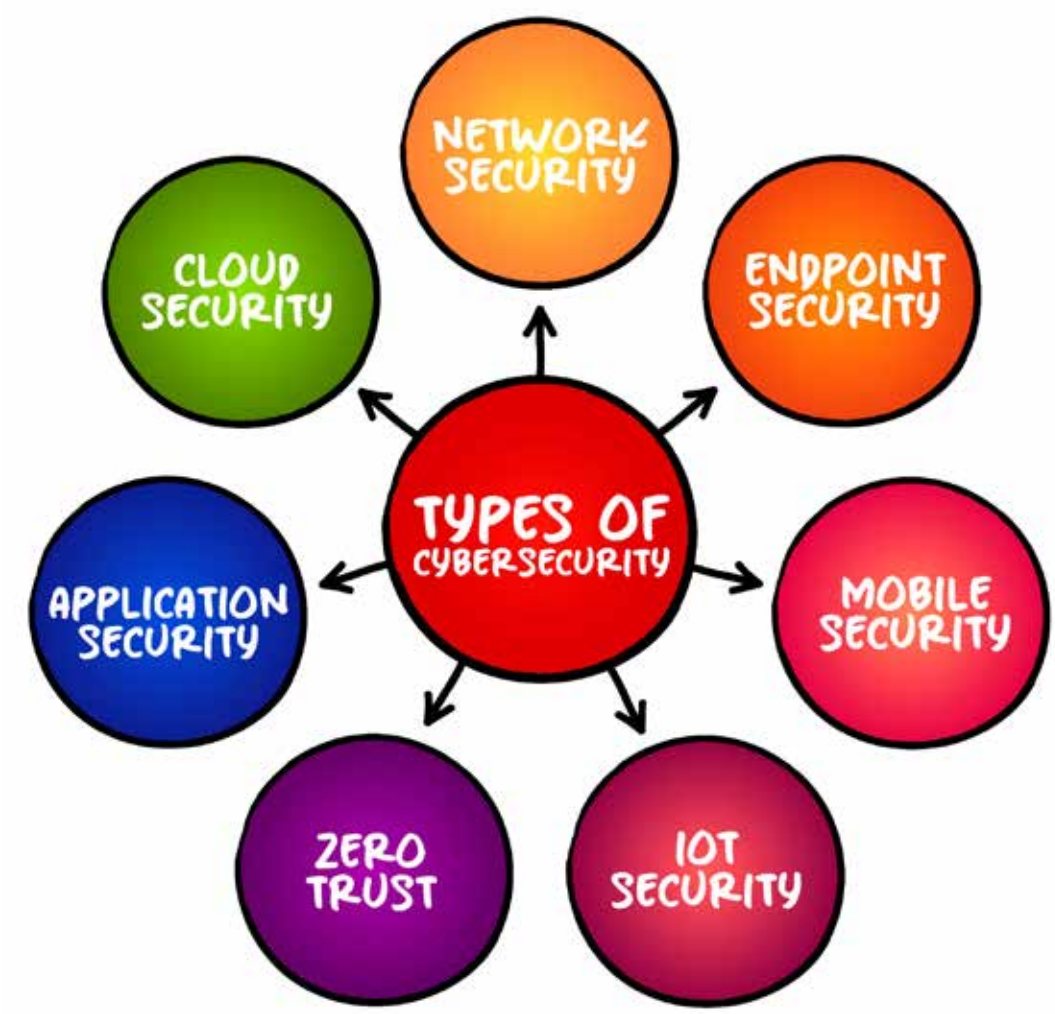
Eigene Vorkehrungen

Die Software aller Geräte sollte stets auf dem neuesten Stand sein, um zu verhindern, dass Angreifer Sicherheitslücken ausnutzen und in das Netzwerk eindringen. Verfügbare Patches müssen umgehend installiert werden, denn Angreifern reichen mitunter schon Zeitfenster weniger Stunden, um Schwachstellen für sich auszunutzen. Ein Threat Intelligence Service stellt dem eigenen IT-Team aus unterschiedlichen Quellen Daten zu Bedrohungen der eigenen IT-Systeme zusammen, damit es über die aktuellen Taktiken und Methoden der Cyberkriminellen informiert ist. Tritt ein Cybersicherheitsvorfall ein, so helfen Incident Response Services, darauf zu reagieren und die Folgen zu minimieren. Es ist sogar möglich, externe IT-Experten in Aktionspläne einzubinden, wenn sie im Vorfeld Kenntnisse der Unternehmensinfrastruktur erlangt haben, sodass im Ernstfall kein Onboarding mehr notwendig ist. ■

Sicherheit als grösstes Problem

Entgegen allgemeiner Erwartungen sehen KMU die globalen Entwicklungen, wie den Krieg in der Ukraine und die fortschreitende Arbeit aus dem Homeoffice nach Corona, nicht als das grösste Sicherheitsrisiko an. Vielmehr gilt das mangelnde Cyber-Bewusstsein ihrer Mitarbeitenden als gefährlichste Schwachstelle.

Niels Gründel



Kleine und mittlere Unternehmen (KMU) klagen über Bedrohungen durch Inflation, Digitalisierung, Fachkräftemangel und hohe Energiekosten. Doch das grösste Problem ist ein Mangel an Cybersicherheit. Ein IT-Security-Hersteller führte eine globale Cybersicherheits-Umfrage bei mehr als 1200 Unternehmen durch. Im Ergebnis zeigt sich eine tiefe Verunsicherung vieler Betriebe in puncto Sicherheit: Fast drei Viertel der Befragten fühlen sich aufgrund ihrer Grösse anfälliger gegenüber Sicherheitsrisiken als Grosskonzerne. Nicht einmal die Hälfte besitzt ein mittleres oder hohes Vertrauen in die eigene Cyber-Resilienz. Und 49 Prozent beklagen Budgetbeschränkungen oder fehlende Investitionen in die Cybersicherheit. Das mangelnde Cyber-Bewusstsein ihrer Mitarbeitenden ist mit 43 Prozent die gefährlichste Schwachstelle. Darüber hinaus werden Angriffe von staatlicher Seite mit 37 Prozent ebenfalls hoch eingeschätzt, ebenso wie Schwachstellen durch Schnittstellen zu Partnerunternehmen und Lieferanten mit 34 Prozent. Weniger überraschend werden auch das hybride Arbeiten (32 Prozent) und die Verwendung des Remote Desktop Protocol (31 Prozent) als Risiko eingestuft. Insgesamt unerwartet ist, dass das allgemeine Vertrauen der befragten Unternehmen in die eigene Cyber-Resilienz gering ist: Lediglich 48 Prozent der Befragten gaben an, ein mittleres oder hohes Vertrauen in ihre Gefahrenabwehr für die nächsten zwölf Monate zu besitzen. Die Unternehmensverantwortlichen fürchten vor allem Datenverluste, die zu schwerwiegenden finanziellen Einbussen führen können. Im vergangenen Jahr waren zwei Drittel der Befragten von einem Datensicherheitsvorfall

betroffen. Dessen Untersuchung dauerte in den meisten Fällen bis zu drei Monate. Die geschätzten Gesamtkosten beliefen sich im Durchschnitt auf fast 220 000 Franken. Während die befragten Entscheidungsträger über die möglichen Auswirkungen eines Angriffs besorgt sind, sahen 70 Prozent ein Ungleichgewicht zwischen Gefahrenpotenzial und Investitionen in die eigene Cybersicherheit; insbesondere haben Veränderungen der Betriebsmodelle wie das hybride Arbeiten zu wenig Aufmerksamkeit bekommen. In den kommenden zwölf Monaten erwarten die befragten Unternehmen Sicherheitsprobleme durch Malware (70 Prozent), webbasierte Angriffe (67 Prozent), Ransomware (65 Prozent), Sicherheitsprobleme durch Dritte (64 Prozent), Denial-of-Service-Angriffe (60 Prozent) und Angriffe über das Remote Desktop Protocol (60 Prozent).

Überwachung der Endpunktesicherheit

Für ein deutlich höheres Sicherheitsniveau können Endpoint Detection und Response-Lösungen (EDR) sorgen. Neben Schulungen der Zuständigen in der IT sinkt damit das Risiko deutlich, ein ernsthaftes Sicherheitsrisiko zu bekommen. Aktuell sind EDR-Lösungen nur bei etwa jedem dritten kleinen und mittleren Unternehmen angekommen. Es besteht daher noch viel Nachholbedarf. Entsprechende Lösungen verhindern Bedrohungen mit Funktionen, welche die gesamte Angriffskette überwachen. Sie identifizieren Bedrohungen frühzeitig, blockieren sie und begegnen Attacken so früh wie möglich. Diese fortschrittlichen Lösungen für die Endpunktsicherheit können auch hochentwickelte Bedrohungen in Echtzeit erkennen. Insbesondere Ransomware-Verschlüsselungsversuche sollen frühzeitig erkannt und verhindert werden.

EDR-Lösungen können mehr als herkömmliche Antivirenlösungen. Mithilfe von Machine-Learning- und Deep-Learning-KI-Modellen sollen sie vor Zero-Day-Angriffen, Ransomware, Cryptojacking und ähnlichen Angriffsszenarien schützen. In der Praxis werden beide Lösungen parallel eingesetzt: Während Antivirenlösungen signaturbasiert bekannte Bedrohungen erkennt, setzen EDR-Lösungen auf Verhaltensanalysen auf den Endgeräten. Damit können EDR-Systeme unbekannte Bedrohungen aufgrund eines abweichenden Verhaltens erkennen: Wird etwa eine bekannte Anwendung auf einem Endgerät durch einen Mitarbeitenden ausgeführt, so ist das per se ein gewöhnlicher und unbedenklicher Vorgang. Wird aber zugleich ein unbekanntes Skript gestartet, wird die EDR-Lösung die Datei markieren und unter Quarantäne stellen. Die meisten Systeme nutzen dafür das Sandboxing, sodass die Sicherheit gewährleistet wird, ohne das System des Nutzenden zu stören.

Im Ergebnis können EDR-Sicherheitssysteme Bedrohungen auf allen Endpunkten ausfindig machen. Angriffe und Bedrohungen können erkannt und in Echtzeit überwacht werden, während sie sich in der eigenen Netzwerkumgebung entwickeln. In Kombination mit anderen Sicherheitstools bietet sich die Möglichkeit für eine hohe Absicherung gegen potenzielle Cyberangriffe. Da die Lösungen auch aus der Cloud als Software-as-a-Service bezogen werden können, bleiben die Aufwendungen für Einrichtung, Betrieb und personelle Ressourcen überschaubar. ■

Homeoffice: Massnahmen für Datenschutz und Datensicherheit

Seit Corona hat das Homeoffice eine neue Bedeutung erfahren. Vor der Pandemie haben nur einzelne Arbeitnehmer – je nach arbeitsvertraglicher Regelung – im Homeoffice gearbeitet. Mit Eintritt der Pandemie kam erstmals eine Homeoffice-Pflicht vor, welche später in eine Homeoffice-Empfehlung umgewandelt wurde. Einige Unternehmen waren aufgrund ihrer IT-Einrichtung besser vorbereitet und haben ihren Arbeitnehmenden erlaubt, Büroeinrichtung wie z.B. Bildschirme auszuleihen und zu Hause zu benutzen, was zu einer Optimierung der Arbeitsplatzeinrichtung im Homeoffice geführt hat.

lic. iur. Ursula Sury

Mittlerweile ist die Situation wie vor der Pandemie und die Arbeitnehmenden sind zumeist zurück im Büro vor Ort. Unternehmen, welche sich zu Beginn kritisch über Homeoffice geäussert haben, dürften mittlerweile eingesehen haben, dass Homeoffice insbesondere bei denjenigen Arbeitnehmenden mit einem langen Arbeitsweg oder mit Familienpflichten Erleichterungen bringt. Aus Sicht der Arbeitnehmenden ist Homeoffice von Vorteil, da es unter anderem zu einer Zeiteinsparung führt. Schliesslich fällt der Arbeitsweg weg und diese Zeit kann vielfältig genutzt werden, sei es für Sport oder für einen kurzen Spaziergang in der Natur, was sich positiv auf die Gesundheit der Arbeitnehmenden auswirken kann. Schliesslich sind gesunde Arbeitnehmende leistungsfähiger, was einen positiven Effekt auf ihre Produktivität während der Arbeit haben dürfte.

Allgemeine und arbeitsrechtliche Vorkehrungen

Im Homeoffice ist die IT-Sicherheit von hohem Stellenwert und es sind diverse Sicherheitsvorkehrungen nötig. Der Arbeitnehmende hat sein WLAN zu Hause mit einem Passwortschutz zu versehen, um unberechtigte Zugriffe auf sein Netzwerk zu verhindern. Schliesslich ist der Passwortschutz des Arbeits-PCs auch im Homeoffice aufrechtzuerhalten, wobei diese Passwörter regelmässig zu aktualisieren sind. Ebenso ist sicherzustellen, dass der Zugriff ins Unternehmensnetzwerk nur via VPN erfolgt. Bei technischen Problemen muss den Angestellten bekannt sein, wen sie kontaktieren können.

Zudem sind Arbeitnehmende zur Wahrung von Berufs- und Geschäftsgeheimnissen verpflichtet. Dies bedeutet, dass sie vertrauliche Gespräche ausserhalb der Hörweite von anderen sich im Haushalt befindenden Personen führen müssen. Ebenso dürfen andere Personen keine Einsicht in Dokumente oder Daten mit Unternehmensrelevanz haben. Dies bedeutet zum Beispiel, dass auch im Homeoffice der PC beim Verlassen des Arbeitsplatzes zu sperren ist und physische Files sicher zu verstauen sind. Somit gilt die Clean Desk Policy auch im Homeoffice.

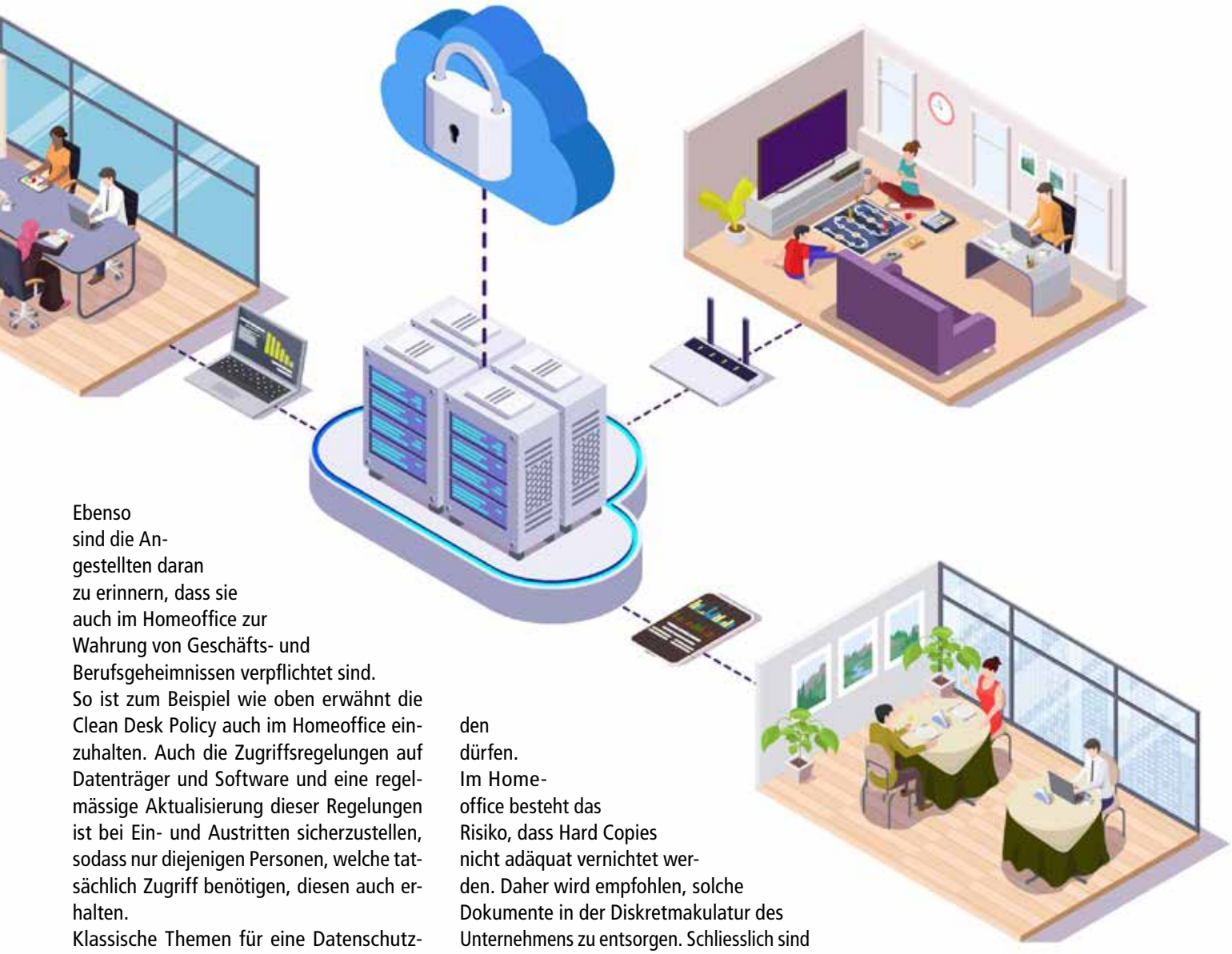
Die Abgrenzung zwischen Arbeitszeit und Freizeit kann im Homeoffice schwerer fallen, da sich der Arbeitsplatz in unmittelbarer Nähe befindet. Jedoch ist auch im Homeoffice sicherzustellen, dass die Arbeits- und Ruhezeiten eingehalten werden. Schliesslich soll mit der Ruhezeit eine echte Erholung des Arbeitnehmenden bezweckt werden.

Generell hat der Arbeitgeber gegenüber den Arbeitnehmenden eine arbeitsrechtliche Fürsorgepflicht, welche er – unabhängig vom gewählten Arbeitsort – sicherzustellen hat.

Schulungen im Bereich der Datensicherheit und des Datenschutzes

Das Unternehmen hat sicherzustellen, dass auch für die im Homeoffice befindlichen Personen Schulungen im Bereich des Datenschutzes und der Datensicherheit angeboten werden und diese auch auf ihre Situation zugeschnitten sind.

Klassische Themen für die Datensicherheit sind beispielsweise die Bekanntgabe der Kriterien für die Wahl von sicheren Passwörtern. Ebenso soll den Arbeitnehmenden anhand von Praxisbeispielen die Gefahr von Phishing sowie weiteren Cyberrisiken nähergebracht werden. Diese beginnt bereits beim Umgang mit E-Mails von unbekannten Absendern. Schliesslich ist die Verwendung von externen Datenträgern wie z.B. USB-Sticks zu regeln.



Ebenso sind die Angestellten daran zu erinnern, dass sie auch im Homeoffice zur Wahrung von Geschäfts- und Berufsgeheimnissen verpflichtet sind.

So ist zum Beispiel wie oben erwähnt die Clean Desk Policy auch im Homeoffice einzuhalten. Auch die Zugriffsregelungen auf Datenträger und Software und eine regelmässige Aktualisierung dieser Regelungen ist bei Ein- und Austritten sicherzustellen, sodass nur diejenigen Personen, welche tatsächlich Zugriff benötigen, diesen auch erhalten.

Klassische Themen für eine Datenschutzschulung sind nebst allgemeinen Informationen über den Datenschutz auch der Umgang mit besonders schützenswerten Personendaten. Dafür muss den Angestellten bekannt sein, welche Daten in die Kategorie von besonders schützenswerten Personendaten fallen. Schliesslich sind die Angestellten über die Bestimmungen der revidierten Datenschutzgesetzgebung zu informieren und es ist sicherzustellen, dass die Änderungen im Unternehmen vor dem Inkrafttreten, d.h. vor dem 1. September 2023, implementiert werden.

Zudem sollen Mitarbeitende ein Bewusstsein über den Lifecycle von Daten haben, dieser betrifft den Umgang mit Personendaten von der Erhebung der Daten bis hin zur Archivierung, Löschung und Vernichtung. Dazu gehört auch die korrekte Ablage der Daten am richtigen (und zugriffsgeschützten) Ort und das Bewusstsein der Angestellten, wann sie welche Daten und Belege wie lange archivieren müssen und wann diese vernichtet werden dürfen.

Im Homeoffice besteht das Risiko, dass Hard Copies nicht adäquat vernichtet werden. Daher wird empfohlen, solche Dokumente in der Diskretmakulatur des Unternehmens zu entsorgen. Schliesslich sind auch die Betroffenenrechte zu gewährleisten. Die Mitarbeitenden, welche Auskunftsgesuche bearbeiten, sind entsprechend zu schulen, um eine speditive Bearbeitung dieser Gesuche innert einer bestimmten Frist zu gewährleisten. Damit die Mitarbeitenden die vom Auskunftsgesuch erfassten Daten vollständig den Kunden mitteilen können, müssen sie wissen, wo überall im Unternehmen Kundendaten vorhanden sind. Dabei hat sich das Unternehmen dementsprechend zu organisieren, sodass die Daten rasch abgerufen werden können und ihre Vollständigkeit gewährleistet ist. Die Auskunftsgesuche werden zurzeit in der Regel auf dem Postweg beantwortet. Dies dürfte für eine Person im Homeoffice schwer fallen, sodass die Beantwortung durch einen Arbeitnehmenden vor Ort zu erfolgen hat, da diese Person schliesslich Zugang zu Logopapier etc. hat. Zudem ist der Ausdruck von Dokumenten im Homeoffice aus Sicherheitsgründen häufig eingeschränkt. Somit hat sich das Unternehmen dementsprechend zu organisieren, sodass die Beantwortung von Auskunftsgesuchen durch eine Person vor Ort erfolgen kann.

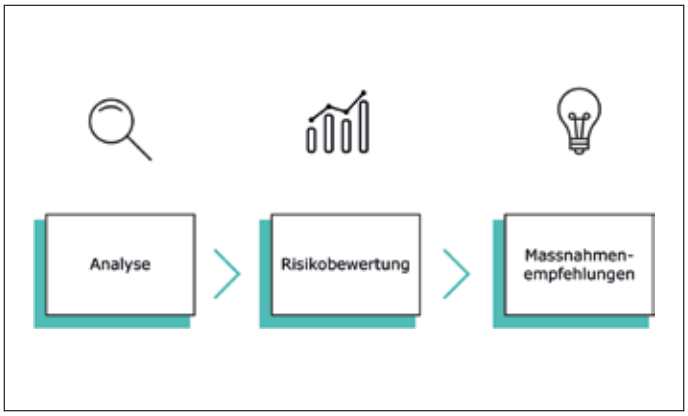
Fazit

Auch im Homeoffice sind die Regelungen bezüglich IT- und Datensicherheit und Datenschutz einzuhalten. Zudem sind die arbeitsrechtlichen Bestimmungen wie beispielsweise Arbeits- und Ruhezeit unabhängig vom gewählten Arbeitsort stets von Relevanz. Ausserdem hat der Arbeitgeber regelmässig Schulungen durchzuführen. Diese sind insbesondere auch für Arbeitnehmende, welche ihren Arbeitsplatz ausserhalb des Unternehmens haben, von Relevanz, da diese mit Homeoffice-spezifischen Risiken konfrontiert sind. Diese Risiken sind in den Schulungen zu berücksichtigen. ■

SAP-Schwachstellen frühzeitig erkennen

Unternehmen, die SAP nutzen, speichern häufig vertrauliche und geschäftskritische Daten in ihren SAP-Umgebungen. Um potenzielle Schwachstellen rechtzeitig zu erkennen, ist es wichtig, den Sicherheitslevel regelmässig zu prüfen. Dies setzt umfassendes Wissen voraus und kann Unternehmen vor einige Herausforderungen stellen.

Berechtigungen in einem SAP-System steuern benutzerbezogen die Zugriffsmöglichkeiten auf die Geschäftsdaten. Bei der Berechtigungsvergabe ist neben Auflagen, gesetzlichen Vorschriften und unternehmenseigenen Vorgaben auch ein restriktiver Umgang nach dem strikten Minimalprinzip einzuhalten. Auch bei SAP steht immer mehr die Sicherheit und die Reduktion – oder im besten Fall gar die Beseitigung – von Risiken im Fokus. Denn durch die Berechtigungsvergabe über Rollen können sich kritische Berechtigungen oder Berechtigungskombinationen ergeben, die man bei der Rollenzuweisung nicht vorhergesehen hat. Daher ist eine periodische Überprüfung der aktiven Benutzer, der zugewiesenen Rollen und natürlich auch der Systemeinstellungen in Form eines Security-Checks ratsam.



SAP Security Check – Sicherheitslevel prüfen

Sicherheitslücken wie beispielsweise zu umfangreiche Tabellenzugriffe oder eine schwache Password Policy (falls kein SSO im Einsatz ist) können potenzielle Schwachstellen in einem SAP sein, die erst durch Auditoren aufgedeckt werden. Mit einem SAP Security Check können Systeme, Daten und Prozesse bereits vor einem Audit auf Sicherheitsmängel untersucht und beseitigt werden. Der Check bildet die Grundlage für ein lückenloses SAP-Sicherheitskonzept. Diese Punkte werden unter anderem analysiert:

- Überprüfen der Rollen auf Qualitäts- und Sicherheitsstandards, beispielsweise Änderungsrechte in Anzeigerollen
- Kritische Berechtigungskombinationen wie Segregation of Duties-Konflikten bei Usern, damit ein einzelner User nicht zu viele Prozesse durchspielen kann wie beispielsweise Erstellen und Genehmigen einer Bestellung
- Vergabe von Profilen SAP_ALL/SAP_NEW an User (auch technische User)
- Systemabänderbarkeit der Mandanten überprüfen
- Passworteinstellungen (ein Passwort sollte den empfohlenen Richtlinien entsprechen), als Alternative kann auch Single Sign-on eingeführt werden
- Nutzung und richtige Konfiguration des Security Audit Logs, damit alle wichtigen Aktivitäten im System geloggt werden
- Aktive Tabellenprotokollierung, um Änderungen zu überprüfen
- Tabellenschutz mittels Berechtigungen, damit nur wenige User auch Tabelleneinträge ändern/löschen können
- Überprüfung potenzieller Zugriffe auf sensible Daten aus dem Personalwesen (wie z. B. Lohndaten und andere persönliche Daten)
- Überprüfung der technischen User, damit sie auch nur die benötigten Berechtigungen zugewiesen haben

Nach dieser Analyse ist eine Bewertung der Risiken aus den eruierten potenziellen Schwachstellen unabdingbar. Aus der Gesamteinschätzung der Analyseergebnisse resultieren dann Empfehlungen zu weiteren Massnahmen zur Schwachstellenbereinigung.

Was bringt es?

Eine regelmässige Systemprüfung deckt allfällige Mängel zeitnah auf und ermöglicht eine effiziente Umsetzung von Massnahmen. Damit werden Risiken verringert und kostspielige Konsequenzen vermieden. Das nächste Audit kann dann entspannt angegangen werden. ■

AVENIQ

Aveniq
Corina Aerni, Team Leader SAP Security Consulting
Bruggerstrasse 68, CH-5401 Baden
✆ +41 (0)58 411 77 77
info@aveniq.ch, www.aveniq.ch

Mit modularen Systemen den Beschaffungszyklus verlängern

Nachhaltigkeit gewinnt für Unternehmen immer mehr an Bedeutung, vor allem bei Technologie-Neuanschaffungen für mobile Mitarbeiter. Mit modular aufgebauten und individuell konfigurierbaren Tablets und Notebooks mit austauschbaren Akkus haben Unternehmen mehr von ihren IT-Investments.

Viele Unternehmen stecken in einem vierjährigen Beschaffungszyklus für die Technologien ihrer mobilen Mitarbeiter fest – trotz des zunehmenden Bewusstseins für Nachhaltigkeit und des Wunsches, Computergeräte länger zu nutzen. Das bestätigt eine Studie (https://info.business.panasonic.eu/sustainabilitygap-en.html) von Opinion Matters im Auftrag von Panasonic Toughbook unter 700 europäischen IT-Einkäufern aus unterschiedlichen Branchen.

Schritt zur mehr Unternehmensnachhaltigkeit

Es gibt Möglichkeiten, die Lebensdauer der von mobilen Mitarbeitern genutzten Geräte zu verlängern. Neben einem langjährigen Support durch die Hersteller ist dabei ein austauschbarerer Akku ein wichtiger Baustein. Denn oft scheitert die Nutzung mobiler Geräte bereits nach wenigen Jahren an einem defekten Akku, der sich nicht ausbauen und erneuern lässt. Im Gegensatz zu vielen anderen Herstellern bietet Panasonic seine Toughbook-Modelle (https://eu.connect.panasonic.com/de/de/toughbook-produktpalette) mit einem austauschbaren Akku an. Durch die Hot-Swap-Funktion können die Mitarbeitenden den Akku dieser mobilen Geräte sogar im laufenden Betrieb wechseln. Die robusten Toughbook-Geräte zeichnen sich ausserdem durch eine sehr lange Akkulaufzeit von rund 20 Stunden aus.

Die fünf wichtigsten Kriterien

Laut der Studie sind diese fünf Kriterien für IT-Einkäufer bei der Anschaffung von Geräten für mobile Mitarbeiter am wichtigsten: Sicherheit (23,7 Prozent), Zuverlässigkeit (23,7 Prozent), Leistung (22,9 Prozent), Akkulaufzeit (19,3 Prozent), Robustheit (18,7 Prozent) und Anschaffungskosten (18,3 Prozent). Das spricht für robuste mobile Geräte mit hoher Zuverlässigkeit und Leistung sowie einer langen Akkulaufzeit.

Nutzer in Entscheidungen einbinden

Überraschenderweise lässt die Hälfte aller IT-Einkäufer neue Computergeräte vor dem Kauf nicht von den späteren Nutzern testen. Dabei könnten und sollten sie durch die Einbindung der Mitarbeiter in Pilotprojekte vor dem Kauf sicherstellen, dass die Geräte tatsächlich auf die Bedürfnisse der Benutzer abgestimmt sind. Dies kann baldige weitere Neuanschaffungen verhindern.

Flexibilität durch modulare Konfigurationen

Mehr Nachhaltigkeit lässt sich auch durch mobile Computergeräte erzielen, die von den Endnutzern für verschiedene Einsatzszenarien vor Ort angepasst werden können. War ein Gerät für ein Projekt beispielsweise ein Jahr lang im Einsatz, kann es durch ein modulares Design anschliessend für einen anderen Zweck umfunktioniert werden. Beispielsweise ist das 12-Zoll-Notebook Toughbook 55 von Panasonic durch Expansion Slots sehr flexibel individuell konfigurierbar. Unter anderem lassen sich je nach Anwendungsfall Smart Card Reader oder eine zweite Batterie anschliessen. Ebenfalls sehr flexibel anpassbar ist das Toughbook G2, ein 10-Zoll-Tablet mit Erweiterungsbereichen für 20 mögliche Kombinationen. Durch diese Flexibilität und

die Möglichkeit, bei Bedarf aufzurüsten, haben Unternehmen die Chance, die Nachhaltigkeitslücke beim Kauf von Technologie für mobile Mitarbeiter zu schliessen. Die Kombination dieser Eigenschaften mit der leistungsstarken CPU- und Speicherleistung der neuesten Gerätegeneration ist ein weiterer Baustein für eine längere Lebensdauer mobiler Geräte. Hinzu kommt der langfristig erweiterte Support, der von Herstellern wie Panasonic angeboten wird. All diese Faktoren tragen dazu bei, dass Unternehmen den bisherigen Vier-Jahres-Zyklus für Technologie-Neuanschaffungen durchbrechen und die Nutzungsdauer ihrer mobilen Computing-Ausstattung verlängern können – in vielen Fällen um Jahre. ■

Panasonic Connect Europe GmbH
Niederlassung Rotkreuz, CH-6343 Rotkreuz
✆ +41 (0)41 203 20 19
www.toughbook.ch

Backup und Recovery in Zeiten von Ransomware

Eine funktionierende Strategie zur Datensicherung und -herstellung wird immer wichtiger, wenn nach einem Ransomware-Angriff die Systeme in einen funktionsfähigen Zustand zurückversetzt werden müssen.

Niels Gründel

Ausfallsicherheit und Verfügbarkeit sind ohnehin eine der höchsten Prioritäten für IT-Verantwortliche. Eine ständige Verfügbarkeit erwarten Kunden und Mitarbeitende. Am besten nachvollziehbar ist die Kundensicht für den Online-Handel: Fällt eine Webseite aus, wechseln die Kunden zur Konkurrenz, denn die ist in den meisten Fällen lediglich einen Klick entfernt. Die Abhängigkeiten von einer funktionierenden IT sind inzwischen immens. Denn auch im eigenen Unternehmen ist ein Stillstand mit Ausfallzeiten zahlreicher oder sogar aller Unternehmensteile gleichzusetzen. Fällt der IT-Betrieb aus, steht das Geschäft still, und das womöglich für immer. Das letzte prominente Beispiel ist der Velo- und E-Bike-Hersteller Prophete. Ein Cyberangriff löste einen mehrwöchigen Pro-

duktionsstopp aus. Die daraus resultierenden zusätzlichen Belastungen führten schliesslich zur Insolvenzanmeldung. Zahlreiche erfolgreiche Ransomware-Angriffe der letzten Jahre haben eindrücklich gezeigt, dass Behörden, Grosskonzerne, aber auch Unternehmen kritischer Infrastrukturen wie Energieversorger und Spitäler ins Visier der Erpresser geraten. Einen absoluten Schutz gegen erfolgreiche Hackerangriffe wird es trotz aller Bemühungen und Investitionen in die IT-Sicherheit niemals geben und so müssen Unternehmen entsprechend gut vorbereitet sein. Funktionierende Backup-und-Recovery-Strategien sind überlebenswichtig. Unternehmen jeder Grössenordnung benötigen einen funktionierenden Notfallplan, um die eigenen Systeme und Daten schnell wiederherstellen zu können. Gute Pläne und Strategien sind das eine, doch sie müssen in der Praxis auch funktionieren. Die Abläufe für Backups und Wiederherstellung müssen getestet werden, und dies regelmässig, weil Systeme und ihre Konfigurationen im Tagesgeschäft erfahrungsgemäss einem stetigen Änderungsprozess unterliegen. Bei entsprechenden Tests wird zugleich ermittelt, wie lange die Wiederherstellungsprozesse dauern. Anbieter von Backup-und-Recovery-Lösungen haben überwiegend automatisierte Funktionen in ihre Anwendungen integriert, sodass sich jederzeit in Echtzeit ablesen lässt, wie lange die Wiederherstellung bestimmter Daten dauert und welche Daten bei einem Totalausfall verloren gehen. Automatisierte Prozesse sind allerdings längst nicht die Regel. Der Aufwand für eine Wiederherstellung wird jedoch meist unterschätzt, denn Schäden durch Systemausfälle nehmen schnell ungeahnte Grössen an. Und Notfalltests werden oft vermieden, weil die Verantwortlichen vielfach ahnen, dass sie nicht gut genug vorbereitet sind. Es bedarf einer Strategie, die auch den schlimmsten anzunehmenden Fall abdeckt, dass es einem Angreifer innert kürzester Zeit gelingt, alle Systeme zu infizieren. Eine Cloud-Sicherung, die mit dem eigenen Unternehmensnetz verbunden ist, genügt deshalb alleine nicht.

Keine Sicherheit durch Cloud-Backup

Für Backups gibt es grundsätzlich drei wesentliche Varianten: «Differenzielles Backup», «Voll-Backup» und «Inkrementelles Backup».

Differenzielles Backup

Das «Differenzielle Backup» basiert darauf, den Zeitaufwand für die Datensicherung zu

optimieren, indem lediglich die Daten gesichert werden, die nach dem letzten vollständigen Backup neu entstanden sind oder sich geändert haben. Der Datenumfang einer entsprechenden Sicherung ist demzufolge eher gering, da sich im Verhältnis zum Gesamtdatenbestand nur wenige Daten ändern. Für eine vollständige Datenwiederherstellung werden nur zwei Sicherungsmedien benötigt, was zu einer schnellen Wiederherstellung führt.

Voll-Backup
Bei einem «Voll-Backup» werden sämtliche Daten gesichert, beispielsweise die eines Servers. Dadurch besitzt man ein aktuelles Backup des gesamten Systems zur Wiederherstellung in einem Datensatz. Für eine vollständige Datenwiederherstellung ist diese Variante die einfachste und sicherste Methode, allerdings mit dem Nachteil behaftet, dass die Anfertigung unverhältnismässig aufwändig ist, weil bei jedem Voll-Backup überwiegend dieselben Daten gesichert werden.

Inkrementelles Backup
Im Gegensatz dazu steht das «Inkrementelle Backup». Dabei werden nicht alle Daten gesichert, sondern lediglich neue und veränderte Daten in die jeweilige Sicherung aufgenommen. Dies führt zu schnellen und effizienten Backups mit dem Nachteil, dass sich die Datensicherungen auf viele Backups verteilen. Eine Wiederherstellung dauert daher erheblich mehr Zeit und es muss sichergestellt werden, dass die einzelnen Sicherungen in der korrekten Reihenfolge wiederhergestellt werden.

Unabhängig von der Backup-Variante haben für ein klassisches Backup Datenbänder inzwischen ausgedient. Inzwischen wird Datensicherungen auf Festplatten und vor allem in der Cloud der Vorzug gegeben. Das ist in Zeiten von Ransomware allerdings nicht ganz risikolos. Wenn Backups über das Dateisystem des Betriebssystems eines Backup-Servers zugänglich sind, können sie durchaus von Erpressungstrojanern verschlüsselt und damit wertlos werden. Mitunter gelingt es Hackern durch die Erlangung bestimmter Rechte, sogar grundsätzlich unveränderliche Dateisysteme zu verschlüsseln. Damit Sicherungen keinen Schaden durch Ransomware nehmen können, muss das Risiko entsprechend abgesenkt werden. Das gelingt, wenn es einen ausreichenden Abstand zwischen dem Ort der Daten und seinen Sicherungen gibt – sie dürfen sich nicht in demselben LAN befinden und auch die entsprechenden Server sollten ein anderes Betriebs- und Authentifizierungs-System nutzen.

Die Cloud als Backup-Lösung?

Viele Unternehmen setzen auf die Cloud als Backup-Lösung, da sie quasi unbegrenzten Speicherplatz bietet. Für stetig wachsende Datenmengen müssen im eigenen Unternehmen keine neuen Kapazitäten geschaffen werden. Die dazugehörigen Systeme sind meist einfach zu bedienen und lassen sich auch in unübersichtlicheren Umgebungen wie einem gemischten Betrieb lokaler Rechenzentren mit Public- und Private-Clouds einbinden. Die Auswahl an Cloud-Service-Providern ist gross und so haben Anwender grundsätzlich die freie Wahl. Die Zusammenarbeit mit einem einzigen Anbieter führt allerdings schnell zu Abhängigkeiten, auch wenn es im Betrieb einfacher ist. Durch den Vendor-lock-in ist ein Umzug zu einem anderen Anbieter schwerer zu realisieren, obwohl der Wechsel ab einer bestimmten Datenmenge prinzipiell aus wirtschaftlichen Gründen angezeigt wäre. Der Betrieb in der Multi-Cloud hat noch den weiteren Vorteil, dass das Risiko gesenkt wird: Auch die Cloud besteht aus physischen Rechenzentren, die nicht vollständig ausfallsicher sind: Hackerangriffe oder menschliches Versagen können sie ebenso ereilen; vor Naturkatastrophen sind auch sie nicht geschützt. Sind die Backups auf mehrere Anbieter an unterschiedlichen Standorten verteilt, steigt die Ausfallsicherheit und es sollte im Ernstfall stets ein funktionsfähiges Backup verfügbar bleiben. Zu den Vorteilen der Cloud-Nutzung zählt die Abrechnung nach Speicherplatz und Rechenzyklen für Workloads auf Basis der tatsächlichen Nutzung. Wer ein eigenes Rechenzentrum betreibt, wird daher vor allem Langzeit-Backups in eine günstige Cloud-Umgebung auslagern und kritische Daten immer auch lokal vorhalten, um sie möglichst schnell im Zugriff zu haben. Grundsätzlich bieten sich als Absicherung gegen eine erfolgreiche Ransomware-Attacke sogar die vielfach als veraltet geltenden Tapes an: Eine Reihe von Unternehmen gibt die physische Kontrolle ihrer Daten ohnehin nur ungern aus der Hand und vermeidet daher die Cloud. Datensicherungen auf Tapes lassen sich gut selbst verwalten und in einem Datensafe verwahren. Dort sind sie – abgesondert von allen elektronischen Systemen – sicher vor jedem Ransomware-Angriff geschützt.

Nicht einfach alle Daten sichern

Im Rahmen der Datensicherung gilt es, auch die Datenverwaltung näher zu betrachten. Vielfach wird erheblicher Aufwand betrieben, um Daten zu sichern, die es nicht wert sind, weil sie nie genutzt werden – eigentlich überflüssige Daten. Das bindet nicht nur Zeit und Ressourcen, sondern kostet am Ende Geld – sowohl bei allen Backups als auch einer etwaigen Wiederherstellung. Entsprechend überflüssige Daten, auch Dark Data genannt, sollten daher vor der Erstellung von Backups identifiziert und ausgelassen werden. Grundsätzlich können «Dark Data» wertvoll für ein Unternehmen sein. Solange sie allerdings in unstrukturierter Form vorliegen, lassen sie sich nicht für Analysen nutzen und bleiben damit von unschätzbarem Wert und zugleich wertlos. Diese Daten zu sichern, bindet unnötige Ressourcen, weil (absehbar) kein Wert aus ihnen gezogen wird. Es ist daher sinnvoll, Daten zweckgebunden zu speichern und sie sinnvoll zu verschlagworten und auszuzeichnen. So lassen sich Regeln für die Aufbewahrung definieren und irrelevante Daten können risikolos gelöscht werden. Auf Dauer steigt die Qualität der Daten für das eigene Unternehmen und der Umfang von «Dark Data» nimmt anteilig ab. Eine Festlegung für alle (kritischen) Anwendungen und Dienste definiert, wie viel Zeit vergehen darf, bis sie wieder verfügbar sind; diese Zeitspanne beschreibt die «Response Time Objective». Darüber hinaus beschreibt das «Response Point Objective», wie viele Daten in dieser Zeit verloren gehen dürfen. Für beides müssen innerhalb des Unternehmens durch die Verantwortlichen realistische Festlegungen erfolgen, die in der Folge auch erreicht werden müssen. Der zugrunde liegende Plan führt alle Massnahmen auf, mit denen die Festlegungen erreicht werden. Die Verantwortlichen setzen dabei im Idealfall auf weitgehend automatisierte Prozesse. Es ist naheliegend, dass Menschen unter Stress eher Fehler unterlaufen als einer Maschine. Und menschliche Fehler können am Ende dazu führen, dass Wiederherstellungsprozesse vollständig scheitern. ■

Cyberangriffe: Wie Unternehmen im Ernstfall reagieren sollten

Cyberangriffe werden in der Schweiz auch 2023 weiter zunehmen. Dabei gilt Ransomware weiterhin als eine der grössten Bedrohungen für Schweizer Unternehmen. Längst stellt sich nicht mehr die Frage, ob ein Unternehmen Opfer eines Ransomware-Angriffs wird – sondern wann. Doch worauf müssen Unternehmen achten, wenn sie Opfer einer solchen Attacke werden? Die TIM Storage Solutions AG zeigt auf, worauf Verantwortliche in der «Stunde Null» nach einem Angriff achten sollten.

Wie eine Studie von Cisco zeigt, machten Ransomware-Attacken allein in der Schweiz im Jahr 2022 rund 20 Prozent der registrierten Angriffe aus. Dabei haben die Angreifer im vergangenen Jahr gezielt Bildungseinrichtungen wie Schulen oder Universitäten ins Visier genommen. Die TIM Storage Solutions AG erklärt, wie Unternehmen bei einem Ransomware-Angriff richtig reagieren sollten. Vor allem das Timing spielt dabei eine entscheidende Rolle. Gemeinsam mit Veritas Technologies unterstützt der erfahrene Distributor seine Kunden dabei, die Datensicherheit in ihren Cloud-Umgebungen zu verbessern.

Viele Cyberkriminelle haben ihre Angriffsmethoden in den letzten Jahren ständig weiterentwickelt. Dadurch werden ihre Angriffe immer gefährlicher. Insbesondere Ransomware-as-a-Service (RaaS) wird immer beliebter und bereitet den internationalen Behörden Sorgen. Dabei bieten professionelle Hacker ihre Schadsoftware als Dienstleistung für Kriminelle an, die nicht die Kapazitäten oder Kompetenzen haben, solche Programme selbst zu entwickeln. Nach einem erfolgreichen Angriff ist vor allem die erste Stunde entscheidend, um sowohl die finanziellen Risiken zu minimieren als auch die Reputation des Unternehmens zu wahren. Daher sollten in der ersten Stunde zwei entscheidende Massnahmen umgesetzt werden: Die infizierten Systeme müssen isoliert werden, um eine weitere Ausbreitung des Schadcodes zu verhindern, und die Ursache des Angriffs muss ermittelt werden.

Sorgfältige Vorbereitung, kontinuierliche Schulung und umfassende Datentransparenz sind dabei hilfreich. Diese Schritte sollten jedoch bereits vor dem Angriff im Unternehmen umgesetzt worden sein, um die betroffenen Systeme so schnell wie möglich zu identifizieren. Das Hauptziel eines jeden Cyberangriffs sind unternehmenskritische Daten. Daher ist es wichtig, stets den Überblick und die Kontrolle über den Datenbestand zu behalten. So kann sichergestellt werden, dass Informationen nach einem erfolgreichen Angriff schnell wiederhergestellt werden können.

Der Zeitpunkt ist entscheidend

Um den Schaden so schnell wie möglich zu begrenzen, zählt jede Minute. Datenmanagement-Tools ermitteln, auf welche Daten welche Benutzer zugreifen. Anhand dieser Informationen lässt sich feststellen, welche Daten infiziert sind oder fehlen. Wurden die Daten des Unternehmens ordnungsgemäss gesichert, können die Informationen problemlos wiederhergestellt werden, ohne dass es zu Betriebsunterbrechungen kommt oder Lösegeld gezahlt werden muss. Mit einer automatisierten Datenverwaltung lassen sich unterschiedliche Workloads und Daten effizient und sicher verwalten. TIM unterstützt Kunden mit «NetBackup» von Veritas. Die Plattform bietet eine hochgradige Automatisierung sowie die Integration in Legacy-Systeme und virtuelle Umgebungen für die meisten Workloads auf dem Markt – On-Premise sowie in der Cloud. Die erfahrenen Consultants von TIM und Veritas beraten gerne – auch bei individuellen Anforderungen. ■

TIM IT Distribution

VERITAS

TIM Storage Solutions AG
Oberneuhofstrasse 3, CH-6340 Baar
✆ +41 (0)41 521 70 00
tim@tim-vad.ch, www.tim-vad.com

Moderne ERP-Systeme – mit eingebauter KI?

ERP-Systeme werden intelligenter, weil nach und nach Mechanismen des «Machine Learning» eingebaut werden. Diese KI automatisiert die Routineprozesse, schafft effizientere Workflows und verwertet einmal erfasste Daten besser. Die interaktive Unterstützung, etwa durch automatische Chatbots, wird so ausgefeilt, dass auch gelegentliche Nutzer oder sogar Kunden und Lieferanten mit dem ERP-System arbeiten können.

Berthold Wesseler

Die Technologien der «Künstlichen Intelligenz» (KI) – und hier insbesondere das «Maschinelle Lernen» – können Behörden und Unternehmen aller Branchen klare Vorteile bringen. Auch das ERP-System, also der digitale Prozess- und Datenhub, wird daher zunehmend mit KI angereichert.

«Bis dato sind jedoch die Zahl der Anwendungsfälle im ERP-Umfeld und das Angebot der ERP-Anbieter im Bereich KI noch überschaubar», schrieb der deutsche Branchenverband Bitkom noch 2019 in seinem nach wie vor aktuellen Positionspapier «Künstliche Intelligenz und ERP». Dabei gäbe es viele attraktive Einsatzfelder: So könnten KI-gestützte Datenanalytik, Prognosesysteme, Suchmaschinen, maschinelle Übersetzungen, Bots und wissensbasierte Expertensysteme Einzug in bestens bewährte Geschäftsanwendungen halten, wobei sich dadurch die ERP-Landschaft deutlich verändere.

Auch heute ist es längst noch nicht so weit – weder bei den Mittelständlern noch bei den einschlägigen Software-Anbietern. Nach wie vor prägen vielmehr einzelne innovative Pilotprojekte das Bild rund um KI im mittelständischen ERP-System. Das zeigt auch eine Recherche nach beispielhaften Referenzprojekten. «Wir haben seit Kurzem ein Analytics-Modul, das in Teilbereichen auf Machine Learning zurückgreift. Allerdings ist unser Pilotkunde leider noch nicht reif für eine Referenz», heisst es von einem ERP-Hersteller, der lieber anonym bleiben möchte.

Erste KI-Angebote stossen auf wenig Nachfrage

Ganz ähnlich wurde die Anfrage von einem renommierten Microsoft-Partner beantwortet: «Als Anbieter von Branchenlösungen im ERP-Markt für diverse Wirtschaftszweige […] betreiben wir keine komplette Eigenentwicklung, sondern setzen mit unseren Branchenerweiterungen auf der international bewährten Plattform Microsoft Dynamics 365 Business Central an. Microsoft hat in die Software an einigen Stellen bereits KI-Funktionen eingebaut. Diese nutzen wir bisher allerdings noch nicht in unseren Erweiterungen, da von Kundenseite diesbezüglich noch keine Anforderungen an uns gestellt wurden.»

Allerdings werben Pioniere unter den mittelständischen ERP-Anbietern inzwischen sogar mit KI, wobei sie nicht immer selbst

entwickeln. Die auch in der Schweiz aktive Tochter eines amerikanischen ERP-Herstellers beispielsweise erweitert ihr Portfolio um eine KI-gestützte Spend-Analytics-Lösung eines spezialisierten Softwarehauses und eröffnet so die Möglichkeit, Einkaufsdaten differenziert nach Kriterien wie Lieferanten, Warengruppen, Organisationseinheiten sowie Transaktionen automatisiert zu analysieren. Diese Kombination in Einkaufs- und Finanzorganisationen soll sowohl Ausgabentransparenz als auch die Kostenstrukturen nachhaltig optimieren.

Ein polnischer ERP-Hersteller verweist auf eine IDC-Studie, die prophezeit, dass Nutzungsrate von KI in den kommenden 24 Monaten rasant steigen werde. Der Grund dafür: Heute sind Unternehmen mit der doppelten Herausforderung konfrontiert, denn alles muss schneller werden bei gleichzeitig steigender Komplexität. Wer es schafft, hier anzusetzen, kann gleich auf mehreren Ebenen wichtige Vorteile erzielen: Kostensenkung, Zeitersparnis durch schnellere Abläufe, Qualitätssteigerung und mehr Nachhaltigkeit. Zudem wird auch der Kundenservice durch Automatisierung auf ein neues Level gehoben.

Mittlerweile sind auch die Ansätze verfügbar, um Probleme ganzheitlich mit modernen Prozessplattformen – z.B. Chatbots, Social Bots oder Avataren – zu lösen. Gleichzeitig hat auch der Individualisierungsbedarf zugenommen, weil der Markt immer kleinere Ausprägungsmengen wünscht und die Kunden das Bedürfnis nach immer individuelleren Lösungen haben.

Der Schweizer Detailhändler Coop nutzt bereits seit über zehn Jahren das sogenannte Sales-Based-Ordering, dessen Algorithmen laufend weiterentwickelt werden. Dabei kommt u.a. auch KI zum Einsatz sowie Advanced Analytics beispielsweise, um die Sortimente zu optimieren; neuronale Netze kommen dagegen bisher noch seltener zum Einsatz. Coop nutzt aber zum Beispiel eine KI-Lösung, um die Bestandsmengen in den vielen Läden zu plausibilisieren.

KI schätzt Werte

In der Tat gibt es auch schon erste Mittelständler, die in der Praxis mit KI experimentieren. So der Juwelier Eppli, der mit rund 70 Mitarbeitern in drei Auktionshäusern Vintage-Luxusobjekte verkauft – auch online und auch in die Schweiz. Dabei handelt es sich um exklusive «Pre-owned Stücke mit Echtheitsgarantie»; versteigert werden mehr als 25 000 Artikel pro Jahr.

Gerade im Markt für Luxusgüter steigt die Nachfrage nach professionellen Bewertungen, Wertschätzungen und Gutachten, sodass der Bedarf nach einer Effizienzsteigerung immer grösser wird. Bislang erfolgen die Bewertungen durch Experten. Sie sind damit sehr zeit- und kostenintensiv, was für die veräussernden Schmuckbesitzer oft undurchsichtig und daher mit Misstrauen verbunden ist.

Eine KI-basierte Lösung soll diese Prozesse nun beschleunigen, transparenter gestalten und optimieren. «Wir haben erkannt, dass KI viele Möglichkeiten zur Prozessoptimierung bieten kann, und möchten diese Chance aktiv für unser Unternehmen nutzen», erklärt Geschäftsführer Ferdinand Eppli. Gemeinsam mit einem Haus mit KI-Expertise strebt er im ersten Schritt die Entwicklung eines funktionsfähigen Prototyps an – und später eine sinnvolle Kommerzialisierungs- und Markteinführungsstrategie für die gemeinsam geschaffene Lösung.

Garbage in, garbage out

In der Praxis gibt es aber trotz solcher Pioniere beim Thema KI und ERP nach wie vor ganz erheblichen Nachholbedarf, vor allem dann, wenn Prognose-Tools bei der Entscheidungsfindung helfen sollen. Denn sind die Eingangsdaten schlecht, so werden auch die Analyse- und Prognose-Ergebnisse dürftig sein. Hier gibt es für die IT-Abteilungen noch sehr viel zu tun, bevor KI im ERP-System nützlich sein kann, denn kritische Faktoren für das Gelingen eines KI-Projekts – besonders beim maschinellen Lernen – sind Qualität und Anzahl der Datensätze für das Training des KI-Systems.

Dabei kann das Modell immer nur so gut sein wie der Input an «sauberen» Daten, mit dem es angelernt wird. Im ERP-Kontext sind aber meistens viel weniger Datensätze (Kunden, Aufträge, Planungsperioden, Artikel etc.) zum Trainieren einer KI verfügbar als bei klassischen Big-Data-Szenarien, z. B. Sensoren-Logs von Maschinen für «Predictive Maintenance». Mittelständische Maschinenbauer mit einer überschaubaren Kundenzahl werden daher kaum den Aufwand betreiben, eine KI für verlässliche Absatzprognose zu trainieren, sondern sich guten Gewissens auf ihr «Bauchgefühl» verlassen. Hingegen können dort Lager oder «Smart Factory» durchaus vielversprechende Einsatzfelder für «intelligente» ERP-Systeme sein.

Ohne Daten keine Analyse

Das wird zum Beispiel in der von IDC und einem US-Softwarehaus veröffentlichten Studie «AI in Manufacturing» deutlich, für die im April 2021 insgesamt 650 leitende Mitarbeiter von Unternehmen der Fertigungsbranche in Europa und den USA befragt wurden. Die Studie untersucht die gegenwärtigen digitalen Reifegrade der Unternehmen, die Investitionsprioritäten im Hinblick auf Smart-Factory-Projekte und bereits bestehende Anwendungsfälle von KI in der Produktion. Demnach wächst das Interesse an KI-fähigen und datengestützten Anwendungsszenarien. Beispiele für solche Anwendungsfälle sind die videobasierte Anomalieerkennung, autonome Transportfahrzeuge oder die digitale Abbildung von Fertigungsprozessen.

Die Umfrage zeigt aber auch, dass bislang nur durchschnittlich 34 Prozent der Fertigungsanlagen vernetzt sind. Und: Die IT-Abteilung ist hier sehr gefragt, denn 32 Prozent der Mitarbeiter in Fertigung und Lieferketten haben keine oder nur geringe Kenntnisse zu prädiktiven Analysen und Datenanalytik einschliesslich KPI-Dashboards (25 Prozent).

In der Realität ist eine KI kein fertiges Programm, das sich auf Knopfdruck installieren lässt. Selbst bei scheinbar sehr generischen Aufgaben stossen KI-Systeme meist schnell an Grenzen: Bei der Umwandlung von Sprache in Text beispielsweise müssen Fachbegriffe oder Produktnamen erst antrainiert werden, weil eine generische KI mit diesen Worten nichts anfangen kann.

Das jeweilige Modell muss also mit den Daten aus der Praxis trainiert werden. Je spezifischer die Aufgabe wird, die KI bewältigen soll, desto aufwendiger werden Aufbereitung und Normalisierung der Daten – und damit dauert der Lernprozess länger. Denn es ist ja so: Jedes Unternehmen nutzt andere Merkmale und Begriffe, die in das KI-Modell eingebunden werden müssen. Auch die Aussagekraft einzelner Parameter sollte, am besten im Rahmen einer Vorstudie, gründlich untersucht werden. Dabei gilt es, auch nachgelagerte Qualitätssicherungs-Massnahmen einzubeziehen. Schnell resultiert daraus ein umfangreiches, sich kontinuierlich weiter entwickelndes KI-Projekt, bei dem dann aber 80 bis 90 Prozent des Aufwandes aus der Auswahl, dem Bereinigen und dem Normalisieren von Daten entsteht. ■

ERP-Branchenlösungen im SaaS-Betrieb

Schnelle Bereitstellung, einfache Skalierbarkeit, automatische Updates, kurze Time-to-Value und branchenspezifische Prozesse: Kumavision kombiniert Vorteile von ERP-Branchenlösungen und SaaS zu attraktiven Angeboten für den Mittelstand.

Unternehmen müssen heute nicht nur effizient arbeiten, sondern vor allem auch agil und anpassungsfähig sein. Denn nur wer in der Lage ist, schnell auf geänderte Rahmenbedingungen zu reagieren, bleibt wettbewerbsfähig. Langwierige ERP-Einführungsprojekte lassen sich mit der geforderten Agilität nicht vereinbaren. Der Microsoft-Partner Kumavision hat daher ein umfassendes Portfolio an ERP-Branchenlösungen entwickelt, die als SaaS-Angebot bereitgestellt werden. Da das Unternehmen sich um den Betrieb, die Weiterentwicklung, Updates und die Wartung kümmert, profitieren SaaS-Kunden von kürzeren Innovationszyklen, einer nachhaltigen Entlastung der eigenen IT-Abteilung und letztlich auch von niedrigeren Gesamtkosten. Gleichzeitig arbeiten sie stets mit einer aktuellen ERP-Software und erhalten kontinuierlich Zugriff auf neue Funktionen und Technologien. Langwierige Update-Projekte entfallen, da die SaaS-Lösungen im Hintergrund automatisch regelmässig aktualisiert werden.

ERP-Branchensoftware mit Best-Practice-Prozessen

Jede Branche ist anders, jede Branche hat eigene Anforderungen. Das SaaS-Angebot umfasst ERP-Branchenlösungen, die optimal auf die Besonderheiten der jeweiligen Branche abgestimmt sind. Kumavision hat dazu die Basis Microsoft Dynamics 365 Business Central um zahlreiche branchenspezifische Funktionen erweitert. Den Kunden steht dabei eine Vielzahl an Best-Practice-Prozessen zur Verfügung, Unternehmen profitieren so von echten Mehrwerten für ihr Business und einer kurzen Time-to-Value: Langwierige und kostspielige Anpassungen sind mit diesem Konzept nicht mehr erforderlich. Die SaaS-Lösungen lassen sich mit Apps aus dem Microsoft AppSource und individuellen Extensions flexibel erweitern. Zusätzlich können Unternehmen die zahlreichen Business-Anwendungen der Technologieplattform Microsoft Dynamics 365 einfach integrieren.

Die SaaS-Lösungen sind einsetzbar in folgenden Bereichen:

- Maschinen- und Anlagenbau sowie Serienfertiger (factory365)
- Grosshandel (trade365)
- Projektdienstleister und Ingenieurbüros (project365)
- Medizinprodukte-Hersteller und -Händler (medtec365)

Schnelle Einführung mit Smart Start

Smart-Start-Pakete vereinfachen und beschleunigen mit zahlreichen Templates und Vorlagen den Umstieg auf eine SaaS-Lösung nochmals. Die ERP-Lösungen sind dabei anwendergerecht vorkonfiguriert, Unternehmen können schnell produktiv arbeiten. Dienstleistungspakete mit einem klar definierten Leistungsumfang und transparenten Preisen machen die Projekteinführung sicher kalkulierbar.

Bereit für die digitale Transformation

SaaS-Projekte sollten die vorhandene IT-Landschaft nicht einfach 1:1 abbilden, sondern sowohl die IT-Strategie als auch die Unternehmensstrategie berücksichtigen. Wie bei jedem Software-Projekt empfiehlt es sich, bei dieser Gelegenheit die eigenen Prozesse auf den Prüfstand zu stellen. Unternehmen müssen diese Schritte jedoch nicht allein gehen. Das Digitalisierungsteam der Kumavision unterstützt und begleitet mit Beratungsangeboten und Dienstleistungspaketen zu IT-Architektur, Digitalisierungsstrategie und Prozessoptimierung.

Maximale Zukunftssicherheit

Als einer der weltweit grössten Partner für Microsoft Dynamics 365 bildet Kumavision mit über 900 Mitarbeitern die gesamte Microsoft Technologieplattform ab. Neben ERP zählen dazu CRM-Lösungen für Vertrieb, Marketing und Service, Business-Intelligence-Anwendungen mit Microsoft Power BI, Dokumentenmanagement (DMS), Workflow-Lösungen, mobile Business Apps, Office- und Collaboration-Lösungen sowie Cloud-Services für IoT und vieles mehr. ■

Kumavision AG, CH-8600 Dübendorf
✆ **+41 (0)44 578 50 30**
schweiz@kumavision.com
www.kumavision.ch

Neugestaltung der Arbeitsplätze verändert die Jobprofile

Die Digitalisierung transformiert nicht nur die Wirtschaft, sondern auch die am Arbeitsmarkt geforderten Qualifikationsprofile vieler Jobs. Innovative Technologien, sich rasch verändernde Erwartungen der Kunden – die Unternehmen, ihr Management und ihre gesamte Belegschaft sehen sich durch die Digitalisierung vor grosse, vielfältige Herausforderungen gestellt. Auf der anderen Seite wollen die Unternehmen gleichzeitig auch neue Chancen in der digitalen Zukunft wahrnehmen. Aber was heisst das Zauberwort Digitalisierung konkret, was genau sind die konkreten Auswirkungen auf die Gestaltung der Arbeitsplätze und Jobprofile?

Berthold Wesseler

Eines ist klar: Digitalisierung ist alles andere als ein neues Phänomen, sorgt sie doch schon seit rund 30 Jahren für einen gravierenden Wandel von Geschäftsprozessen, Kommunikationswegen und damit letztlich auch Arbeitsplätzen und Jobprofilen. Letztlich handelt es sich beim Zeitalter der Digitalisierung um den 5. Kondratieff, also um die fünfte Welle in dem vom russischen Wirtschaftswissenschaftler Nikolai Kondratieff im Jahre 1926 erstmalig beschriebenen Modell einer in langen Wellen verlaufenden Weltkonjunktur mit abwechselnden Hochs und Tiefs. In den letzten Jahren kamen jedoch einige Faktoren hinzu, die der digitalen Veränderungsgeschwindigkeit zusätzlichen Schub gaben: Zunächst das Internet, dann mobiles Internet und das «Industrial Internet of Things» (IIoT) und zuletzt vor zwei Jahren Corona – mit den bekannten Folgen wie zum Beispiel Homeoffice oder «Distance Learning».

Die resultierenden Fortschritte bei der digitalen Vernetzung und Kommunikation haben eine der bisher rasantesten Transformationen von Gesellschaft, Kunden, Märkten und Arbeit ausgelöst. Etliche Experten sprechen in diesem Zusammenhang gar von einer digitalen Revolution, also nicht mehr nur von Digitalisierung bzw. digitaler Transformation. Dieser Wandel hat gravierende Auswirkungen gerade auch auf die Weiterbildung in IT-Themen.

Allerdings richten nicht alle – vor allem nicht alle mittelständischen – Arbeitgeber genügend Augenmerk auf die Weiterbildung ihrer Mitarbeiter, speziell auch im IT-Bereich. In der Wahrnehmung von Experten gehen gerade die mittelständischen Unternehmer sehr unterschiedlich vor. Manche sehen Weiterbildung als «ungeliebtes Muss», andere hingegen als «geliebtes Must-Have», um die Belegschaft und damit das eigene Unternehmen fit zu machen bzw. zu halten für die Herausforderungen des Marktes.

In den letzten Jahren ist zudem vermehrt eine Professionalisierung des Bildungsmanagements zu beobachten. Dazu gehört beispielsweise die strategische Ausrichtung der Bildungsmassnahmen, die zu einer positiveren Wahrnehmung beim Management führt. Gleichzeitig sehen wir, dass Lernen und Arbeiten zusammenwachsen. Lernen wird im Idealfall sogar zum strategischen Erfolgsfaktor – und zwar dann, wenn alle Mitarbeiter sowohl permanent als auch im «Moment of Need» die Möglichkeit geben, sich Wissen anzueignen. Es gilt also, das Training zu den Lernwilligen zu bringen und nicht umgekehrt. In diesem Zusammenhang haben viele mittelständische Unternehmer erkannt, Lernen ganzheitlich zu denken und digitale wie analoge Lernformate miteinander zu verbinden.

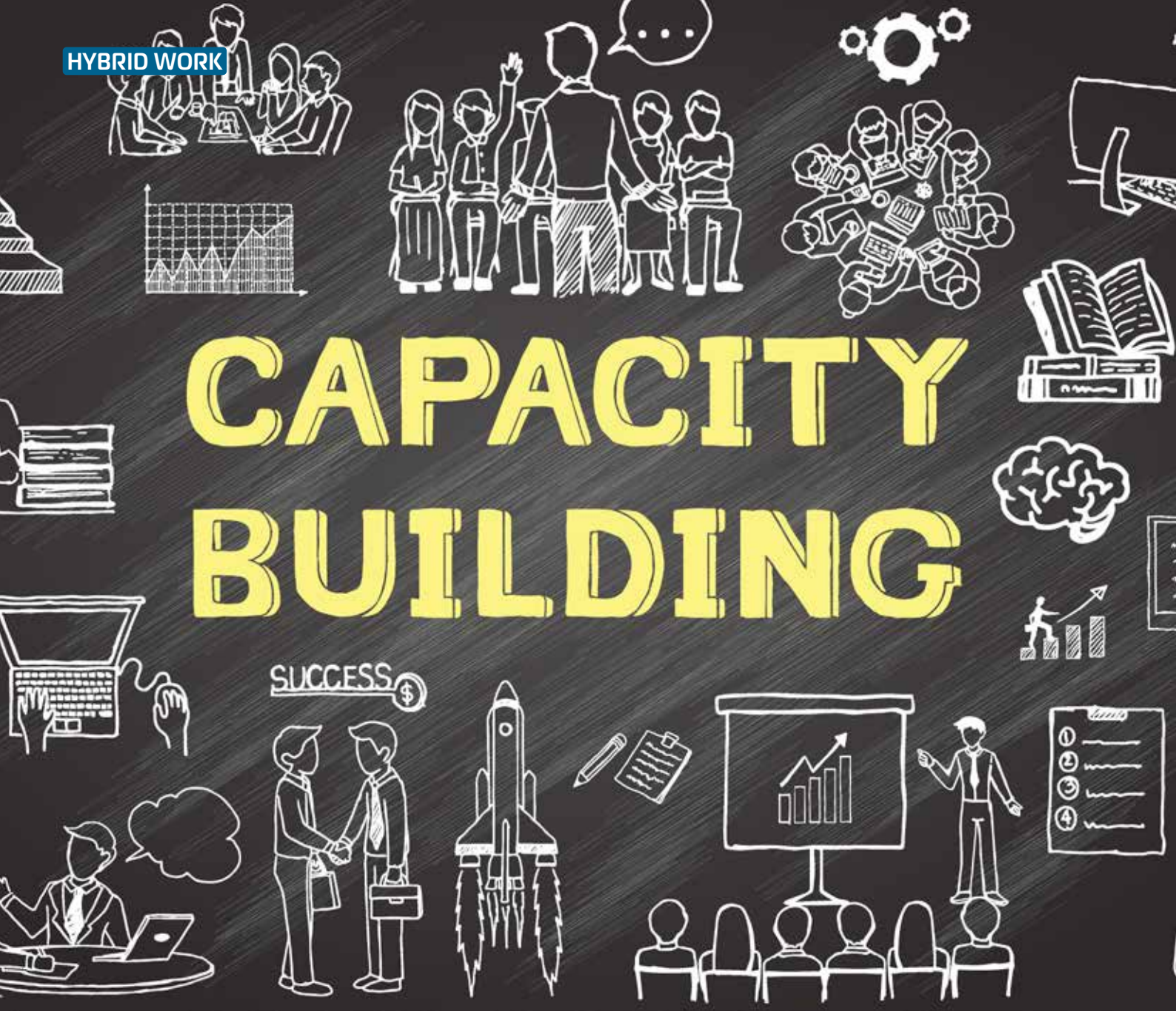
Stichwort «Moment of Need»: Gerade im Kontext von IT-Schulungen liegt es ja förmlich auf der Hand, dass «Lernen auf Vorrat» nicht gut funktioniert. Es macht mehr Sinn – kontextsensitiv und im Sinne eines guten Performance Supports – kleinere und grössere «Weiterbildungs-Häppchen» digital anzubieten, die der Belegschaft bedarfsorientiert zur Verfügung stehen. Mittelständische Unternehmen können so ganz pragmatisch auch sehr innovative Lernkonzepte umsetzen. Das ist wichtig, denn gerade mittelständische Unternehmen sind auf die Fort- und Weiterbildung ihrer Beschäftigten angewiesen, weil die digitale Transformation immer neue Berufsbilder schafft und rasch andere Anforderungen an die Kompetenzprofile der Beschäftigten stellt. Das sprichwörtliche lebenslange Lernen und digitale Schlüsselqualifikationen sind daher unabdingbar, um die Beschäftigungs- und Innovationsfähigkeit im Mittelstand zu sichern.

Dabei sind auch adäquate Rahmenbedingungen erfolgsentscheidend. Um insbesondere kleine und mittlere Unternehmen in der digitalen Transformation zu begleiten, müssen Politik und Wirtschaft gemeinsam Strukturen schaffen, die es Beschäftigten ermöglichen, zielgerichtet neue Fähigkeiten für die transformierte Arbeitswelt zu erlangen – und das unabhängig von arbeitsfreien Phasen oder vollen Auftragsbüchern.

Denn nicht nur im IT-Sektor, sondern über alle Branchen hinweg werden die Anforderungen für die Beschäftigten immer komplexer. Es sind auch künftig klassische Kompetenzen wie Lösungsfähigkeit, Resilienz gefragt, aber auch Teamfähigkeit und Belastbarkeit.

Hinzu kommt jedoch: Für eine selbstbestimmte Teilhabe an einer digitalisierten Arbeitswelt benötigen alle Menschen digitale Grundfähigkeiten, zum Beispiel in der Nutzung von Videokonferenz-Systemen. Besonders im IT-Bereich sind digitaltechnische Fertigkeiten gefragt. Hier geht es um die effiziente Nutzung etablierter Systeme, aber auch die Entwicklung neuer, innovativer Technologien. Kenntnisse zum Beispiel in Data Analytics, Künstlicher Intelligenz, Cloud-Computing und Blockchain sind heutzutage besonders gefragt.

Dazu gibt es auch unterschiedliche Untersuchungen. Zum einen sind sicherlich die klassischen Software-Schulungen, Trainings zu IT-Infrastruktur und Programmiersprachen kontinuierlich gefragt. An Relevanz werden Themen rund um IT/Data-Security und KI



gewinnen sowie Qualifizierungen in Bereichen wie Datenanalyse und agile Methoden. Künftig könnten auch Entwicklungen wie Metaverse vermehrt in den Fokus gerückt werden. Wünschenswert ist ausserdem, dass mehr Kompetenzen bezüglich innovativer Lerntechnologien aufgebaut werden – und zwar besonders mit Blick auf die bleibende Vermittlung wichtiger Lerninhalte.

Angesichts des akuten IT-Fachkräftemangels sind aber darüber hinaus auch Strategien gefragt, mit denen Mittelständler Quereinsteiger aus ihrem eigenen Unternehmen für solche Jobs gewinnen und qualifizieren können. Zunächst gilt es dann zu schauen, welche Mitarbeiter aus den eigenen Reihen überhaupt weiterentwickelt werden wollen und das auch können.

Durch die Digitalisierung verändern sich Berufsfelder, manche fallen gar weg. Daher ist ein an der Strategie des Unternehmens ausgerichtetes Bildungsmanagement entscheidend. Das hilft, Talente zu identifizieren, notwendige Kompetenzen aufzubauen und somit die gesamte Organisation weiterzuentwickeln. Eine solche Strategie steigert auch die Attraktivität des Arbeitgebers an sich.

Um von extern Quereinsteiger anzuwerben, hilft es, eine klare Qualifizierungs-Strategie zu haben und diese aktiv zu kommunizieren. Dazu gehört auch, nicht nur Wissen zu vermitteln, sondern darüber hinaus auch die neuen Mitarbeiter permanent zu unterstützen und zu begleiten. Das liefert Erfolgserlebnisse, Vertrauen und somit Loyalität. Das Investment in die Qualifizierung soll ja möglichst nachhaltig sein.

Genauso wichtig ist der Dialog unter allen Beteiligten und das Beachten der individuellen Kompetenzniveaus. Ausserdem müssen zunächst folgende Fragen gestellt werden: Was sind die strategischen Ziele meines Unternehmens? Wie sehen künftige Kompetenz- und Jobprofile aus? Welche Qualifikationen werden dafür gebraucht? Hierbei kann die Politik mit der Schaffung eines Online-Weiterbildungsmonitors unterstützen. Ein solcher Monitor sollte sowohl den Mittelständlern als auch ihren Belegschaften helfen, Chancen und Fortbildungsbedarf, Weiterbildungsangebote und Fördermöglichkeiten unkompliziert zu identifizieren. Gerade auch der Einsatz digitaler Weiterbildungsangebote kann dann entscheidend dazu beitragen, flexibel und entlang der individuellen Bedarfe jeder Mitarbeiterin und jedes Mitarbeiters fort- und weiterzubilden – mit Rücksicht auf die jeweiligen zeitlichen, familiären und sozialen Randbedingungen. ■

Mehr Sicherheit und Einsparpotenzial dank der Cloud

Wörter wie Cloud, Homeoffice und virtuelle Arbeitsplätze sind heute für viele Personen bekannte Begriffe. Doch noch nicht alle leben diese in ihrem Arbeitsalltag aktiv aus. Warum das so ist und weshalb ein Wechsel in die Cloud grundsätzlich und noch vor dem 1. September 2023 empfohlen ist, wird in diesem Artikel beschrieben.

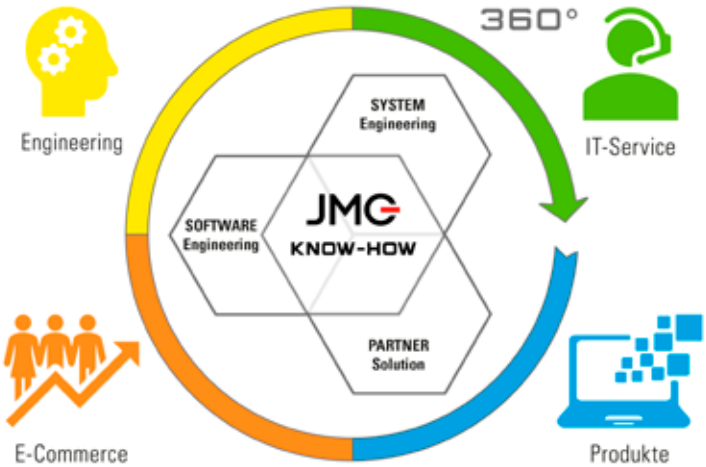
Die heutige Zeit birgt laufend neue Herausforderungen für die IT. Nicht nur aufgrund kontinuierlich neu- oder weiterentwickelten Technologien, sondern auch wegen des wachsenden Bewusstseins für Datenschutz und IT-Sicherheit sowie den momentan kritischen politischen Situationen. Dabei fühlen sich viele Unternehmungen, speziell im KMU-Sektor, überfordert. Kombiniert mit dem gleichzeitig herrschenden starken Bedürfnis nach der höchstmöglichen Sicherheit, liegt für viele Unternehmungen eine Lösung nahe: die Daten auf einem eigenen Server in den betrieblichen Räumlichkeiten zu deponieren. Doch das damit verbundene Sicherheitsgefühl trügt.

Risiko auf Cyberangriffe minimiert

Beim Wechsel zu einem professionellen IT-Anbieter, wie zum Beispiel der JMC, werden die Daten in einem modernen und hochsicheren Datencenter aufbewahrt. Diese Datencenter verfügen im Fall der JMC über den FINMA-zertifizierten Sicherheitsstandard Tier 3+ und Tier 4 und werden rund um die Uhr durch Sicherheitspersonal physisch bewacht. Zusätzlich sind die Datencenter Geo-Redundant, da die einzelnen Standorte mit einer Glasfaserverbindung (dark-fiber) ausgestattet und miteinander verbunden sind, welche ausschliesslich die Daten der JMC übermittelt. Das bedeutet, dass die Daten beim Ausfall eines Rechenzentrums auch an einem anderen JMC-Datenstandort gesichert werden und daher nicht verloren gehen. Ausserdem werden Firewalls und IT-Sicherheitsvorkehrungen durch qualifiziertes Fachpersonal installiert, gewartet und überwacht, was das Risiko auf Cyberangriffe minimiert. Die Relevanz dieser Gegebenheiten steigt vor allem ab dem 1. September 2023, wenn das neue Schweizer Datenschutzgesetz (DSG) für einen besseren Schutz der persönlichen Daten in Kraft tritt. So gelten neue Bestimmungen in Bezug auf die Handhabung und die Aufbewahrung von Daten und erhöhte Anforderungen an die Sicherheitsstandards. Bei Nichteinhaltung des DSG drohen ab September 2023 Bussen in der Höhe ab CHF 250 000.–. Bei einem Wechsel zu einem professionellen IT-Anbieter, wie der JMC, ist die DSG-Konformität automatisch sichergestellt.

Wichtigster IT-Trend der Zukunft

Als einer der wichtigsten IT-Trends der Zukunft bietet die Desktop-Virtualisierung jedoch nicht nur sicherheitstechnische Vorteile. Virtuelle Arbeitsplätze wirken sich positiv auf das Betriebsklima aus,



indem sie durch das ortsunabhängige Arbeiten sowohl die Work-Life-Balance als auch die Unternehmensidentifikation steigern. Ausserdem können Unternehmen mithilfe von virtuellen Arbeitsplätzen aktiv Geld einsparen. Denn einerseits werden dank der Desktop Virtualisierung keine leistungsstarken und teuren Computer mehr für die Angestellten benötigt. Andererseits kann auf eigene Server verzichtet werden, da sich alle Daten in den Datencentern des IT-Anbieters, wie der JMC, befinden. Dies hat zur Folge, dass die Kosten für die Instandhaltung der Geräte wegfallen und sich der eigene Stromverbrauch massiv minimiert. Vor allem zum jetzigen Zeitpunkt, in welchem die Strompreise sehr hoch sind, birgt die Virtual-Workplace-Lösung grosses Einsparpotenzial. Weitere Informationen zu virtuellen Arbeitsplätzen finden sich unter www.jmc-software.ch. ■

JMC
«We Digitize Business»

JMC Software AG
Riedstrasse 1, CH-6343 Rotkreuz
✆ +41 (0)41 799 02 20
info@jmc-software.ch, www.jmc-software.ch

«Sie sind Brückenbauer zwischen den verschiedensten Anspruchsgruppen»

Diesen Sommer werden die ersten Lernenden in die neue Berufslehre «Entwickler/in digitales Business EFZ» starten. Angela Munz war bereits im Bereich Digital Business tätig, bevor es die Ausbildung gab. Heute baut sie als Lehrbeauftragte die neue Berufslehre mit auf. Im Interview erzählt sie, weshalb sie vom Potenzial dieses Berufs überzeugt ist und was ihr daran besonders gefällt.

Elisa Marti

Wie sind Sie zur Tätigkeit im Bereich Digital Business gekommen?
Angela Munz: Bereits während meiner kaufmännischen Berufslehre hat mich gestört, dass die eingesetzte Software die Benutzer zu Fehlern verleitet und nur lückenhaft die Arbeitsprozesse unterstützt hat. Deshalb habe ich bald versucht, Verbesserungspotenzial zu erkennen, und habe dabei die Gelegenheit erhalten, dies auch gleich selbst umzusetzen. So habe ich früh erlebt, wie stark sich der optimale Einsatz von digitalen Hilfsmitteln auf die Effizienz von Ressourcen auswirkt. Diese wertvollen Erfahrungen helfen mir noch heute immer wieder, die Chancen für Verbesserungen zu erkennen und die Freude an der Nutzung von neuen Technologien weiterzugeben.

Hätten Sie «Entwicklerin digitales Business» gelernt, wenn es den Beruf zu Ihrer Zeit schon gegeben hätte?
Ja, auf jeden Fall. Ich befinde mich sehr gerne an der Schnittstelle zwischen Mensch, Technik und Wirtschaft. Umgesetzte digitale Lösungen müssen aus meiner Sicht immer auf die entsprechende Benutzergruppe zugeschnitten sein, den aktuellen technischen Anforderungen und Entwicklungen entsprechen, aber auch wirtschaftlich getragen werden können. Genau dort setzt der neue Beruf an.

Heute sind Sie als Lehrbeauftragte tätig und helfen dabei mit, die neue Lehre aufzubauen. Was motiviert Sie?
Mich hat in meinem Berufsleben bis jetzt am meisten fasziniert, so viele verschiedene Geschäftsbereiche und Branchen sehr nahe erleben zu können. Keine Lösung sieht bei einer anderen Firma oder Institution gleich aus. Nach 15 Jahren Erfahrung in der Digitalisierung von Prozessen möchte ich meine Faszination für diesen Beruf weitergeben. Persönlich finde ich es sehr wichtig, dass es nun einen Beruf gibt, in dem von Grund auf die nötigen Fertigkeiten vermittelt werden und man sich nicht mehr, wie bis anhin, im IT-Berufsalltag alles selbst erarbeiten muss. Zudem kann ich nun mit Stolz sagen, dass es meinen Beruf auch als Lehre gibt, und hoffe, dass dies auch viele meiner ehemaligen Berufs- und Projektteamkollegen dazu ermutigt, die Lehre als Ausbildungsbetrieb anzubieten.

Wie muss man sich den Berufsalltag einer Entwicklerin digitales Business vorstellen?
Da gibt es verschiedenste Arbeitssituationen. Wenn beispielsweise die Erneuerung einer Softwarelösung ansteht, wirkt man in einem Projektteam mit. Man holt die Bedürfnisse der Anwendergruppen ab, analysiert Prozesse, hilft bei der Einführung und den Schulungen mit. Danach gilt es, laufend Optimierungsschritte bei bereits eingeführten Lösungsumgebungen zu erkennen und umzusetzen. Der Beruf ist somit extrem vielseitig und der Alltag immer anders. Zudem hat die entsprechende Branche, in der man tätig ist, einen grossen Einfluss auf die Tätigkeiten.

Mit welchen Tools arbeitet eine Entwicklerin digitales Business?
Welche Werkzeuge verwendet werden, ist abhängig vom jeweiligen Arbeitsgebiet. Mein Grundsatz ist, wenn immer möglich selbst die gleichen digitalen Tools einzusetzen wie die betreuten Fachgebiete. Dazu gehören beispielsweise Tools zur digitalen Kollaboration, Analyse, Visualisierung, Automatisierung und viele mehr.

Hat man viel Kontakt mit Personen aus anderen Fachgebieten?
Definitiv. Damit ein durchgängiger Prozess auch richtig analysiert, abgebildet und eine

Zur Person Angela Munz

Angela Munz kommt aus Lyss und hat nebst der höheren Fachschule für Betriebswirtschaft den Fachausweis in Erwachsenenbildung absolviert. In den letzten 15 Jahren konnte sie in verschiedensten Funktionen der IT Prozesse digitalisieren, Mitarbeitende, Trainer und End User ausbilden sowie Events und Lernplattformen mitgestalten. Aktuell baut sie als Lehrbeauftragte der Wirtschaftsschule Thun an der Einführung des Berufs «Entwickler/in digitales Business EFZ» mit. In ihrer Freizeit liebt sie es, Zeit mit Freunden und der Familie in der Natur zu verbringen.

passende Lösung gefunden werden kann, braucht man den Kontakt zu Personen aus den jeweiligen Fachgebieten. Häufig ist man dort tätig, wo das aktuelle digitale Entwicklungspotenzial vorhanden ist, und gehört da auch direkt ins Team.

Was gefällt Ihnen besonders an dem Aufgabengebiet?

Ich schöpfe meine grösste Motivation daraus, etwa ein halbes Jahr nach einer erfolgreichen Umsetzung in die dankbaren Augen der betroffenen Benutzer schauen und mich persönlich überzeugen zu können, dass ich für den Arbeitsalltag dieser Menschen und ihre Unternehmung einen Fortschritt bewirken konnte.

Was sind die Herausforderungen in diesem Beruf?

Dass Veränderungen im Arbeitsalltag oft nicht erwünscht sind und der aktuelle technologische Wandel für sehr viele Leute einfach zu schnell geht. Hier ist wichtig, sich genügend Zeit zu nehmen, um die Betroffenen abzuholen und möglichst zum richtigen Zeitpunkt das nötige Know-how aufzubauen.

Wem empfehlen Sie die neue Ausbildung?

Allen, die ein technisches Flair sowie Freude am Fortschritt haben; die zuhören, hinschauen und daran glauben, dass immer etwas verbessert werden kann.

Was sind für Sie die wichtigsten Voraussetzungen in diesem Beruf?

Die zukünftigen Lernenden sollten sich als Brückenbauer zwischen den verschiedensten Anspruchsgruppen sehen. Man muss also neben den fachlichen Fähigkeiten unbedingt auch vermitteln können und sehr lösungsorientiert sein. Ausserdem muss man Freude an der Zusammenarbeit mit Menschen haben und diese auch für Neues begeistern können.

Was kann man mit dieser Ausbildung tun?

Man hat die Möglichkeit, sich nach dem Lehrabschluss eher generalistisch zum Wirtschaftsinformatiker weiterzubilden oder sich in einem passenden IT-Bereich zu spezialisieren – etwa in Richtung Applikationsentwicklung.

Wo sehen Sie den Mehrwert für Unternehmen?

Mit der Unterstützung von Entwicklerinnen und Entwicklern digitales Business werden Lösungen auch tatsächlich mit einem Mehrwert eingeführt. Unternehmen profitieren zudem davon, dass sie eine treibende Kraft für Innovationen und neue Technologien haben.

Haben Sie ein bestimmtes Ziel, das Sie verfolgen?

Mein Ziel ist es den Aufbau des neuen Berufs möglichst positiv mitgestalten zu können, weil damit genau die Leute ausgebildet werden, die es jetzt braucht.

Gibt es etwas, das Sie jungen Menschen in der Berufswahlphase auf den Weg geben möchten?

Ja. Bitte auf keinen Fall die ICT als Berufsfeld unterschätzen und nur einen bestimmten Typ Mensch da sehen. In der ICT kann sich fast jeder Personentyp auf seine Art verwirklichen. Dadurch, dass es ein sehr dynamisches Berufsfeld mit einem zunehmenden Fachkräftebedarf ist, hat man ausgezeichnete Berufsaussichten in den nächsten Jahren. Mit dem grossen Entwicklungspotenzial in dem Bereich und dem technologischen Fortschritt ist man hier am Puls der digitalen Gesellschaft und kann die Zukunft aktiv mitgestalten. ■

Neuer Beruf: Entwickler/in digitales Business EFZ

- Ausbildung: Berufslehre mit eidg. Fähigkeitszeugnis
- Ausbildungsdauer: 4 Jahre
- Haupttätigkeitsfelder: Vernetzung, Kommunikation, Datenanalyse, Produkteoptimierung
- Anforderungen: Vernetztes Denken, Interesse an digitalen Trends, Team- und Kommunikationsfähigkeit, Kreativität und Organisationstalent

www.ict-berufsbildung.ch/edb

KI und HR: Geheimnisse einer Hassliebe

Künstliche Intelligenz (KI) verspricht, das Arbeiten einfacher, schneller und objektiver zu machen.

Text: Hogan Assessments

Inzwischen hatten viele Unternehmen Zeit und Gelegenheit, sich mit dieser Automation vertraut zu machen oder sie in ihre täglichen Routinen zu integrieren. Hat es die KI geschafft, diese Versprechen einzulösen? Fachleute bei Hogan Assessments haben Erfolge und Defizite der KI in HR-Prozessen analysiert, um zu ermitteln, wie nützlich diese Technologie langfristig für Organisationen sein könnte.

Der Einsatz der KI bei der Personalbeschaffung kann die Fähigkeit einer Organisation, schnell die richtigen Mitarbeiter zu finden, deutlich steigern und der Personalabteilung helfen, Bewerber mit den erforderlichen Fähigkeiten und der nötigen Erfahrung zu ermitteln. Zudem kann die KI potenziellen Bewerbern Stellen vorschlagen und sogar die Arbeitsleistung interviewter Bewerber vorhersagen. Die KI kann ausserdem ein strategischer Verbündeter sein, denn sie hat das Potenzial, einstellende Manager durch Schaffung eines ansprechenderen Bewerber-Erlebnisses zu unterstützen. Auch lassen sich mit ihrer Hilfe subjektive Voreingenommenheiten vermeiden und gezielte Fragen für das Vorstellungsgespräch vorbereiten.

Doch es gibt auch eine Kehrseite: Voreingenommenheit. KI-Systeme, die auf vergangenen, durch Voreingenommenheit geprägten Personalbeschaffungs- und -einstellungspraktiken beruhen, führen ebendiese Voreingenommenheiten fort und verschärfen sie sogar. Umfassende Tests mit unterschiedlichen Zielgruppen und die kontinuierliche Überwachung der Auswahlquoten sind entscheidend, um sicherzustellen, dass neue KI-Systeme diese alten Voreingenommenheiten nicht übernehmen und fortschreiben. Ein weiteres Problem ist der Mangel an Transparenz. Erstens wird die KI von technisch weniger versierten Personen häufig nur schlecht verstanden, was das Gefühl hervorruft, dass ein Computersystem wichtige Entscheidungen auf willkürliche und unbekannte Weise trifft. Zweitens können manchmal selbst die technisch beschlagenen Entwickler von KI-Systemen die Funktionsweise des KI-Systems oder die Relevanz seiner Funktionen für die Tätigkeit nicht wirklich erklären. «Die Menschen haben ein Recht darauf, zu wissen, wie sie bewertet werden, dass diese Bewertungen fair sind und dass sie in Bezug zur jeweiligen Tätigkeit stehen», erklärt Dr. Sherman, Chief Science Officer bei Hogan Assessments. ■

Leistungsstarke Versorgung mit Breitbandinternet

Die Schweiz hat eine phänomenal hohe Abdeckung mit leistungsfähigem Internet: Rund 80 Prozent der Haushalte haben schon heute die Bandbreite für die Anforderungen der Zukunft, ein internationaler Spitzenwert. Möglich machen dies die Mitglieder von «SUISSEDIGITAL».

Mit ihren Glasfaserkabelnetzen leisten die Mitglieder von Suissedigital einen wichtigen Beitrag zur digitalen Grundversorgung in der Schweiz – flächendeckend in städtischen ebenso wie in ländlichen Gebieten. Wer an eines der 180 Kommunikationsnetze angeschlossen ist, hat überall Zugang zu Radio, Fernsehen, Replay-TV, Telefonie und Hochgeschwindigkeitsinternet mit Bandbreiten bis zu 1 Gigabit pro Sekunde. Möglich ist dies, weil die Netze der Mitglieder mehr als 80 Prozent aller Schweizer Haushalte erreichen und bereits heute zu 95 Prozent aus Glasfasern bestehen. Die Netze werden zudem laufend an die neuesten technischen Standards angepasst.

Lokale Verankerung als Trumpf

Die Suissedigital-Mitglieder, die heute rund 2,2 Millionen Haushalte und zahlreiche Geschäftskunden mit ihren Dienstleistungen versorgen, sind vor mehr als 50 Jahren in den verschiedenen Regionen der Schweiz entstanden. Ausgangspunkt war das Bedürfnis nach einer qualitativ hochstehenden Radio- und Fernsehversorgung. Seither haben sich die Kommunikationsnetze rasant entwickelt, ihr Angebot wurde laufend ausgebaut. Jedoch sind sie ihrer Entstehung treu geblieben, indem sie auch heute noch zu ihrer lokalen Verankerung stehen. Das hat Vorteile: So bieten die lokalen Kommunikationsnetze dank überschaubaren Verbreitungsgebieten und kurzen Distanzen einen schnellen, flexiblen und unkomplizierten Kundendienst. Zudem können sie bei Bedarf auf lokale Bedürfnisse und Gegebenheiten eingehen. Davon können gerade auch Geschäftskunden profitieren. ■

Die 180 Kommunikationsnetze von Suissedigital versorgen auch viele Geschäftskunden mit leistungsfähigem Breitbandinternet.

Drei Fragen an Simon Osterwalder, Geschäftsführer von Suissedigital

Warum braucht es Suissedigital?
Die Digitalisierung erfasst immer mehr Bereiche unseres Lebens. Deshalb braucht es einerseits eine starke Infrastruktur für alle sowie einen starken Verband, der sich für die Anliegen der Branche wie auch der Schweizer Bevölkerung und Unternehmen einsetzt. Andererseits dürfen wir nicht zurück zum Monopol wie zu PTT-Zeiten. Die Bevölkerung will und braucht die Wahlfreiheit.

Wer sind die Mitglieder von Suissedigital?
Unsere Mitglieder sind zum einen privatwirtschaftliche Unternehmen wie Sunrise/UPC, Quickline oder Net+, zum anderen öffentlich-rechtliche Unternehmen wie Gemeinden und Energieversorger, die ein Kommunikationsnetz betreiben. In der Summe sorgen die Mitglieder für die Grundversorgung und treten als Telekom-Partner der Bevölkerung auf.

Warum setzen die Mitglieder von Suissedigital auf Regionalität?
Sie kennen ihre Kunden oft persönlich und richten sich gezielt nach ihren Wünschen. Die regionale Präsenz ist ein grosser Wettbewerbsvorteil: In einer Tourismusregion kann etwa das Angebot nicht nur auf die Bedürfnisse der lokalen Bevölkerung, sondern auch auf diejenigen von Hotels und internationalen Gästen zugeschnitten werden.

SUISSEDIGITAL
VERBAND FÜR KOMMUNIKATIONSNETZE

Suissedigital – Verband für Kommunikationsnetze
Bollwerk 15, CH-3011 Bern
✆ +41 (0)31 328 27 28, 🖷 +41 (0)31 328 27 38
info@suissedigital.ch, www.suissedigital.ch

Was es beim Kauf oder Verkauf von IT-Unternehmen aus rechtlicher Sicht zu beachten gilt

Neben den klassischen Themen Prüfung Eigentumsverhältnisse, Rechtsstreitigkeiten etc. gibt es bei IT-Unternehmen oder Unternehmen mit einem digitalen Geschäftsmodell zusätzliche Punkte zu prüfen, bei denen ein IT-rechtliches Wissen wichtig ist. Der nachfolgende Artikel rückt diese Themen in den Fokus.

Yves Gogniat

Allgemein empfiehlt es sich, bei Unternehmenstransaktionen erfahrene Berater beizuziehen. Bei Käufern ist dies üblich, aber bei KMU sieht man immer wieder eine eher blauäugige Herangehensweise auf der Verkäuferseite. Schlechte Vorbereitung und vor allem fehlende oder unstrukturierte Informationen können negative Effekte auf den Preis haben oder führen schlimmstenfalls zum Abbruch von Verhandlungen.

Eine gute Vorbereitung schafft Mehrwert

Die allgemeinen Punkte lassen sich in Zusammenarbeit mit einem Treuhänder oder dem Hausanwalt prüfen, sofern Erfahrung mit Unternehmenstransaktionen besteht. Doch fehlt oft das IT-rechtliche Spezialwissen. Ein IT-Experte, der die Marktstandards kennt, wird meist schneller und effizienter eine Einschätzung und Empfehlung abgeben können als ein Berater, der sich zuerst in die Thematik einarbeiten muss. Obwohl die Due Diligence von der Käuferseite durchgeführt wird, kann es für den Verkäufer sinnvoll sein, sich mit einem Experten darauf vorzubereiten. Werden bei der Vorbereitung ungenügende Dokumentationen oder Unklarheiten erkannt, lassen sich diese oft vorgängig nachbessern. Eine unklare Lizenzsituation kann bereinigt oder eine ungenügende Datenschutz-Governance nachgebessert werden. Entdeckt der potenzielle Käufer diese Punkte während der Due Diligence, ist ein kurzfristiges Nachbessern durch den Verkäufer oft nicht möglich. Zudem fehlen meist auch die Ressourcen, da alle mit Verkaufsverhandlungen absorbiert sind. Ein Käufer wird solche Mängel vielfach als Argument für eine Preisreduktion oder zusätzliche Gewährleistungsklauseln nutzen. Nicht ganz zu Unrecht, da diese entsprechende Risiken darstellen oder Nachbesserungskosten verursachen.

Das Geschäftsmodell ist entscheidend

Unter IT-Unternehmen werden unterschiedliche Geschäftsmodelle zusammengefasst. Je nach Geschäftsmodell gibt es unterschiedliche Schwerpunkte zu setzen. Bei einer Agentur, die im Projektgeschäft tätig ist, gilt es die Entwicklungsverträge sowie die grösseren Projekte zu prüfen. Es sind insbesondere Haftungs- und Gewährleistungsrisiken zu prüfen. Bei IT-Service-Unternehmen gilt es neben den Musterverträgen, die Nutzung von Drittanbietern oder eingekaufte Lizenzen zu prüfen. Daneben hat die Einhaltung der Datensicherheit und des Datenschutzes in den letzten Jahren an Wichtigkeit gewonnen. Es gibt daher nicht das eine Prüfschema für IT-Unternehmen.

Wem gehören die Immaterialgüterrechte?

Immaterialgüterrechte («IP») spielen bei IT-Unternehmen eine zentrale Rolle. Am wichtigsten sind die Urheberrechte, da die meisten Computerprogramme und deren Code unter Urheberrecht geschützt sind. Patente spielen im europäischen Raum meist eine untergeordnete Rolle, können aber für Hardware oder Software, die mit Hardware kombiniert wurde, relevant sein. Markenrechte sind vor allem für einzelne Softwareprodukte relevant. Um die IP-Situation sowie entsprechende Risiken einschätzen zu können, ist eine gute Übersicht in Form einer Liste notwendig. Eine Liste muss ausreichend detailliert sein. Es reicht nicht aus, nur zu erwähnen, dass Software X entwickelt wurde. Alles von der Entwicklung bis zur IP-Regelung mit den Kunden muss aus der Liste ersichtlich sein. Es muss dokumentiert werden, welche Arbeitsergebnisse eigene IP darstellen und was auf Open Source, lizenzierter Software, API, eingekaufter Entwicklung etc. basiert. Bestenfalls wird verifiziert, dass die IP umfassend beim Unternehmen liegen. Schlimmstenfalls wird festgestellt, dass die Software im Wesentlichen auf Basis einer Open-Source-Software mit Copyleft entwickelt wurde und das Arbeitsergebnis ebenfalls Open Source ist. Auf der Kundenseite gilt es zu prüfen, ob eine IP-Übertragung oder Lizenzierung der Rechte stattgefunden hat. Als Nebenbemerkung sei noch festzuhalten: Eine unvollständige Liste deutet allgemein auf eine rudimentär dokumentierte Entwicklung hin, womit u.a. die Abhängigkeit von Mitarbeitern steigt.

Die vertragliche Regelung gilt es zu prüfen

Aus der Übersicht lassen sich die notwendigen rechtlichen Dokumente ableiten. Aufgrund eingeschränkter Ressourcen wird kaum jeder Vertrag geprüft werden

können, weshalb die Risiken meist jeweils über eine Gewährleistungsklausel abgesichert werden. Zumindest aber die Musterverträge sind zu prüfen sowie wesentliche oder Spezialverträge. Bei Grossprojekten oder Grosskunden werden oft individuelle Klauseln verhandelt. Grossprojekte stellen aufgrund des Volumens meist sowieso zu prüfende Verträge dar. Allgemein ist wichtig, sich einen Überblick über das Vertragsmanagement zu verschaffen. Bei KMU trifft man es immer wieder an, dass teilweise Verträge nur mündlich geschlossen wurden, schriftliche Verträge ungenügend dokumentiert sind oder bei alten Bestandskunden die bestehenden Verträge nie auf die neuen Vorlagen nachgezogen wurden oder die verwendeten AGB spiegeln das heutige Geschäftsmodell nicht mehr ausreichend wider. Dies führt zu Rechtsunsicherheiten und kann schlussendlich die Verkaufsbedingungen beeinflussen. Die Bereinigung der Vertragssituation ist machbar, aber mit entsprechendem Aufwand verbunden. Bei einer frühzeitigen Analyse besteht das Potenzial, gleichzeitig auch die kommerzielle Seite zu optimieren. Zum Beispiel durch bessere Lizenzverträge. Da bei IT-Unternehmen zurzeit mit hohen Multiples gerechnet wird, können auch kleinere Optimierungen preisrelevant sein.

Datensicherheit und Datenschutz immer wichtiger

Ein vertieftes Datenschutz- oder Datensicherheits-Audit wird im Rahmen einer Due Diligence kaum möglich sein. Es sollte aber geprüft werden, ob marktübliche Zertifizierungen vorliegen (z.B. ISO, SOC2 etc.). Diesfalls hat ein Käufer zumindest die Sicherheit, dass ein gewisser Framework besteht. Zertifizierungen sind gute Indikatoren, aber es sollte auch ein kurzer Blick auf den unternehmensinternen Framework geworfen werden. Ein Datenschutz- oder Sicherheitsexperte kann schnell feststellen, ob wesentliche Richtlinien für eine Datenschutz-Governance vorhanden sind.

Mitarbeitende bleiben wichtig

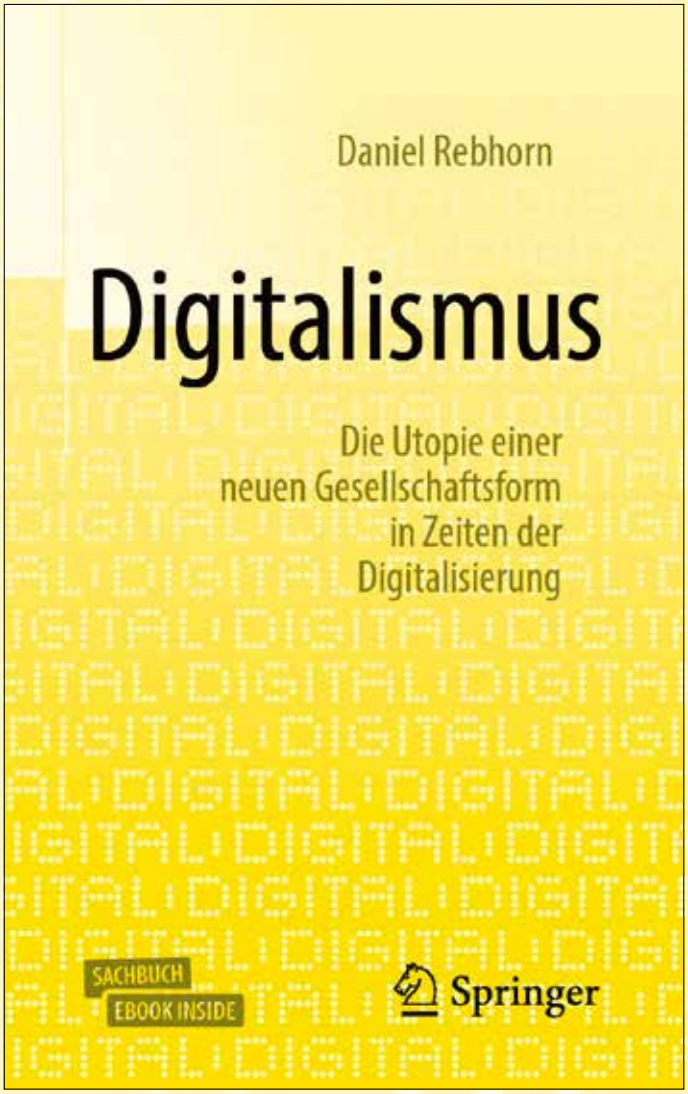
Wie bei jeder Unternehmenstransaktion gilt es auch einen Blick auf die Mitarbeitenden zu werfen. Wenn die Eigentümer das Unternehmen verkaufen, steht oft gleich ein Austritt als Mitarbeitende aus dem Unternehmen im Raum. Dies kann zu einem Vakuum bei Schlüsselpositionen führen. Als Verkäufer sollte daher längerfristig geplant werden, vielfach verlangt ein Käufer, dass Eigentümer dem Unternehmen als Mitarbeitende oder beratend für einen Zeitraum zur Verfügung stehen. Es kann auch auf unteren Ebenen Mitarbeitende geben, die für eine Transaktion relevant sind. Im Falle, dass die Due Diligence eine schlechte Dokumentation der Software aufgedeckt hat, ist das Entwickler-Know-how absolut relevant. Allgemein sind gewisse Spezialisten schwer zu rekrutieren und spielen daher in die Bewertung mit ein. Denn ein Käufer will nach Möglichkeit verhindern, dass das Unternehmen nach dem Kauf wertvolle und erfahrene Mitarbeiter verliert.

Rekapitulation

Somit kann gesagt werden, dass bei IT-Unternehmenstransaktionen neben den üblichen Themen weitergehendes Spezialwissen grosse Vorteile sowohl auf Käufer- wie auch Verkäuferseite bringen kann und es sich lohnt, den IT-rechtlichen Spezialthemen ausreichend Beachtung zu schenken. ■

Digitalismus

Die Utopie einer neuen Gesellschaftsform in Zeiten der Digitalisierung



Daniel Rebhorn
Digitalismus
Die Utopie einer neuen Gesellschaftsform
in Zeiten der Digitalisierung
Verlag Springer Gabler
342 Seiten, 24,99 Euro
ISBN 978-3-658-26131-3

Demokratiefrust und Umweltschutz. Digitalisierung und Arbeitsmarkt. Extremismus und Wandel. Die aktuellen Themen sind vielfältig. Nicht nur einzelne Aspekte des Lebens verändern sich, sondern auch die Gesellschaft als Ganzes unterzieht sich einer grossen Veränderung.

Doch wo bleibt ein Lösungsmodell, das aus einer völlig anderen Idee erwächst und sich eine Denkweise zutraut, die bisher unausgesprochen blieb? Daniel Rebhorn wagt mit «Digitalismus» genau das und zeichnet eine neue Gesellschaftsform, die es in sich hat: Was wäre, wenn zukünftig anstatt menschlicher Eliten in Politik, Gesellschaft und Ökonomie die Künstliche Intelligenz für uns alle Entscheidungen treffen würde? Wenn die Maschine berechnet, was die Menschheit in welchem Mass braucht und bekommt – logisch, unvoreingenommen und vor allem nicht korrumpierbar? Kommen wir zu einem gerechteren Staats- und Lebensmodell, wenn das typisch menschliche Machtstreben einer neuen Version von Gerechtigkeit weicht? Und was bedeutet das im Gegenzug für unsere Freiheit, unsere Bildung und unsere Arbeitsweisen?

Daniel Rebhorn geht der Frage nach einer Neudefinition unserer Staatsformen, der Wirtschaftssysteme und auch der Kooperationen zwischen Mensch und Maschine nach. Aus diesem Gedanken entsteht mit «Digitalismus» eine ungewöhnliche Antwort – nämlich darauf, wie wir uns die Vorteile der künstlichen Intelligenz zu Nutze machen und sich daraus eine neue und vor allem zukunftsfähige Form der Gesellschaft entwickeln kann.

«Die Dystopie halte ich für realistischer, als sie hoffentlich gemeint ist. Aber die Utopie ist für mich viel mehr als nur Inspiration, sondern konkreter Anreiz.» So beschreibt es ein Leser. «Mir ist klar, dass meine Utopie durch ihre alternativen Ansätze sehr kontrovers ist. Doch eine Utopie hat gerade den enormen Vorteil, dass sie gedacht werden darf, ohne sich in sich selbst gleich allen Gegenargumenten aussetzen zu müssen», sagt Rebhorn.

Seine These: Die neue und digitalisierte Gesellschaft kann weder im Rahmen eines Kapitalismus noch einer sozialen Marktwirtschaft weiter existieren. Damit würden die riesigen Potenziale der KI für die Gesellschaft verschenkt. Wir müssen eine neue Gesellschaftsform denken und gestalten. Was aber können wir tun, um diese zu finden? Wie genau sieht sie aus? Und welche Rolle spielt dabei die technische Entwicklung? Wie wird der Transformations-Prozess sich entwickeln? Rebhorn gibt einen Wegweiser, eine Handreichung und ein Konzept für die Zukunft unserer Gesellschaft: Er geht davon aus, dass es eine Super-KI geben wird, die als übergeordnete Instanz fungiert. Sie bereitet Entscheidungen vor, überprüft die Auswirkungen und trifft sie dann – zum Wohle aller. Das Ergebnis: Im Digitalismus werden für jeden Menschen bessere Rahmenbedingungen geschaffen. Denn die KI berechnet das Optimum für Gesellschaft, Menschen und Umwelt. Die Maschine ist per se nicht korrumpierbar. Daher kommt dieses System zu den bestmöglichen Ergebnissen – für alle, solange wir die KI nicht korrumpieren. ■

28./29. März 2023, Zürich

HR FESTIVAL EUROPE 2023

Grösster Schweizer Event für HR-Professionals.

www.hrfestival.ch

4. April 2023, Baden

TEC FORUM 2023

Fachvorträge und Ausstellung in den Bereichen Rechenzentrum, Gebäudeverkabelung, Breitband, Industrie sowie Energie, Verkehr und Überwachung. www.tec-forum.ch

17.–21. April 2023, Hannover

HANNOVER MESSE 2023

Schaffen wir die Industrie von morgen.

www.hannovermesse.de

24./25. Mai 2023, Bern

ELECTRO-TEC 2023

Nationaler Branchentreffpunkt für Kommunikations-, Gebäude-, Licht- und Installationstechnik. www.electro-tec.ch

6.–9. Juni 2023, Bern

SUISSE PUBLIC 2023

Grösste Schweizer Fachmesse für den öffentlichen Sektor.

www.suissepublic.ch

27. Juni 2023, Bern

SWISS TELECOMMUNICATION SUMMIT 2023

Resilienz in einer vernetzten Welt. www.asut.ch

27./28. Juni 2023, Bern

SWISS EGOVERNMENT FORUM 2023

Führendes Forum in der Schweiz im Bereich E-Government.

https://e-governmentforum.ch

28./29. Juni 2023, Berlin

HUB.BERLIN 2023

Eines der wichtigsten Treffen, um die Digitalisierung in die Realität umzusetzen. www.hub.berlin

29./30. Juni 2023, Bern

SWISS EHEALTH FORUM 2023

Führendes Forum in der Schweiz im Bereich E-Health.

https://e-healthforum.ch

31. August 2023, Zürich

SWISS CRM FORUM 2023 www.swisscrm.ch

7. September 2023, Brugg

KMU SWISS SYMPOSIUM 2023

«Versorgungssicherheit… Der Stoff, aus dem Träume sind?» «it business» ist Medienpartner. www.kmuswiss.ch

20./21. September 2023, Bern

SWISS CYBER SECURITY DAYS 2023

Die derzeit führende Cybersecurity-Konferenz der Schweiz.

https://swisscybersecuritydays.ch

28. September 2023, Zürich

12. CONFARE SWISS CIO SUMMIT 2023

«CREATE + ACT = creACTe». www.ciosummit.ch

10.–12. Oktober 2023, Nürnberg

IT-SA 2022

Fachmesse für IT-Security. www.it-sa.de

30. Oktober 2023, Bern

CNO PANEL 2023

Schweizer Plattform für das Top-Management. «it business» ist Medienpartner. www.cno-panel.ch

30./31. Januar 2024, Interlaken

18. ALPENSYMPOSIUM 2024

Zweitgrösste interdisziplinäre Konferenz für Politik, Wirtschaft, Sport und Kunst in der Schweiz. https://alpensymposium.ch

vorschau

Zero Trust

IT-Security neu gedacht

Cloud

Hybrid, Public,
Private oder Multi?

Hochverfügbarkeit, Backup & Storage

Datensicherungsstrategien
für Unternehmen

Dokumentenmanagement

Einfach und digital

Events

Swiss Cyber Security Days 2023
kommt nach Bern

... sowie eine Fülle Wissenswertes zu weiteren aktuellen Themen aus der IT-Szene.

Ausgabe 2/2023 erscheint am 3. Juli 2023

IMPRESSUM

itbusiness

23. Jahrgang, erscheint 4-mal jährlich
ISSN-Nr. 1424-8867

HERAUSGEBER
Fractal Verlag GmbH
Postfach
CH-4124 Schönenbuch
www.itbusiness.ch

REDAKTION
Petra De Meo
pdm@itbusiness.ch

MARKETING & VERKAUF
Leonardo De Meo
Ldm@itbusiness.ch

REDAKTIONELLE MITWIRKUNG
Yves Gogniat
Niels Gründel
Elisa Marti
lic. iur. Ursula Sury
Berthold Wesseler

SATZ UND DRUCK
Werner Druck & Medien AG
Leimgrubenweg 9
4053 Basel

AUFLAGE
10 000 Exemplare

ABONNEMENT
Schweiz CHF 40.–
Ausland (Europa) CHF 60.–
Probeabo (Schweiz) CHF 15.–
Digital CHF 30.–

Wissensvorsprung für IT-Entscheider!

Informieren Sie sich besser rechtzeitig und bestellen Sie jetzt Ihr it business-Abonnement!

FIRMA

NAME, VORNAME

FUNKTION

STRASSE

LAND-PLZ/ORT

TELEFON

E-MAIL

DATUM UNTERSCHRIFT

Gewünschtes bitte ankreuzen:

- ☐ **1-Jahres-Abo** für 4 Ausgaben — CHF 40.–
  Bei Ausland-Lieferung (Europa) — CHF 60.–
- ☐ **1-Jahres-Digital-Abo**
  für 4 Ausgaben — CHF 30.–
- ☐ **Probe-Abo** für 2 Ausgaben — CHF 15.–
  Bei Ausland-Lieferung (Europa) — CHF 25.–

Preise (Inland) inkl. 2,5% MwSt.

Bitte per E-Mail senden an abo@itbusiness.ch