Herausgeber mediaworld GmbH | www.service-seiten.com | Ausgabe Braunschweig/Wolfsburg 2023

BS | WOB

SERVICE-SEITEN

IT & Digitalisierung

Sicherheit & Haftung | Ratgeber für Unternehmer*innen

Schönes neues Metaversum
Wie real wird es sein?

IT-Sicherheit
vs. Cyberkriminalität

Künstliche Intelligenz
Wie weit darf sie gehen?

mediaworld
AGENTUR FÜR MARKETING & VERLAG

APPELHAGEN

LET'S TALK ABOUT YOUR DIGITAL FUTURE

SO DIGITALISIEREN SIE STEUERRELEVANTE PROZESSE IN IHREM UNTERNEHMEN

Maximilian Gerdesmann
Tax & Tax Process Manager
Tax Compliance Officer

Karin Kutz
Steuerberaterin und Wirtschaftsmediatorin
Fachberaterin für Internationales Steuerrecht

STEUERPROZESSE IM UNTERNEHMEN INDIVIDUELL DIGITALISIEREN

Nutzen Sie die Vorteile der Digitalisierung. Wir bringen Sie steuerlich sicher in das digitale Zeitalter. Gerne erstellen wir Ihr individuelles und bedarfsgerechtes Angebot.

KONTAKT:

Karin Kutz
Steuerberaterin und Wirtschaftsmediatorin
Fachberaterin für Internationales Steuerrecht

Telefon: +49 (0) 531 28 20-456
E-Mail: kutz@appelhagen.de

SCAN MICH

APPELHAGEN Rechtsanwälte Steuerberater PartGmbB - Theodor-Heuss-Straße 5A, 38122 Braunschweig

HACKERANGRIFFE

[FACH]KRÄFTEMANGEL

ENERGIEKRISE

BLACKOUT

STÄRKE ZEIGEN | HERAUSFORDERUNGEN ANGEHEN UND LÖSEN

Mandala Internet, EDV-Service GmbH

lädt Sie zur 5. Mittelstand-trifft-Mittelstand Tagung ein.

Was erwartet Sie:

 # Hochkarätige Referenten zu aktuellen Themen

 # Informations- und Erfahrungsaustausch der KMU´s

 # Diskussionsforum und Netzwerk Lounge mit Experten

 # Messe und Informationsstände

 # Mehr Wissen als zuvor

Jetzt Gratis anmelden unter:

mittelstand-trifft-mittelstand.de

save the date

15.03.2023

Jetzt Platz sichern und sofort anmelden

SERVICE-SEITEN
INFORMATIV – SACHLICH – UNABHÄNGIG

Impressum

Service-Seiten IT & Digitalisierung
Sicherheit & Haftung
Ratgeber für Unternehmer*innen
Ausgabe Braunschweig/Wolfsburg 2023

Jahresausgabe
Nr. 01

Herausgeber (V. i. S. d. P.)
mediaworld GmbH
Timo Grän, Martin Voß

Verlag
mediaworld GmbH
Agentur für Marketing & Verlag
Bankplatz 8
38100 Braunschweig

Telefon 0531 482010-20

info@mediaworldgmbh.de
www.mediaworldgmbh.de
www.service-seiten.com

Geschäftsführer
Timo Grän

Schriftleitung
RA Martin Voß, LL.M.

Grafische Gestaltung
Florian Bonau, Leon Lohre, Sina Schulz

Auflage
18.000 Stück

Verteilung
Beilage „IHK wirtschaft“ (Ausgabe 02/2023)
Beilage „Unsere Wirtschaft“ (Ausgabe 03/2023)

Druck und Auflagennachweis
Strube Druck & Medien GmbH

Verlagsrechte
Nachdruck nur mit Genehmigung des Verlags. Einsender von Manuskripten, Briefen u. ä. erklären sich mit einer redaktionellen Bearbeitung einverstanden. Alle Angaben ohne Gewähr.

Anzeigen/Projektsteuerung
Daniel Adams, Timo Grän

Anzeigentarif
Mediadaten Ausgabe 2023

Titelbild
Adobe Stock/ ink drop

Nächste Ausgabe
4. Quartal 2023

Hinweis
Die einzelnen Beiträge haben ausschließlich informatorischen und unverbindlichen Charakter und basieren auf der Rechtslage zum Zeitpunkt der Veröffentlichung dieser Ausgabe. Sie stellen keine Rechtsberatung dar und können eine individuelle Beratung, welche die jeweiligen Besonderheiten des Einzelfalls berücksichtigt, nicht ersetzen.

Veröffentlichungen
Timo Grän, GF mediaworld GmbH
Telefon 0531 482010-10
graen@mediaworldgmbh.de

mediaworld
AGENTUR FÜR MARKETING & VERLAG

Editorial

5 Vorwort Herausgeber
50 Autorenübersicht

Online weiterlesen!

Veröffentlichungen

6 „Warum dieses Meta-Dings?“
8 Schönes neues Metaversum
10 Wegweiser im Digitalisierungs-Dschungel
14 Nicht nur „digitalisieren“, sondern auch „automatisieren“?
16 Intelligente Lösungen für eine sichere IT-Infrastruktur
19 Smart Energie sparen mit bedarfsgerechtem Heizen
20 Costumer Relationship Management
22 Digitale Finanzdienstleistungen im Mittelstand als ein Schlüssel zum Erfolg
25 Kryptowährung, NFT und Blockchain-Transaktion – steuerlich alles geregelt?
26 Wo kommen wir her? Wo gehen wir hin?
28 Sicherheit in der Betriebsprüfung
29 Angemessene Sanktionslistenprüfung im Betrieb vornehmen
30 Gewachsene IT-Strukturen im Unternehmen
31 KI fordert: „Alle Feministinnen sollen in der Hölle schmoren”
32 Notfallkonzepte als Anforderung des Datenschutzes
33 Hinweisgeberschutzgesetz praktisch umsetzen
34 Digitalisierung mit Nebenwirkungen
38 IT-Security und Awareness
41 Cyberangriffe durch IT-Penetrationstests und Awareness vermeiden
42 Partner für Datenschutz und Informationssicherheit
44 Cyber-Risiken im Mittelstand
46 Braucht man eine Cyberversicherung?
48 Cyber-Kriminalität – „Risiken kennen und im Voraus handeln!“

Timo Grän

Martin Voß, LL.M. | Rechtsanwalt

Vorwort Herausgeber

Sehr geehrte Unternehmerinnen und Unternehmer,

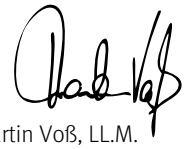
haben Sie sich schon einmal Gedanken darüber gemacht, was Sie täglich alles mit Ihrem Handy umd damit digital erledigen? Termine, E-Mails, News abchecken, Besorgungen und eventuell auch schon einen Teil Ihrer beruflichen Aufgaben erledigen – all dies ist heutzutage für viele Menschen Standard. Redaktionelle Beiträge werden ab 2024 oftmals mit künstlicher Intelligenz (KI) geschrieben – diejenigen in diesem Ratgeber nicht(!) – und mein Kühlschrank ist mit dem Internet verbunden und erledigt Einkäufe selbständig. Gleichzeitig ist Deutschland in Teilen immer noch eine Fax-Republik und tut sich mit dem Digitalen häufig schwer. Die unzureichende Netzabdeckung (bis zur letzten Milchkanne) sei hier nur exemplarisch genannt.

Wie real wird die „schöne neue Welt" also tatsächlich werden? Was wird uns das neue Internet in 3D – das Metaversum – bringen? Welche Chancen, aber auch welche Risiken zieht die fortschreitende Digitalisierung und Entwicklung der Informationstechnologie nach sich? Wie wichtig ist es, schon jetzt eine Strategie für die Verknüpfung der realen mit der (neuen) virtuellen Welt zu entwickeln? Welche Gefahren lauern? Und welche Herausforderungen ergeben sich daraus und wie gelingt es uns, die Digitale Transformation sinnvoll anzugehen und sicher zu gestalten?

Eines steht jedenfalls fest: Wir befinden uns tatsächlich in einer Zeitenwende – und das ganzheitlich betrachtet! Eine Rückkehr ist ausgeschlossen.

Wir hoffen, Sie finden einige Antworten auf Fragen, die Sie sich möglicherweise noch nicht einmal gestellt haben. Wir danken der Kriminalpolizei und dem Verfassungsschutz sowie den Autorinnen und Autoren dieser Ausgabe, die Sie mit hoffentlich nützlichen Informationen ausstatten und sich zudem mit dieser Publikation als IT- und Digitalisierungspartner für Sie und Ihr Unternehmen zeigen.

Herzlichst,



Timo Grän Martin Voß, LL.M.

„Warum dieses **META-DINGS?**“

Eine Strategie für das Neue im Metaverse

Das Feuilleton- und Marketing-Schlagwort zur Erklärung aller neuen Unsicherheiten und Herausforderungen heißt „VUCA“. VUCA steht für Volatilität, Unsicherheit, Komplexität und Ambiguität. Auch das Metaverse als das neue Internet ist für viele Unternehmen eine „VUCA-Welt“. Sollten die Unternehmen wirklich eine virtuelle Umgebung schaffen, in der ihre Kunden interaktiv Produkte und Dienstleistungen kaufen? Und wollen die lieben Kunden das überhaupt?

Diese Frage ist nicht neu. 1999 fragte Boris Becker in einem berühmten AOL-Werbespot, ob er schon „drin“ sei, im Internet – und gab sich selbst die Antwort: „Das ist ja einfach!“ Bundeskanzler Helmut Kohl hatte schon 1994 in einem Interview das World Wide Web und die „Datenautobahn“ mit der Autobahn verglichen und auf die Zuständigkeiten „der Länder“ verwiesen.

Das Neue ist also nicht immer hoch willkommen und wird gerne missverstanden. Es macht Angst und sorgt für Unsicherheit. Auf der anderen Seite werden an das Neue auch geradezu religiöse Heilserwartungen geknüpft, wie etwa aus dem Cyberspace-Manifest von John Perry Barlow (1996) hervorgeht, der Blaupause der „kalifornischen Ideologie“: „Regierungen der Industriellen Welt, ihr müden Riesen aus Fleisch und Stahl, ich komme aus dem Cyberspace, dem neuen Zuhause des Geistes.“

Von Unternehmen wird zuerst auf den Business Case geschaut. Es wird gefragt, ob es „sich lohnt“, bei einer neuen Technologie „mitzumachen“ oder ob es besser sei, erst einmal die Entwicklungen abzuwarten. Auch bei der Entwicklung des Metaversums. Das Metaversum, auch Metaverse genannt, soll das neue Internet zum Anfassen und Ausprobieren sein. Ein Internet in 3D, das immer da ist und keine Sperrstunden oder Betriebszeiten kennt.

Das Metaverse – das neue große Ding oder „nur“ ein Hype?

Es gibt nicht das EINE Metaverse, es ist nicht einfach nur eine neue Plattform, auch wenn das der Meta-Konzern und Facebook gerne so hätten. Es gibt viele Metaversen. Und Anbieter, die es anders nennen werden: „Web 3“ oder „Mixed Reality“, beispielsweise. Seit über 20 Jahren beobachte ich, wie die reale und virtuelle Welt zusammenwachsen. Heute brauchen wir unser Smartphone nur in Richtung Eiffelturm

zu bewegen und bekommen alle Informationen über dieses Bauwerk und seinen Schöpfer Gustave Eiffel angezeigt oder vorgelesen. Bei dem Themen Augmented Reality (AR) und Virtual Reality (VR) sind wir also längst in der Phase der realistischen Nutzungen und Geschäftsmodelle angekommen.

Das Metaverse geht einen Schritt weiter: Wie wäre es, wenn wir unseren Paris-Urlaub zum Beispiel bei Google Streetview planen und dort auch auf unsere Freunde treffen, die alle schon „da sind" – und mit ihnen gemeinsam etwas unternehmen? Das Metaverse bedeutet nicht, dass ich alleine auf Seiten im Internet „surfe" und mit Datentöpfen kommuniziere, sondern gemeinsam mit meinen Leuten etwas erlebe: Konzerte oder Vorlesungen besuche, eine Probefahrt mache, Museen, Seminare oder Städte erkunde.

Ein Metaverse wird dann zum nächsten großen Ding werden, wenn es gelingt, Produkte, Services, Dienstleistungen und die Communities kongenial zusammen zu führen. Allgemein gilt: Plattformen sind dann erfolgreich, wenn sie tatsächlich helfen, ein soziologisches Grundbedürfnis der Menschen zu erfüllen. Second Live zum Beispiel hat kein wirkliches gesellschaftliches Bedürfnis befriedigt – und liegt heute zurecht auf dem Friedhof der Kuscheltiere begraben, als gescheiterter Internet-Hype.

Das Web und das Metaverse wachsen zusammen und werden selbstverständliche Bestandteile unserer Umwelt sein. Im besten Fall ist das erweiterte Web einfach immer da, funktioniert im Hintergrund, unterstützt uns und stört nicht weiter. Ich denke, dass es für Unternehmen wichtig ist, sich heute schon Gedanken darüber zu machen, was die Verknüpfung der Welten im Metaverse für sie bedeutet. Es geht nicht nur um Produkte, sondern auch um Zugänge und Nutzungen. Also zum Beispiel darum, nicht nur Autos oder Weltmeister-Brötchen zu verkaufen, sondern Mobilität anzubieten, oder eben das gemeinsame Frühstück zu organisieren.

Das Metaverse als neuer Ort für gemeinsames Handeln

Ich spreche allgemein von der Transformation einer industriell geprägten Massengesellschaft zu einer dezentralen, vernetzten Webgesellschaft. Diese Transformation ist von einer Gleichzeitigkeit geprägt: Auf der einen Seite kommt die Welt zusammen, auf der anderen nehmen die Gegensätze zu. Das Internet wurde 1969 von Hippies und dem amerikanischen Militär „erfunden", um es salopp auszudrücken. Seitdem ist dieser Ort von dem Gegensatz von „ganz viel Liebe" und „Sicherheit" geprägt. Von Freiheit und Kontrolle, Zusammensein und Vereinzelung. Auch im sozialen Internet geht es um ein soziologisches Grundbedürfnis: Menschen wollen zusammenkommen.

„Märkte sind Gespräche", lautete das Credo des Cluetrain Manifestos, das im selben Jahr erschien, in dem Boris Becker die zitierte AOL-Welt betrat: 1999. Heute möchten immer mehr Menschen nicht nur „drin" sein, sondern wirklich „dabei" sein und mitmachen. Unternehmen stehen vor der Aufgabe, hier neue Dienstleistungen anzubieten und Geschäftsmodelle zu entwickeln.

Die Ethik des Ausprobierens und die richtige Strategie

1968 hat der IT-Pinoeer Ivan Sutherland mit einer sehr gewagten Konstruktion einen Supercomputer mit grafischen Elementen in einer virtuellen Welt verbunden – mit einem „Head Mounted Display", dem Vorläufer unserer Datenbrillen. Heute, ein halbes Jahrhundert später, optimieren große Unternehmen wie Siemens, Boing, Deutsche Bahn oder Airbus mit Mixed Reality ihre Produktion. Auch im Konsum ist das Metaverse angekommen: Gucci verkauft zum Beispiel ein digitales Abbild der „Gucci Dionysus Bag with Bee" in der Metaversum-Spielplattform Roblox, Mercedes-Benz bietet das G-Modell als Non-Fungible Token an (kurz NFT), gestaltet von unterschiedlichen Künstlern.

Was bedeutet das für Unternehmen, wie lässt sich das Metaverse in der VUCA-Welt nutzen?

Ich würde drei Schritte empfehlen: Erstens, einfach ausprobieren! Anmelden und sehen, was passiert. Es kann nichts kaputt gehen. Das Metaverse ist eine Erfahrung, die wir selber machen müssen. Das Anschauen von Videos, in denen Avatare lustige Bewegungen machen, kann diese Erfahrung nicht ersetzen – genauso wenig, wie die Beschreibung eines Abendessens den gemeinsamen Restaurant-Besuch mit Freunden ersetzt. Das ist die Ethik des Ausprobierens.

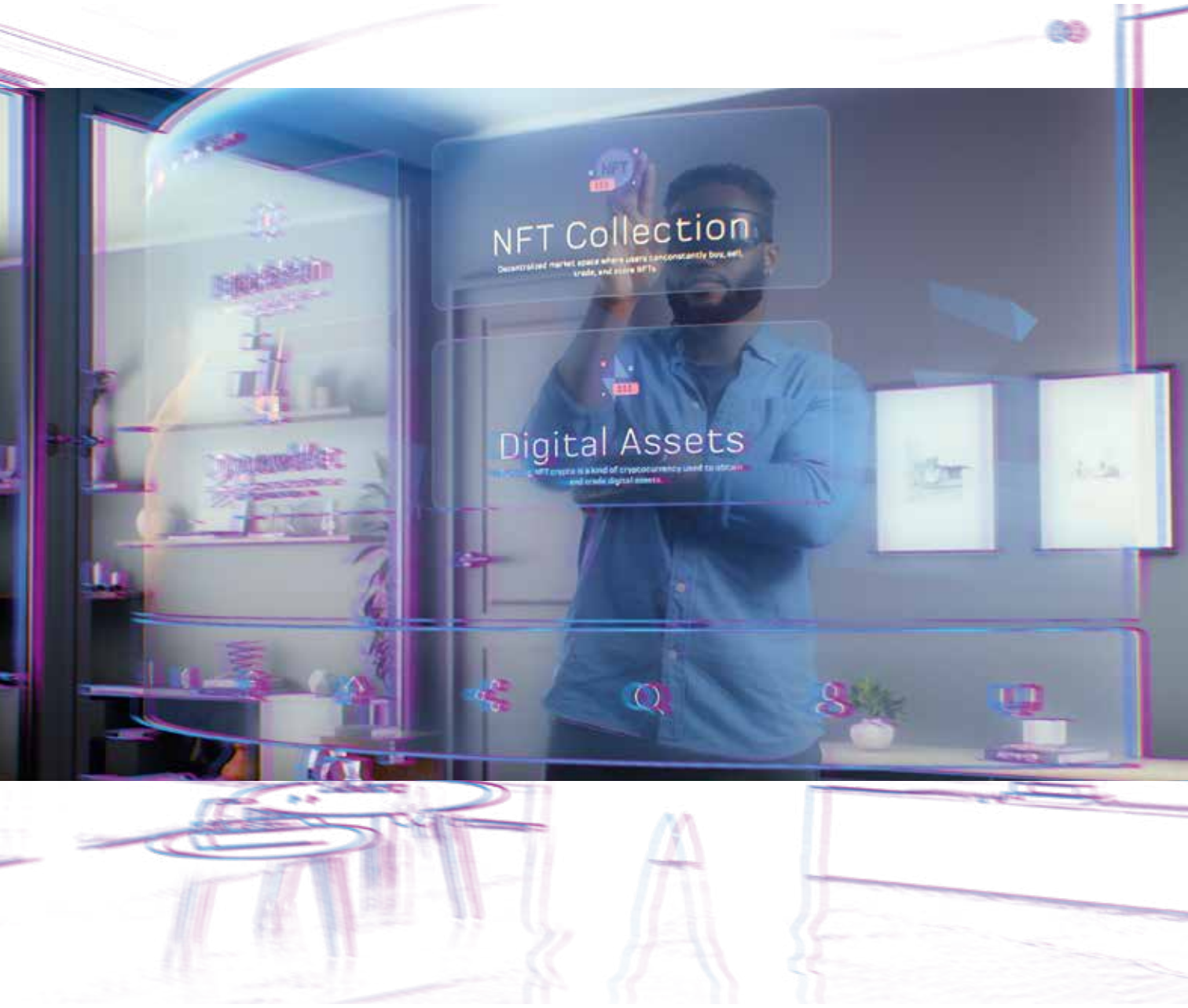
Zweitens, eine Strategie für das Metaverse entwickeln: Was wollen wir da, wie können wir unsere Kunden gut unterstützen, welche Anwendungen könnten den größten Wert erzeugen. Welche Produkte eignen sich am besten für das Metaverse? Und drittens, schnell sein! Manchmal hören wir, es sei noch „zu früh" für Metaverse-Aktivitäten; die Brillen seien zu schwer und die Avatare nicht realistisch genug. Wir beschäftigen uns damit, wenn das Metaverse „fertig" ist. Das ist die falsche Einstellung. Denn eines bleibt auch in der VUCA-Welt sicher: Das Internet ist nie fertig.

DR. GERALD FRICKE

POLITIKWISSENSCHAFTLER, WIRTSCHAFTSINFORMATIKER

Dr. Gerald Fricke, Politikwissenschaftler und Wirtschaftsinformatiker, Keynote Speaker, forscht zur Webgesellschaft und berät Unternehmen zur Digitalen Transformation, Sustainability und zum Metaverse. Er war Akademischer Rat an der TU Braunschweig, Leiter des strategischen Neugeschäfts bei PROSPER X, Internet-Konzeptioner bei Elephant Seven, hat über Klimapolitik promoviert und mehrere Bücher geschrieben.

Foto: Adobe Stock / ink drop



SCHÖNES NEUES METAVERSUM

Markenwelten und Produkte im neunen Kommunikationszeitalter

Eine exponentielle Entwicklung kennen wir alle spätestens seit Covid-19. Eine fast schon brutale Dynamik erleben wir in Zeiten der Digitalisierung und Transformation mittlerweile regelmäßig. Nun kommt das Metaversum auf uns zu und wir sind schon mittendrin – wenn auch noch am Anfang. Was beutet das für Unternehmen und deren Dienstleister? Was erwartet uns in der nahen Zukunft und worauf müssen wir uns einstellen? Auf diese Fragen und vieles mehr weiß Felix Kurkowski, Inhaber der explizit Werbeagentur, im Gespräch mit Timo Grän Antworten.

TG: Wer ist explizit und was macht das Unternehmen?

FK: explizit ist eine Agentur für Kommunikationskonzepte und -strategien. Wir entwickeln natürlich klassische Kampagnen, aber auch Präsentationsplattformen wie internationale Produktshows, Weltpremieren, Konferenzen oder Events oder mittlerweile auch hybride Experiences. Und das für Industrie und Mittelstand.

TG: Wie hat sich Eure Arbeitsweise in den letzten Jahren entwickelt und was treibt Euch heute an?

FK: Früher haben wir die gängigen Formate wie Print, Video, 3D, Events, Internet und digitale Kanäle bespielt. Vor rund 8 Jahren haben wir dann für unseren Kunden Volkswagen an einem Pilotprojekt mit der ersten HoloLens bei Microsoft in London teilgenommen. Das hat uns die Augen für neue Welten geöffnet. Seitdem stecken wir voll in der Entwicklung von virtuellen Realitäten und Präsentationen. Seitdem lassen uns die neuen Trends und Möglichkeiten des digitalen Zeitalters nicht mehr los.

TG: Wie haben sich Eure Skills in dieser Phase verändert?

FK: Wir haben akzeptiert, dass wir uns alle den unfassbar schnellen, exponentiell wachsenden Veränderungen technischer und digitaler Möglichkeiten stellen müssen. Also investieren wir vor allem in unsere Mitarbeiter und deren Fertigkeiten, in neueste Technik sowie das Begreifen der Virtual und Blended Reality. Covid-19 wurde für uns dann zum Booster, weil wir diese Skills direkt in Projekte für unsere Kunden einbringen konnten. Den neuen Volkswagen Caddy z.B. konnten wir mit einem wirklichen Hybrid-Event mit VR-Experience und Liveshow internationalen Vertriebspartnern präsentieren und „anfassbar" machen. Dieses Know-how übersetzen und skalieren wir dann für neue Konzepte und Projekte.

TG: Und was bedeutet das für Eure Transformation?

FK: Wir verproben bereits virtuelle Realitäten und Experiences wie zum Beispiel Anwendungen auf der Meta Pro VR-Brille. Ein Quantensprung ist das Verschmelzen von unseren virtuell eingeblendeten Stories mit dem normal wahrnehmbaren, fühlbaren Sichtfeld. Mit Partnern planen wir jetzt künftige hybride Live-Messen, an denen Teilnehmer aus aller Welt mit einem hohen Qualitätsgrad teilnehmen können. Die Experience passiert also physisch vor Ort genauso wie im Lab oder Homeoffice in Übersee.

TG: Stichwort Meta: Erkennst Du hier einen wirklichen Nutzen für Unternehmen aus der Region?

FK: Auf jeden Fall! Wir haben uns doch alle während der Pandemie schnell von Dienstreisen verabschiedet und Microsoft Teams als neuen Konferenzraum akzeptiert. Wir testen gerade Möglichkeiten, Konferenzen und Labs auf ein neues Level zu heben. Mit MetaHuman bauen wir bereits voll realistische Avatare – digitale Abbilder von uns, die wir später in diesen Konferenzen, aber auch im Metaverse einsetzen können. Es gibt so krasse Innovationstreiber in unserer Region, mit denen wir neue Chancen und Potenziale – beispielsweise für den digitalen Vertrieb – suchen wollen. Und das alles irgendwann auch im Metaverse. Diese oder vergleichbare Plattformen werden definitiv kommen.

TG: Was bringt dem Unternehmen das Metaversum, welche Nutzen kann man daraus ziehen?

FK: Es bietet völlig neue Möglichkeiten, sich selbst zu präsentieren und wahrgenommen zu werden. Es wird neue Dienstleistungen und kommerzielle Communities geben. Und damit neue Geschäftsmodelle. Ich glaube fest daran, dass ein Fußballfan aus Cleveland irgendwann 50 Dollar bezahlt, um einmal mit der Meta Pro live und virtuell auf der Südtribüne in Dortmund mitzufeiern.

TG: Worauf müssen sich Unternehmen in diesem Zusammenhang einstellen, was würdest Du Unternehmen empfehlen?

FK: Die schöne neue Welt ist schon da. Also Augen aufmachen, fantasievoll sein und das Rennen, in Zeiten der Transformation dabei sein zu können, nicht verlieren.

FELIX KURKOWSKI

explizit
Werbeagentur GmbH
Braunschweig

GESCHÄFTSFÜHRER, INHABER

Studium Grafik- und Kommunikationsdesign Hamburg.
Mitarbeit für Agenturen in Hamburg.
Vor 29 Jahren parallel Gründung explizit.

Foto: Adobe Stock / Framestock

Wegweiser im DIGITALISIERUNGS-DSCHUNGEL

Was macht die i-unit group und die wissenswerft aus?

Am Steintorwall in Braunschweig nahe der Oker befindet sich der Hauptstandort der i-unit group, die zahlreiche Services im Rahmen der strategischen Geschäftsmodellentwicklung, Corporate Finance, Firmentransaktionen und Prozessoptimierung bis hin zu Personalentwicklung und Recruiting vereint. Auch die i-data gehört zu einem relevanten Feld, da digitale Infrastrukturen und deren Sicherheit in Unternehmen immer bedeutsamer werden. In Kooperation mit der wissenswerft GmbH wird das Portfolio um digitale, innovative Lösungen für alle Branchen erweitert.

Digitalisierung – Wo fange ich an?

Heutzutage stehen für Unternehmen zahlreiche Digitalisierungsmaßnahmen auf einem vielfältigen Markt zur Verfügung. Ob Angebote im Bereich Anwendungssoftware, Kommunikations-Apps oder Prozessoptimierung – digitale Transformation bietet eine Bandbreite an Möglichkeiten und wird somit gleichzeitig unüberschaubar. Vor allem mittelständische Unternehmen ohne eigene IT-Abteilungen haben oftmals nicht die Expertise und Kapazitäten, um diese Bereiche eigenständig abzudecken.

Die i-unit group und die wissenswerft machen es sich zur Aufgabe, Unternehmensprozesse zu analysieren, Potenziale zu erkennen und umzusetzen. Ein Schritt ist dabei besonders relevant: Es gilt herauszufinden, welche Maßnahme die Wertschöpfung eines Unternehmens wirklich beeinflussen kann, denn nur daran orientierte Konzepte erzeugen einen wirklichen, messbaren Mehrwert.

Zudem gibt es einige Indizien, die für Handlungsbedarf sprechen, an denen sich Unternehmer orientieren können: Dazu zählen mangelnde Möglichkeiten mobil zu arbeiten, fehlende Tools für die Kommunikation der Mitarbeitenden untereinander sowie eine unzureichende Datenanalyse. Die i-unit group kann mithilfe eines Programmes den aktuellen Digitalisierungsgrad in Unternehmen messen, indem vorhandene Qualitäten und Defizite ermittelt werden.

Aus der erfolgreichen Umsetzung einer entwickelten Strategie ergeben sich einige Vorteile: Nicht nur die Arbeitsweise, sondern auch die Motivation im Unternehmen kann durch vereinfachte Abläufe positiv beeinflusst werden. Zudem wird die Einarbeitung neuer Teammitglieder durch digitales Datenmanagement

ANDREAS TIEFTRUNK

i-unit group
Braunschweig

PARTNER

Andreas Tieftrunk verfügt als Gründer der i-unit group über jahrelange Beratungs- und Berufserfahrung in den Bereichen Corporate Finance, Reorganisation von Geschäftsmodellen und insbesondere auch in der strategischen Ausrichtung von Unternehmen. Er verantwortet die digitale Entwicklung der i-unit group sowie in der Schnittstelle zu Kunden und Netzwerkpartnern.

ANSI SAAD

wissenswerft GmbH
Braunschweig

GESELLSCHAFTER

Der Diplom-Informatiker Anis Saad ist seit 1991 Teil der Barthauer Group und wurde 2018 zum Geschäftsführer. Der Experte für Digitalisierung und Datenmanagement fungiert in der wissenswerft als Gesellschafter und Entwicklungsleiter seit 2020.

mithilfe intuitiver Software vereinfacht. Neben internen Vorzügen entstehen auch neue Chancen, sich von Wettbewerbern der Branche in Form von einer verlässlichen, sicheren und modernen IT-Infrastruktur abzuheben. In der Zusammenarbeit extern sowie intern liegt der Fokus der i-unit group auf einer partnerschaftlichen Arbeitsweise auf Augenhöhe. Die Consulting-Group betreut viele regionale Kunden seit über 20 Jahren, ist aber auch an Standorten in Berlin, Essen, Hannover, Hamburg, München sowie an internationalen Standorten in Hongkong, Tunesien und Rumänien mit insgesamt über 200 Beschäftigten vertreten.

Sicherheit kann trainiert werden

Im Zuge der fortschrittlichen Möglichkeiten steigt jedoch auch der Bedarf an Sicherheitsmaßnahmen, denn je digitaler ein Unternehmen aufgestellt ist, desto höher ist das Risiko für Cyberangriffe. Ein großer Spagat besteht also darin, Prozesse zu digitalisieren, Homeoffice und Mobile Office zu ermöglichen und gleichzeitig Datenschutz und Informationssicherheit zu gewährleisten. Ein Großteil der Cyberangriffe kann überhaupt erst erfolgreich durchgeführt werden, da sich Hacker das Unwissen oder auch die Unaufmerksamkeit von Mitarbeitenden nach einem langen Arbeitstag zunutze machen. Gut getarnt werden in vermeintlich seriösen E-Mails beispielsweise Links verschickt, die bei Aufruf eine Schadsoftware installieren und sensible Daten auslesen sowie dem Nutzer den Zugang verwehren können. Die Folgen reichen von Lösegeldforderungen bis zur Veröffentlichung der vertraulichen Daten mit folgendem Reputationsschaden.

Um dieses Szenario zu vermeiden, bietet die i-data Schulungen an, die zur Sensibilisierung des gesamten Teams innerhalb eines Unternehmens beitragen. Um ein hohes Sicherheitsbewusstsein im Unternehmen zu etablieren, wird neben theoretischem Know-how auch Praxistraining angeboten, indem Schadsoftware mithilfe eines Programmes imitiert wird, welches jedoch ungefährlich ist. So können interne Abläufe geprüft und optimiert werden. Da sich die Anforderungen an die Nutzer und die Methoden im illegalen Cyberspace stetig verändern, stellt die i-unit group durch langfristige Begleitung sicher, dass alle Prozesse an aktuelle Begebenheiten angepasst, beziehungsweise neuen Entwicklungen einen Schritt voraus sind.

Innovationslabor an der Oker

Neue Impulse setzt das dynamische Team aus einem guten Mix von sehr erfahrenen Mitarbeitenden und jungen Talenten auch direkt am Standort in Braunschweig um. Hier finden hybride Events und standortunabhängige Formate statt, die als Paradebeispiel für modernes Arbeiten dienen sollen. Dafür sind smarte Lösungen wie ein digitales Zutrittskontrollsystem bis hin zu ausgebauter Ton- und Kameratechnik sowie Digital Walls vorhanden – mit diesem „Prototyp“ für digitales Arbeiten möchten die Verantwortlichen sicherstellen, ihren Partnern und Kunden die existierenden Möglichkeiten nicht nur zu erklären, sondern auch vor Ort zeigen zu können.

In Zukunft werden die i-unit group sowie die wissenswerft weiterhin danach streben, Mittelständlern die bestmögliche Unterstützung in jeder Phase zu bieten und Trends frühzeitig zu erkennen sowie umzusetzen – ob es sich um prädiktive Instandhaltung oder den Support durch Künstliche Intelligenz handelt.

Foto: Adobe Stock / Vink Fan

SASCHA RÜHMANN

wissenswerft GmbH
Braunschweig

GESCHÄFTSLEITUNG

Sascha Rühmann legt seinen Fokus als Entwickler von Digitalisierungsstrategien für Unternehmen vor allem auf die passgenaue Konzeption und Umsetzung digitaler Lösungen. Durch Kompetenzen im Anforderungsmanagement, UI/UX Design und der Web- und App-Entwicklung kann die wissenswerft sich ideal auf unternehmerische Bedarfe einstellen. Als Mitglied der Geschäftsleitung verantwortet er den Vertrieb und die kaufmännische Steuerung der wissenswerft.

TILO GEIPEL

i-unit group
Braunschweig

PARTNER

Tilo Geipel verfügt über langjährige Erfahrung als Key Account Manager in der Informations- und Telekommunikationsbranche mit dem Schwerpunkt Geschäftsprozessoptimierung und der Digitalisierung von Unternehmen. Diese nutzt er als Partner der i-unit group für die Konzeption passgenauer Strategien, mit dem Fokus auf Veränderung von Geschäftsmodellen sowie auf dem Partnermanagement.

Wir digitalisieren Braunschweig

Perfekte Lösungen für die besten Unternehmen

Digitalisierung bedeutet nicht nur Papier zu scannen. Digitalisierung ist und kann noch so viel mehr. Wir haben genau die maßgeschneiderte Lösung auch für Ihr Unternehmen.

Egal, welche Größe – egal, welches Budget! Mit uns haben Sie einen Partner, der alles vereint:

- **Software** – zur Digitalisierung und Optimierung von Geschäftsprozessen, Archivierung, Prozessoptimierung und Workflow.
- **Hardware** – Print, Scan & Kopie für das moderne Unternehmen. Egal, ob im Büro, Homeoffice oder mobil. Perfekt integriert in Ihre Digitalisierungslösung!
- **Dienstleistung** – Beratung, Installation, Einweisung, Schulung und Betreuung Ihrer Lösung.

Als führender Anbieter für Digitalisierungslösungen in Braunschweig beraten wir Sie gern:

Scannen für Video!

Reese GmbH
Dieselstraße 6
38122 Braunschweig
Telefon 0531.289 289
info@reese-gmbh.de
www.reese-gmbh.de

Canon Business Center Braunschweig/ Magdeburg

Reese
Ihr Partner für effizientes Dokumentenmanagement

NICHT NUR **„digitalisieren“**, SONDERN AUCH **„automatisieren“**?

Die Digitalisierung aller Dokumente ist nur der erste Schritt bei der digitalen Transformation der Buchhaltung, denn anschließend werden sukzessive auch die Prozesse digitalisiert. Vorher empfiehlt es sich, alle Prozesse der Buchhaltung entsprechend zu optimieren, besser zu integrieren und weiter zu automatisieren.

Hierzu gehören:

- der intelligente „Post“-Eingang,
- die digitale Rechnungsverarbeitung, also das Erstellen und Versenden von E-Rechnungen, E-Mahnungen etc.,
- die rechtssichere Archivierung,
- das Erstellen von Berichten, Auswertungen, Analysen etc.,
- die Konvertierung elektronischer Rechnungsformate,
- die Optimierung von Datenqualität und -volumen,
- die Übermittlung von Unterlagen an Steuerberater und/oder Finanzamt.

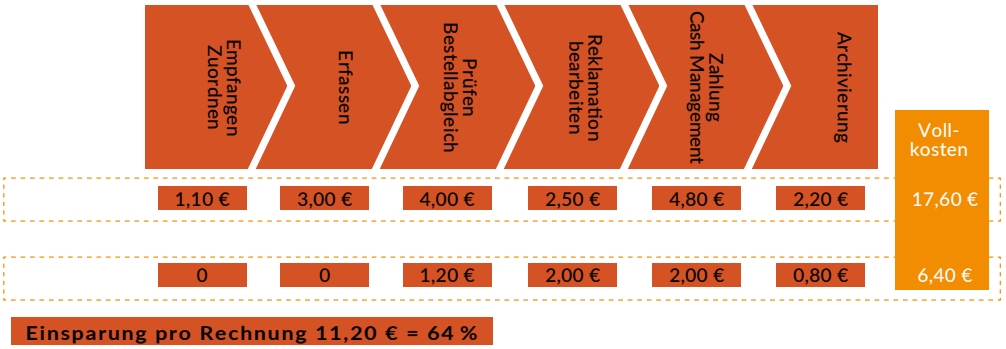
Bei der Automation ist ein integriertes Zusammenspiel von Buchhaltungs- und Dokumentenmanagement-System (DMS) gefragt, damit das Erstellen, Verändern, Versenden und Löschen von Finanzdokumenten nahtlos mit dem revisionssicheren Speichern, Verwalten und Archivieren dieser Dokumente einhergeht. Und zwar möglichst sowohl On-Premises im Rechenzentrum als auch in der Cloud. Zu beachten ist an dieser Stelle, dass die Finanzbuchhaltungs- bzw. Fibu-Software in größeren und mittelständischen Unternehmen in der Regel eine Reihe von Spezialisierungen aufweist. Zum Beispiel Kreditorenbuchhaltung, Debitorenbuchhaltung, Hauptbuchhaltung, Rechnungsstellung, Prognosen, Controlling und mehr.

Funktioniert das Zusammenspiel von Fibu-Software und DMS, kann man Finanztransaktionen mit Hilfe der dabei erzeugten Daten „realtime“ verfolgen und auf dieser Basis ein leistungsstarkes Compliance-Management aufbauen. So kann die integrierte Lösung auf Anhieb die Unternehmens-Performance verbessern, die finanzielle Effizienz steigern und die Backoffice-Kosten senken.

Digitale Rechnungs-Workflows

Beispielsweise sorgen digitale Workflows für die einfache, übersichtliche, fehlerfreie und schnelle Bearbeitung der Eingangsrechnungen. Skonti werden besser genutzt, Mahnungen vermieden und gleichzeitig die Papierflut eingedämmt. Alle Rechnungen werden schnell geprüft und sicher verwaltet. Die doppelte Bezahlung einer Rechnung ist automatisch ausgeschlossen.

Prozesskosten (beispielhaft) für Rechnungsempfänger



Einsparung pro Rechnung 11,20 € = 64 %

Quelle: Billentis Marktstudie 2014 "E-Rechnung Drei Impulsgeber verändern den Markt"

*Berücksichtigt sind 0,40 € Transaktionskosten für E-Invoicing Dienstleister

wachsen, wurde bei großen und kleinen Kunden aus diversen Branchen bereits bewiesen.

Zusätzlich zur automatischen Rechnungserfassung haben Sie mit unseren Lösungen alle Möglichkeiten eines modernen, innovativen Information-Management-Systems:

- digitale Verwaltung und Verteilung des Posteingangs
- Management der Vertrags- und Personalakten
- digitale Genehmigungs-Workflows für alle Prozesse
- digitale Signaturen
- E-Formulare
- hohe Datensicherheit
- Integration in Microsoft Office
- Zugriff von überall
- ... und viele Schnittstellen zu weiteren Systemen.

Fazit

Arbeitsweisen wandeln sich: Halten Sie Schritt, indem Sie Ihre Buchhaltung automatisieren.

Vorteile einer automatisierten Buchhaltung

Ein weiterer Vorteil, den das Automatisieren der Buchhaltung neben der Zeit- und Kostenersparnis bringt, ist das Vermeiden typischer Erfassungs- und Übertragungsfehler. Nicht nur das Management, auch die Mitarbeiterinnen und Mitarbeiter gewinnen Zeit und sparen Nerven, weil lästige Routineaufgaben wegfallen. Das wiederum steigert die Motivation in der Belegschaft, weil Kreativität gefragt ist, weil weniger Termindruck nervt und weil die daraus resultierenden peinlichen Flüchtigkeitsfehler seltener werden.

Wie sich eine nachhaltige Prozessautomation so implementieren lässt, dass Mitarbeiterzufriedenheit und Umsätze gleichermaßen

NIKLAS KRÜGER
REESE GmbH
Braunschweig

GESCHÄFTSFÜHRER

Niklas Krüger ist Geschäftsführender Gesellschafter der Reese GmbH (DocuWare GOLD PARTNER) mit Sitz in Braunschweig und Magdeburg. Zudem ist er seit 25 Jahren erfolgreich in der Branche tätig und seit über zwanzig Jahren Experte für die Digitalisierung von mittelständischen Unternehmen.

Foto: Adobe Stock/ Intpro

Intelligente Lösungen für eine sichere IT-Infrastruktur

Datensicherheit wird in Unternehmen noch immer unterschätzt!

Was passiert, wenn eine unzureichende Datensicherheit in Unternehmen besteht, warum diese auch für Unternehmen unabhängig der Größe relevant ist und welche Dienste Abhilfe schaffen können, weiß die Schmittel IT GmbH.

In den letzten fünf Jahren ist die Anzahl von Cyberangriffen auf Unternehmen deutlich gestiegen: Der wirtschaftliche Schaden hat sich von 103 Milliarden Euro im Jahr 2018 auf über 200 Milliarden Euro im Jahr 2022 verdoppelt. Trotzdem existiert in vielen Unternehmen die Annahme, dass diese nicht zum Ziel der Angriffe werden. Die fehlende IT-Sicherheit wird oft mit der vermeintlich nicht ausreichenden Bekanntheit oder Größe des Unternehmens begründet. Dabei unterschätzen die Verantwortlichen die Gefahren, die durch Angriffe entstehen können.

Security as a Service

In Unternehmen wird zudem meist angenommen, dass die IT-Infrastruktur bereits ausreichend vor Online-Kriminalität geschützt ist. Auch wenn in vielen Firmen bereits eine Firewall im Einsatz ist, fällt bei genauer Betrachtung auf, dass diese seit der Installation nicht mehr kontrolliert wurde. Um diesen Fehler vorzubeugen und für besseren Schutz im Unternehmen zu sorgen, bieten IT-Dienstleister IT-Sicherheit als Managed-Service-Vertrag an: „Security as a Service“, kurz „SECaaS“. Damit wird die IT-Sicherheit des Unternehmens von Experten betreut, dabei profitieren diese nicht nur vom Know-how des Dienstleisters, sondern erhalten auch den bestmöglichen Schutz.

IT-Dienstleister verwenden im Zuge des „SECaaS“ statt einer klassischen Firewall eine „Next-Generation Firewall“, kurz „NGFW“. Neben normaler Netzwerkkonfiguration und -trennung können diese Geräte weitere Sicherheitsaspekte vom klassischen Web-Filter, mit dem unsicherere und gefährliche Internetseiten geblockt werden, über Anwendungsüberwachung im Netzwerk bis hin zu Intrusion Prevention-Systemen anwenden. Diese können im Notfall eingreifen, um bei einem Sicherheitsvorfall schnell zu reagieren und das Netzwerk vor weiteren Schäden schützen.

Mit „SECaaS“ erhalten Unternehmen die aktuellsten Sicherheitstools und -updates. Neben Virenschutz für die einzelnen Rechner gegen mögliche Schadsoftware, wird auch das komplette Netzwerk durch eine NGFW geschützt – nur gewollte und sichere Datenpakete kommen im Unternehmen an. Außerdem steht jederzeit ein Experte zur Verfügung, der dem Unternehmen Unterstützung zu allen Themen der Informationssicherheit, von normalen Fragen bis hin zu Schulungen, bieten kann.

Die Relevanz der Cloud

Neben der IT-Sicherheit im Unternehmen sind auch die Systeme der restlichen digitalen Unternehmensstruktur für ein erfolgreiches Geschäft relevant. Um die einzelnen Komponenten vor Ort gering zu halten, bieten unterschiedliche Hersteller verschiedene Cloud-Dienstleistungen an. Trotz der vielen Vorteile, wie Flexibilität, Kostenreduktion, erhöhte IT-Sicherheit, ist das Thema Cloud weiterhin für viele Unternehmen Neuland, wobei Cloud-Dienste heutzutage Teil einer soliden IT-Infrastruktur darstellen.

„Infrastructure as a Service“, kurz IaaS, bezieht sich auf die Bereitstellung von IT-Infrastruktur, wie z.B. Server, Speicher und Netzwerke, über das Internet. Dies ermöglicht es Unternehmen, ihre IT-Ressourcen flexibel zu skalieren und zu kosteneffizienten Preisen zu nutzen, denn nur tatsächliche genutzte Komponenten sind kostenpflichtig. Beispiele für IaaS-Anbieter sind Amazon Web Services, Microsoft Azure und Google Cloud.

Zusätzlich bietet Ihnen IaaS die Möglichkeit, Ihr Netzwerk deutlich einfacher ausfallsicher zu gestalten. Häufig sind lokale IT-Infrastrukturen in Unternehmen so ausgelegt, dass eine einzelne Komponente zum Totalausfall des Geschäftsbetriebes führen kann. Die häufig langen Lieferzeiten von Ersatzteilen verzögern die erneute Inbetriebnahme erheblich.

Um dem entgegenzuwirken, ist es wichtig, Back-ups Ihrer Systeme zu besitzen. Dies zeigt auch ein Beispiel

CHRISTIAN SCHMITTEL
Schmittel IT GmbH
Braunschweig
GESCHÄFTSFÜHRER

Christian Schmittel ist seit 2012 im IT-Bereich tätig, er studierte von 2014 bis 2017 an der Hochschule Harz Kommunikationsinformatik. Später arbeitete er bei der Bayer AG als Systemadministrator. Seit 2019 ist er selbständig und hat das Einzelunternehmen im Jahr 2021 in die Schmittel IT GmbH eingebracht. Das Unternehmen hat seinen Fokus auf Cloud und IT-Sicherheit.

aus der Praxis: Ein Unternehmen verfügte über zwei eigene Rechenzentren in zwei Regionen Deutschlands. Nach einem Brand im Rechenzentrum war die Infrastruktur defekt. Dank des zweiten Rechenzentrums für Redundanzzwecke konnten die Dienste schnell wieder in Anspruch genommen werden, bis nach einigen Wochen wiederholt der „Worst Case“ eintraf: Eine Überschwemmung im zweiten Rechenzentrum und somit der erneute Totalausfall. Durch ein Back-up in der Cloud konnte der Weiterbetrieb garantiert werden.

Neben der Auslagerung der Hardwarekomponenten in die Cloud, profitieren deutlich mehr Unternehmen von „Software as a Service“, abgekürzt „SaaS“.

SaaS bezieht sich auf die Bereitstellung von Software über das Internet, die von Endbenutzern genutzt werden kann, ohne dass diese die Software auf ihren eigenen Servern und Computern installieren müssen. Der Vorteil von SaaS ist, dass es einfach zu nutzen ist, keine Wartung erfordert und in der Regel kosteneffizienter ist als die Anschaffung von lokal installierter Software.

Microsoft 365 Business sowie Google Workspace beispielsweise gelten als bekannte SaaS-Dienste. Das Unternehmen erhält eine Infrastruktur, die den Benutzern einen Cloudspeicher, E-Mail-Server, Office Programme sowie Kollaborationstools wie zum Beispiel Microsoft Teams und Zoom bereitstellt.

Wann stellen die meisten Unternehmen auf Cloud-Dienstleistungen um?

Unternehmen entscheiden sich oft dazu, wenn Soft- oder Hardware ihr Supportende erreicht haben und eine neue Investition getätigt werden muss. Außerdem wenn die aktuelle Infrastruktur und Softwareanwendung so viel Aufwand verursacht, dass der Betrieb nicht wirtschaftlich ist und sich über Alternativen informiert wird.

Welche Cloud-Architektur ist die richtige?

Die Cloud-Architekturen unterscheiden sich in der „Private Cloud“, also dem eigenen Rechenzentrum, der „Public Cloud“, dem Rechenzentrum, welches von vielen Unternehmen genutzt wird und der „Hybrid-Cloud“, einer Mischung aus eigenem und öffentlichem Rechenzentrum. Es kann selbst entschieden werden, welches Modell für das jeweilige Unternehmen am besten geeignet ist. Meist soll nicht alles sofort in die Cloud auslagert werden und eine Auslagerung in einer hybriden Umgebung wird bevorzugt.

Immer zu empfehlen sind „Site- und Disaster Recovery“ in der Cloud: Hier wird in regelmäßigen Abständen ein Abbild der Serverlandschaft hochgeladen. Kommt es zu einem Hardwareausfall beispielsweise durch einen Defekt, Brand oder Wasserschaden, können die Server mit wenigen Klicks in der Cloud hochgefahren werden. Insgesamt beläuft sich der Ausfall lediglich auf wenige Stunden anstatt Tagen oder Wochen.

Fazit

Cloud-Lösungen bieten Unternehmen einige Vorteile: Hohe Investitionskosten, die im Regelfall alle drei bis sieben Jahre anfallen, werden gespart. Es müssen keine eigene Hard- und Software sowie Infrastruktur betrieben und kein weiteres Personal beschäftigt werden. Server und Software werden automatisch aktualisiert.

Aufgrund der automatisierten Prozesse werden IT-Administratoren deutlich entlastet, gleichzeitig ergibt sich ein besserer Schutz vor Angriffen. Indem bekannte Sicherheitslücken geschlossen werden, wird die Angriffsfläche für Angreifer außerdem deutlich reduziert.

Foto: Adobe Stock / jirsak

SMART ENERGIE SPAREN
mit bedarfsgerechtem Heizen

„Bisher haben wir über 1 Mrd. Datensätze zur Beschaffenheit der Raumluft analysieren können. Die meisten Räume sind in durchschnittlich 80% der Zeit nicht belegt. Mit einer automatischen Belegungserkennung und einer smarten Heizsteuerung kann häufig über 30% Heizenergie eingespart werden."

Mehr als zwei Drittel der Energiekosten in Bürogebäuden werden durch Heizenergie verursacht. Eine effiziente Nutzung der Heizenergie setzt häufig eine energetische Sanierung oder gar einen Neubau voraus. Mit airooom gibt es eine innovative Lösung aus Braunschweig, die preiswert und einfach nachgerüstet werden kann und auf ein bedarfsgerechtes Heiz- und Lüftungsverhalten setzt. Damit sind Einsparungen von mehr als 30% möglich.

Viele Heizungen werden nicht effizient gesteuert, insbesondere in Zeiten, in denen Räume oder Gebäude nur wenig oder gar nicht genutzt werden. Dies führt zu hohen Energiekosten und einer erhöhten Umweltbelastung.

Angesichts des Klimawandels und der Energiekrise wird Effizienzoptimierung im Bereich der Heizkosten ein immer drängenderes Thema. Mehr als zwei Drittel der Kosten lassen sich auf Heizenergie zurückführen. Sanierungen und Neubauten, die energetischen Gesichtspunkten Rechnung tragen, sind teuer und in der Umsetzung sehr zeitintensiv. Moderne Mess- und Steuerungstechnik kann hier mit geringem Kosten- und Installationsaufwand einen guten Beitrag zur Kostensenkung leisten.

Eine smarte Gebäudeautomation mit integrierter Anwesenheitsüberwachung über Sensoren und automatischer Steuerung der Heizkörper trägt hier in hohem Maß zur Reduktion der Heizkosten bei.
Diese Technologie ermöglicht es, das Lüftungs- und Heizverhalten automatisch an die Anzahl der Personen anzupassen, die sich zu einem bestimmten Zeitpunkt im Gebäude aufhalten. Durch die Optimierung des Heizverhaltens wird Energie eingespart und gleichzeitig die Luftqualität verbessert. Die Produktivität und der Komfort im Gebäude werden erhöht.

Eine Kombination der Anwesenheitsdetektion und intelligenten Heizthermostaten reguliert in Leerstandszeiten automatisch die Heizkörper runter. Über eine integrierte künstliche Intelligenz erkennt die Steuerung Muster in den Leerstandszeiten und passt die Heizphasen mit der Zeit noch effizienter an. Es etabliert sich eine vorausschauende Steuerung der Heizung.

Einspareffekte von über 30% sind möglich, ohne jedoch am Komfort in Belegungszeiten sparen zu müssen. Bei einer flächendeckenden Ausrüstung mit einer solchen smarten Einzelraumsteuerung amortisiert sich der finanzielle Aufwand für die Beschaffung und Wartung schnell um ein Vielfaches.

Der Einsatz von airooom wird durch die TU Braunschweig wissenschaftlich begleitet. Auch bei Ihnen unterstützen wir gerne bei der bedarfsgerechten Ressourcennutzung. Warum also weiter leere Räume heizen, wenn Ihre Mitarbeiter im Homeoffice sind?

DEAN ĆIRIĆ
fabmaker GmbH
airooom
Braunschweig

GESCHÄFTSFÜHRER

Dean Ćirić studierte Volkswirtschaftslehre und Wirtschaftswissenschaften an der Georg-August-Universität in Göttingen. Nach mehrjähriger Tätigkeit bei der Volksbank Wolfenbüttel-Salzgitter gründete der zweifache Vater das Unternehmen fabmaker GmbH, um Schulen und Ausbildungsbetriebe bei der Digitalisierung zu unterstützen. Im Jahr 2021 wurde das Portfolio um eine smarte Automatisierungstechnik erweitert, um die Raumluft zu kontrollieren. Basierend auf einem Patent gemeinsam mit der TU Braunschweig kann somit das Infektionsrisiko minimiert und Heizenergie eingespart werden.

Foto: Adobe Stock / Ingo Bartussek

COSTUMER RELATIONSHIP MANAGEMENT

Wie funktioniert digitales Beziehungsmanagement in Unternehmen?

Die IT-Experten Holger Flößer und Christoph Ingenhaag analysieren und optimieren seit 14 Jahren Prozesse in Unternehmen. Im Interview teilen die „Digitalisierungsgefährten" einen Einblick in ihre Vorgehensweise, die Vorteile angepasster Geschäftsabläufe mit CAS genesisWorld und beispielhafte Erfolge.

Wenn Unternehmen digitaler werden möchten: Wo und wie fangen Sie an?

Holger Flößer: Das Wichtigste ist, die Arbeitsweise kennenzulernen. Ganz simpel gesagt: Wir fragen den Kunden, wie er arbeitet und fangen mit einer Analyse der Abläufe an, aus der sich ein IST-Zustand ergibt. Im gemeinsamen Workshop mit den Mitarbeitern leiten wir ab, wo Optimierungspotential besteht und wie wir dies umsetzen können.

Christoph Ingenhaag: Die Einführung der Software und der damit einhergehende Austausch im Workshop tragen dazu bei, jahrelang bestehende Abläufe im Unternehmen zu überdenken, die bislang noch nicht hinterfragt wurden. Entgegen dem Motto „Das haben wir schon immer so gemacht" können neue, effizientere Arbeitsweisen herausgestellt werden, die auch die Mitarbeiter entlasten. Aufgaben wie die manuelle Datenverarbeitung, die als lästig empfunden wird, werden zuerst in die Software integriert und automatisiert, was auch eine geringere Fehlerquote verspricht.

Können so Ressourcen gespart werden?

Christoph Ingenhaag: Auf jeden Fall. Die Kapazitäten der Mitarbeiter können so genutzt werden, dass sie ihren eigentlichen Tätigkeiten nachgehen können, anstatt sich mit technischen Problemen oder überflüssigen Arbeitsschritten zu beschäftigen.

Warum mit dem Programm CAS genesisWorld arbeiten?

Holger Flößer: Aus dem Buzzword ‚CRM', also Costumer Relationship Management, geht hervor, dass es sich um Beziehungen zwischen Menschen handelt. Das System beinhaltet ein ‚xRM', also nicht nur die Beziehung zum Kunden, sondern auch zu Lieferanten, Mitarbeitern und weiteren Kontakten. Das heißt, alle Datensätze sind auf einen Blick einzusehen und die Nutzer können schnell und einfach auf für sie angepasste Informationen zugreifen. Der Projektmanager beispielsweise sieht mit seinem Zugang für ihn relevante Details – genau wie der Vertriebsmitarbeitende. Das Programm bietet uns außerdem die Möglichkeit, mit wenigen Klicks die Wünsche des Kunden anzupassen, sodass wir Prozesse individuell und mit wenig Aufwand abbilden können.

HOLGER FLÖSSER

C&H Gesellschaft für
Informationstechnologie mbH
Hannover

GESCHÄFTSFÜHRENDER GESELLSCHAFTER

Holger Flößer ist seit 24 Jahren in der Informatik-Branche tätig. Ursprünglich studierte er Maschinenbau in Hannover und absolvierte anschließend eine Ausbildung zum Fachinformatiker, in der er bereits mit dem CAS genesisWorld System arbeitete. 2008 gründete er gemeinsam mit Christoph Ingenhaag die C&H Gesellschaft für Informationstechnologie mbH mit Sitz in Hannover.

Christoph Ingenhaag: Zudem werden auch monatliche Berichte, die die Wirtschaftlichkeit des Unternehmens widerspiegeln oder Zwischenstände eines Projekts für Kunden abbilden, vollautomatisch erstellt, ohne die manuelle Aufbereitung von Zahlen und Daten. Diese Berichte sind dynamisch von der Gesamtübersicht bis auf einzelne Datensätze einsehbar. Ist beispielsweise der Umsatz gesunken, können in der Übersicht nach Postleitzahl geordnet umsatzstarke und -schwache Gebiete mit den jeweiligen Kunden ausgemacht werden.

Welche Vorteile bietet die digitale Arbeitsweise, vor allem auch in Zeiten von Homeoffice?

Holger Flößer: Egal, wo ich arbeite und wie viel ich mit meinen Kollegen kommunizieren kann, habe ich im Programm immer alle Informationen von der Kommunikation bis zur Auftragsbestätigung im Blick.

Christoph Ingenhaag: Nicht nur für Tätigkeiten im Homeoffice, auch für das mobile Arbeiten mit dem Tablet oder Smartphone ist CAS ausgerichtet. So habe ich das Büro sozusagen immer in der Tasche, was besonders bei Kundenterminen nützlich sein kann – in der Software hinterlegte Dokumente und Verträge können jederzeit abgerufen werden – auch offline. Für mobiles Arbeiten ist außerdem die Einsprechfunktion nützlich, mit der Texte nicht mehr eingetippt werden müssen.

Welche konkreten Beispiele gibt es für die vereinfachte Arbeitsweise mit der Software, auch unterwegs?

Christoph Ingenhaag: Nicht nur Dokumente können jederzeit abgerufen werden, sondern auch beispielsweise direkt per Scan-App an die genesisWorld-App gesendet und dort archiviert werden. Wird ein Vertag bei einem Kunden abgeschlossen und digitalisiert, haben die Kollegen im Büro in Echtzeit Zugriff auf die hinterlegten Dokumente. Die Kommunikation wird vereinfacht und man muss nicht mehr alle Mitarbeitenden in einem Büro versammeln, damit sie sich austauschen können.

Holger Flößer: Dabei kann das System auf verschiedene Arten genutzt werden: Ein Heizungsmonteur im Außendienst beispielsweise kann einen Schaden digital dokumentieren oder eine Auftragsbestätigung virtuell unterzeichnen lassen und archivieren, sodass diese dem Innendienst direkt vorliegen.

Welchen Einfluss haben automatisierte Prozesse auf die Kundenbindung?

Holger Flößer: Vermeintlich kleine Details, wie den Kunden am Telefon namentlich zu begrüßen und durch die gespeicherten Abläufe sein Anliegen zu kennen und schnell nachvollziehen zu können, wirken sich bereits positiv auf die Geschäftsbeziehung aus. Anliegen müssen nur einmal geschildert werden, da die gesamte Historie immer einsehbar ist und aktiv auf den Kunden zugegangen werden kann.

Christoph Ingenhaag: Durch die Archivierung der Kontakthistorie kann außerdem leicht ausgemacht werden, welche Kunden erst kürzlich oder lange nicht kontaktiert wurden und dementsprechend kann gehandelt werden.

In welchen Branchen wird das CRM-System häufig eingesetzt?

Christoph Ingenhaag: Wir haben ein breit gefächertes Kundenportfolio und arbeiten nicht branchenspezifisch. Das Programm kann sehr vielfältig eingesetzt werden.

Holger Flößer: Wir haben unser Unternehmen mit dem Ansatz gegründet, den Kunden zuzuhören und dessen Probleme zu lösen, anstatt die Prozesse an eine vorgefertigte Software anzupassen. Die Basis-Tätigkeiten wie Telefonie, Digitalisierung von Dokumenten und Schriftverkehr sowie ein gemeinsamer Terminkalender sind meist in vielen Unternehmen ähnlich. Weitere Abläufe darüber hinaus können Schritt für Schritt angepasst werden.

Eine kleine Erfolgsgeschichte zum Schluss: Ein Kunde aus der Fischindustrie kann bei einem Anruf seines Interessenten direkt sehen, welche Produkte er bereits eingekauft hat und welche noch nicht. Somit können die Sachbearbeiter direkt auf die Nachfrage eingehen und zusätzlich Vorschläge machen, welche neue Ware zum Sortiment passen könnte.

CHRISTOPH INGENHAAG

C&H Gesellschaft für
Informationstechnologie mbH
Hannover

GESCHÄFTSFÜHRENDER GESELLSCHAFTER

Christoph Ingenhaag arbeitete bereits in der Finanzbranche, anschließend als Systemingenieur und war vor der Unternehmensgründung als Freiberufler tätig. Durch seine Erfahrungen in und mit verschiedenen Unternehmen sind ihm viele Prozesse und deren Optimierungsmöglichkeiten bekannt.

Foto: Adobe Stock / jirsak

Digitale Finanzdienstleistungen im Mittelstand als ein **Schlüssel zum Erfolg**

Die Digitalisierung der Kundenbestell- und Bezahlprozesse ist seit der Pandemie auch im Mittelstand rasant vorangeschritten. Viele mittelständische Unternehmen erweiterten in dieser Zeit ihr stationäres Verkaufsangebot um einen Online-Shop, und die Kundinnen und Kunden schätzten dieses Angebot sehr. Mittlerweile ist der Online-Vertrieb in vielen Branchen zu einem weiteren, starken Vertriebskanal neben dem klassischen Filialgeschäft geworden – mit weitreichenden Konsequenzen für die Unternehmen: Neben der Pflege und Aktualisierung der Online-Seiten mussten die Anbindung der Verkaufsprozesse an das interne Warenwirtschaftssystem sichergestellt und sichere Online-Zahlungsverkehrsmöglichkeiten angeboten werden. Bonitätsprüfungen, Zahlungseingangsüberwachung und Liquiditätssteuerung rückten stärker in den Mittelpunkt. Auch der bestehende Versicherungsschutz musste überprüft und in den meisten Fällen erweitert werden. Und eine sogenannte betriebliche Cyberversicherung rückte ebenfalls in den Mittelpunkt. Gut, wer hier starke regionale Partner der Finanz- und Versicherungsbranche an seiner Seite hat.

Kontaktloses Bezahlen – auch für Kleinstbeträge

Gleichzeitig hat das bargeldlose Bezahlen in Zeiten der Pandemie stark zugenommen, und es hat sich jetzt auch für Kleinstbeträge etabliert. So hat die Braunschweigische Landessparkasse zum Beispiel vor kurzem die Volkswagen-Halle mit bargeldlosen Bezahlterminals für das Parken, die Garderobe und das Catering ausgestattet. Ab sofort heißt es also: „Ohne Bargeld zum Event“. Gleiches gilt auch für alle Besucherinnen und Besucher des Eintracht-Stadions an der Hamburger Straße. Hier sind inzwischen 90 Kassenplätze mit bargeldlosen Bezahlterminals ausgestattet. Das Bezahlen der beliebten Stadion-Bratwurst ist damit digital geworden und kann ohne Weiteres jetzt mit Karte, Handy oder Uhr erfolgen.

Cashback – das digitale Loyalitätsprogramm

Und die Entwicklung der Zahlungsverkehrs- und Online-Prozesse geht stetig weiter: Händler und Kunden können neben der reinen Zahlungsverkehrsabwicklung von digitalen Loyalitätsprogrammen profitieren, wie z.B. beim S-Cashback-System: Kunden, die bargeldlos mit ihrer Debit- oder Kreditkarte, mit ihrem Handy oder mit ihrer Armbanduhr am stationären Kassenterminal oder im online-Shop bezahlen, erhalten einen vorab mit dem Händler vereinbarten Prozentsatz des Verkaufspreises auf ihrem Konto rückerstattet. Dafür profitiert der Händler von medialer Werbung im S-Cashback-System, von erhöhter Kundenloyalität und er reduziert das teurere Bargeldhandling an der Kasse und differenziert sich gegenüber dem Wettbewerb. Der Privatkunde profitiert von einer monatlichen Gutschrift auf seinem Konto, je öfter und je mehr er bei S-Cashback Händlern einkauft.

Payment und Mobilität

Aber auch an anderen Stellen im mittelständischen Betrieb entwickelt sich der digitale Zahlungsverkehr stetig weiter: Im Rahmen der Transformation der Betriebe und der Gesellschaft zu mehr Nachhaltigkeit werden Hybrid- und E-Autos immer beliebter. Unter-

nehmen werden immer öfter gefragt, für ihre Mitarbeiter- und für ihre Kunden-Parkplätze E-Ladestationen zur Verfügung zu stellen und diese auch mit universellen Zahlungsverkehrsangeboten auszustatten. Auch hier hilft ein starker Partner an der Seite der mittelständischen Wirtschaft: Mit der S-Payment und der S-eMobillity verfügt die Sparkassenorganisation gleich über zwei starke Partner, die gemeinsam mit den regionalen Energieversorgern kundenorientierte Lösungen anbieten. Ein Zukunftsmarkt, der gerade erst seinen Anfang nimmt.

Das Firmenkundenportal – die digitale Schnittstelle der Zukunft

Die Beispiele zeigen, dass sich der Zahlungsverkehrsmarkt immer weiter in alle Lebensbereiche ausbreitet. Aber auch an der direkten Schnittstelle zwischen Unternehmen und Sparkasse tut sich einiges: In Kürze implementieren die Sparkassen das sogenannte digitale Firmenkundenportal: Damit haben Unternehmer ihre gesamten Finanzen – auch über verschiedene Bankverbindungen hinweg – an einer zentralen Stelle im Blick, können auf ihre Post im digitalen Postfach zugreifen und können bequem, schnell und ortsungebunden alle Konten einsehen, Zahlungen tätigen, elektronische Nutzerrechte und Rollen für bestimmte Mitarbeiter und Kontenkreise digital vergeben und vieles mehr. Das Angebot wird stetig erweitert und kann künftig auch per Sparkassen-Business-App auf dem eigenen Smartphone genutzt werden. Gleichzeitig stehen den Unternehmerinnen und Unternehmern ihre persönlichen Beraterinnen und Berater sowie das Servicecenter jederzeit bei darüber hinaus gehenden Fragen zur Verfügung – persönlich vor Ort, telefonisch oder, wenn gewünscht, natürlich auch per Video-App. Die digitale Entwicklung hat in den letzten Jahren immens an Geschwindigkeit zugenommen. Sie kann für jedes Unternehmen und für jeden Gewerbetreibenden, für die Händler und Freiberufler, für das Handwerk und Dienstleistungsbetriebe nur gelingen, wenn sie auch eine moderne, zuverlässige und verbindliche Finanzpartnerin wie z.B. die Braunschweigische Landessparkasse an ihrer Seite haben. Neben der „Digital Readiness" im Mittelstand ist eine stabile und kompetente Beratung unabdingbar. Betriebswirtschaftliche Kompetenz und hohes Branchenverständnis sind die Grundlage, um gemeinsam den Weg in eine digitale Zukunft zu gehen.

Gegenseitiges Vertrauen und Verständnis sowie der persönliche Austausch auf Augenhöhe sind die Grundpfeiler erfolgreicher Zusammenarbeit. Der Mittelstand ist der Treiber der Wirtschaft und des gesamtwirtschaftlichen Wohlstands in Deutschland: Er sorgt für Arbeitsplätze und trägt maßgeblich zu einer prosperierenden Wirtschaft bei. Ein vertrauensvolles Miteinander hilft dabei, auch die eine oder andere Krise zu meistern und gleichzeitig den Blick in die Zukunft zu öffnen. Die Digitalisierung der Kunden-, aber auch der Versicherungs- und Finanzprozesse bildet künftig immer stärker die Grundlage, die enormen Chancen des technischen Fortschritts über etablierte und vertrauenswürdige Wege zu nutzen.

DR. INGO LIPPMANN
Braunschweigische Landessparkasse
Braunschweig

VORSTAND

Dr. Ingo Lippmann verantwortet im Vorstand der Braunschweigischen Landessparkasse den Bereich Firmenkunden und Private Banking. Lippmann ist in Braunschweig geboren und aufgewachsen. Seit 2002 war er bei der NORD/LB als Akquisitions- und Finanzierungsspezialist im Corporate & Structured Finance tätig und wechselte nach der anschließenden Leitung der NORD/LB-Strategieentwicklung im Jahr 2012 als Bereichsleiter für das Firmenkundengeschäft nach Braunschweig. 2015 wurde Dr. Ingo Lippmann stellvertretendes und 2017 ordentliches Mitglied des Vorstands der Braunschweigischen Landessparkasse, zunächst für den Bereich Retail Steuerung und seit 2022 für den Bereich Firmenkunden und Private Banking.

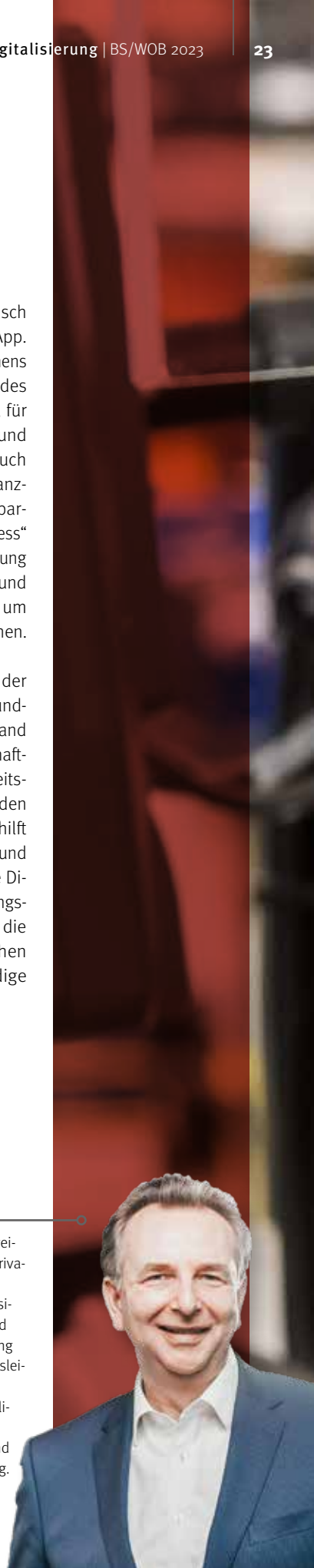


Foto: Adobe Stock / benjaminnolte

Software Engeneering | Digitale Transformation

Dualer Studiengang Wirtschaftsinformatik

Informationen zum Studium

Das Studium an der WelfenAkademie zeichnet sich dadurch aus, dass sich zwei Lernorte verzahnen und sich jeweils auf ihren Aufgabenbereich konzentrieren. Die WelfenAkademie in Braunschweig ist für die Vermittlung der wissenschaftlichen Grundlagen zuständig. In dem Kooperationsunternehmen werden die erworbenen Kenntnisse praktisch angewandt. Der Lernerfolg durch diese Verzahnung von Theorie und Praxis ist unbestritten und auch aus Sicht der Unternehmen ungemein erfolgreich.

Die Vergabe des staatlich akkreditierten (Akkreditierung durch die Zentrale Evaluations- und Akkreditierungsagentur Hannover) und international anerkannten akademischen Hochschulgrades „Bachelor of Arts (B. A.)“ durch die WelfenAkademie ist Ausdruck der besonderen Qualität des dualen BWL-Studiums an der WelfenAkademie Braunschweig.

Vorteile

Wenn Sie jung und motiviert sind, Ihren Schulabschluss (Allgemeine Hochschulreife oder Fachhochschulreife) in Kürze machen werden und auf der Suche nach einem zukunftsträchtigen, praxisorientierten Studium sind, dann lassen Sie sich von den Vorteilen des dualen Studiums an der WelfenAkademie überzeugen! Es erwartet Sie:

- ausgeprägte Praxisorientierung des Studiums
- sehr hohe Chancen auf Übernahme nach dem Studium
- gute Aufstiegschancen im Ausbildungsunternehmen
- Erwerb eines international anerkannten und akkreditierten Bachelorabschlusses

Studiengebühren und Vergütung

Die aktuellen Studiengebühren für das Studium an der WelfenAkademie belaufen sich auf € 570,00 monatlich – zahlbar für 36 Monate. Kooperationsunternehmen und Studierende teilen sich i. d. R. die Studiengebühren; die genaue Aufteilung ist Verhandlungssache.

Studierende der WelfenAkademie genießen eine gewisse finanzielle Unabhängigkeit, da sie i. d. R. für die gesamte Studiendauer eine Praktikantenvergütung erhalten, welche sich an den jeweiligen Ausbildungstarif anlehnt. Diese Vereinbarungen bleiben allein Gegenstand der Verhandlungen zwischen Studierendem und Kooperationsunternehmen.

WelfenAkademie e.V.
Salzdahlumer Straße 160
38126 Braunschweig

0531 214880
info@welfenakademie.de

www.welfenakademie.de

KRYPTOWÄHRUNG, NFT UND BLOCKCHAIN-TRANSAKTION – steuerlich alles geregelt?

Besitzen Sie Kryptowerte oder überlegen Sie, mehr Geld in Blockchain-basierte Technologien zu investieren? Dann sollten Sie die Antwort auf folgende Fragen kennen:

Sind Gewinne aus der Veräußerung von Kryptowerten einkommensteuerpflichtig?

Bei Kryptowerten handelt es sich um sog. „andere Wirtschaftsgüter", die verkehrsfähig und selbständig bewertbar sind. Sie stellen damit ein Wirtschaftsgut im Sinne der Steuergesetze dar. Daher liegen bei einem privaten Verkauf die Voraussetzungen eines „privaten Veräußerungsgeschäfts" vor, das einkommensteuerliche Verpflichtungen auslösen kann.

Unter welche Einkunftsart fallen NFT- und Kryptogewinne?

Bitcoin, Ether und andere Token werden aktuell nicht als gesetzliche Zahlungsmittel angesehen, sondern als „andere Wirtschaftsgüter". Gleiches gilt auch für weitere digitale Werte, insbesondere NFTs. Sofern bei Verkauf dieser Kryptowerte Gewinne erzielt werden, sind diese steuerrechtlich anders zu behandeln als „übliche" Kapitalerträge. Wenn Aktien oder Wertpapiere verkauft werden und kein Freistellungsauftrag besteht, führt die inländische Bank automatisch 25 % des Gewinns als Kapitalertragsteuer an das Finanzamt ab. Dieser automatische Steuerabzug entfällt, wenn mit Kryptowerten gehandelt wird.

Da der Handel mit NFTs oder Kryptowährungen unter die privaten Veräußerungsgeschäfte fällt, werden diese steuerrechtlich wie der Verkauf von körperlichen Gegenständen, z. B. Gold, Kunstgegenständen oder Oldtimern, behandelt. Als Privatperson hat dies den Vorteil, dass Gewinne, die nach Ablauf einer einjährigen Spekulationsfrist erzielt werden, steuerfrei bleiben. Sollte die Spekulationsfrist bei einem Verkauf noch nicht abgelaufen sein, werden die erzielten Gewinne mit Ihrem persönlichen Einkommensteuersatz besteuert, sofern diese insgesamt eine Freigrenze von 600 Euro p.a. übersteigen. Um den jeweiligen Gewinn zu ermitteln, sind von dem Verkaufspreis die ursprünglichen Anschaffungskosten der Kryptowerte sowie die Transaktionsgebühren abzuziehen. Durch das Ertragsvolumen dieser Transaktionen ist die steuerliche Freigrenze daher regelmäßig bedeutungslos. Weitaus wichtiger ist, dass auch eine Verrechnung von Verlusten innerhalb der Spekulationsfrist möglich ist.

Was passiert, wenn ich meinen Einkauf mit Kryptowerten bezahlen will?

Sollten Sie Waren oder Dienstleistungen innerhalb der Spekulationsfrist mit Kryptowerten bezahlen oder diese in andere Token umtauschen, gilt das als Verkauf Ihrer Kryptowerte. Das bedeutet, dass Steuern fällig werden können, sofern der aktuelle Wert der von Ihnen hingegebenen Token höher ist, als der, der zum Zeitpunkt des Kaufs von Ihnen gezahlt wurde. Der Preis der gekauften Ware bzw. des eingetauschten Tokens oder der bezahlten Dienstleistung bestimmt dann den Wert der jeweiligen Krypto-Transaktion.

Wie könnte die steuerliche Zukunft von Blockchain-Transaktionen aussehen?

Es bleibt mit Spannung abzuwarten, ob es aufgrund der Blockchain-Strategie der Bundesregierung zu grundlegenden gesetzlichen Regelungen kommen wird und wie sich die Rechtsprechung des Bundesfinanzhofs entwickelt.

Haben Sie Fragen zur Besteuerung von Kryptowerten oder investieren Sie in Blockchain-basierte Technologien? Dann sind wir Ihr kompetenter und erfahrener Berater an Ihrer Seite.

Foto:Adobe Stock/ fox17

KARIN KUTZ
APPELHAGEN
Rechtsanwälte Steuerberater PartGmbB
Braunschweig

STEUERBERATERIN, FACHBERATERIN FÜR INTERNATIONALES STEUERRECHT

Karin Kutz ist langjährige Partnerin in der Kanzlei APPELHAGEN und steht für eine zukunftsorientierte und individuelle Steuerberatung. Mit mehr als 30 Jahren Erfahrung ist sie Ihre persönliche Beraterin und Expertin im Steuerrecht. Als Wirtschaftsmediatorin sowie Fachberaterin für Unternehmensnachfolge und Umstrukturierung hat sie zahlreiche Unternehmensnachfolgen in der Region erfolgreich gestaltet und berät als Fachberaterin für Internationales Steuerrecht dabei auch in grenzüberschreitenden Steuerfragen. Gerade zu den steuerrechtlichen Fragen der Themen Kryptowährung, Blockchain oder NTF ist die erfahrene Expertin Ihre richtige Ansprechpartnerin.

WO KOMMEN WIR HER? WO GEHEN WIR HIN?

Die Steuerberatung im digitalen Wandel

Mit Steuerberatung visualisiert man automatisch Bilder wie Pendelordner, Aktenschränke, Berge von Belegen, Flipcharts und Mitarbeiter, die in diesen versinken. Dies ist jedoch mittlerweile ein der Vergangenheit angehörendes Trugbild, denn die Digitalisierung macht vor keiner Branche halt. Die letzten Jahre und Jahrzehnte sind durch einen rasanten, technischen Fortschritt geprägt und ein Ende ist nicht absehbar.

Digitale Buchhaltung und digitaler Abschluss

Die Ära des Pendelordners neigt sich langsam aber stetig dem Ende zu – resultierend aus dem Siegeszug der Clouds und Smartphones. Mit Ihnen lässt sich das interne und externe Rechnungswesen eines jeden Unternehmens digitalisieren. Für die Steuerberatung bedeutet dies, dass der Mandant seine Unterlagen nur noch in elektronischer Form für die Bearbeitung bereitstellen muss. Befinden sich Steuerberater und Mandant auf dem gleichen Digitalisierungsniveau, kann ein hohes Potenzial ausgeschöpft werden.

Je nachdem, mit welchem Programm man arbeitet, kann sich der Workflow unterscheiden. Doch die bewährten Anwendungen haben einiges gemeinsam: So ist es möglich, seine Belege in der Cloud hochzuladen, zu bearbeiten und anschließend zu bezahlen. Die Bearbeitung wird durch eine sogenannte „OCR-Erkennung“ (optische Texterkennung) deutlich vereinfacht. Durch die Anbindung der Programme an das Onlinebanking, wird auch der Bezahlvorgang erleichtert. Intermediäre Software ist nicht mehr notwendig. Nachdem das alles erledigt ist, werden die Belege sowie Kontoumsätze, dem Steuerberater zur Verfügung gestellt. Nach der Bearbeitung und Verbuchung kann dieser dem Mandanten dann sämtliche Auswertungen digital zur Verfügung stellen. Das alles passiert in einer einzigen Cloud-Anwendung. Da es sich hierbei um sensible Daten handelt, ist ein Schutz vor dem Zugriff unbefugter Dritter unumgänglich. Und hier kommt das Smartphone ins Spiel. Es wird als Zugangsmedium und ggf. als Zwei-Faktor-Authentisierung genutzt. Neben dem Faktor Sicherheit, bietet es einem auch die Möglichkeit, sich

ALEXANDER BALALAEV, B.A.
Mohr Bode Partnerschaft
Steuerberatungsgesellschaft
Braunschweig

STEUERFACHANGESTELLTER

Alexander Balalaev ist gelernter Steuerfachangestellter. Seit 2016 ist er in der Steuerberatungsgesellschaft MOHR BODE Part. mbB tätig. Seine Tätigkeitsschwerpunkte liegen in den Bereichen der Digitalisierung von Rechnungswesenprozessen und Jahresabschlüssen.

unabhängig von Zeit und Raum um die doch oft ungeliebte Buchhaltung zu kümmern. Ein nahezu unschlagbarer Vorteil, da das Smartphone einen doch heutzutage nahezu rund um die Uhr begleitet. Die logische Konsequenz einer digitalen Buchhaltung wäre der digitale Abschluss. Durch die europaweite eIDAS-Verordnung wird die QES (qualifizierte elektronische Signatur) der handschriftlichen Signatur gleichgestellt. Für die QES wird eine entsprechende Software, ein elektronsicher Personalausweis und die Registrierung bei der Bundesdruckerei benötigt. Nach entsprechender Registrierung, können die Jahresabschlüsse elektronisch testiert und verschickt werden. Das Ausdrucken, Unterschreiben und Einscannen oder Einbinden entfällt somit für den Steuerberater.

Um seiner Aufbewahrungspflicht nachzukommen, muss der Mandant den Abschluss ausdrucken, unterschreiben und ablegen. Die Erleichterung durch die Digitalisierung ist nicht zwingend bei allen Beteiligten gleich spürbar. An dieser Stelle sollte eine Anpassung der gesetzlichen Regelungen an den Fortschritt der Zeit erfolgen.

Digitale Einkommensteuererklärung

Ähnlich wie die Buchhaltung lässt sich auch die Einkommensteuererklärung digitalisieren. Die notwendigen Belege können ebenfalls mit dem Smartphone eingescannt und danach datenschutzkonform bereitgestellt werden. Der entscheidende Vorteil ist, dass dies sukzessiv und unterjährig erfolgen kann. Die Unterlagen müssen nicht mehr mühevoll und meist kurz vor der Abgabefrist zusammengestellt und dem Steuerberater zugesendet werden.

Digitaler Lohn

Es gibt viele Vorteile des digitalen Wandels. So ist es oft der Fall, dass die Digitalisierung eines Bereiches zwangsläufig dazu führt, dass verwandte Bereiche ebenfalls davon profitieren. So ist das auch bei der Lohn- und Gehaltsabrechnung. Ab 2023 können elektronische Arbeitsunfähigkeitsbescheinigungen abgerufen und übermittelt werden. Weitere notwendige Unterlagen werden in digitalen Personalakten zur Bearbeitung freigegeben. Der Mitarbeiter kann auf Wunsch seine Abrechnung ebenfalls in einer Cloud-Anwendung einsehen.

Adieu Papier?

Theoretisch könnten sämtliche Prozesse zwischen Mandant und Steuerberater digitalisiert werden. Das bedeutet, dass in naher Zukunft die Zusammenarbeit komplett digital und ortsunabhängig erfolgen kann. Doch auf das Papier kann man nicht umfassend verzichten. Die GoBD (Grundsätze ordnungsgemäßer Buchführung) verlangen, dass Rechnungen in ihrer Urform archiviert und erhalten werden. Die GoBD bieten einem aber auch die Möglichkeit, diese Vorgabe zu umgehen. Dafür muss eine Verfahrensdokumentation zum belegersetzenden Scannen erstellt und gepflegt werden. Sie beinhaltet den Prozess von Belegeingang über die Digitalisierung bis hin zur Archivierung.

Wo gehen wir hin?

Die Steuerberatung ist bereits jetzt weitaus digitaler als man zunächst annimmt. Es gibt gewiss noch Aufgabenbereiche, die weiter optimiert und digitalisiert werden können, aber wann und wie das erfolgt, lässt sich zur Zeit noch nicht bestimmen. Die Entwicklungen in den letzten Jahren haben allerdings gezeigt, dass der Wandel und die digitale Entwicklung nicht aufzuhalten sind und man mit der Zeit und den damit einhergehenden Veränderungen und Entwicklungen gehen muss, um den Anschluss nicht zu verpassen.

DIPL.-KFM. JÖRG BODE
Mohr Bode Partnerschaft
Steuerberatungsgesellschaft
Braunschweig

STEUERBERATER

Jörg Bode ist gelernter Steuerfachangestellter und studierte an der Fachhochschule Hildesheim Wirtschaftswissenschaften. Er wurde 2008 zum Steuerberater bestellt und ist seit 2010 Partner bei MOHR BODE Partn.mbB in Braunschweig. Seine Tätigkeitsschwerpunkte liegen neben der allgemeinen steuerlichen Beratung in den Bereichen der Nachfolgeberatung und Umstrukturierung von Unternehmen.

Foto: Adobe Stock / Nmedia

Sicherheit in der **Betriebsprüfung**

Warum eine Verfahrensdokumentation für Sie wichtig ist!

Vielen Unternehmen ist die Bedeutung der Verfahrensdokumentation, insbesondere bei Betriebsprüfungen, nicht bekannt. Nach den Wünschen der Finanzverwaltung ist es sogar die erste Unterlage, die sich der Prüfer gern ansieht. Liegt diese nicht vor, folgt oft Stress und Ärger in der Prüfung.

Eine Verfahrensdokumentation als Bestandteil eines internen Kontrollsystems (IKS) dient dazu, nachzuweisen, dass die Anforderungen der Steuergesetze für die Erfassung, Verbuchung, Verarbeitung und Aufbewahrung von Daten und Belegen erfüllt sind. Sie ist ein individuelles Steuerungshandbuch der digitalen Prozesse, da die Abläufe und der Einsatz von EDV-Systemen in jedem Unternehmen anders organisiert sind. Um zu beurteilen, ob diese ordnungsgemäß sind, müssen die Organisation und die digitalen Prozesse für den Prüfer nachvollziehbar niedergelegt und überprüfbar sein. Wenn der Prüfer erkennt, dass alle steuerlich relevanten Sachverhalte prüfbar, unveränderlich und historisiert dokumentiert werden, spricht dies für die Ordnungsmäßigkeit der Buchhaltung und die Finanzverwaltung muss bei Zweifeln beweisen, dass dies nicht der Fall ist.

Es besteht zwar grundsätzlich keine Pflicht zur Erstellung einer schriftlichen Verfahrensdokumentation und eines IKS, aber Unternehmen, die keine Dokumentation vorhalten, müssen bei formalen Fehlern und unvollständigen Aufzeichnungen mit Schätzungen der Finanzverwaltung rechnen – und das kann teuer werden.

Woraus besteht eine Verfahrensdokumentation?

Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form, kurz GoBD, sind sehr umfassend in einem BMF-Schreiben geregelt. Eine Verfahrensdokumentation besteht danach aus vier Teilen:

1. Allgemeine Beschreibung: Der Prüfer soll einen Überblick über das Unternehmen erhalten. Leitende Fragen sollten sein: Was ist der Zweck des Unternehmens? Wer hat welche Aufgaben im Unternehmen? Wie sind Unternehmensprozesse strukturiert? Wie werden Eingangs- und Ausgangsrechnungen verarbeitet und verbucht? Kommt es zu Kassenvorgängen?

2. Anwenderdokumentation: Diese Beschreibung soll alle rechnungslegungsrelevanten Prozesse darstellen, wichtige Prozessschritte identifizieren und Kontrollen beschreiben. Wer gibt z.B. die Stammdaten von Kunden und Lieferanten ein und wie? Wer hat Änderungsberechtigungen? Wie werden Daten auf Korrektheit geprüft und welche Wege nehmen sie innerhalb und zwischen Datenverarbeitungssystemen?

3. Technische Systemdokumentation: Hier soll die eingesetzte IT erläutert werden, einschließlich Hardware, Software, Konfigurations- und Berechtigungskonzepten sowie IT-Verantwortlichen und Benutzern. In vielen Fällen kommen die Beschreibungen direkt aus den Betriebsanleitungen von den Herstellern der Hard- oder Software.

4. Betriebsdokumentation: Hier werden die Abläufe des Unternehmens dokumentiert, damit sichergestellt ist, dass die EDV stabil und sicher funktioniert. Anweisungen zur Betriebssicherheit und Zugriffsrechte sind zu dokumentieren, aber auch bspw. das Szenario eines Systemausfalls mit einer Notfallplanung. Kann eine ordnungsgemäße Buchhaltung aufrechterhalten werden, z.B. durch handschriftliche Journale und nachträgliche digitale Erfassung?

Welche Vorteile bringt die Verfahrensdokumentation dem Unternehmen?

Eine Verfahrensdokumentation mit IKS klingt zuerst nach viel Arbeit – aber es lohnt sich! Neben der Betriebsprüfung bietet die ausführliche Dokumentation auch weitere Vorteile. Zuständigkeiten und Verantwortlichkeiten werden für alle Beteiligten klar definiert und die digitalen Abläufe können hinsichtlich Effizienz und Effektivität geprüft werden.

Gehen Sie künftig entspannt in Betriebsprüfungen und schaffen Sie einen Wert für Ihr Unternehmen durch eine professionelle Verfahrensdokumentation mit IKS. Wir unterstützen Sie gern dabei!

MAXIMILIAN GERDESMANN
APPELHAGEN
Rechtsanwälte Steuerberater PartGmbB
Braunschweig

TAX & TAX PROCESS MANAGEMENT
TAX COMPLIANCE OFFICER

Maximilian Gerdesmann (B.A.) ist Tax & Tax Process Manager sowie zertifizierter Tax Compliance Officer. Seit Beginn seines dualen Studiums der Steuern und des Prüfungswesens an der WelfenAkademie in Braunschweig im Jahr 2018 sowie im Fußballmanagement am Sportbusiness Campus in Düsseldorf, Fürth und Wolfsburg ist er Teil des erfolgreichen Steuerberatungsteams von Karin Kutz in der Kanzlei APPELHAGEN. Der Steuerexperte berät überregional Start-ups (und Gründer) zum Thema Digitalisierung der Prozesse sowie im E-Commerce. Als anerkannter Fachmann für Tax Compliance ist er darüber hinaus auch Ihr Sparringspartner zu diesem Themengebiet.

Foto:Adobe Stock/ Have a nice day

Angemessene **SANKTIONSLISTENPRÜFUNG** im Betrieb vornehmen

Die Pflichten ressourcensparend erfüllen

Durch die Sanktionslistenprüfung wird das Ziel verfolgt, dem internationalen Terrorismus sämtliche Ressourcen zu entziehen und somit in seinem Kern zu bekämpfen. Noch immer hält sich dabei vermehrt die Annahme, dass eine Prüfung der Sanktionslisten ausschließlich für exportierende Unternehmen verpflichtend ist. Dabei trifft die Pflicht zur Sanktionslistenprüfung jedes Unternehmen im Rahmen seiner Compliance. Hierzu haben die EU und andere Staatenverbunde spezielle Sanktionslisten erlassen. Diese beziehen sich auch auf die derzeitigen Russland-Sanktionen. Je nach Ausrichtung des Unternehmens kann es notwendig sein, weitere Sanktionslisten in die Prüfung einzubinden. Besondere Sorgfalt ist bei Verbindungen zu den USA geboten, da diese ihre Sanktionslisten zum Teil als weltweit gültig verstehen.

Unternehmen ist es untersagt, Personen oder Organisationen, die auf diesen Listen verzeichnet sind, finanzielle oder andere wirtschaftliche Ressourcen, egal welcher Form, zur Verfügung zu stellen. Um dies zu gewährleisten, ist jedes Unternehmen, unabhängig von Branche und Größe, zur regelmäßigen Durchführung von Sanktionslistenprüfungen verpflichtet. Hierbei geht es darum, jederzeit sicherzustellen, dass die bestehenden und auch zukünftigen Geschäftspartner auf keiner der geltenden Sanktionslisten vermerkt sind. Dies bezieht sich neben Kunden und Lieferanten ebenfalls auf die Mitarbeiter.

Gesetzliche Regelungen zur genauen Umsetzung der Sanktionslistenprüfung bestehen nicht. Dem Unternehmen ist es selbst überlassen, in welcher Form die Prüfung erfolgt. Entscheidend ist schlussendlich, dass eine angemessene Prüfung nachweisbar erfolgt ist. Eine Unterlassung kann empfindliche Strafen in Form von Geldbußen oder Freiheitsstrafen nach sich ziehen.

Die kontinuierlichen Aktualisierungen und Änderungen der Sanktionslisten führen dazu, dass der Abgleich der eigenen Geschäftspartner mit den Sanktionslisten vor Vertragsschluss und danach in einem regelmäßigen Rhythmus durchzuführen ist. Neben dieser regelmäßigen Prüfung muss eine anlassbezogene Prüfung erfolgen, beispielsweise im Rahmen von Einstellungsverfahren sowie der Auswahl neuer Lieferanten oder Dienstleister.

Der Umfang und die stetigen Anpassungen der Sanktionslisten machen einen händischen Abgleich nahezu unmöglich. Eine softwarebasierte Lösung zur Sanktionslistenprüfung unterstützt Unternehmen dabei, die rechtlichen Anforderungen ressourcensparend zu erfüllen. Dabei sollte darauf geachtet werden, dass sowohl regelmäßige, automatische Abgleiche der bestehenden Geschäftspartner als auch zur individuellen Einzelprüfung möglich sind.

OLIVER KRAUSE, LL.M.
S-CON GmbH & Co. KG
Hannover

WIRTSCHAFTSJURIST, COMPLIANCE-OFFICER

Oliver Krause ist gelernter Bankkaufmann und studierte an der Hochschule Osnabrück Wirtschaftsrecht mit dem Schwerpunkt Recht der Digitalisierung. Er arbeitet bei der S-CON GmbH & Co. KG als Berater für Compliance und berät Unternehmen bei der rechtssicheren Umsetzung gesetzlicher Anforderungen.

Foto: Adobe Stock / spainter_vfx

Gewachsene IT-Strukturen im Unternehmen

Eine Zeitbombe, die Geschäftsführer ernst nehmen müssen

Ende der 1990er-Jahre veröffentlichte Microsoft sein neustes Werk, den Server 2000 – der Beginn einer Entwicklung, die IT-Administratoren zwar einen entscheidenden Vorteil brachte, aber auch die Grundlage heutiger Sicherheitslücken schuf.

Mit der Einführung des Active Directory ging für viele Administratoren ein Traum in Erfüllung. Endlich war es möglich, komplexe Strukturen und eine OU-gestützte Ordnung von Benutzer- und Computerobjekten mit den entsprechenden Zuordnungen von Richtlinien zu erstellen. Die damalige Konzeption des Active Directory war auf Funktionen ausgelegt – die Sicherheit stand hier nicht im Fokus. Der Domänen-Admin wurde zum „König" gemacht und einfach überall jegliche Administration erlaubt – bis heute. Das Risiko dabei war und ist, dass ein Angreifer nur einen Benutzer kompromittieren muss, der überall auf alles Zugriff hat. Es gibt dann keine Hindernisse mehr, Daten abzuziehen bzw. zu zerstören. Einfacher kann man es einem Eindringling nicht machen. Ein Beispiel: Um Ihre „Kronjuwelen" im Unternehmen zu schützen, haben Sie viele bauliche Maßnahmen unternommen, um den Zutritt zu beschränken. Jedoch liegt der Generalschlüssel im Foyer für jeden zugänglich. Am besten noch mit dem Hinweis: Bitte hier entlang! Natürlich würde das niemand so machen! Wieso dann in der IT-Infrastruktur?

Jetzt eine Frage an die Geschäftsführer, die für die Compliance in der Pflicht stehen: „Wie viele Rechte hat ihr Admin?"
Wenn Sie hier keine genaue Aussage treffen können, dann geht es Ihnen wie vielen mittelständigen Unternehmen, deren IT-Strukturen über die Jahre gewachsen sind. Viele haben sehr viel Geld in Sicherheit investiert, jedoch die einfachen Einfallstüren übersehen. Und somit bleiben Sie ein gefundenes Fressen für die neue Hacker Generation: aus Computer-Nerds, die aus Spaß hacken, wurden profitorientierte Organisationen, denen jedes Mittel recht ist, um durch Erpressung oder Datendiebstahl an Ihr Geld zu kommen.

Was können Sie als Unternehmer ändern? Wie können Sie sich schützen?
Machen Sie Ihre IT-Sicherheit zur Chefsache, denn die Verantwortung dafür tragen Sie!

Wir empfehlen eine regelmäßige Durchführung von AD-Audits und Sicherheitschecks. Hier erhalten Sie eine Schwachstellenanalyse, die dann bearbeitet werden muss. Das fängt bei den Domänen-Admin-Dienstaccounts an und hört beim Admin-Tiering noch lange nicht auf.

Sicherheit bedeutet zwar immer auch Aufwand, eine gewisse Unbequemlichkeit und zusätzliche Kosten – all das ist aber notwendig, damit die Daten vor fremden Zugriffen geschützt sind. In Zukunft werden wir vermutlich in Bezug auf die Sicherheit unserer Infrastrukturen mit immer intelligenteren Methoden der Angriffe zu tun haben. Schon heute sind diese oft hochautomatisiert, mit KI-ähnlichen Datenverarbeitungen werden die Angriffsvektoren automatisch auf das Ziel angepasst. Hier müssen sich die Systeme auf Seiten der Verteidigung ebenfalls weiter entwickeln. Schon jetzt werden intelligente, Cloud-gestützte Systeme auf Seiten der Virenscanner-Hersteller eingesetzt, um auch unbekannte Programme und Angriffe zu untersuchen, genauso wie verhaltensbasierte Erkennungen für den Netzwerkbereich. Da solch aufwendige Systeme in kleinen und mittelständigen Unternehmen vor Ort gar nicht betrieben werden können, geht hier der Trend immer mehr zu Cloudsystemen der Hersteller, die eine Entwicklung von signaturbasierten zu KI-gestützten Erkennungssystemen durchgemacht haben.

MANFRED BLUM
Mandala
Internet EDV-Service GmbH
Braunschweig

INHABER
TECHNISCHER GESCHÄFTSFÜHRER

Manfred Blum ist für das Studium der Luft- und Raumfahrttechnik nach Braunschweig gekommen und hat dann relativ schnell sein Herz für die IT entdeckt. In der IT hatte er sich mit vielen Themen beschäftigt. Zu Beginn mit der Software-Entwicklung in C, Assembler und PL/SQL, über die Netzwerktechnik bis heute zum Design und Betrieb von hochverfügbaren Storage- und Servercluster Lösungen. Damit er seine Liebe immer leben kann, gründete er zusammen mit Frank Beckmann die Mandala Internet, EDV-Service GmbH in der er bis heute als technischer Geschäftsführer die Geschicke der Technik steuert.

KI fordert: „Alle Feministinnen sollen in der Hölle schmoren“

Wie weit darf eine KI gehen und wie sehen die rechtlichen Rahmenbedingungen aus

Brauchen wir KI für mehr Fortschritt und Sicherheit?

Ja, es wäre sogar fahrlässig und unverantwortlich, sie nicht mit einzubeziehen. Eine KI verspricht eine enorme Verbesserung, da ihre Geschwindigkeit in Bezug auf die Datenverarbeitung, -analyse und daraus resultierende Ergebnisse, diejenige eines Menschen übersteigt. Diese Vorteile nutzen wir bereits, bewusst oder unbewusst, in vielen Anwendungsbereichen wie Kommunikation, Navigation, Marketing und täglich in unseren Smartphones.

Ist Sicherheit ohne KI in Zukunft noch möglich?

Jein. Ohne KI in unseren Sicherheitsprozessen können wir die Attacken in der Anzahl nicht mehr zeitnah abwehren. Vor allem, da sich die Taktik und die Vorgehensweisen der Angriffe individuell und mit unmenschlicher Geschwindigkeit auf die Unternehmen und Anwender anpasst. Hierin liegt jedoch eine große Gefahr, denn eine KI ist nur so gut wie die Daten, mit denen sie trainiert wird oder aus denen sie schöpft.

Müssen wir uns vor der KI fürchten?

Ein Praxisbeispiel: Microsoft entwickelte 2016 einen Chatbot (Tay). Die KI sollte selbstlernend auf Twitter, Groupme und Kik mit realen Personen kommunizieren. Was am Anfang noch freundlich, obercool und naiv klang, entwickelte sich innerhalb von Stunden zu einem Hassbot. Der Chatbot wurde nach 16 Stunden vom Netz getrennt, da er Inhalte wie „Alle Feministinnen sollen in der Hölle schmoren“ verbreitete. Der Grund dafür lag am BIAS-Problem. Tay wurde durch Trolle im Netz mit einer großen Menge falschen Aussagen gefüttert und hat dadurch deren Vorurteile und Vorlieben in seinen KI-Algorithmus eingebettet.

Foto: Adobe Stock / metamorworks

Was passiert, wenn die KI versagt und falsche Entscheidungen trifft? Wer haftet für die Entscheidung und trägt die Verantwortung?

Aktuell gibt es keine direkte Haftung der KI. Die Europäische Union hat das Problem erkannt und im Dezember 2022 die Verordnung zur künstlichen Intelligenz erlassen. Diese unterscheidet zwischen unterschiedlichen Systemen: den nicht riskanten, den hochriskanten und den verbotenen Systemen. Für die nicht riskanten und die verbotenen Systeme muss nichts geregelt werden. Der Fokus der Verordnung liegt hier auf den hochriskanten Systemen, zum Beispiel der Steuerung von kritischer Infrastruktur oder Gesichtserkennung. Sie beschreibt die umfangreichen Pflichten der Hersteller, der Importeure, der Händler und der Anwender, die die KI einsetzten.

Pflichten der Anwender sind:
- Nutzung nur entsprechend der Gebrauchsanweisung
- Erfüllung der Anforderungen an die menschliche Aufsicht
- Eingabedaten müssen der Zweckbestimmung des KI-Systems entsprechen
- laufende Überwachung des Betriebes anhand der Gebrauchsanweisung
- Aufbewahrung der erzeugten Protokolle.

Verletzt man eine dieser Pflichten, könnte dies geschädigte Personen zum Schadensersatz berechtigen. Die Unternehmensleitung muss dafür sorgen, dass beim Einsatz von KI diese Anforderungen eingehalten werden. Dazu müssen Prozesse innerhalb des Unternehmens eingerichtet und von der Geschäftsleitung regelmäßig kontrolliert werden.

MEHR INFORMATIONEN UND DETAILLIERTERE AUSFÜHRUNGEN AUS DER KI-REALITÄT ERHALTEN SIE AM 15.03.2023 AUF DER „5. MITTELSTAND TRIFFT MITTELSTAND“ VON MANDALA INTERNET, EDV-SERVICE GMBH. TREFFEN SIE DIE EXPERTEN LIVE UND NUTZEN SIE DIE MÖGLICHKEIT, ANTWORTEN AUF IHRE FRAGEN ZU ERHALTEN.

PROF. ANDREAS GÖBEL
Honorarprofessor der FH Südwestfalen

RECHTSANWALT,
FACHANWALT FÜR IT-RECHT UND ARBEITSRECHT

Rechtsanwalt Professor Andreas Göbel ist Fachanwalt für das Recht der Informationstechnologien und seit 30 Jahren hauptsächlich in diesem Rechtsgebiet tätig.

Er ist Professor an der Fachhochschule Südwestfalen für IT-Recht, Datenschutzrecht und seit 2022 auch für das Recht der Künstlichen Intelligenz. Er berät seine Mandanten außergerichtlich, vertritt sie bei Rechtsstreitigkeiten und erstellt in erheblichem Umfang IT- Verträge. In diesem Jahr wird Herr Göbel als Keynote Speaker, bei der Mittelstand-trifft-Mittelstand Tagung von Mandala Internet, EDV-Service GmbH, aus dem „Nähkästchen“ berichten.

NOTFALLKONZEPTE

als Anforderung des Datenschutzes

Business Continuity Management ist wichtiger denn je

In der heutigen Arbeitswelt sind die meisten Prozesse abhängig von IT-Systemen. Wenn im Unternehmen diese Systeme ausfallen, gleich ob durch technische Probleme oder Angriffe von außen, herrscht sofort Alarmstimmung, da der Geschäftsbetrieb oftmals empfindlich gestört ist oder sogar komplett eingestellt werden muss.

Der hundertprozentig sichere Schutz vor solchen Vorfällen durch technische und organisatorische Maßnahmen ist eine Utopie. Ein gut durchdachtes und vollständig implementiertes Notfallkonzept hilft jedoch, bei einem eingetretenen Notfall die Handlungsfähigkeit im Unternehmen schnell und strukturiert wiederherzustellen. Die schnelle Wiederherstellung des normalen Betriebsablaufs wird auch als Business Continuity Management bezeichnet und ist in der digitalisierten Arbeitswelt eine zentrale Anforderung.

Ein Notfallkonzept enthält Vorgaben, wie in bestimmten Situationen zu agieren ist, es klärt Zuständigkeiten und ist eng mit den implementierten technischen und organisatorischen Maßnahmen verzahnt und ein elementarer Teil dieser. Damit ist das Konzept ein wichtiger Bestandteil des Datenschutzes im Unternehmen. Dies ist in der EU Datenschutz-Grundverordnung (DSGVO) verankert, denn Art. 32 Abs. 1 lit. b) DSGVO definiert die Schutzziele des Datenschutzes als Vertraulichkeit, Integrität und Verfügbarkeit. Ein funktionierendes Notfallkonzept hilft dabei, alle drei Schutzziele so gut wie möglich zu gewährleisten.

Klare ablauforganisatorische Vorgaben sollen dabei helfen, schnelle Entscheidungen über das weitere Vorgehen herbeizuführen. Dabei werden verschiedene Szenarien mit den entsprechenden Handlungsabläufen dargestellt. Was ist beispielsweise zu tun, wenn Malware im System aktiv ist und es offensichtlich einen Datenabfluss an Hacker gibt? Welches Vorgehen greift, wenn Ransomware Server und andere IT-Komponenten sperrt?

Notfälle beschränken sich jedoch nicht nur auf Angriffe von außen, sondern können auch durch physische Schäden, beispielsweise durch Defekte an der Hardware oder durch Naturkatastrophen, wie Überschwemmungen oder Brände, ausgelöst werden.

Notfallkonzepte sind stets an den individuellen Anforderungen des Unternehmens auszurichten, um die dargestellten Szenarien passgenau auf die Gegebenheiten im Unternehmen abzustimmen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Januar 2021 seinen BSI-Standard 200-4 zum Notfallmanagement veröffentlicht, der wertvolle Hinweise und Herangehensweisen enthält. Es lohnt sich für Unternehmen, sich mit diesem Thema zu befassen, um auf den Ernstfall bestmöglich vorbereitet zu sein.

Foto: Adobe Stock / eyetronic

FABIAN HIENTZ, M.A., LL.B.
S-CON GmbH & Co. KG
Hannover

WIRTSCHAFTSJURIST

Fabian Hientz studierte an der Brunswick European Law School in Wolfenbüttel Wirtschaftsrecht mit dem Schwerpunkt Gewerblicher Rechtsschutz und Urheberrechte in der Informationsgesellschaft. Seit einigen Jahren arbeitet er bei der S-CON GmbH & Co. KG als Projektleiter für die Datenschutz-Beratung.

HINWEISGEBERSCHUTZGESETZ praktisch umsetzen

Anforderungen des Whistleblowings rechtssicher erfüllen

Im Dezember 2022 hat der Bundestag das Hinweisgeberschutzgesetz beschlossen und stellt deutsche Unternehmen damit vor neue Herausforderungen, die über die europäischen Bestimmungen hinausgehen. Ziel ist es, Personen, die Hinweise auf (potenzielle) Gesetzesverstöße geben, vor Sanktionen zu schützen und gleichfalls Meldekanäle für entsprechende Hinweise im Unternehmen gesetzeskonform zu etablieren. Im Hinblick auf die möglichen neuen Bußgelder lohnt es sich, dem Gesetz zu entsprechen.

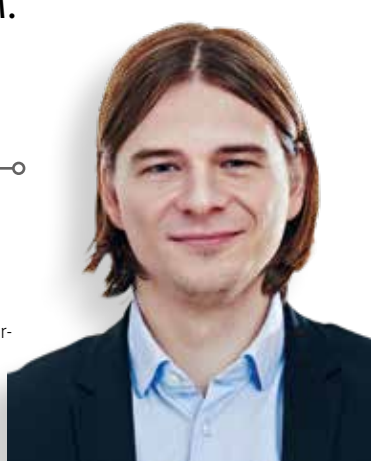
Im Fokus des Gesetzes steht aus unternehmerischer Sicht die Pflicht zur Einrichtung einer internen Meldestelle, die Hinweise vertraulich entgegennimmt. Diese Pflicht trifft Organisationen mit mindestens 50 Beschäftigten, unabhängig davon, ob es sich um Organisationen des öffentlichen oder privaten Rechts handelt. Unternehmensgruppen haben die Möglichkeit, eine konzernweite zentrale Meldestelle einzurichten. Dabei ist zu beachten, dass die Verantwortung zur Verfolgung von Hinweisen bei dem betroffenen Unternehmen verbleibt.

Die genaue Etablierung der Meldestelle überlässt der Gesetzgeber den Unternehmen. Vorgeschrieben werden jedoch gewisse Rahmenparameter. So muss die Abgabe von Hinweisen mündlich oder schriftlich sowie persönlich möglich sein und der Umgang mit den erhaltenen Informationen vertraulich erfolgen. Auch in anonymer Form soll die Möglichkeit zur Abgabe von Hinweisen gewährleistet werden. Ferner bestehen für das Unternehmen gewisse Informationspflichten. So muss die hinweisgebende Person innerhalb festgelegter Fristen eine Bestätigung des Eingangs ihres Hinweises sowie eine Rückmeldung über den Status der Bearbeitung erhalten.

Ein digitales Hinweisgebersystem bietet die Möglichkeit, die gesetzlichen Anforderungen in einer effizienten und praktikablen Lösung umzusetzen. Durch eine genaue Bestimmung, der auf das Hinweisgebersystem zugriffsberechtigten Personen, kann die Vertraulichkeit hinsichtlich der erhaltenen Informationen und der hinweisgebenden Person bestmöglich gewahrt werden. Das digitale Hinweisgebersystem dient hierbei als Schnittstelle zwischen der hinweisgebenden Person und dem Hinweisempfänger. Damit wird eine direkte und dokumentierte Kommunikation ermöglicht, sodass die vorgeschriebenen Informationspflichten fristgerecht erfüllt und weitere notwendige Informationen zur Klärung eingeholt werden können. Um die Kommunikation auch bei anonym abgegebenen Hinweisen zu gewährleisten, ist es notwendig, dass das Hinweisgebersystem derart gestaltet ist, dass ein Zugriff auch ohne die Angabe persönlicher Daten erfolgen kann.

Foto: Adobe Stock / alexkoral

DR. IUR. TIMO BITTNER, LL.M., LL.M.
S-CON GmbH & Co. KG
Hannover
GESCHÄFTSFÜHRER



Dr. Bittner hat sich bereits zu Beginn seines Studiums auf das Datenschutz- und IT-Recht spezialisiert und vertiefte dies in seinem Masterstudiengängen im IT-Recht und Recht des geistigen Eigentums an der Uni Oslo und Hannover. Seit 10 Jahren berät der promovierte Jurist Unternehmen auch in englischer Sprache zu allen Fragen des Datenschutzes, der Compliance und der Informationssicherheit.

Digitalisierung mit Nebenwirkungen

Ein Blick auf die Risiken erhöht die Sicherheit

„Schneller, höher, stärker“: Das Motto der Olympischen Spiele ist uns allen gut bekannt. Seit wir vor einigen Jahren das Zeitalter der Digitalisierung ausgerufen haben, leben wir quasi in allen Arbeits- und Lebensbereichen in einer immerwährenden Olympiade. Fortschritt hat es zwar schon immer gegeben, aber die Digitalisierung verlieh ihm einen ungeheuren Schub. Wir sitzen alle in diesem Boot. Aussteigen können wir nicht – umdrehen auch nicht. Es spielt auch keine Rolle, ob wir das gut oder schlecht finden, ob wir die Vorteile zu schätzen wissen, unsere Prozesse angepasst, vielleicht sogar neue Geschäftsideen entwickelt haben oder uns die analoge Zeit zurückwünschen. Mit der Digitalisierung gehen erhebliche Veränderungen einher, die nicht nur Vorteile bieten, sondern auch Nebenwirkungen zeigen. Schon 2018 warnte der Chaos Computer Club (CCC) mit den Worten „Wir bauen unsere digitale Welt auf ganz schön viel Schrott“: Recht haben sie damit. Haben wir vor 30 Jahren noch überlegt, ob sich die Digitalisierung durchsetzen wird, dominiert sie heute unseren Alltag. Wir vernetzten damit Türschlösser, medizinische Geräte, Produktionsanlagen und jegliche Art von kritischer Infrastruktur. Die Architektur dahinter stammt noch aus der Mitte des letzten Jahrhunderts, weil die Idee dessen, was wir heute Internet nennen, eigentlich eine ganz andere war. Es ist naheliegend, dass in der schillernden Cyberwelt nicht nur hehre Ziele verfolgt werden. Es bewegen sich dort auch Personen, deren Ziel es ist, unsere Erleichterungen und Möglichkeiten in die ihren zu verwandeln und zu kriminellen Zwecken auszunutzen. Dass dies mit voranschreitender Vernetzung und Digitalisierung weiter zunehmen wird, ist zu erwarten.

Angefangen von relativ einfachen DDoS-Angriffen, die (nur) auf die Verfügbarkeit von Servern oder Webanwendungen abzielen, über Aktionen von Hacktivisten und dem Ausnutzen falsch konfigurierter oder schlichtweg in Vergessenheit geratener Server bis hin zum zahlenmäßig größten Problem der Ransomware-Attacken (Verschlüsselung mit Lösegeldforderung) oder gar Angriffen von Geheimdiensten oder ihnen nahestehenden Hackergruppierungen. Jede Person und jedes Unternehmen kann von dem einen und/oder anderen betroffen sein. Einstellungen wie „Ich habe keine sensiblen Daten“ oder „Mein Unternehmen ist zu klein oder nicht interessant für Angriffe“ haben bereits manches Mal für böses Erwachen gesorgt, denn spätestens bei einer Ransomware-Attacke spielt weder die Größe noch die mögliche Sensibilität eines Unternehmens eine Rolle. Davon abgesehen zeigt die Erfahrung, dass sich manches Unternehmen des Wertes und dessen Bedeutung nicht bewusst ist. Möglich ist auch, selbst gar nicht das direkte Ziel, sondern im Dunstkreis eines Konzerns, sei es als Kunde oder Zulieferer, einfach nur Mittel zum Zweck zu sein.

Vollständig verhindern lässt sich ein digitaler Angriff nicht. Man kann und sollte es den Angreifenden nur so schwer wie möglich machen. Zu einer effektiven Prävention gehört auch, sich auf den Ernstfall vorzubereiten. Doch wie kann sich ein Unternehmen gut vorbereiten?

Die richtige konkrete Lösung gibt es nicht. Die Erfahrung der Sicherheitsbehörden zeigt vielmehr, dass die IT-Sicherheit einen ständigen Prozess der Anpassung an die aktuelle digitale Bedrohungslage darstellt. Dieser Prozess sollte iterativ, also sich ständig wiederholend, erfolgen. Auch das Abarbeiten einer (imaginären) Checkliste hilft nur bedingt weiter, da sich viele konkrete Sicherheitsmaßnahmen an der Ausrichtung des betroffenen Unternehmens sowie dessen interne Arbeitsabläufe orientieren sollten. Maßnahmen, die bei einem Unternehmen unerlässlich sind, können bei einem anderen aufgrund betrieblicher Entscheidungen gar nicht umgesetzt werden.

Foto: Adobe Stock / Framestock

MARKUS BÖGER
Niedersächsisches Ministerium für Inneres und Sport
Verfassungsschutz

LEITER WIRTSCHAFTSSCHUTZ

Erster Polizeihauptkommissar, begann seine Laufbahn bei der Landespolizei Niedersachsen und wechselte 2005 zum Niedersächsischen Verfassungsschutz. Nach einer Verwendung in mehreren operativen Bereichen arbeitet er seit 2011 im Fachbereich Wirtschaftsschutz, deren Leitung er 2020 übernahm.

*„Man kann und sollte es den **Angreifenden nur so schwer wie möglich machen.** “*

Sofern es mehrere sensible digitale Bereiche gibt, sollte eine Prioritätenliste erstellt werden. Ein Angriff auf die Plattform eines Onlinehändlers dürfte folgenschwerer sein als der auf die Internetpräsenz eines Handwerkbetriebes. Arbeiten in einem Handwerksbetrieb Maschinen rechnergestützt und funktionieren wegen eines Angriffes (z.B. mittels Ransomware) nicht mehr, steht auch ein Handwerksbetrieb vor großen Problemen.

In diesem ständigen Prozess können folgende Fragen sehr hilfreich sein: Wie ist die IT-Infrastruktur im Unternehmen aufgebaut und was soll konkret geschützt werden? Gibt es existenzielle Bereiche, die besonders zu schützen sind? Wie häufig werden Back-ups getätigt und wo werden diese abgelegt? Wie schnell können Back-ups zurückgespielt und Systeme wiederhergestellt werden? Wird das Wiederherstellen regelmäßig getestet?

Weitere wesentliche Bestandteile präventiver Maßnahmen sind Schulungs- und Sensibilisierungsmaßnahmen im Unternehmen sowie eine Vorbereitung auf den Ernstfall, also die Fertigung von Notfallplänen, um bei einem Angriff entsprechend vorbereitet reagieren zu können. Notfallpläne müssen aktuelle Gefahren und einzuleitende Maßnahmen bei einem möglichen Cyberangriff berücksichtigen. Es versteht sich von selbst, dass solche Notfallpläne sinnvollerweise auf Papier abgelegt sein müssen, um auch im Falle eines Systemausfalls oder vollständiger Verschlüsselung darauf zurückgreifen zu können.

MARIO KRAUSE
Zentrale Kriminalinspektion Braunschweig
Fachkommissariat Cybercrime
Braunschweig

LEITER FACHKOMMISSARIAT CYBERCRIME

KHK Krause, Leiter Fachkommissariat Cybercrime in der Zentralen Kriminalinspektion Braunschweig
Fachliche Zuständigkeit: Alle Formen der Cyberkriminalität, insbesondere Organisierte Kriminalität.

Foto: Adobe Stock/Framestock

Theoretisch kann sich ein Unternehmen allerdings auch bis in die Insolvenz sichern, weil bei zu hoch gehängten Hürden die Arbeitsfähigkeit auf der Strecke bleibt. Sicherheit (Security) und Funktionalität (Usability) bilden zwei Schalen einer Waage, die es in einem Unternehmen sinnvoll in Einklang zu bringen gilt. Beide nach oben geht (leider) nicht. Seitens der Sicherheitsbehörden halten wir natürlich alles rund um die Security sehr hoch, wissen aber auch, dass es auf unternehmerischer Seite auch den anderen Part abzubilden gilt. Letztlich muss das Unternehmen entscheiden, welche Maßnahmen umgesetzt werden und welche nicht.

Im Unternehmen sollte auch die Verantwortung für die IT-Sicherheit klar definiert sein. Sie der Einfachheit halber auf den Administrator zu übertragen, ist ein grundlegender Fehler. Wer für den Betrieb verantwortlich ist, sollte nicht gleichzeitig auch die Vorgaben für die Sicherheit machen. Ist dies der Fall, leidet einer der verantworteten Bereiche darunter, und zwar meistens die Sicherheit. Dieser Grundgedanke liegt jedem Informationssicherheitsmanagementsystem (ISMS) zugrunde, wie z.B. dem BSI-Grundschutz, der ISO 27001 oder VdS 10000.

Hilfestellung bietet die Transferstelle IT-Sicherheit im Mittelstand (TISiM) unter www.tisim.de. Weitergehende Sicherheitsempfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) finden sich unter www.bsi.bund.de.

Direkte Ansprechpartner in Niedersachsen stehen für Sie beim Niedersächsischen Verfassungsschutz im Fachbereich Wirtschaftsschutz sowie der Zentralen Ansprechstelle Cybercrime für die niedersächsische Wirtschaft (ZAC) beim Landeskriminalamt zur Verfügung.

IT-SECURITY UND AWARENESS

Jeden kann es treffen und der „Human factor“ entscheidet!

Allen technischen Maßnahmen zum Trotz ist eine E-Mail weiter unangefochten das beliebteste und wirksamste Mittel für Angriffe auf die digitale Infrastruktur. Immer neue Strategien umgehen systematisch die technischen Sicherheitsvorkehrungen. Aufgrund der zunehmenden Transparenz von Unternehmen und deren Mitarbeitern und durch die Präsenz in sozialen Medien sind Kriminelle dazu noch in der Lage, Angriffe automatisiert zu personalisieren. Und damit in eine vermeintliche Vertrauensposition dem Empfänger gegenüber zu kommen, ihn dazu zu bringen, Dateien zu öffnen, Links zu klicken oder Login-Daten preiszugeben. Knapp fünfzig Prozent der Nutzer öffnen Phishing-Mails, jeder Dritte klickt auf darin enthaltene Links und 58 Prozent interagieren mit den Inhalten und geben ggf. Login-Daten in fingierte Masken ein.[1]

Tritt dann der Ernstfall ein, sind viele Manager und Unternehmen auf diese Situation nicht ausreichend vorbereitet. Denn wenn eine Lösegeldforderung vorliegt oder ein System verschlüsselt ist, sind die IT-Systeme bereits infiltriert, dann sind bereits Daten abgeflossen, Back-ups gelöscht und Admin-Konten übernommen. Für diesen ernst zu nehmenden Krisenfall gibt es häufig keine Notfallpläne oder Handlungsanweisungen, sodass die involvierten Mitarbeiter in IT und Management regelmäßig wertvolle Zeit verstreichen lassen.

Weniger Digitalisierung ist keine Option! Digitalisierung und Automation im Unternehmen voranzutreiben sind Garanten für Wettbewerbs- und Zukunftsfähigkeit. Das fordert Management und Organisation auf mehreren Fronten:

Zum einen treibt uns die Notwendigkeit, schneller zu agieren, Prozesse zu automatisieren und effizienter zu arbeiten. Die Zusammenarbeit mit Kollegen, Kunden und Lieferanten hat sich grundlegend verändert durch die permanente und ortsunabhängige Verfügbarkeit von Systemen und Informationen. Freie Wahl von Arbeitsort und auch Arbeitszeit wird immer mehr zum entscheidenden Faktor für Mitarbeitende.

Zum anderen wächst aber auch täglich die Gefahr, dass Daten und Informationen gestohlen oder verschlüsselt werden können. Denn gerade kriminelle Organisationen machen sich die Schwachstellen, die durch das Internet, die Anwendungen oder die ihr zugrundeliegende technische Infrastruktur entstehen, zu Nutze. Und deren Ransomware-Attacken und Angriffe werden zusehend ausgefeilter und erreichen mit immenser Streuwirkung und industriellen Prozessen im Hintergrund auch vermeintlich „uninteressante“ Zielpersonen.

2021 bezifferte die Allianz Versicherung den globalen Schaden durch Cyberangriffe und ihre Folgen auf mehr als 1 Billionen US$.[2] Und damit gab es einen Zuwachs von über 50% innerhalb von 2 Jahren. Hier zeigt sich deutlich, dass gezielte Angriffe weiter zunehmen und groß angelegte Aktionen von Kriminellen nach dem Gießkannenprinzip immer individueller werden und mit industriellen Prozessen hocheffizient abgeerntet werden.

Es geht um Vorsorge, Verteidigung und zielgerichtete Reaktion im Krisenfall!

Um diese digitalen Einbrüche grundsätzlich zu verhüten, ist es neben einem angemessenen Security-Konzept von entscheidender Wichtigkeit, dass Mitarbeiter trainiert und sensibilisiert werden, um in der steigenden Flut von E-Mails die gefährlichen Phishing-Mails erkennen zu können. Sie brauchen in Ihrer Organisation nicht ein kleines Team von IT-Sicherheits-Experten, vielmehr muss jeder Ihrer Mitarbeiter auf dem Gebiet der Gefahrenabwehr ein Spezialist werden, zumindest an seinem Arbeitsplatz.

Idealerweise wird so eine Maßnahme mit einer ersten selbst initiierten Phishing-Kampagne und anschließendem Sicherheitstraining gestartet, um die Belegschaft effizient und nachhaltig zu sensibilisieren. Es gibt eine Vielzahl passender Schulungsanbieter, die sowohl das Verhalten Ihrer Mitarbeiter überprüfen als auch nach einer Analyse des Ist-Zustandes die passenden Online-Schulungen für Ihre Mitarbeiter anbieten.

Im Bereich des Risikomanagements ist es wie bei der schnellen Eingreiftruppe. Es braucht Firewall, Virenschutz, ein echtes unabhängiges Back-up und weitere technische Maßnahmen, um den Angriffen zu begegnen. Es braucht also Abwehrpläne, klare Meldeketten, Prozesse und einen Zugriff auf schnelle Eingreiftruppen (Incident Response Teams), die eine Antwort auf den Angriff geben und retten, was sonst nicht mehr zu retten wäre. Wenn dazu noch Pläne für einen IT-Notfall-Betrieb in der Schublade liegen, zum Beispiel in einem externen Rechenzentrum, wo idealerweise auch ein unabhängiges verschlüsseltes Back-up liegt, dann lassen sich Schäden begrenzen und Ihr Unternehmen existiert auch nach einem Angriff weiter.

1 Sosafe Human Risk Review 2022, Seite 42

2 Allianz (2022) Allianz Risk Barometer 2022: Cyber perils outrank Covid-19 and broken supply chains as top global business risk.

Foto: Adobe Stock / Song_about_summer

DIPL.-ING. HOLGER KÄMMERER
ATD GmbH
IT-Systemhaus
Braunschweig

GESCHÄFTSFÜHRER

Dipl.-Ing. Holger Kämmerer schloss 1995 sein Studium als Bauingenieur an der TU in Brauschweig ab. Er gründete 1996 die ATD GmbH, das IT-Systemhaus, in dem er bis heute als Geschäftsführender Gesellschafter aktiv ist. 2011 startete er seine Beratungen in der UBEGA. Seine Schwerpunkte bilden Unternehmensstrategien, Entwicklung agiler Unternehmensstrukturen, Fortbildungen für Führungskräfte und Systemische Analysen.

DÖHLER HOSSE STELZER
VERSICHERUNGSMAKLER

Christian Gerstung
Direktor Kundenmanagement
Experte für Cyberversicherungen

c.gerstung@dhs-makler.de

Döhler Hosse Stelzer GmbH & Co. KG
Versicherungsmakler
Haus der Versicherungen

Bankplatz 7a, 38100 Braunschweig
TEL +49 (0) 531. 24 25 4 - 0
EMAIL info@dhs-makler.de

CYBERANGRIFFE
durch IT-Penetrationstests und Awareness vermeiden

Cyberangriffe stellen eine immer größer werdende Bedrohung für Unternehmen und Organisationen dar. Sie können nicht nur finanzielle Schäden verursachen, sondern auch das Vertrauen von Kunden und Mitarbeitern beschädigen. Um sich vor Cyberangriffen zu schützen, gibt es verschiedene Maßnahmen, die Unternehmen ergreifen können.

Eine Möglichkeit, um das Risiko von Cyberangriffen zu minimieren, sind regelmäßig durchgeführte IT-Penetrationstests. Diese, auch als „Pen-Tests“ oder „Penetrationstest“ bezeichnet, sind simulierte Angriffe auf IT-Systeme, die von qualifizierten Sicherheitsexperten durchgeführt werden. Die Tests dienen dazu, Schwachstellen in der IT-Infrastruktur rechtzeitig aufzudecken und entsprechende Gegenmaßnahmen zu ergreifen und Lücken zu schließen. Sie sollten regelmäßig durchgeführt werden, um sicherzustellen, dass die geprüften IT-Systeme auf dem neuesten Stand der Technik sind und auch fortlaufend keine Sicherheitslücken aufweisen, welche nach Updates aufkommen können. Durch IT-Penetrationstests können Schwachstellen in der IT-Infrastruktur frühzeitig aufgedeckt werden, bevor sie von Angreifern ausgenutzt werden können.

Eine weitere wichtige Maßnahme zur Verhinderung von Cyberangriffen ist das Schaffen von Awareness bei den Beschäftigten. Durch Schulungen und regelmäßige Informationen über aktuelle Sicherheitsbedrohungen und -verfahren können Mitarbeiter sensibilisiert werden, wodurch sie ihr Sicherheitsbewusstsein verbessern und sich besser gegen potenzielle Bedrohungen schützen können. Dazu gehört unter anderem das Verwenden von starken Passwörtern, das Meiden von verdächtigen Links und E-Mails sowie das Einhalten von Sicherheitsbestimmungen im Unternehmen. Eine gute Awareness-Strategie kann dazu beitragen, dass Nutzer für Bedrohungen sensibilisiert sind und die notwendigen Schutzmaßnahmen ergreifen, um sich dagegen zu schützen und nicht auf die Tricks der Hacker einzugehen. Zudem kann Awareness dazu beitragen, dass Unternehmen ihre Informationssicherheit verbessern und ihre Resilienz gegenüber Angriffen erhöhen.

Um Cyberangriffe wirksam zu verhindern, sind sowohl regelmäßige IT-Penetrationstests und Phishing-Simulationen als auch Schulungs- und Awarenessmaßnahmen notwendig. Unternehmen und Organisationen sollten daher beide Aspekte in ihre Sicherheitsstrategie einbeziehen, um sich vor den vielfältigen Gefahren im Cyberraum zu schützen.

MARC PÖLCKOW, LL.B.
S-CON GmbH & Co. KG
Hannover

WIRTSCHAFTSJURIST

Marc Pölckow studierte an der Brunswick European Law School in Wolfenbüttel Wirtschaftsrecht mit dem Schwerpunkt Informations- und Telekommunikationsrecht und gewerblichen Rechtsschutz. Seit einigen Jahren arbeitet er bei der S-CON GmbH & Co. KG als Berater für Datenschutz sowie als Teamleiter für Informationssicherheit und berät Unternehmen bei dem Aufbau entsprechender Managementsysteme.

Foto: Adobe Stock/ Oleksii

Partner für **Datenschutz** und **Informationssicherheit**

Kämmer Consulting aus Braunschweig

„Wir sind nicht die Oskar Kämmer Schule“, sagt Axel Vogelsang, Prokurist der Kämmer Consulting GmbH. 2002 gegründet, wird die Kämmer Consulting immer noch häufig mit der Oskar Kämmer Schule gleichgesetzt. Intention von Geschäftsführer Rüdiger Schmidt, der seit Gründung die Geschicke des Unternehmens lenkt, war es, den Unternehmen in der Region 38 einen starken Partner im Bereich der Aus- und Weiterbildung zur Seite zu stellen. Das Seminarangebot reicht von Anwenderschulungen im Microsoft-Office-Umfeld über Seminare zu den Themen Datenschutz und Informationssicherheit bis hin zu Angeboten von sog. Soft-Skills wie Mitarbeiterführung, Zeitmanagement und Projektmanagement. Außerdem stellt die Beratungsfirma mit einer eigenen Abteilung den IT-Support für die über 60 Standorte der Oskar Kämmer Schule und weitere Kunden. Im Laufe der Jahre kamen noch weitere Geschäftsfelder hinzu: Seit 2016 berät das Haus mit einem Team aus mittlerweile vier Consultants im Bereich Datenschutz und stellt externe Datenschutzbeauftragte. Seit 2022 wird das Portfolio durch die Beratung zu Themen der Informationssicherheit und der Vorbereitung auf das TISAX® Label oder der ISO 27001 Zertifizierung ergänzt.

Um mit den ständig wachsenden Anforderungen des digitalen Zeitalters mithalten zu können, investieren Unternehmen regelmäßig in die IT-Infrastruktur, vernachlässigen dabei aber häufig die menschliche Komponente der Informationssicherheit. Auch die Mitarbeiter müssen mit den neuesten Entwicklungen und Technologien vertraut gemacht werden. Hier steht Kämmer Consulting mit einem Seminarangebot als Partner auf Augenhöhe zur Seite. Sei es die Vermittlung der neuesten Möglichkeiten und Funktionen von Microsoft-Office-Programmen wie Excel, Word oder Outlook, die Administration von Servern oder auch die Einführung in die Programmierung.

Durch die mehr als 20-jährige Erfahrung wissen die Trainer genau, was für Probleme im täglichen Arbeitsumfeld auftauchen und wie man sie umgehen oder lösen kann. Dieses Wissen wird mit hohem Praxisbezug in offenen Seminaren vermittelt, die je nach Vorkenntnissen der Teilnehmer Inhalte auf Basis oder Advanced Niveau enthalten. Die offenen Seminare werden im firmeneigenen Schulungszentrum in der Nordstraße im Braunschweiger Uni-Viertel durchgeführt. Zum Portfolio zählt neben den offenen Seminaren auch die Möglichkeit, auf individuelle Bedürfnisse abgestimmte Semina-

AXEL VOGELSANG

Kämmer Consulting GmbH
Braunschweig

LEITER DES BEREICHES DATENSCHUTZ, SCHULUNGSLEITER, PROKURIST

Axel Vogelsang ist seit 2003 in der Kämmer Consulting GmbH beschäftigt und momentan als Leiter des Bereiches Datenschutz sowie Schulungsleiter und Prokurist tätig.

re zu konzipieren und durchzuführen. Mit dem mobilen Seminarraum besteht natürlich auch die Option, diese Seminare als Inhouse-Schulungen direkt beim Kunden oder in Räumlichkeiten seiner Wahl durchzuführen.

Datenschutz ist lästig, macht Arbeit und kostet Geld!

So oder so ähnlich klingen häufig die ersten Reaktionen, die die Datenschutz-Consultants bekommen, wenn sie in den Kick-off-Veranstaltungen das Thema Datenschutz in den Unternehmen angehen. Aufgrund der langjährigen Expertise der Berater sehen die Entscheider und Mitarbeiter der Unternehmen aber sehr schnell, dass dem nicht so ist und die Anforderungen der Datenschutzvorschriften, allen voran der EU-Datenschutz-Grundverordnung (DSGVO), auch mit pragmatischen, für alle Mitarbeiter einfach umzusetzenden Prozessen einzuhalten sind.

Das Team um Axel Vogelsang betreut in der Region 38 (und vereinzelt bundesweit) Unternehmen aus den unterschiedlichsten Branchen – wie z.B. Sozialwesen, Ingenieurbüros, Maschinenbau bis hin zu Tierarztpraxen, Energieversorgern, Lebensmittelindustrie und Baugewerbe. Im Rahmen der Beratung als externe Datenschutzbeauftragte prüfen die Consultants die Einhaltung der gesetzlichen Vorschriften im Datenschutz, erstellen in Zusammenarbeit mit den Kunden die gesetzlich geforderten Dokumente und Informationen und führen Awareness-Schulungen der Führungskräfte und Mitarbeiter durch.

Auch hier sieht sich man sich als Partner auf Augenhöhe für seine Kunden und stellt so sicher, dass Mängel im Datenschutz nicht zum Wettbewerbsnachteil werden oder sogar in Ermittlungsverfahren durch die Aufsichtsbehörden der Länder (Landesdatenschutzbeauftragte) enden. Auch fünf Jahre nach Inkrafttreten der DSGVO bestehen bei vielen Unternehmen in Bezug auf die Einhaltung der Datenschutzvorschriften immer noch einige Defizite, die durchaus zu Bußgeldern führen können. Hier wird Unternehmen die Möglichkeit geboten, in einer kostenlosen Erstberatung eine Bestandsaufnahme durchzuführen und somit offene Punkte zu identifizieren.

Informationssicherheit zur Stärkung der Wettbewerbsfähigkeit

„Vernachlässigung der Informationssicherheit kann Unternehmen Kunden und Geld kosten", sagt Andreas Stammhammer, Vertriebsleiter und Informationssicherheitsberater des Hauses. Für viele Unternehmen in der Metropolregion Hannover Braunschweig Göttingen Wolfsburg wird in der nahen Zukunft das Thema Informationssicherheit sehr weit oben auf der To-do-Liste stehen, da viele Unternehmen von ihren Zulieferern ein TISAX® Label oder eine ISO 27001-Zertifizierung verlangen und oftmals eine Zusammenarbeit ohne diese Zertifizierung nicht mehr weitergeführt wird.

Aber auch, wenn die Zertifizierung nicht gefordert ist, müssen sich Unternehmen heute mit dem Thema Cybersicherheit auseinandersetzen. Im „Bericht zur Lage der IT-Sicherheit in Deutschland 2022" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) stellt das BSI fest, dass sich die zuvor schon angespannte Lage im Berichtszeitraum weiter zugespitzt hat. Die Bedrohung im Cyber-Raum sei damit so hoch wie nie. Es wurde im Berichtszeitraum eine hohe Bedrohung durch Cybercrime beobachtet. Die Consultants der Kämmer Consulting unterstützen Unternehmen bei der Vorbereitung auf die o.g. Zertifizierungen.

Hierbei profitieren die Kunden von der langjährigen Expertise der Experten und der Tatsache, dass die Consultants auch zertifizierte Auditoren sind, also genau wissen, wo die Schwerpunkte in den Zertifizierungsaudits liegen. Neben der Vorbereitung auf die Zertifizierung können Kunden auch einen einfachen Sicherheitscheck nach ISO-Standard beauftragen, der dazu dient, Schwachstellen in der Informationssicherheit aufzudecken und Maßnahmenempfehlungen zur Abstellung der Schwachstellen zu erhalten.

Um Unternehmen die Möglichkeit zu geben, sich über die aktuellsten Entwicklungen im Bereich Datenschutz, Informations- und Cybersicherheit zu informieren, veranstaltet die Kämmer Consulting mit wechselnden Kooperationspartnern regelmäßig Fachkonferenzen zu dem Themenkomplex.

Ein attraktiver Arbeitgeber

„Flache Hierarchien, Kommunikation auf Augenhöhe und ein freundschaftliches Miteinander, sind die Punkte, die Mitarbeiter häufig nennen, wenn sie gefragt werden, warum sie gerne bei uns arbeiten", sagt Jonas Methner, Leiter Zentrale Dienste. Aber auch die flexiblen Arbeitszeitmodelle und die Möglichkeit des hybriden Arbeitens sind Punkte, die für das Unternehmen als Arbeitgeber sprechen. Grundlage einer guten Arbeit der Consultants sei u.a., dass diese sich auf ihre eigentliche Arbeit konzentrieren können, ohne sich um lästige Verwaltungstätigkeiten kümmern zu müssen. Diese Arbeit nehmen ihnen die Mitarbeiter aus dem Backoffice ab, die sich um die allgemeine Verwaltung, das Rechnungswesen und die Personalwirtschaft kümmern.

Foto: AdobeStock/ 2ragon

JONAS METHNER

Kämmer Consulting GmbH
Braunschweig / Magdeburg

LEITER ZENTRALE DIENSTE,
IT- & PERSONALMANAGEMENT,
GESCHÄFTSLEITUNG JUNIOR LÖWEN

Jonas Methner ist seit 2007 an verschiedensten Projekten der Kämmer Consulting GmbH beteiligt. Anfangs nur im IT-Bereich, seit 2014 auch im Personalmanagement/ Vermittlung & direkt im operativen Geschäft.

ANDREAS STAMMHAMMER

Kämmer Consulting GmbH
Braunschweig

LEITER DES VERTRIEBS,
BERATER FÜR INFORMATIONSSICHERHEIT

Andreas Stammhammer ist Vertriebsleiter und Informationssicherheitsberater für TISAX® und ISO 27001.

Cyber-Risiken im Mittelstand:
So schützen Geschäftsführer Ihr Unternehmen vor Datenverlust und Reputationsschäden

In den Nachrichten erfahren wir täglich von Cyber-Security-Attacken, Einsatz von Erpressungssoftware oder ausgenutzte Sicherheitsschwachstellen, die es Hackern ermöglicht, in Systeme einzugreifen. Auch Statistiken zeigen, dass die Zahl von Cyber-Security-Angriffen massiv steigt.

VLADIMIR AFONICHEV
re:think Innovations GmbH
Braunschweig

GESCHÄFTSFÜHRER

Vladimir Afonichev ist Geschäftsführer und verantwortet den gesamten Consulting Bereich bei der re:think Innovations GmbH. Er war in seiner Karriere für verschiedene Top Management Beratungen im Bereich der digitalen Transformation für mittelständische Unternehmen und multinationale Konzerne tätig. Vladimir absolvierte sein Diplom im Maschinenbau / Flugzeugbau an der TU Braunschweig.

Wie kostspielig kann ein Angriff sein?

Vladimir: Schauen wir uns zum Beispiel einen Angriff einer Erpressungssoftware (Ransomware) an, bei der Erpresser Daten klauen und das Systeme stillgelegt haben und für die Zurückgabe der Daten und des Systems Geld verlangen. Nehmen wir an, Sie entscheiden sich, den Betrag zu zahlen, weil Sie die Daten brauchen und Ihre Systeme verfügbar sein müssen. Dabei müssen Sie nicht nur den Preis für die Ransomware berücksichtigen, der durchschnittlich 1 Mio. Euro beträgt, sondern auch die Kosten für den Ersatz von Geräten, Versicherungsabzüge, Rechtsberatung, Arbeitszeit, forensische Untersuchungen und die Reaktion auf den Vorfall, die sich auf 250.000 Euro pro Woche belaufen können. Neben dem finanziellen Aspekt schädigt der Angriff den Ruf und das Vertrauen von Kund:innen und Partner:innen.

Warum ist Cyber Security so wichtig?

Irina: Wir hören von Unternehmen oft Aussagen wie: „Wir haben es so lange ohne geschafft, warum sollten wir etwas ändern?“, „Wir sind nicht wichtig genug, um ein Ziel zu sein!“, „Sicherheit ist zu kompliziert und teuer!“ und „Wir wissen nicht, wo und wie wir anfangen sollen!?“.

Diese Fehleinschätzungen können jedoch tückisch sein. Es ist nicht die Frage, ob man gehackt wird, sondern wann. Es ist inzwischen nur noch eine Frage der Zeit – egal, ob man subjektiverweise wichtig ist oder ob

man über sensible Daten verfügt. Für Hacker können Sie auch nur ein Mittel zum Zweck sein – das schwächste Glied in der Lieferkette. Sie können lediglich als Zugangspunkt zu größeren Kund:innen oder Partner:innen ins Visier genommen werden.

Bereiten Sie sich jetzt darauf vor, damit Sie bereit sind und die nötige Sorgfalt walten lassen, um Ihr Unternehmen und Ihre Geschäftsbeziehungen zu schützen.

Was sind die Herausforderungen für kleine bis mittlere Unternehmen (KMU)?

Vladimir: Die größte Herausforderung ist wahrscheinlich das Budget, die Qualifikationslücke und die Personal- bzw. Ressourcenprobleme. Kleine und mittlere Unternehmen verfügen nicht über das gleiche Budget und die gleichen Ressourcen wie ein Großunternehmen oder sie ziehen es manchmal vor, das Budget für andere geschäftskritische Dinge zu verwenden. Außerdem erscheint die Cybersicherheit oft als zu kompliziert und überfordert Unternehmer:innen. Genau die richtigen Leute mit den richtigen Fähigkeiten am Arbeitsmarkt zu finden und für das Unternehmen zu gewinnen, ist eine zusätzliche Barriere.

Was brauchen Sie, um loszulegen?

Irina: Es klingt offensichtlich, aber es geht in erster Linie darum, das Unternehmen zu verstehen. Sie müssen die Bedrohungen für Ihr Unternehmen kennen, um zu verstehen, wovor Sie sich schützen wollen. Sie werden überrascht sein, wie viele Manager:innen jedoch den allgemeinen Auftrag und die Ziele des Unternehmens nicht verstehen und kennen. Das ist jedoch essenziell, damit Sie sich ein besseres Bild davon machen können, was Sie schützen wollen und in welchem Umfang. Außerdem müssen Sie Ihre Sicherheitskontrollen einführen und kontrollieren.

Wie können wir helfen?

Irina: IT-Sicherheit soll dabei helfen, die Geschäftsfunktionen komplementär zu unterstützen und sie zu schützen. Was die meisten Unternehmer:innen nicht verstehen, ist, dass Sicherheit nicht kompliziert, sondern einfach sein sollte – nicht zu viel und nicht zu wenig. IT-Sicherheit darf auch nicht zu teuer sein, sondern funktional. Sie brauchen nicht das nächste „glänzende" Ding auf dem Markt. Wir können kleinen und mittelständischen Unternehmen helfen, das richtige Gleichgewicht zwischen Sicherheit und Geschäft zu finden. Wir helfen, die beste Lösung mithilfe einer Kosten-Nutzen-Analyse zu finden und zu implementieren.

Warum re:think?

Vladimir: Wir sind ein Team von Experten mit einer Vielzahl von Fähigkeiten. Sicherheit sehen wir nicht als Add-on, sondern sie ist integriert in unsere Mission. Wir sind engagierte und motivierte Spezialisten, die sich nicht nur auf die theoretische Beratung, sondern auch auf die operative Seite konzentrieren. Wir beraten Sie nicht nur, was zu tun ist, sondern auch wie es zu tun ist. Dabei begleiten wir Sie vom ersten bis zum letzten Schritt.

Wie würde die Zusammenarbeit mit uns ablaufen?

Irina: Wie bereits erwähnt, ist es wichtig, das Unternehmen zu verstehen. Deshalb machen wir es uns zur Aufgabe, Ihr Unternehmen kennenzulernen, damit wir die beste Lösung für Ihre geschäftlichen Anforderungen finden können. Wir analysieren Ihre Umgebung, um einen besseren Überblick zu bekommen, damit wir den Wert und die Priorität im Auge haben. Nachdem wir die wichtigen Teile des Puzzles kennen, können wir die Gefährdungen analysieren und mit der Auswahl, Implementierung, Prüfung und Wartung der Lösung beginnen.

IRINA NORK

re:think Innovations GmbH
Braunschweig

HEAD OF CYBER SECURITY

Irina Nork ist Cybersicherheitsexpertin mit mehr als 15 Jahren Erfahrung in IT und Cybersicherheit.
Ihre berufliche Laufbahn begann bei der israelischen Bundeswehr als IT-Systemadministratorin und Sicherheitsanalystin. Sie verfügt über umfangreiche Erfahrung in strategischer und operativer Cybersicherheit.

Foto: Adobe Stock / rrice, Tierney

Braucht man eine **CYBERVERSICHERUNG?**

Wie Unternehmen und Privatpersonen sich gegen Cyberkriminalität wappnen können

Man kommt morgens ins Büro, fährt mit dem ersten Kaffee auf dem Tisch den Rechner hoch und erledigt alltägliche Aufgaben – ein ganz normaler, selbstverständlicher Arbeitsablauf für viele Berufstätige. Nahezu in jeder Branche werden unternehmensbezogene Daten, Kundendaten und weitere Prozesse digitalisiert, was einerseits die Arbeit erleichtert, andererseits aber auch Maßnahmen zum Erhalt der Sicherheit erfordert – denn Hacker machen sich die Entwicklung der Digitalisierung zunutze: Sie verschaffen sich Zugriff auf die IT-Infrastruktur, können nicht nur vertrauliche Daten einsehen und weiterverwenden, sondern auch Systeme komplett lahmlegen. Wenn dieses Szenario eintritt, ist eine gute Absicherung von Vorteil. Wer von einer Cyberversicherung profitiert und wie im Ernstfall vorgegangen wird, erklären die Produktmanagerinnen Sarah Hahn und Sandra Staßar von der Öffentlichen Versicherung Braunschweig.

SARAH HAHN
Öffentliche Versicherung
Braunschweig

PRODUKTMANAGERIN

Die Kauffrau für Versicherungen und Finanzen ist seit 2007 bei der Öffentlichen Versicherung in Braunschweig tätig. Hier kümmert sie sich im Produktmanagement vorrangig um die Bereiche Firmen- und Cyberversicherung.

Risiken der Digitalisierung

Dass die Digitalisierung nicht nur viele Vorteile, sondern auch Gefahren birgt, zeigt eine Publikation zur „Lage der IT-Sicherheit in Deutschland 2022“, in der die größten Bedrohungen von drei Zielgruppen ermittelt wurden: Für die Gesellschaft sind diese unter anderem „Identitätsdiebstahl“ und „Fake-Shops im Internet“. Für die Wirtschaft sowie den Staat und Verwaltung können „Ransomware“ (diese verschafft Eindringlingen Zugang zum System und kann Daten verschlüsseln) und „Schwachstellen“ besonders gefährlich werden. Haben sich Hacker erst einmal in die IT-Infrastruktur eingeschleust und diese verschlüsselt, kommt es nicht selten vor, dass hohe Summen Lösegeld für die Freigabe der Systeme und Daten in Form von Bitcoins verlangt werden.

Wie können Unternehmen sich schützen?

Um das Risiko eines erfolgreichen Cyberangriffs zu reduzieren, sind neben technischen Maßnahmen wie der Installation einer Firewall und der fortlaufenden Aktualisierung aller Systeme, vor allem die Mitarbeitenden gefragt. Im Arbeitsalltag einen sensiblen und aufmerksamen Umgang mit verdächtigen E-Mails und Virenmeldungen zu gewährleisten, gilt als wichtige Komponente für die Sicherheit des ganzen Unternehmens. Denn mit fortschreitender Digitalisierung haben sich auch die Möglichkeiten für Hacker, anonym und bequem vom Bildschirm aus Geschäfte zu machen vervielfältigt. Die Entwicklung hin zu Homeoffice und Mobile Office sowie permanenter Online-Präsenz tragen ebenfalls dazu bei, dass die Angriffsfläche größer wird.

Cyberkriminalität kann jeden treffen

Unabhängig von Größe und Branche ist IT-Sicherheit relevant für jedes Unternehmen. Dieses Bewusstsein als Geschäftsführer und Mitarbeitender auch in kleinen und mittelständischen Unternehmen zu schaffen, ist ein wichtiger Schritt, denn Digitalisierung betrifft alle Branchen: Ob Handwerker, Spedition oder Arztpraxis, ob selbständig oder angestellt. Je stärker der Unternehmenserfolg von der Technik abhängt, desto mehr Schaden richtet ein Angriff an.

Nicht nur im Joballtag, sondern auch in der privaten Online-Nutzung bestehen vielfältige Methoden, um an persönliche Daten zu gelangen. Per E-Mail, Post oder Telefon versuchen Betrüger den Usern Daten zu entlocken, die sie für eigene Zwecke nutzen können. Häufig werden direkte Appelle mit Zahlungsaufforderungen oder Passworteingaben verschickt. Besonders wachsam sollte man bei E-Mails, die weiterführende Links enthalten, sein – mit einem Klick kann im Hintergrund ein ungewolltes Programm installiert werden, welches Daten verschlüsselt oder kopiert. Diese „Phishing-Mails“ beispielsweise sind heutzutage kaum noch von Mails seriöser Unternehmen zu unterscheiden: Wo uns früher kryptische Zeichen und Rechtschreibfehler stutzig machten, müssen wir heute ganz genau hinschauen. Mit einem achtsamen Umgang und geeigneten Passwörtern kann sich im beruflichen sowie privaten Alltag geschützt werden.

Wie wird im Ernstfall vorgegangen?

Wird eine Firma bzw. Person Opfer einer Cyberattacke, die mit Datenverlust und eventueller Lösegeldforderung einhergeht, ist es wichtig, nicht in Panik zu verfallen. Mithilfe eines Ansprechpartners der Versicherung wird sich zunächst ein Überblick verschafft: Wen betrifft der Angriff, wie hoch ist das Ausmaß? Sind auch externe Partner und Kunden durch Datenverlust und -missbrauch geschädigt und müssen darüber informiert werden? Wie kann ein Reputationsschaden minimiert werden? Jeder dieser Schritte sowie einer fachlichen Beratung gehört zur Expertise des Ansprechpartners, der außerdem anfallende Aufgaben übernimmt. In Zusammenarbeit mit Spezialisten, sogenannten IT-Forensikern, wird für die Datenwiederherstellung im Unternehmen gesorgt.

Cyberversicherungen decken eine Bandbreite von Leistungen ab, die individuell an den eigenen Bedarf angepasst werden können. Im Durchschnitt beläuft sich der wirtschaftliche Schaden durch Onlinekriminalität in Unternehmen auf rund 50.000 Euro.

Mit Sicherheit regional

Als öffentlich-rechtliche Versicherungsgesellschaft, die vom Land Niedersachsen unterstützt wird, sieht sich die Öffentliche Versicherung regional verbunden und setzt sich dafür ein, Braunschweig und Umgebung voranzutreiben – mit auf den Bedarf der Menschen angepasster Produktentwicklung vom Standort in der Theodor-Heuss-Straße, bis zur Förderung von Kunst, Kultur, Sport und Forschung. Beispielsweise mit der Unterstützung vom „RENEW“ Festival und Eventlocations wie dem „381“ möchten die Verantwortlichen die Lebensqualität im Umkreis weiterhin steigern.

SANDRA STAßAR
Öffentliche Versicherung
Braunschweig
PRODUKTMANAGERIN

Sandra Staßar ist seit 2003 bei der Öffentlichen Versicherung tätig und absolvierte dort bereits ihre Ausbildung. Aktuell arbeitet sie in der Abteilung Produktmanagement Komposit und ist in einem breiten Produktportfolio unter anderem mit für den Bereich Cyberversicherung zuständig.

CYBER-KRIMINALITÄT – „RISIKEN KENNEN UND IM VORAUS HANDELN!“

Das Risiko Feuer kennt jeder – aber das Risiko Cyber?

Schon im Kindesalter hören wir: „Spiel nicht mit dem Feuer!“ Viele Maßnahmen schützen uns vor dem Ausbruch eines Brandes, der unser Hab und Gut beschädigen oder sogar vernichten könnte. Maßnahmen wie E-Check, TÜV-geprüfte Geräte, Rauchmelder, Brandmauern, Brandmeldeanlagen, Notausgänge, Rettungsplane, Feuerlöscher und Sprinkleranlagen verhindern oder dämmen das Ausmaß bestenfalls ein. Unternehmen beschäftigen Brandschutzbeauftragte zur Wahrnehmung des betrieblichen Brandschutzes.

Sollte es doch mal brennen, haben wir mit der Notrufnummer einen schnellen Zugriff auf die Feuerwehr und am Ende steht die Feuerversicherung für die Absicherung der finanziellen Folgen ein.

Wie ist das bei unserem heutigen Thema?

Ob die Datenkommunikation gestört oder vertrauliche Informationen gestohlen werden, Unternehmen haben stets das Nachsehen und nicht selten steht dabei ihre Existenz auf dem Spiel. Daher sollte für jede Organisation die IT-Sicherheit oberste Priorität haben, völlig unabhängig von ihrer Größe.

Alle sind betroffen: Selbständige, Freiberufler, Gewerbetreibende, Unternehmen, Vereine, Verbände, öffentliche Einrichtungen u.v.m. sind im Zeitalter der Digitalisierung auf die eigene Informationstechnologie und die Verfügbarkeit von Daten angewiesen! Die IT-Sicherheit muss in deutschen Unternehmen/Organisationen stärker berücksichtigt werden und gehört in den Verantwortungsbereich der Geschäftsführung und des Vorstands.

Laut des Digitalverbandes Bitkom e.V. investieren zuletzt 43 % der KMU in Deutschland jährlich weniger als 10.000 Euro in die IT-Sicherheit des eigenen Unternehmens. Die Folge: Neun von zehn Unternehmen (88 %!) waren 2020/21 von Cyber-Angriffen betroffen. Hackerangriffe, Cyber-Erpressungen, Netzwerksicherheitsverletzungen, Datenrechtsverletzungen, Datenmissbrauch oder -verlust und Sabotage, führen in der deutschen Wirtschaft laut Bitkom zu mehr als 223 Mrd. Euro Schaden im Jahr 2021. Somit sollte jedem klar sein: „Die IT-Security eines Unternehmens – egal welcher Größe – muss ein wesentlicher Bestandteil in der Unternehmensstrategie sein!“

Auf der nachfolgenden Basis können konkrete Sicherheitsmaßnahmen für alle Unternehmen etabliert werden!

Sechs wesentliche Fragen zu der IT-Strategie einer Organisation oder eines Unternehmens:

Ist eine eigene IT-Sicherheitsabteilung vorhanden? Gemeint ist nicht der Datenschutzbeauftragte, sondern Experten, welche sich laufend und professionell mit der unternehmenseigenen IT-Sicherheitsstrategie beschäftigen. Dies können sowohl eigene qualifizierte Mitarbeiter*innen oder externe Dienstleister sein.

Auf der Agenda der IT sollte die Sicherheit deshalb an allererster Stelle stehen – genauer gesagt: eine zentrale IT-Sicherheitsabteilung.

Wurde IT-Abhängigkeit und Anfälligkeit evaluiert?

Um die richtigen Entscheidungen zu treffen, ist in der Analyse herauszuarbeiten, wie sich die einzelnen Geschäfts- und IT-Prozesse auf die Geschäftsfähigkeit auswirken. Sind Unternehmensprozesse bei einem Ausfall der IT, bei Nichtverfügbarkeit von Daten betroffen? Anhand dessen werden die konkreten Schwachstellen aufgespürt und nach Abwägung von Alternativen, Kosten, Risiken und Nutzen verschiedene Ansätze und Maßnahmen erarbeitet. Nur wer viel über seine Infrastruktur und Ablauforganisation weiß und richtig priorisiert, kann diese auch gut schützen.

Ist ein übergreifendes Risikomanagement implementiert?

Ein Risikomanagement ist ein systematischer Ansatz, um den Handlungsbedarf, welcher sich aus Risiken und Chancen ergibt, frühzeitig zu erkennen und wirtschaftlich umzusetzen. Die Früherkennung dieses Handlungsbedarfs ermöglicht, die Risikohandhabung und Chancennutzung optimal zu planen und effizient und effektiv zu realisieren. Der durch das Risikomanagement ausgelöste Wertbeitrag ist nicht zu unterschätzen. Schadenvermeidung ist wesentlich wirtschaftlicher als Schadenbehebung. Der Zeitpunkt der Wandlung einer Chance in einen nutzbaren Wertbeitragsfaktor bestimmt wesentlich dessen Wert für das Unternehmen. Viel wichtiger als nur die

CHRISTIAN GERSTUNG
Döhler Hosse Stelzer GmbH & Co. KG
Braunschweig
DIREKTOR KUNDENMANAGEMENT

Christian Gerstung ist seit 1999 in der Versicherungsbranche tätig. Seine Expertise als Meister des Handwerks und Versicherungsmakler ist das Analysieren und Bewerten von Gefährdungspotenzialen von Firmen- u. Unternehmenskunden. Seit 8 Jahren ist er Spezialist für die Absicherung von Cyber-Risiken. Als Direktor im Team von DHS ist er für den Bereich Kundenmanagement verantwortlich.

Foto:Adobe Stock / Andrii Yalanskyi

Kenntnis aller Angriffsmöglichkeiten ist die Kenntnis der eigenen Verwundbarkeit, internen Strukturen und Prozesse!

Ist ein Krisenplan vorhanden?

Nicht jedes mögliche Krisenszenario ist vorhersehbar. Es sollte für den Ereignisfall ein anwendbarer eingeübter Maßnahmenplan zur Krisenbewältigung vorhanden sein. Eine erfolgreiche Krisenbewältigung ist abhängig von einer raschen Umsetzung von notwendigen Sofortmaßnahmen zur Eindämmung des Krisenausmaßes. Durch effiziente Zusammenarbeit des Krisenstabs und der Interventionsteams und Unterbindung einer Eskalation der Ereigniskette kann die Handlungsfähigkeit in einer Krise bestenfalls aufrechtgehalten werden. Auch eine professionelle Kommunikation nach innen und außen sollte gewährleistet werden können.

Wie ist der Umgang mit Gesetzgebung und Rechtsprechung (DSGVO) geregelt?

Ein wichtiges Beispiel für rechtliche Vorgaben, die für die IT-Compliance einzuhalten sind, ist der Datenschutz. Die IT muss so gestaltet und genutzt werden, dass der Schutz personenbezogener Daten gewährleistet ist. Was dies konkret bedeutet, regelt auf EU-Ebene seit Mai 2018 die Datenschutz-Grundverordnung (DSGVO).

Compliance in der IT bedeutet, dass mit der IT nicht alles umgesetzt wird, was technisch und organisatorisch möglich ist, sondern nur das, was innerhalb des Regelwerkes erlaubt ist. Unternehmen und Behörden sind deshalb laufend gefordert zu prüfen, ob ein bestimmtes Vorhaben in der IT auch regelkonform und damit compliant ist. Die Führung und Organisation der IT, die IT-Governance, muss sich also mit ihren Entscheidungen und Maßnahmen innerhalb des Rahmens bewegen, der sich aus den Vorgaben der IT-Compliance ergibt.

Besteht ein Ad-hoc-Zugriff auf spezialisierten Dienstleister im Schadenfall?

Moderne, vernetzte Technologien und Wertschöpfungsprozesse führen dazu, dass fast jedes Unternehmen überall auf der Welt Opfer oder Werkzeug eines Cyberangriffs werden kann. Viele Unternehmen sind für einen solchen Fall organisatorisch schlecht oder nicht vorbereitet.

Der Aufbau dieser Strukturen – so sinnvoll er auch im Einzelfall sein mag – überfordert viele Unternehmen sowohl technisch als auch finanziell. Die meisten Unternehmen sind auch nicht auf die Zusammenarbeit zwischen dem strategisch ausgerichteten Krisenmanagement und der operativen Notfallbewältigung im Rahmen des Business Continuity Managements eingerichtet. Auf diese Weise entstehen einerseits hohe Reibungsverluste im Krisenmanagement (das nicht ausreichend schnell mit notwendigen und verständlichen Informationen versorgt wird) und andererseits im Notfallmanagement (das unklare oder unrealistische Vorgaben aus dem Krisenmanagement erhält). In diesem Fall ist es sinnvoll, entsprechend spezialisierte IT-Dienstleister beratend und auch zur Unterstützung im Notfall heranzuziehen. Dabei gilt es, sich gegen Vorfälle aller Art abzusichern – besonders wenn man deren Lösung nicht selbst in der Hand hat.

Im Voraus zu handeln, macht fast alles weitere planbar und das Unternehmen ist im Krisenfall bestenfalls weiterhin handlungsfähig! Das Resultat einer durchdachten IT-Strategie und der damit verbunden Maßnahmen bringt letztendlich alle Geschäftsprozesse voran – auch wenn nichts passiert.

Gefahr/Risiko: Feuer

Maßnahmen:
- E-Check & TÜV-geprüfte Geräte
- Feuerlöscher
- Rauchmelder
- Brandmeldeanlagen
- Notausgänge
- Rettungspläne
- Sprinkleranlagen
- Löschsysteme
- Brandschutzbeauftragten

Notrufnummer & Feuerwehr

Gefahr/Risiko: Cyber

Maßnahmen:
- Vier-Augen-Prinzip
- Regelmäßige Auditierungen
- Virenscanner & Firewall
- Patch-Management-Prozess
- ISMS Zertifizierung, Standards/Normen
- Zwei-Faktor Authentifizierung/MFA
- Sensibilisierung Mitarbeiter*innen
- Datensicherungssysteme
- IT-Security-Beauftragten

Krisenhotline & Krisendienstleister

und am Ende steht eine Versicherung für die Absicherung der finanziellen Folgen!

„Man kann nur schützen, was man kennt. Man kann nur versichern, was geschützt ist."

Eine Absicherung durch eine mögliche Versicherungslösung die „Cyber-Police" sollte ein wesentlicher Baustein des Versicherungsmanagement eines Unternehmens sein, denn ein Cyber-Schadenfall kann die Existenz eines Unternehmens bedrohen!

Autorenübersicht

APPELHAGEN Rechtsanwälte
Steuerberater PartGmbB

Theodor-Heuss-Straße 5a, 38122 Braunschweig
Telefon 0531 2820-0
info@appelhagen.de
www.appelhagen.de
Autoren: Karin Kutz (S. 25),
Maximilian Gerdesmann (S. 28)

ATD GmbH

Linnéstraße 5, 38106 Braunschweig
Telefon 0531 23824-0
info@atd.de
www.atd-systemhaus.de
Autor: Holger Kämmerer (S. 38 – 39)

Braunschweigische Landessparkasse
Anstalt öffentlichen Rechts

Friedrich-Wilhelm-Platz, 38100 Braunschweig
Telefon 0531 4870
kundenservice@blsk.de
www.blsk.de
Autor: Dr. Ingo Lippmann (S. 22 – 23)

C&H GESELLSCHAFT FÜR INFORMATIONS-
TECHNOLOGIE MBH

Große Düwelstraße 28, 30171 Hannover
Telefon 0511 475362-40
info@cundh.com
www.cundh.com
Autoren: Holger Flößer,
Christoph Ingenhaag (S. 20 – 21)

DÖHLER HOSSE STELZER GmbH & Co. KG
VERSICHERUNGSMAKLER

Bankplatz 7a, 38100 Braunschweig
Telefon 0531 24254-0
info@dhs-makler.de
www.dhs-versicherungsmakler.de
Autor: Christian Gerstung (S. 48 – 49)

Explizit Werbeagentur GmbH

Wolfenbütteler Strasse 45a, 38124 Braunschweig
Telefon 0531 2819110
info@explizit.de
www.explizit.de
Autor: Felix Kurkowski (S. 8 – 9)

Intelligence Unit Service AG

Steintorwall 3, 38100 Braunschweig
Telefon 0531 180 59 300
info(at)i-unit.de
www.i-unit.group
Autoren: Tilo Geipel, Sascha Rühmann,
Anis Saad, Andreas Tieftrunk (S. 10 – 12)

KÄMMER CONSULTING GmbH

Jasperallee 23, 38102 Braunschweig
Telefon: +49 531 2343-165
info@kaemmer-consulting.de
www.kaemmer-consulting.de
Autoren: Andreas Stammhammer, Axel Vogelsang,
Jonas Methner (S. 42 – 43)

Niedersächsisches Ministerium
für Inneres und Sport
- Verfassungsschutz -

Büttnerstraße 28, 30165 Hannover
Telefon 0511 6709 – 284
oeffentlichkeitsarbeit@
verfassungsschutz.niedersachsen.de
www.verfassungsschutz.niedersachsen.de
Autor: Markus Böger (S. 34 – 37)

MANDALA Internet, EDV-Service GmbH

Wendenring 1, 38114 Braunschweig
Telefon 0531 3489-0
info@mandala.de
www.mandala.de
Autoren: Manfred Blum (S. 30),
Prof. Andreas Göbel (S. 31)

ALLE BERICHTE ONLINE

www.service-seiten.com

MOHR BODE Partnerschaft mbB Steuerberatungsgesellschaft

Am Fallersleber Tore 6, 38100 Braunschweig
Telefon 0531 1220-0
info@mohr-bode.de
www.mohr-bode.de
Autoren: Alexander Balalaev, Jörg Bode (S. 26 – 27)

Öffentliche Versicherungsanstalt des öffentlichen Rechts

Theodor-Heuss-Straße 10, 38122 Braunschweig
Telefon 05 31/ 2 02-14 49
Sebastian.Heise@oeffentliche.de
www.oeffentliche.de/sebastian.rau
Autoren: Sarah Hahn, Sandra Staßar (S. 46 – 47)

REESE GMBH

Dieselstraße 6, 38122 Braunschweig
Telefon 0531 289289
info@reese-gmbh.de
www.reese-gmbh.de
Autor: Niklas Krüger (S. 14 – 15)

re:think

re:think Innovations GmbH
Wilmerdingstraße 9A, 38118 Braunschweig
Telefon 0531 257 340 82
info@rethink.de
www.rethink.de
Autoren: Vladimir Afonichev, Irina Nork (S. 44 – 45)

Schmittel IT GmbH

Büchtingenstr. 42, 38855 Wernigerode
Telefon 03943 50 994 50
info@schmittel-it.de
www.schmittel-it.de
Autor: Christian Schmittel (S. 16 – 18)

S-CON GmbH & Co. KG

Podbielskistraße 386, 30659 Hannover
Telefon 0800 88 44 66 88
timo.bittner@s-con.de
www.s-con.de
Autoren: Oliver Krause (S. 29), Fabian Hientz (S. 32), Dr. Timo Bittner (S. 33), Marc Pölckow (S. 41)

Zentrale Kriminalinspektion Braunschweig Fachkommissariat Cybercrime

Friedrich-Voigtländer-Straße 41, 38104 Braunschweig
Telefon 0531 4760
www.pd-bs.polizei-nds.de
Autor: Mario Krause (S. 34 – 37)

mediaworld
AGENTUR FÜR MARKETING & VERLAG

BERATEN. QUALIFIZIEREN. ENTWICKELN.

KÄMMER CONSULTING

7. Fachkonferenz „Cybersicherheit“ am 23. Februar 2023

- **Datenschutz**
- **Informationssicherheit**
  (ISO 27001 | TISAX®)
- **Seminare**
  (MS-Office, Datenschutz, Informationssicherheit, Softskills)

Kämmer Consulting GmbH
Nordstraße 11
38106 Braunschweig
0531 702249-42

www.kaemmer-consulting.de

Andreas Stammhammer
- Leiter Vertrieb
- Berater Informationssicherheit

Axel Vogelsang
- Leiter Datenschutz
- Prokurist