IT-MITTELSTAND 4/2023

G59638 www.itmittelstand.de

ÖSTERREICH: 3,30 EUR
LUXEMBURG: 3,45 EUR

SCHWEIZ: 5,90 SFR
DEUTSCHLAND: 3,00 EUR

IT MITTELSTAND

IT-BUSINESS IM MITTELSTAND

IM INTERVIEW

Vorstand
Michael Everts (l.)
und IT-Leiter
Thomas Weinberger

Seite **18**

LEISTRITZ AG

AGIL UND FLEXIBEL ZUM

HIDDEN CHAMPION

SPECIAL: IT-SECURITY

Unternehmen im Visier der Cyberkriminellen

Seite **26**

ERP-SYSTEME

Wenn der Release-Wechsel nicht mehr reicht

Seite **42**

MEDIENHAUS VERLAG
Postfach 300111 • 51411 Bergisch Gladbach
Postvertriebsstück • »Entgelt bezahlt«

MIT APPLUS EINFACH MAL VERWÖHNEN LASSEN.

Lehnen Sie sich zurück und genießen Sie die neue Art des Arbeitens.

Ihr **persönlicher digitaler ERP-Assistent** liefert mit Hilfe von mitlernenden KI-Modulen vom ersten Tag an konkrete Handlungsempfehlungen. Und unterstützt Sie so in Ihrem Daily Business.

applus-erp.de

asseco SOLUTIONS

Sicherheit gibt es nicht zum Nulltarif

Mit der Verlagerung der Arbeitsschritte von der analogen in die digitale Welt bieten Unternehmen Hackern immer mehr Angriffsfläche – und die Qualität der Cyberattacken hat sich nicht zuletzt durch den Russland-Ukraine-Krieg deutlich erhöht. Auf die veränderte Gefahrenlage muss sich auch der deutsche Mittelstand einstellen.

GERADE DIE ANGRIFFE AUS RUSSLAND UND CHINA sind laut einer Studie im Auftrag des Digitalverbands Bitkom 2022 sprunghaft angestiegen: 43 Prozent der betroffenen Unternehmen haben mindestens eine Attacke aus China identifiziert (2021: 30 Prozent). 36 Prozent haben Urheber in Russland ausgemacht (2021: 23 Prozent). Immer häufiger seien die Angreifer im organisierten Verbrechen zu finden, meint Bitkom-Präsident Achim Berg, wobei die Abgrenzung zwischen kriminellen Banden und staatlich gesteuerten Gruppen zunehmend schwerfalle. Er rät Unternehmen, bei den Ausgaben für IT-Sicherheit dringend zuzulegen. „Die Erkenntnis, welche dramatischen Folgen ein erfolgreicher Angriff haben kann, ist längst da – den notwendigen Schutz davor gibt es aber nicht zum Nulltarif."

Unterstützung bei der Auswahl geeigneter Sicherheitsanbieter und -lösungen können sich Mittelständler, die häufig keine oder nur schlanke IT-Sicherheitsabteilungen und geringe finanzielle Ressourcen haben, z.B. bei der Transferstelle IT-Sicherheit im Mittelstand (TISiM) holen. Ihr zentrales Werkzeug, der Sec-O-Mat, bewertet den Bedarf an IT-Sicherheitsmaßnahmen eines Betriebs und erstellt eine strukturierte To-Do-Liste mit konkreten Handlungsempfehlungen. Aber auch die Sicherheitsexperten im aktuellen IT-Security-Special ab Seite 26 geben Unternehmen einige Tipps mit auf den Weg, um der wachsenden Cyberbedrohungslage Herr zu werden.

Vielen Spaß beim Lesen dieser Ausgabe!

Lea Sommerhäuser

Lea Sommerhäuser,
Redaktion IT-MITTELSTAND

› **SCHREIBEN SIE UNS:** **E-Mail:** redaktion@itmittelstand.de | **Twitter:** @ITMredaktion | **Facebook:** IT-Mittelstand

INHALT

MARKT

TRENDS

DIGITALISIERUNG

NACHHALTIGKEIT

LOGISTIK

ANWENDER IM PORTRÄT

PERSONALITY

ORGANISATION
TITELINTERVIEW

AGIL UND FLEXIBEL ZUM HIDDEN CHAMPION

Die Leistritz AG ist Vorreiter gleich in mehreren innovativen Technologiefeldern. Aktuell lagert der Mittelständler aus Nürnberg einen Teil seiner IT-Systeme in das Rechenzentrum der Noris Network AG aus. Im Titelinterview erläutern Vorstand Michael Everts (l.) und IT-Leiter Thomas Weinberger, warum sie sich für das Outsourcing entschieden haben.

STANDARDS

SPECIAL

SEITE 26

ZUGRIFF AUS DEM NETZ

Massive Hackerangriffe sorgen vielerorts für Unsicherheit. Es ist also an der Zeit, einen Blick auf mögliche Lösungen zu werfen.

SEITE 42

SOFTWARE ERP

WENN DER RELEASE-WECHSEL NICHT MEHR REICHT

Was bei der ERP-Einführung seinerzeit noch modern war, wird irgendwann altbewährt oder gar altbacken. Eine Modernisierung ist dann dringend geboten.

PERSONALIE

STÄRKUNG DES FÜHRUNGS-TEAMS

Johannes Klutz ist neuer Chief Financial Officer (CFO) bei SER. Er verfügt über mehr als zehn Jahre Investment- und Finance-Erfahrung und tritt an, um beim Anbieter von Intelligent-Content-Automation-Lösungen das Wachstum und die Profitabilität weiter zu steigern.

Vor seinem Wechsel war Klutz CFO bei der PTV Group (später umbenannt in Umovity und PTV Logistics). Er startete seine Karriere bei der Investmentbank Rothschild, wo er mehrere M&A-Transkationen von mittelständischen und Großunternehmen begleitete. Danach wechselte er in die Investmentabteilung der Porsche SE, die damals u.a. in die PTV Group und mehrere Start-ups investierte.

Klutz freut sich, angesichts der Wachstumsmöglichkeiten im Content-Services-Markt und der Positionierung von SER die Weiterentwicklung aktiv mitzugestalten. „Mein Know-how einzubringen, um ein schnelles und profitables Wachstum auch international zu unterstützen, sehe ich als meine Hauptaufgabe an."

www.sergroup.com

KMU-DIGITALISIERUNG

EUROPA SCHLÄGT USA

KLEINE UND MITTELSTÄNDISCHE UNTERNEHMEN (KMU) IN DEUTSCHLAND VERZEICHNEN IM EUROPÄISCHEN VERGLEICH NEBEN DEN FIRMEN IN GROSSBRITANNIEN MITTLERWEILE DEN BESTEN DIGITALISIERUNGSSTATUS. Für die Studie befragte Yougov im Auftrag von Ionos im Januar 2023 insgesamt ca. 4.800 Personen aus Unternehmen mit bis zu 250 Mitarbeitern in Deutschland, Großbritannien, Spanien, Frankreich und den USA. Deutschland soll demnach das einzige Land sein, in dem sich der Digitalisierungsgrad durchweg verbessert hat – vor allem mit Blick auf die Sichtbarkeit im Internet: So haben je 68 Prozent der befragten Unternehmen eine Website (+5 Prozent im Vergleich zum Vorjahr) und eine professionelle E-Mail-Adresse (+4 Prozent). Nur Großbritannien liegt mit je 76 Prozent weiter vorn. In Spanien und Frankreich ist ein leichter Abwärtstrend erkennbar, Schlusslicht in fast allen Bereichen sind die USA: Hier hat laut Umfrage z.B. nicht einmal die Hälfte der KMU eine Website (44 Prozent), das sind über ein Fünftel weniger als im Vorjahr.

Kosten und Zeitmangel

Als größte Hürden bei der Digitalisierung sehen die Firmen in Deutschland nach wie vor die Kosten (50 Prozent) und den Zeitmangel (48 Prozent) sowie Bedenken bezüglich Sicherheit und Datenschutz (41 Prozent). Auch in den anderen Ländern spielen diese Aspekte eine wichtige Rolle, die KMU in Spanien und Frankreich halten allerdings die Inflation für die zweitgrößte Hürde.

Als größten Nutzen der Digitalisierung sieht die breite Mehrheit (etwa 80 Prozent) der Befragten in Deutschland wie in den anderen Ländern die Präsenz ihres Unternehmens im Internet. Über die Hälfte der KMU in Deutschland (51 Prozent) möchte diese Sichtbarkeit weiter ausbauen. Konkret investiert wird vor allem in die Website (29 Prozent), ins Online-Marketing (21 Prozent) und bei Social Media (19 Prozent). Großes Augenmerk legen die Befragten darüber hinaus auf ihre IT – 34 Prozent planen Investitionen in den Bereichen „IT-Sicherheit" und „Datenschutz", ein Viertel (24 Prozent) hat Budget für Investitionen in die IT-Infrastruktur eingeplant.

www.ionos.de

Wer die Digitalisierung *nicht fest in seiner Business-Strategie verankert, wird es perspektivisch schwer haben, auf dem Markt zu bestehen.*

Quelle: Online-Umfragen der YouGov Deutschland GmbH unter je ca. 1.000 Personen aus Unternehmen mit bis zu 250 Mitarbeitern (Januar 2022 / Januar 2023)

KURZ-MELDUNGEN

PERSONALIEN

NEUANFANG AUF ALLEN EBENEN

Zalaris-Urgestein Arnold Altmann, der bisher als Vice President Professional Services tätig war, hat zum 1. April 2023 offiziell die Geschäftsführung der Vyble GmbH übernommen.

NEUER CTO FÜR IP-VIDEOSPEZIALISTEN

Christian Cabirol hat Anfang April seine Position als CTO bei der Mobotik AG angetreten und wird alle F&E-Schwerpunkte und Technologiepartnerschaften verantworten.

FÜR DIE INDUSTRIE

5G-CAMPUS ALS TESTGELÄNDE

Das Beratungsunternehmen Detecon hat in der Kölner Bayenwerft ein Testgelände für 5G-Campusnetze im Unternehmensumfeld eröffnet.

Vorstellung verschiedener Use Cases *bei der Eröffnung des FiveGDock in der Bayenwerft in Köln*

Im FiveGDock will das Unternehmen interessierten Anwendern Orientierung innerhalb vielfältiger Optionen und Voraussetzungen bieten. Dabei baut der Anbieter ein 5G-Campusnetz in eigenen Open Spaces auf und verwandelt diese in ein Smart Building. Das Headquarter wird so zum Labor für innovative und konnektivitätsgetriebene Geschäftsprozesse. Es entsteht ein branchenübergreifendes Demonstrationszentrum mit Szenarien für innovative Office-, Logistik- oder Produktionsanwendungen, um die Potenziale von 5G zu veranschaulichen.

Plattform für innovative Konzepte

Das 5G-Campusnetz am Kölner Rheinauhafen wird eine Plattform für flexibel erweiterbare Showcases wie zum Start etwa AGV Robotics, Wifi/5G-Vergleiche, IoT-Sensorik sowie Demos für Augmented und Virtual Reality (AR/VR) sein. Unternehmen erhalten damit die Chance, ihr Konzept zu testen, bevor es an den konkreten Aufbau eines entsprechenden eigenen Netzwerkes geht. Statt groß ins Ungewisse zu investieren, kann im Kleinen ausprobiert, getestet und justiert werden. Der Campus ist in der Lage, unterschiedlichste Use Cases abzubilden, und ermöglicht es Verantwortlichen, entsprechende Schlüsse auf die entwickelte Strategie zu ziehen.

Erste Kunden haben laut Anbieter bereits ihr Interesse bekundet: So wird das Unternehmen beispielsweise die Validierung und Prüfung einzelner, weltweiter Anwendungsfälle für Campusnetze beim Hochtechnologiekonzern Zeiss durchführen und auf Basis einer laborhaften Erprobung im Kölner 5G-Campusnetz einen globalen Blueprint für die Zeiss-IT erstellen.

Ein Schlüssel für neue Geschäftsmodelle

Mit Campusnetzen erhalten Unternehmen die Möglichkeit zum Aufbau eigener 5G-Netze. Hierzu stellt die Bundesnetzagentur lokale 5G-Frequenzen für Unternehmen bereit, die auf eigenem Gelände Netze für lokale Anwendungen errichten wollen. So kann damit zellularer Mobilfunk autonom und maßgeschneidert von Industrien in privaten Netzen genutzt werden.

Campusnetze bieten enorme Chancen: Insbesondere höhere Flexibilität, Effizienz sowie die sehr hohe Zuverlässigkeit der Vernetzung sind wesentliche Motive zum Einsatz von 5G in eigenen Geschäfts- und Produktionsprozessen und damit ein Schlüsselfaktor für moderne, digitale Geschäftsmodelle.

www.detecon.com/de

FÖRDERUNG FÜR DIGITALISIERUNGSPROJEKTE

KEINE ANGST VOR GELD VOM STAAT!

Warum Unternehmen sich viel mehr für öffentliche Förderangebote interessieren sollten, erklärt *Benjamin Springub,* VP Operations Development bei der Deutschen Telekom, im Kommentar.

Benjamin Springubs Appell *an alle Mittelständler lautet: „Haben Sie keine Angst vor geschenktem Geld! Nehmen Sie es und investieren Sie so in Ihre Zukunftsfähigkeit!“*

Dass der digitale Wandel kontinuierlich Anpassungen nötig macht, ist den Unternehmensverantwortlichen im Land eigentlich klar – aber Digitalisierungsprojekte lassen sich nicht zum Nulltarif umsetzen. Mit ein paar 1.000 Euro für digitales Customizing ist es nur selten getan. Viel häufiger müssen für das Entwickeln von individuellen Lösungen 100.000 Euro in die Hand genommen werden. Kein Wunder, dass viele Entscheider da angesichts einer mehr als schwierigen Konjunkturlage zurückhaltend sind. Was sie dabei außer Acht lassen, ist das Thema „öffentliche Förderungen“.

„GEGEN UNINFORMIERTHEIT HILFT SCHON EIN KURZER BLICK INS INTERNET UND FEHLENDER ÜBERBLICK IST SCHLICHT EIN BERATUNGSDEFIZIT.“

In wirtschaftlich schwierigen Zeiten ist die öffentliche Hand besonders freigiebig, denn Bund und Länder wollen die Wirtschaft stabil halten. Hinzu kommen die intensiver werdenden nationalen Bemühungen um mehr Nachhaltigkeit, für die klare Anreize gesetzt werden müssen. Als Konsequenz davon listet die Förderdatenbank des Bundesministeriums für Wirtschaft und Klimaschutz derzeit rund 2.500 Förderprogramme auf. Dass dennoch nur etwa 18 Prozent der Unternehmen im Mittelstand Fördergelder für Digitalisierungsvorhaben in Anspruch nehmen, hat im Wesentlichen vier Gründe bzw. Vorurteile.

UNINFORMIERTHEIT: Die meisten Mittelständler wissen schlicht nicht, dass und in welchem Umfang Digitalisierungsprojekte gefördert werden.

FEHLENDER ÜBERBLICK: Die riesige Zahl an Fördermöglichkeiten schreckt ab. Man befürchtet, nicht „durchzusteigen“.

ZU VIEL BÜROKRATIE: Viele Unternehmen glauben, dass der zur Bewältigung der bürokratischen Hürden erforderliche Arbeitsaufwand in keinem Verhältnis zum möglichen Benefit steht.

STOLZ: Das Beantragen von Fördergeldern wird mit dem Eingeständnis von Hilfsbedürftigkeit gleichgesetzt.

Empfehlung: jetzt aktiv werden!

Alle diese Gründe sind nicht stichhaltig. Gegen Uninformiertheit hilft schon ein kurzer Blick ins Internet und fehlender Überblick ist schlicht ein Beratungsdefizit. Wir haben deshalb z.B. mit der Initiative „Schubkraft“ ein umfassendes Beratungs- und Hilfsprogramm aufgelegt, über das jedes interessierte Unternehmen weitreichende Unterstützung erhält.

Bürokratie ist im Zusammenhang mit Fördergeldbeantragung zwar tatsächlich ein Thema, die Dimension wird aber stark überschätzt. Bleibt noch der Stolz – dieser Grund ist der irrationalste von allen. Das Nutzen von Fördergeldern ist kein Zeichen von Schwäche, sondern ein strategisch äußerst starker Schachzug: Wer die öffentliche Hand an seinen Digitalisierungskosten beteiligt, ohne dies wirklich nötig zu haben, kann auf denkbar günstige Weise seine Wettbewerbsposition verbessern.

KURZMELDUNGEN

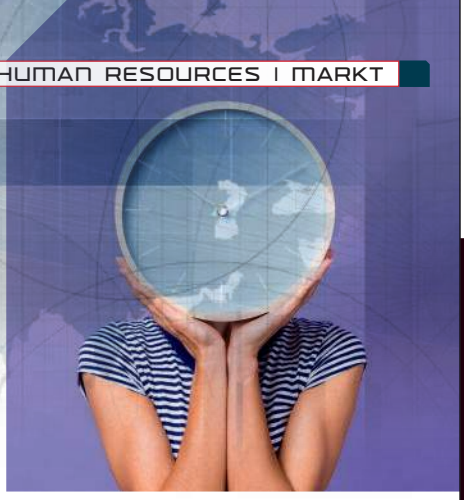
ANWENDUNGEN

ELEKTRONISCHE ABWICKLUNG

- Computop hat sich in einer europaweiten Ausschreibung durchgesetzt und übernimmt zukünftig die Zahlungsabwicklung der Lkw-Maut von Toll-Collect-Kunden.

OPTIMIERTE VERFÜGBARKEIT

- Mit hyperkonvergenten Appliances von Dell Technologies hat Otto Fuchs eine hochverfügbare IT-Infrastruktur aufgebaut, die Flexibilität bietet und sich einfach verwalten lässt.



ARBEITSZEIT-ERFASSUNGSPFLICHT

POSITIVES ECHO AUS DEM MITTELSTAND

Beschäftigte im deutschen Mittelstand stehen der Arbeitszeiterfassungspflicht eher positiv gegenüber – zu diesem Ergebnis kommt eine aktuelle Studie von Tisoware, einem Unternehmen der Proalpha-Gruppe. Ende 2022 stellte das Bundesarbeitsgericht (BAG) durch ein Grundsatzurteil die generelle Pflicht zur systematischen Arbeitszeiterfassung fest. Während die Politik noch intensiv über die konkrete Ausgestaltung einer Gesetzesnovelle zur Arbeitszeiterfassungspflicht diskutiert, sind die Beschäftigten im Mittelstand der anstehenden Neuregelung gegenüber eher positiv eingestellt. Sie sehen sogar eine Win-win-Situation für Arbeitnehmer und -geber.

Die große Mehrheit (89 Prozent) der Arbeitnehmer erfasst bereits ihre Arbeitszeit. 69 Prozent der Beschäftigten sind zudem der Meinung, dass durch das Eintragen der Arbeitszeit die eigenen Überstunden für den Arbeitgeber sichtbar werden; währenddessen befürchten 34 Prozent, dass die Dokumentation der Arbeitszeit sie zum gläsernen Arbeitnehmer macht. Jeder Dritte (33 Prozent) sieht gar keinen Sinn in der Arbeitszeiterfassung.

www.tisoware.com

SMARTE ZEITERFASSUNG

IM WETTLAUF MIT DER ZEIT?

Digitalisierung ist in aller Munde – doch beim Thema „Zeiterfassung“ haben viele Unternehmen immer noch Nachholbedarf. Doch spätestens mit Implementierung der Vorgaben des Europäischen Gerichtshofs im deutschen Arbeitszeitgesetz müssen Unternehmen eine Aufschlüsselung der Arbeitszeit ihres Personals vorweisen können, sonst drohen Bußgelder. Wie die systematische Erfassung erfolgt, ist gesetzlich nicht vorgeschrieben, allerdings sollte die Lösung rechtssicher sein.

Bürokratie abbauen

Viele unterschätzen den Aufwand für eine manuelle Zeiterfassung wie z.B. in Excel-Tabellen. Bei einer smarten Lösung laufen alle Prozesse automatisiert. Wer sich digital aufstellt, sollte auf eine übersichtliche Benutzeroberfläche sowie eine einfache Bedienbarkeit für eine möglichst effiziente Abwicklung setzen.

Individuelle Skalierbarkeit

Smarte Software passt sich an die internen Strukturen von Betrieben an und nicht umgekehrt. Parametrierbare Module wie z.B. MTZ Time von Miditec Datensysteme lassen sich bezüglich der Arbeitszeitmodelle individuell konfigurieren.

Digitale Personalarbeit

Die gespeicherten Informationen in smarten Zeiterfassungslösungen finden etwa Verwendung für die weiterführende Datenverarbeitung in einem entsprechend integrierten Lohn- und Gehaltssystem. Wer auf integrierte Systeme statt auf einzelne Lösungen setzt, kann die Funktionen jederzeit nach Bedarf erweitern.

www.miditec.de

KURZ-MELDUNGEN

PRODUKTE

EINFACH UND ERSCHWINGLICH

Aryaka hat erweiterte SD-WAN- und SASE-Angebote vorgestellt, die speziell auf die Bedürfnisse von Mittelstandsunternehmen zugeschnitten sind.

MINIMALER CO_2-FUSSABDRUCK

Österreichs größter IT-Dienstleister ACP hat die ersten Weichen für seine klimaneutrale Zukunft gestellt. Der neue Unternehmensstandort der ACP Tekaef in Hohenzell in Oberösterreich soll nicht nur einen klimaneutralen Büroalltag ermöglichen, sondern auch dafür sorgen, dass der CO_2-Fußabdruck der gesamten Belegschaft so gering wie möglich ausfällt.

Beim Neubau des Bürogebäudes wurde auf durchgehende CO_2-Neutralität und eine hohe Energieeffizienz geachtet. Um den Energiebedarf des Gebäudes zu minimieren, wurde besonders Augenmerk auf eine energieeffiziente Haushalts- und Bürotechnik sowie eine energiesparende Beleuchtung gelegt. Als Energiequelle dient eine hauseigene Photovoltaikanlage mit inkludiertem Batteriespeichersystem. Zusätzlich erfolgt ein Ausgleich der Emissionen über zertifizierte Klimaschutzprojekte.

Darüber hinaus wurde auch die zukünftige klimaneutrale Mobilität der Belegschaft von Beginn an in die Planungen eingebunden. Das Ergebnis sind acht E-Ladestationen für die Fahrzeuge der Mitarbeiter, die über die hauseigene Photovoltaikanlage mit integriertem intelligenten Lademanagement gespeist werden.

www.acp.at

Gut gepflegter und effizienter Code *kann sehr viel mehr zum Energiesparen beitragen, als es auf den ersten Blick scheint.*

PROGRAMMIERTE NACHHALTIGKEIT

GREEN CODING RICHTIG UMSETZEN

Das Bewusstsein für Klimaschutz und Nachhaltigkeit hat die IT-Welt längst erreicht. Eine Möglichkeit zur Einsparung von Rechenleistung und Strom ist das Schreiben von energieeffizientem Code.

Deutschland soll bis 2045 klimaneutral sein, so sieht es der Koalitionsvertrag der Bundesregierung vor. Auch auf die IT-Branche kommt es dabei an. Ein Baustein der Strategie: klimabewusstes Programmieren für effektivere und klimaschonende Anwendungen. Der IT-Dienstleister Avision zeigt, welche Punkte dabei den Unterschied machen können:

EFFIZIENTE DATENSTRUKTUREN WÄHLEN: Um den Energieverbrauch von Systemen zu reduzieren, eignen sich einige Datenstrukturen besser als andere, da sie weniger Rechenleistung und Speicherplatz benötigen. Beispiele dafür sind Vektoren, verkettete Listen oder auch Hash-Tabellen.

DAS FRONTEND SCHLANK GESTALTEN: Die eigene Webseite nach Gesichtspunkten der Effizienz zu überarbeiten, birgt enormes Potenzial für die Einsparung von Ressourcen. Für eine Senkung der Rechenleistung bietet sich etwa das Optimieren der Ladezeiten an. Weitere Faktoren sind verwendete Medien wie große Bilder oder Videos und Hintergrundprozesse, die den Energiebedarf oft unnötig erhöhen. In der Gesamtheit können die genannten Punkte die benötigte CPU-Last deutlich senken.

CACHING-TECHNIKEN VERWENDEN: Anstatt alle Werte immer zu aktualisieren, sinkt der Energieverbrauch mit dem Einsatz von Caching. Häufig abgerufene Daten sind dabei temporär im Cache gespeichert – bei einer erneuten Anfrage haben die Nutzer einen schnelleren Zugriff darauf und müssen keine neue Serveranfrage senden. Durch die sinkende Zahl der Aktualisierungen reduzieren sich die benötigte Arbeitslast und der Netzwerkverkehr. Für die verschiedenen Anforderungen gibt es unterschiedliche Techniken, z.B. Client-Caching, Server-Caching oder CDN-Caching.

CLOUD COMPUTING UND VIRTUELLE MASCHINEN (VM) NUTZEN: Der große Vorteil liegt in ihrer Skalierbarkeit. Sie sind an die benötigte Rechenleistung anpassbar und Nutzer können etwa Testsysteme direkt herunterfahren, um auf diese Weise Geld und Strom zu sparen. Bei dedizierter Hardware kann häufiges Abschalten hingegen zu Schäden führen. Auch das Ausführen von mehreren Anwendungen auf einer einzigen VM anstatt auf mehreren physischen Geräten hilft bei der Einsparung von Strom. Nicht zuletzt helfen VMs auch bei der Reduzierung des Platzbedarfs auf der Hardware.

www.avision-it.de

KURZMELDUNGEN

PERSONALIEN

ERFAHRENER FINANZEXPERTE

Das globale Cloud-Kommunikationsunternehmen Infobip hat Richard Kraska zum Chief Financial Officer (CFO) ernannt. Der erfahrene Finanzexperte kommt von Realpage.

GESCHÄFTSFÜHRERWECHSEL

Mario Aguilar Alonso (45) ist seit dem 24. März 2023 als neuer CEO für die kaufmännische Geschäftsführung bei der Bintec Elmeg GmbH verantwortlich.

AUF DEM RICHTIGEN WEG

WIE DIE NACHHALTIGE TRANSFORMATION GELINGT

Eine Nachhaltigkeitsstrategie sollte auch die digitale Infrastruktur ins Visier nehmen. Welche Handlungsfelder als Startpunkt dienen, erklärt *Dr. Christopher Jahns,* Gründer und CEO von XU, im Kommentar.

Die Ressourcen unseres Planeten sind begrenzt und müssen mit Bedacht eingesetzt werden. Auch das seit Jahresbeginn geltende Lieferkettensorgfaltspflichtengesetz (LkSG) bekräftigt den Druck, nachhaltiger zu wirtschaften. Um bei dem Thema Fortschritte zu machen, setzen viele Organisationen auf Digitalisierung. So weit, so gut? Ja, wenn digitale Tools und Künstliche-Intelligenz-Anwendungen (KI) in der Logistik genutzt werden, um Routen und Warenbewegungen zu optimieren, ist das ein guter erster Schritt.

Steigender Energiebedarf

Doch dabei droht ein Kipppunkt: Obwohl Server immer effizienter werden und die Auslastung von IT-Systemen insbesondere in Cloud-Rechenzentren steigt, führt der stark erhöhte Leistungsbedarf vieler Branchen zu einem steigenden Energiebedarf in deutschen Rechenzentren. Laut Borderstep Institut lag dieser im Jahr 2021 mit rund 17 Terawattstunden höher als der Bedarf ganz Berlins. Würde sich dieser Trend fortsetzen, könnte der Energieverbrauch der Rechenzentren in Deutschland trotz deutlicher Effizienzgewinne bei IT und Infrastrukturkomponenten bis 2030 auf rund 28 Terawattstunden ansteigen. Das gilt es dringend zu vermeiden.

Software auf Nachhaltigkeit prüfen: IT-Verantwortliche sollten die genutzte Software hinterfragen. Wie effizient ist der Code, wie hoch die Kompatibilität für unterschiedliche Hardware-Voraussetzungen und wie steht es um die Emissionsbilanz der gesamten Architektur? So können Optimierungspotenziale schnell identifiziert und klare Grundsätze für die Re-Evaluation des Software-Portfolios festgesetzt werden – um Effizienzfortschritte künftig geeignet zu berücksichtigen.

Klimafreundliche Dienste nutzen: Der Blick auf digitale Betriebsprozesse wie Web-Hosting-Modelle und Cloud-Services lohnt sich. Welche Energien werden für deren Betrieb genutzt? Wo stehen die Server? Wie viel Wert legt der Anbieter auf Fairness und Datentransparenz? Durch Drittanbieter anfallende Emissionen und Fragen der Fairness werden oft vergessen.

> „Eine auf Nachhaltigkeit vorbereitete IT-Ausrichtung kann womöglich viele verschiedene Unternehmensbereiche bei der Transformation unterstützen."

Synergieeffekte nutzen: Eine auf Nachhaltigkeit vorbereitete IT-Ausrichtung kann womöglich viele verschiedene Unternehmensbereiche bei der Transformation unterstützen – etwa bei der Erfassung und Bewertung von CO_2-Emissionen. IT-Verantwortliche sollten daher gemeinsam mit den verschiedenen Abteilungen prüfen, welche bereits im Unternehmen genutzten Lösungen auch in anderen Geschäftsbereichen Emissionen reduzieren können.

Das Thema „Nachhaltigkeit" im digitalen Kontext erfordert viel neues Wissen, um bestehende Strukturen hinterfragen, auf Sustainability zugeschnittene neue Antworten liefern sowie deren Potenziale geeignet miteinander verquicken zu können. Damit sind Digital- und Logistikbranche nicht allein, denn wir alle müssen beim Thema dazulernen und uns neue Kenntnisse aneignen.

IT-MITTELSTAND befragt die Verantwortlichen verschiedener IT-Anbieter. In dieser Ausgabe:

Christopher Lohmann, Mitglied im Board von Eye Security

„DAS HERZ AM RECHTEN FLECK“

Unter Mittelstand verstehe ich ...

... vor allem hart arbeitende Menschen und agile Familienunternehmen, die ihr Herz am rechten Fleck haben. Mittelständische Unternehmen verkörpern wichtige Werte wie Unternehmertum, Innovation und gesellschaftliches Engagement und spielen eine entscheidende Rolle für Wirtschaftswachstum und Stabilität.

Der Mittelstand hebt sich von Großkonzernen dadurch ab, dass ...

... Mittelständler in langen Zyklen denken und planen. Für sie sind Qualität und nachhaltiges Wirtschaften wichtiger als Quantität. Das beeinflusst Investitionsentscheidungen z.B. in innovative Technologien oder Geschäftsmodelle. Außerdem nehme ich ein stark ausgeprägtes Gemeinschaftsgefühl wahr, obwohl Gewinn für kleine und mittelständische Unternehmen (KMU) ebenso wichtig ist wie für Großunternehmen. Gerade KMU verstehen sich aber oft als Familie mit einer tieferen persönlichen Verbindung und einem gemeinsamen Einsatz für den Erfolg des Unternehmens.

Um als IT-Spezialist im Mittelstand Erfolg zu haben, bedarf es ...

... der Unterstützung der Geschäftsführung und des Zugangs zu den notwendigen Ressourcen. Das unterscheidet sich nicht grundsätzlich von anderen Unternehmen eben mit Ausnahme davon, dass die Geschäftsführung oder die Eigner eben anders, langfristiger denken und handeln. Wichtig ist, dass der Wert der IT und der Digitalen Transformation für die Zukunft erkannt werden. Ein Schlüsselfaktor, um sicherzustellen, dass IT angemessen in die Gesamtstrategie integriert ist, ist die Zusammenarbeit mit anderen Abteilungen.

Was die IT anbelangt, ist der Mittelstand ...

... damit beschäftigt, Prozesse zu automatisieren, um effizienter zu arbeiten und Betriebsabläufe zu skalieren. Der Fokus gilt dem Kerngeschäft. Dagegen hinken sie oft noch hinterher, wenn es um die Cybersicherheit geht, die angesichts der immer ausgefeilteren Cyberbedrohungen zu einem wachsenden Problem wird. Mittelständische Unternehmen wissen zwar genau, wie wichtig es ist, in Maßnahmen für ihre Cybersicherheit zu investieren, um ihr Geschäft und ihre Kunden zu schützen und zu bewahren. Wirksame Lösungen waren allerdings lange sehr teuer und oft erkennt der Mittelstand in der Fülle der Möglichkeiten nicht, wo er anfangen soll. Genau da setzen wir mit unseren Angeboten an.

Die durchschnittliche IT-Grundausstattung im Mittelstand besteht aus ...

... sehr unterschiedlichen Lösungen und hängt stark von der Branche und den speziellen Anforderungen eines Unternehmens ab. Im Allgemeinen gehören allerdings Produktivitäts-Tools, CRM-Software, Buchhaltungs- und Finanzsoftware, Sicherheitslösungen und natürlich das IT-Personal dazu. In jedem Fall spielt die IT-Infrastruktur von mittelständischen Unternehmen eine entscheidende Rolle, wenn es darum geht, effizient zu arbeiten und im digitalen Zeitalter wettbewerbsfähig zu bleiben.

Charakteristisch für IT-Investitionsentscheidungen im Mittelstand ist, dass ...

... sie dem gesamten Unternehmen großen Nutzen bringen können, da sie die Skalierbarkeit und Flexibilität erhöhen. Um den Nutzen von IT-Investitionen zu maximieren, ist es wichtig, dass der Mittelstand diese als strategische Entscheidungen ansehen, die langfristiges Wachstum und Erfolg fördern und so das Unternehmen sichern. Durch Investitionen in IT-Infrastrukturen und -Lösungen können Unternehmen ihre Betriebsabläufe verbessern, ihre Wettbewerbsposition stärken und sich vor Cyberbedrohungen schützen.

Die typischen IT-Probleme des Mittelstands sind ...

... sind u.a. begrenzte Budgets, zu wenige IT-Ressourcen und ein Mangel an IT-Fachwissen. In der Folge kämpfen viele mit veralteter Technologie und der Schwierigkeit, neue Technologien in die bestehende Infrastruktur zu integrieren. Diese Herausforderungen können die Produktivität, Effizienz und Wettbewerbsfähigkeit eines Unternehmens beeinträchtigen.

Als Lösung für diese Probleme favorisiere ich ...

... einen ganzheitlichen Ansatz, der Investitionen in Cybersicherheitsmaßnahmen, die Bereitstellung der erforderlichen Ressourcen und die Schulung der Mitarbeiter in neuen Technologien umfasst. Priorisierung ist wichtig, um knappen Mitteln zu begegnen, und sollte eben Cybersicherheit nicht außen vorlassen. Die Zusammenarbeit mit externen IT-Anbietern kann dazu beitragen, Lücken in Bezug auf Fachwissen und Ressourcen zu schließen. Zu guter Letzt ist es für mittelständische Unternehmen wichtig, einen zukunftsorientierten Ansatz zu verfolgen, der Innovation und Digitale Transformation in den Mittelpunkt stellt.

Handlungsbedarf auf IT-Seite im Mittelstand sehe ich ...

... wenn es darum geht, dem Thema „Cybersicherheit“ einen höheren Stellenwert einzuräumen. Mit der zunehmenden Menge an Daten, die digital verarbeitet und gespeichert werden, steigt für Unternehmen jeder Größe das Risiko von Cyberangriffen. KMU fehlen oft die Ressourcen, um sich effektiv vor diesen Bedrohungen zu schützen. Deswegen gibt es einen wachsenden Bedarf an IT-Spezialisten, die auf die speziellen Bedürfnisse zugeschnittene Cybersicherheitslösungen anbieten können. Indem wir diese Herausforderungen angehen, können wir dazu beitragen, den langfristigen Erfolg und das Wachstum dieser Unternehmen sicherzustellen.

Persönliche Daten

NAME: Christopher Lohmann
ALTER: 54 Jahre
FAMILIENSTAND: ledig
GRÖSSTES HOBBY: Langstreckenlauf

Karriere

AUSBILDUNG: Diplom-Kaufmann der Universität Würzburg, Dr. rer. pol. der Universität Freiburg
BERUFLICHER WERDEGANG: mehr als 20 Jahre Erfahrung in leitenden Management- und Vorstandspositionen in der Versicherungsbranche
DERZEITIGE POSITION: Gründer von The Mulberry Ventures, Mitglied im Board von Eye Security, HR Pioneers und Neodigital

ZP SÜD

HR HAUTNAH ERLEBEN

Am 9. und 10. Mai 2023 trifft sich die HR-Community auf der ZP Süd in Stuttgart. Fokus der Veranstaltung sind die Trends der Arbeitswelt von heute und morgen. Für alle relevanten Personalfragen zeigt die Fachmesse in Stuttgart Produktinnovationen und Entwicklungen auf. Eperten aus der Praxis sprechen in Vorträgen über die aktuellen Fragen aus der Welt der Arbeit in allen relevanten Themenbereichen: Recruiting & Attraction, Operations & Services, Learning & Development, Corporate Health und Future of Work. Neu in Stuttgart sind im Jahr 2023 die Kamin-Lounge, wo HR-Experten in intimer Atmosphäre über ihre Erfahrungen sprechen und sich mit der Community austauschen können, und die Business-Bar, wo sich Interessenten zum Networking mit anderen HR-Experten treffen können. Dazu kommt Corporate Health im Fokus: Nachdem die Corporate Health Convention in den vergangenen Jahren parallel zur ZP Süd lief, laufen 2023 beide Veranstaltungen unter der Marke „Zukunft Personal“, ohne dass der Fokus der Veranstaltung verloren gehen soll.

www.zukunft-personal.de

FACHKONGRESS IN KARLSRUHE

DIE ZUKUNFT DES BILDUNGSMARKTS

AUF DER LEARNTEC PRÄSENTIEREN VOM 23. BIS ZUM 25. MAI 2023 IN KARLSRUHE NATIONALE UND INTERNATIONALE AUSSTELLER DIE NEUESTEN TECHNOLOGIEN ZUM DIGITALEN LERNEN UND ARBEITEN.

Der Fachkongress in Karlsruhe *hält spannende Keynotes und Schwerpunktthemen für die Besucher bereit.*

Der begleitende Fachkongress bietet einen Blick in die Zukunft des digitalen Bildungsmarkts und verknüpft diese mit dem Ausstellerangebot auf der Fachmesse. Schwerpunktthemen sind in diesem Jahr u.a. das Metaverse, Learning Ecosystems, New und Agile Learning, Lernen mit Künstlicher Intelligenz (KI) und adaptives Lernen.

Herzstück des Kongresses sind die hochkarätigen Keynotes. Mit dabei: Prof. Dr. Jörg Desel, Mitglied im Präsidium der Gesellschaft für Informatik, zum Thema „In 30 Jahren vom E-Learning zur Digitalisierung der Bildung“ und die niederländische Hi-Tech Fashion Designerin und Innovatorin Anouk Wipprecht. Getreu dem Motto „Lernen geht unter die Haut“ fragt sie, wie die Entwicklung elektronischer Kleidung beim Lernen und Leben helfen kann. Der US-amerikanische Bildungsexperte Elliot Masie diskutiert im interaktiven Austausch das Zukunftsthema Open AI. Außerdem widmet sich Prof. Dr. Rafaela Kraus, Vizepräsidentin für Entrepreneurship der Universität der Bundeswehr, mit ihrer Keynote dem Thema KI in der Bildung.

www.learntec.de

E-LÖSUNGEN

VON DIGITALISIERUNG BIS METAVERSE

AUF DEN BME-E-LÖSUNGSTAGEN AM 23. UND 24. MAI 2023 IN DÜSSELDORF ERHALTEN BESUCHER EINEN KOMPAKTEN MARKTÜBERBLICK ÜBER INNOVATIVE LÖSUNGSANSÄTZE FÜR IHRE BESCHAFFUNGSORGANISATION.

Die zunehmende Digitalisierung hat längst auch den Einkauf erfasst. Dabei geht es nicht allein um den Einsatz digitaler Tools und E-Lösungen, sondern vielmehr um eine umfassende Analyse und Optimierung der gesamten Einkaufsorganisation, um die richtigen Weichen für den Einkauf der Zukunft zu stellen. Auf der Veranstaltung für E-Sourcing und E-Procurement erwartet die Interessierten ein umfangreiches Fachprogramm mit Fachvorträgen, Workshops, Round Tables und Solution Foren sowie mehr als 80 Ausstellern und Partnern, die ihre neuesten Produkte demonstrieren. Themen-Highlights der E-Lösungstage 2023 sind u.a. „Das Metaverse – von der Vision zur gelebten Realität in der Industrie“, „Digitalisierungskonzepte richtig entwickeln – Roadmap, Implementierung, Umsetzung“, „Lieferkettengesetz: Sorgfaltspflichten und Risikomanagement umsetzen“ und „Automatisierung des Einkaufs: P2P-Prozesse effizient und transparent gestalten.“

www.bme.de/eloesungstage

KURZMELDUNGEN

UNTERNEHMEN

STRATEGISCHER ZAHLUNGSPARTNER

- Stripe wird den Großteil aller Zahlungstransaktionen von Free Now u.a. in Deutschland, Irland, Großbritannien, Frankreich, Spanien, Italien, Polen und Griechenland abwickeln.

ERFOLGREICHES GESCHÄFTSJAHR

- Der IT-Dienstleister Adesso hat ein erfolgreiches Geschäftsjahr absolviert. So ist ihm im Jubiläumsjahr eine Umsatzsteigerung um 33 Prozent auf 900,3 Mio. Euro gelungen.

BUCHTIPPS

Zusammengestellt von Alexander Lorber

Grundlagen der Künstlichen Intelligenz

Autor: Tom Taulli
Verlag: Springer
Seitenzahl: 211
UVP: 22,99 Euro

GOOGLE, AMAZON, FACEBOOK UND ÄHNLICHE TECH-GIGANTEN sind nicht die einzigen Unternehmen, auf die Künstliche Intelligenz (KI) eine bedeutende Auswirkung hat. KI berührt fast jeden Teil des Alltags und ist damit sowohl die Gegenwart als auch die Zukunft von Unternehmen und aller Privatleben. Über Technologien wie intelligente Lautsprecher und digitale Assistenten hinaus hat sich KI schnell zu einer Allzwecktechnologie entwickelt, die in Branchen wie dem Transportwesen, dem Gesundheitswesen, den Finanzdienstleistungen und vielen mehr Einzug gehalten hat. Das Buch von Tom Taulli vermittelt ein grundlegendes, zeitgemäßes Verständnis von KI und ihren Auswirkungen.

New Work Dystopia

Autor: Carsten C. Schermuly
Verlag: Haufe
Seitenzahl: 180
UVP: 29,99 Euro

SPÄTESTENS SEIT 2020 HAT DIE POPULARITÄT DES BEGRIFFS „NEW WORK“ sprunghaft zugenommen, steht aber zunehmend für Änderungen jeder Art in der Arbeitswelt. Dieses Buch greift das Scheitern von New Work in Form einer Dystopie auf und gibt ihm ein Gesicht. Dazu stellt der Autor das fiktive Unternehmen Kaltenburg als „bösen Bruder“ von Stärkande aus seinem vorherigen Werk „New Work Utopia“ vor, in dem alles schiefläuft, was bei New Work schiefl aufen kann. Das Empowerment der Mitarbeiter spielt keine große Rolle, stattdessen gilt als Maxime Kontrolle statt Vertrauen. Impulse und Konzepte des New Work werden vorgeschoben, um die Profitabilität auf Kosten der Belegschaft zu maximieren. Im zweiten Teil des Buchs erfolgt schließlich aber die Wende hin zum Positiven.

ChatGPT und LaMDA sind erst der Anfang

Autoren: Andreas Dripke, Tony Nguyen, Horst Walther
Verlag: DC Publishing
Seitenzahl: 179
UVP: 18,90 Euro

BÜCHER ÜBER DEN UMGANG MIT CHATGPT entstehen derzeit zuhauf. Das neue Werk „ChatGPT und LaMDA sind erst der Anfang: Wie Künstliche Intelligenz unser aller Leben verändert“ ist anders, weil es in die Zukunft blickt statt nur den Status quo zu beschreiben. Künstliche Intelligenz wird künftig alles verändern. Genauso grundlegend, wie der Personalcomputer, das Internet und das Smartphone unser Leben auf den Kopf gestellt haben. Von diesen Veränderungen werden keine Branche, kein Arbeitsplatz und kein Aspekt unseres Privatlebens verschont bleiben. Wir sind daher gut beraten, uns heute schon auf diese Veränderungen vorzubereiten.

Haltet den Datendieb!

Autor: Achim Barth
Verlag: Gabal
Seitenzahl: 224
UVP: 24,90 Euro

Was weiß Amazon über uns? Wie verdient Facebook sein Geld? Liest Google unsere Nachrichten? Die Themen „Datenschutz“ und „digitale Privatsphäre“ sind so brisant wie unterschätzt. Jeder, der an der modernen Welt teilnimmt, ist betroffen. Doch kaum jemand durchblickt die mafiösen Strukturen hinter den Kulissen des Cyberuniversums. In seinem Buch nimmt der Autor und Datenschutzexperte Achim Barth kein Blatt vor den Mund. Als digitaler Aufklärer folgt er seiner Mission: Datenschutz für jedermann, Licht in die schummerigen Ecken des Webs, Nutzer informieren und ein Bewusstsein für unsere Zeit, Zukunft und Freiheit schaffen. Denn die Internetfirmen ignorieren unsere digitale Privatsphäre und machen uns gläsern.

KURZMELDUNGEN

PRODUKTE

CLOUD-BASIERTE TELEFONANLAGE

Mit „Procall Voice Services“ als Erweiterung zum Kernprodukt „Procall Enterprise“ bietet Estos ein Komplettangebot für kleine und mittelständische Unternehmen.

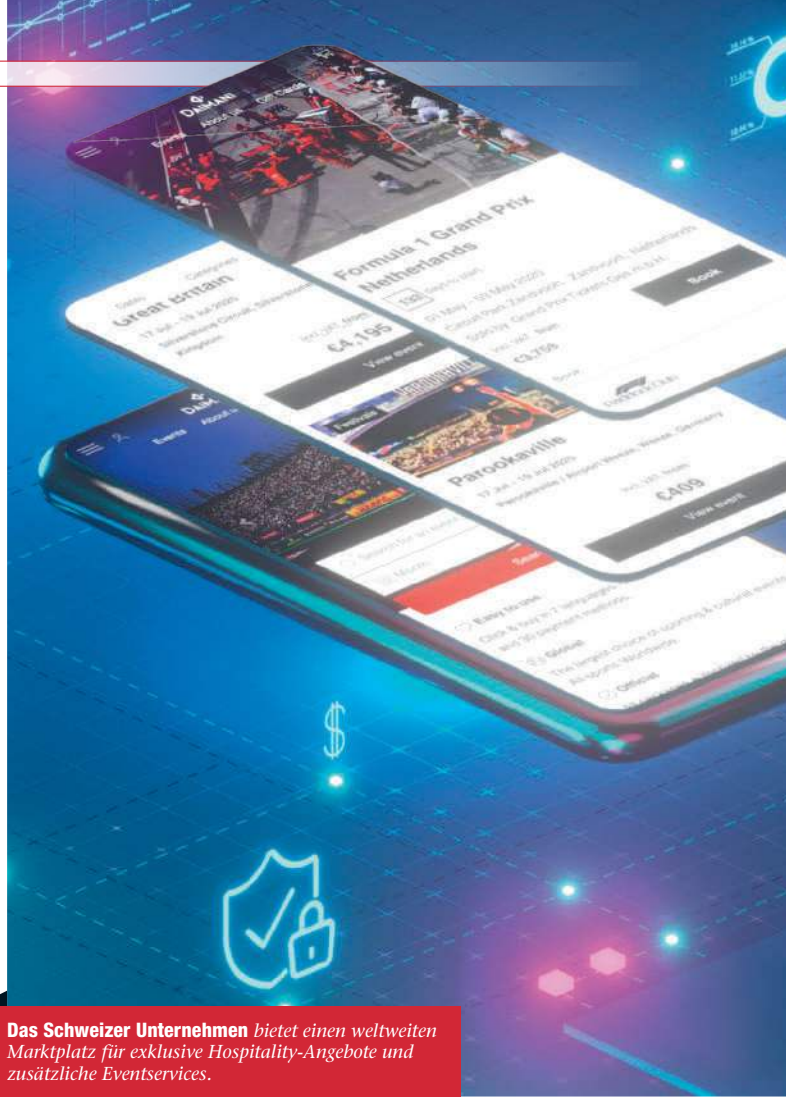
NEUE KOMMUNIKATIONSLÖSUNG

Ringcentral, Anbieter u.a. von KI-gestützten Cloud-Kommunikationslösungen, hat eine neue Kommunikationslösung für Frontline-Mitarbeiter gelaunchet.

CLOUD-LÖSUNG

PASSENDE EVENT-PAKETE FÜR VIPS

Dank einer internationalen Buchungsplattform in der Cloud kann Daimani bis zu 70.000 Tickets für mehrere 1.000 Events gleichzeitig verwalten.



Das Schweizer Unternehmen *bietet einen weltweiten Marktplatz für exklusive Hospitality-Angebote und zusätzliche Eventservices.*

Sie möchten im Mai zu Elton John nach Manchester reisen oder im Juni zum DFB-Pokalfinale nach Berlin? Dann aber schnell an den Laptop, Hospitality-Tickets ergattern, Airlines und Züge vergleichen und ein Hotelzimmer reservieren! Bis alles für die entsprechende Reise gebucht ist, sind wahrscheinlich Stunden oder mehrere Tage vergangen. Gerade für VIP-Gäste, die es gerne möglichst komfortabel haben, kann das abschreckend sein. Dabei bietet sich ein Eventbesuch gut für einen internationalen Kurztrip mit diversen Annehmlichkeiten an. Dazu gehören eigene Sitzbereiche, der optimale Blickwinkel aufs Geschehen und kulinarische Appetithäppchen – aber eben kein holpriger Start im Internet. Doch auf eine Lösung, mit der sie weniger aufwendig ans Ziel kommen, mussten VIP-Kunden lange verzichten. Denn auch wenn Veranstaltungen, Unterkünfte und Reisen längst digital buchbar sind, gab es bislang keinen Dienst, der all diese Services bündelte.

Hier sah das Schweizer Unternehmen Daimani Potenzial für ein Geschäftsmodell. „Buche ich ein Event, möchte ich doch auch im Vorfeld schon in Urlaubsstimmung kommen. Deshalb wollten wir unseren Kunden einen neuen, vernetzen Service anbieten, der den Buchungsprozess deutlich vereinfacht“, erklärt CEO und Co-Gründer Max Müller. „Die meisten Veranstalter verkaufen VIP-Angebote noch analog, etwa per Telefon. Eine digitale Evolution in der Eventbranche gab es lange nicht. Deshalb nutzen wir heute neue technische Möglichkeiten – zum wesentlichen Vorteil der Kunden.“ Mittlerweile verkauft das Unternehmen seit 2018 online VIP-Tickets, vor allem für Sport- und Musikveranstaltungen, aber auch andere Kulturevents wie Comedy-Auftritte.

Immense Datenmengen zusammengebracht

Doch wie kann ein Unternehmen mit geringer Zahl an Mitarbeitern die Digitalisierung im Veranstaltungsbereich vorantreiben? Müller erzählt, dass Daimani eine SAP-Cloud-Lösung einführte, mit der das Unternehmen seine Vision skalierbar umsetzen kann: „Es gibt eine enorme Auswahl an Hotels und Anreisewegen – außerdem können Kunden zahlreiche Webportale zum Vergleich heranziehen. Das überfordert schnell“, so der Geschäftsführer.

Die Cloud bringt diese immense Datenmenge zusammen und erstellt in wenigen Momenten passende Angebotspakete. Dabei berücksichtigt die Analyse individuelle Anforderungen wie die Preislage. Ob in der Schweiz, Großbritannien, Deutschland, den USA oder den Vereinigten Arabischen Emiraten: Das Cloud-System kann bis zu 70.000 Tickets für eine einzige Veranstaltung verwalten und gleichzeitig die Verfügbarkeit von Hotels und Flügen prüfen. Um dieses breite Angebot seinen internationalen Kunden datenschutzkonform und flexibel bereitzustellen, greift das Anwenderunternehmen auf Datenzentren in mehreren Ländern zurück. „Unser Ziel ist es, dass Kunden letztlich nur einen Kauf tätigen und nicht unterschiedliche Anbieter kontaktieren müssen. Dazu liefern ihnen unsere Mitarbeiter übersichtliche Eventpakete, erstellt in der Cloud“, betont Müller.

Daimani

Branche: Events
Gründung: 2018
Hauptsitz: Zürich, Schweiz
Mitarbeiter: rund 25

www.daimani.com

Sport- und Kulturevents *können ad hoc online gebucht werden.*

Servicegedanke wird großgeschrieben

Mithilfe der Cloud schafft es der Eventspezialist, den Anfragen der Kunden problemlos nachzukommen. Selbst große Firmen, die mit einem Team verreisen möchten, kann Daimani effizient bedienen. Dazu braucht es nicht in jedem der 20 Länder, in dem auch Veranstaltungen stattfinden, Mitarbeiter. Denn über die Datenplattform können die Beschäftigten auf Angebote in jedem Land zugreifen. Das Team arbeitet in sieben Büros verteilt auf Europa, Asien und Südamerika, in sieben Sprachen, mit mehr als 30 Bezahlmethoden und 70 Währungen. Dabei sind Ansprechpersonen jederzeit per Telefon, E-Mail oder Chat erreichbar. So kann sich das Team die Beratung je nach Zeitzone passend aufteilen und kurzfristig reagieren, wenn Fragen oder besondere Wünsche aufkommen.

Nach dem Kauf bleibt Daimani mit seinen Kunden in Kontakt und schickt ihnen etwa personalisierte Angebote als Inspiration für den nächsten Ausflug. Wenn das mal nicht gute Voraussetzungen für den aufkommenden Eventhunger nach rund drei Jahren Pandemie sind.

LUZIA LANGHANS

Max Müller
Alter: 46 Jahre
Ausbildung und Werdegang: Er war Project Director des offiziellen Hospitality-Programms der letzten drei FIFA-Fußball-Weltmeisterschaften mit Umsätzen von mehr als 1,25 Mrd. US-Dollar.
Derzeitige Position: Chief Executive Officer der Daimani & Fortius AG

KURZ UND KNAPP

In unserem Betrieb spielt die Informations- und Kommunikationstechnologie (ITK) ...
... die zentrale Rolle. Wir sind ein Sales- und Technologie-Unternehmen – ITK ist für uns quasi das „Rückgrat".

In unserer Branche muss IT-seitig in der Regel am meisten investiert werden in ...
... Datenharmonisierung und Infrastruktur, z.B. Bandbreite in Stadien etc.

Die notwendigen Mittel vorausgesetzt, würde ich sofort ...
... als Nächstes alle Ticketing- und Accommodation-Anbieter auf einer Plattform verbinden – wenn wir in Bezug auf das Geschäftswesen sprechen.

Von ITK-Anbietern für den Mittelstand erwarte ich ...
... schnelle Interaktionen und effiziente Lösungen. Wichtig sind auch persönliche Kontakte und nicht nur ein „namenloser" Support.

Optimaler Support zeichnet sich durch ...
... eine Kontinuität in den Mitarbeitern aus. Diese sollten Fragen nicht nur reaktiv beantworten, sondern auch aktiv beraten.

Umbau zum datengetriebenen Industrieunternehmen

AGIL UND FLEXIBEL ZUM

HIDDEN CHAMPION

Die Leistritz AG ist Vorreiter gleich in mehreren innovativen Technologiefeldern. Aktuell lagert der Mittelständler aus Nürnberg einen Teil seiner IT-Systeme in das Rechenzentrum der Noris Network AG aus – und legt damit erfolgreich die Basis für innovationsgetriebenes Wachstum.

Das Ziel des Projekts: die Kontrolle über die IT behalten, aber gleichzeitig flexibel bleiben – und das Kundenbedürfnis nach zertifizierten Datensicherheitsstandards erfüllen. Im Interview mit IT-MITTELSTAND erläutern Vorstand Michael Everts und IT-Leiter Thomas Weinberger, warum sie sich für das Outsourcing entschieden haben, weshalb Agilität für sie ganz entscheidend ist und welche Rolle das Thema „Nachhaltigkeit“ in ihrem Unternehmen spielt.

ITM: *Herr Everts, in welchem Markt bewegen Sie sich, was produzieren Sie und was hebt Ihre Produkte am Markt ab?*

MICHAEL EVERTS: Wir sind ein mittelständisches Unternehmen mit vier sehr unterschiedlichen Business-Units. Allen gemeinsam ist jedoch, dass wir uns durch Produktinnovation und Prozessinnovation abheben und in allen vier Geschäftsbereichen und Märkten als Hidden Champion aufgestellt sind. Da ist zum einen die Turbinentechnik mit Komponenten für den Aerospace-Bereich. Wir liefern Technologie, die in den neuesten und modernsten Triebwerken zum Einsatz kommt, die derzeit auf dem Markt sind. Wir stellen auch Pumpentechnik für den Hygiene- oder Kraftstoffbereich her, etwa für die Batteriekühlung in der E-Mobilität. Sie sorgen für mehr Reichweite bei niedrigerem CO_2-Ausstoß und kürzeren Ladezeiten.

DIE LEISTRITZ AG ...

[→ ... ist **Spezialist für High-Tech-Lösungen** in der Turbinen-, Pumpen-, Extrusions- und Produktionstechnik. Die Produkte des Unternehmens stecken in vielen Dingen des täglichen Lebens: in Flugzeugen, Fahrzeugen und Fußböden, in Maschinen und Medizintechnik, in Lebensmitteln sowie Recycling-Verpackungen. Der Hauptsitz ist in Nürnberg, wo das Unternehmen um 1905 gegründet wurde. 1.800 Mitarbeiter in vier unabhängigen Geschäftseinheiten und an 13 Standorten versorgen 21 Industrien rund um die Welt. ←]

www.leistritz.com

MICHAEL
EVERTS

Alter: 51 Jahre
Familienstand: verheiratet, zwei Kinder
Werdegang: Studium der Betriebswirtschaftslehre, seit 2019 Vorstand bei Leistritz
Derzeitige Position: Vorstand, Vorstandssprecher, CFO

THOMAS
WEINBERGER

Alter: 47 Jahre
Familienstand: verheiratet, zwei Kinder
Werdegang: Studium der Informatik und internationaler MBA, seit 2003 bei Leistritz, seit 2016 Leiter IT
Derzeitige Position: Leiter IT

ITM: *Das waren zwei Bereiche, was stellen Sie noch her?*
EVERTS: Der dritte Bereich ist die Extrusions-Technologie. Mit unseren Maschinen werden z.B. aus geschredderten PET-Flaschen neue Produkte oder im Pharmabereich in fortlaufenden Prozessen aus Rezepturen neue Grundstoffe hergestellt. Die Autoindustrie nutzt ebenfalls unser Kunststoff-Compounding. Auch proteinreiches Plant-Based Food, das einen Beitrag zur CO_2-Reduktion leistet, wird mit unseren Extrudern produziert. So arbeiten wir beispielsweise mit dem Staat Singapur zusammen: Der Stadtstaat hat das Ziel, bis 2030 rund 30 Prozent seiner Lebensmittel selbst herzustellen. Darüber hinaus stellen wir Produktionstechnologie in Form von Werkzeugen für die Schienen her, wie Wirbelmaschinen für elektrische Lenkungen sowie Spezial- und Sonderwerkzeuge.

ITM: *Welche Herausforderungen beschäftigen Sie derzeit besonders?*
EVERTS: Wir sind ein sehr stark wachsendes, innovationsgetriebenes Unternehmen mit 13 Standorten auf drei Kontinenten, das sich seit gut drei Jahren in einem intensiven Wandel der Digitalen Transformation zu einem neuen, modernen Industrieunternehmen befindet. Agile Arbeitsmethoden sind für uns eine wichtige Basis, um Wachstum zu gestalten.

ITM: *Welchen Stellenwert hat die IT in Ihrem Unternehmen?*
EVERTS: Die IT hat aus meiner Sicht eine sehr wichtige Rolle als Enabler für alle Prozesse und ein gesundes, ertragreiches Wachstum. Die Datenqualität und -integrität sind dafür ebenso entscheidend wie ein durchgängiges IT-System. Unsere IT-Strategie ist deshalb zentral einheitlich aufgestellt, es gibt aber auch dezentrale Dependancen. Wir geben im Schnitt jährlich zwischen 1 und 2 Prozent des Umsatzes für das IT-Budget aus.

ITM: *Herr Weinberger, wie viele Mitarbeiter mit IT-Bezug gibt es im Unternehmen?*
THOMAS WEINBERGER: International sind es ungefähr 30 Mitarbeiter, 19 davon in Deutschland. Wir setzen auch angesichts des Fachkräftemangels darauf, selbst auszubilden. Aufgrund der Spezifika in unseren Prozessen und Anwendungen ist die Ausbildung von Menschen, die sich mit unseren Systemen auskennen und identifizieren, für uns aber auch grundsätzlich sehr sinnvoll.

ITM: *Wie ist Ihre IT-Landschaft aufgestellt? Welche Systeme nutzen Sie?*
WEINBERGER: Wir versuchen, soweit wie möglich mit IT-Standardprodukten zur Lösung zu kommen. Wir möchten konsequent alle vier Business-Units mit den gleichen Systemen zum Ziel bringen. Aktuell sind wir dabei, die heute noch fragmentierte Landschaft mit sechs Enterprise-Resource-Planning-Systemen (ERP) weltweit in einem System zusammenzuführen. Wir setzen ein Customer-Relationship-Management-System (CRM) ein, unsere Computer-Aided-Design-Welt (CAD) ist mit einem Product-Lifecycle-Management-System (PLM) verbunden. Das nutzen wir insbesondere dort, wo wir eigene Maschinen konstruieren. Ein Manufacturing-Execution-System (MES) ist in der nächsten Ausbaustufe mit dem neuen ERP-System geplant.

ITM: *Spielt die Cloud jetzt oder perspektivisch eine Rolle?*
WEINBERGER: Dort, wo die Abwägung zwischen Know-how-Schutz und Mehrwert ein gutes Ergebnis ergibt, nutzen wir Cloud-Lösungen – beispielsweise im Office-Umfeld. Wir setzen allerdings definitiv nicht auf Cloud First und wollen auch nicht alle Daten von On-Premises in die Cloud schieben. Ein wichtiger Grund dafür sind Restriktionen und die hohen Anforderungen an Datenintegrität, die in mehreren Bereichen von unseren Kunden vorgegeben werden. Wir haben uns bewusst entschieden, mit Unterstützung von externen Partnern essentielle Systeme bevorzugt im Private-Cloud-Ansatz selbst zu betreiben.

ITM: *Warum haben Sie sich für die Zusammenarbeit mit einem externen Rechenzentrumsanbieter entschieden?*
WEINBERGER: Treiber war unsere Strategie der Flexibilisierung. Wir wollten die Systeme nicht mehr ausschließlich im eigenen Rechenzentrum (RZ) mit unseren Mitarbeitern betreiben wie bisher, sondern uns die Unterstützung externer Partner ins Haus holen, um so IT-Lösungen 24/7 anbieten zu können. Kundenseitig wachsen zudem die Anforderungen an Standards und Zertifizierungen, die wir bei unseren Systemen beachten müssen. Eine eigene Zertifizierung wäre ein erheblicher Aufwand hinsichtlich Zeit, Ressourcen und Kosten, etwa bei Themen wie Anbindung, Brandschutz, Klimatisierung, Stromversorgung und physische IT-Sicherheit. Da stellt sich die Frage, ob man das in-house abbilden will oder im Rahmen einer vertrauensvollen Zusammenarbeit von spezialisierten Partnern einkauft. Dafür haben wir uns entschieden.

ITM: *Wo haben sich die Anforderungen durch Ihre Kunden in den letzten Jahren verändert?*
EVERTS: Gerade die Anforderungen der Kunden im Militärbereich sind immer detaillierter geworden, der Zertifizierungsbedarf ist mit Blick auf die interne Datenspeicherung gestiegen. Das war für uns einer der Gründe, auf Noris Network als Partner zu setzen, der das Thema „Datacenter“ als Kerngeschäft ganz anders beherrschen kann und alle wichtigen Zertifizierungen mitbringt.

ITM: *Wann und wie wurde die Entscheidung getroffen?*
WEINBERGER: Die Entscheidung haben wir im letzten Jahr getroffen, um eine Grundlage für weiteres Wachstum zu schaffen. Im Auswahlprozess wurden mehrere Anbieter anhand eines Kriterienkatalogs geprüft, die endgültige Wahl fiel dann auf Noris Network und deren RZ in Nürnberg. Wichtig waren für uns die Spezialisierung, die Größe des Anbieters, ebenso Regionalität und die positiven Erfahrungswerte aus der bisherigen Zusammenarbeit. Besonders entscheidend war für uns auch die Anbindung an die wichtigen Knotenpunkte im internationalen Netz, da wir unser neues und globales ERP-System zentral betreiben wollen.

> **„Wir sind ein sehr stark wachsendes, innovationsgetriebenes Unternehmen. Agile Arbeitsmethoden sind für uns eine wichtige Basis, um Wachstum zu gestalten.“**
> *Michael Everts*

ITM: *Wie lange dauerte es von der Idee bis zur Umsetzung? Wie gut hat das Projekt geklappt?*
EVERTS: Der Umzug läuft derzeit noch, weil sich der Zeitplan durch die deutlich längeren Lieferzeiten bei Komponenten wie Halbleitern verlängert hat. Da wir den Umzug gleichzeitig mit einer Modernisierung verbinden, hat die Beschaffung Priorität. Dennoch sind wir mit dem Projekt zufrieden. Der Entscheidungsprozess selbst ist bei uns sehr schlank, denn die IT ist direkt dem Vorstand unterstellt: Von der Idee bis zur Entscheidung sind gerade mal drei Wochen vergangen.

ITM: *Welche Verbesserungen wollten Sie mit der RZ-Auslagerung erreichen?*
WEINBERGER: Im Wesentlichen ging es um das Thema „Verfügbarkeit der Systeme“. Wir haben bei uns keine 24/7-Betreuung, das ist beim RZ-Anbieter mit dem Hinzubuchen von Managed Services nun anders. Jetzt erreichen wir mit einer Colocation-Lösung gemäß Service Level eine Verfügbarkeit von annähernd 100 Prozent. Dabei hat der Anbieter physikalischen Zugang zu unseren Servern. Zwei Racks stehen in unterschiedlichen Brandabschnitten, um Redundanz zu gewährleisten. Wir haben eine redundante, kreuzungsfreie High-Speed-Standortanbindung über Glasfaser ins RZ Nürnberg. Die Beschaffung ist offen, d.h. entweder der Dienstleister oder wir beschaffen die Komponenten und nehmen sie im angemieteten Bereich in Betrieb. Einige wenige Server betreiben wir noch in-house.

ITM: *Welche Rolle spielt die Hochverfügbarkeit der IT für Ihr Unternehmen?*
EVERTS: Das ist auch perspektivisch ein wichtiges Thema. Der Anbieter hat uns versichert, dass bei einem Blackout Notstromkapazitäten vorhanden sind, um den Serverbetrieb für zwei Wochen aufrechtzuerhalten. Das war eine wichtige Hintergrundinformation für uns.

ITM: *Wie passt die Entscheidung, die IT zu einem externen Anbieter auszulagern, in Ihre gesamte IT-Strategie?*
WEINBERGER: Wir haben praktisch unseren Serverraum in das RZ des Dienstleisters verlängert. So können wir jetzt auch Dienste in gleicher Qualität wie On-Premises, allerdings mit deutlich mehr Flexibilität, hinzubuchen. Zudem haben wir die Flexibilität, für einzelne Systeme leichter Dienstleister an Bord zu nehmen, die im RZ Zutritt haben und unsere Systeme so betreiben, als wären sie direkt bei uns im Haus. In der Produktion würde man es als ›

verlängerte Werkbank bezeichnen. Zuvor hatten wir nur eine Internetanbindung, die nicht für die Übertragung großer Datenmengen oder das Betreiben von hochperformanten Systemen designt war. In der IT ist mehr Raum entstanden, um Systeme und Prozesse intensiver zu betreuen. Zukünftig können wir uns statt auf den Betrieb stärker auf die Leistritz-spezifischen Anwendungsfälle und Prozesse konzentrieren.

EVERTS: Wir sehen den Umzug als Investition in die Zukunft und zugleich als sinnvollen Weg, bei dem wir einerseits die Verantwortung für unsere Systeme nicht aus der Hand geben, aber gleichzeitig mit einem professionellen Partner an unserer Seite für die steigenden Anforderungen gerüstet sind.

> **„Wir setzen auch angesichts des Fachkräftemangels darauf, selbst auszubilden. Aufgrund der Spezifika in unseren Prozessen und Anwendungen ist die Ausbildung von Menschen, die sich mit unseren Systemen auskennen und identifizieren, für uns aber auch grundsätzlich sehr sinnvoll.“**
>
> *Thomas Weinberger*

ITM: *Welche Aspekte waren Ihnen an einem Outsourcing-Partner besonders wichtig? Inwieweit gehört Innovationsfähigkeit dazu?*
WEINBERGER: Ganz wesentlich waren für uns die Verfügbarkeit von Ressourcen, die Größe und vergleichbare Referenzen: Dass wir nicht der erste Kunde und bei weitem nicht der größte sind, war ausschlaggebend. Uns ging es vor allem auch darum, dass der Anbieter das Outsourcing nicht nur als ein Produkt unter vielen sieht, sondern als Kernaufgabe, in die massiv investiert wird. Wir haben in der Evaluierungsphase gesehen, dass Wissen und professionelle Prozesse dahinterstehen, die einige andere Anbieter so nicht darstellen konnten. Die Innovationsfähigkeit war übrigens eines der Kriterien, die der Vorstand für die Anbieterauswahl vorgegeben hat.

ITM: *Welche Einsparungen oder Entlastungen konnten Sie durch die Auslagerung des Rechenzentrums erzielen?*
EVERTS: Ich würde eher sagen, dass wir bei Kostengleichheit eine deutlich erhöhte Flexibilität, Skalierbarkeit, Professionalität und Innovationsfähigkeit erreicht haben. Wir müssten intern deutlich mehr Know-how vorhalten, um ein ähnliches Niveau zu erreichen. Auch in puncto Cybersicherheit bietet unser RZ-Dienstleister eine wichtige Unterstützung.

ITM: *Würden Sie sagen, dass die Daten aus Ihren Produkten im Sinne von Internet of Things (IoT) und Datenanalytik wichtiger geworden sind? Gibt es bereits digitale Services und Geschäftsmodelle oder sind diese künftig angedacht?*
WEINBERGER: Wir haben bereits Digital Services eingeführt, darunter die Fernwartung. Wir stellen auch Messwerte zum Status der Produkte und Maschinen zur Verfügung, um sie in den optimalen Leitplanken zu betreiben und für eine besser planbare Maintenance. Allerdings sind wir da z.B. im Bereich der Pumpen eher die Treiber, als dass es schon von den Kunden gefordert wird. Dennoch: Es ist ein starker Trend, dass die Kunden in allen Bereichen Mehrwerte erhalten.

ITM: *Wie wichtig sind Themen wie Industrial IoT perspektivisch für Ihr Unternehmen?*

EVERTS: Der Markt ist stark im Wandel. Einige Kunden, die in ihrer Digitalisierung schon weiter sind, erwarten entsprechend mehr. Dabei kommt es ihnen vor allem auf eine hohe Datensicherheit und Recovery-Pläne an. Die Bedeutung datenbasierter Services wird jedoch aus unserer Sicht exponentiell wachsen. Virtuelle Inbetriebnahme, Predictive Maintenance und virtueller Support sind erst der Anfang. Allerdings gilt auch, dass unsere Produkte überall auf der Welt eingesetzt werden und die Verfügbarkeit von Wlan oder Mobilnetzen nicht überall gegeben ist. Da müssen die Kunden dort abgeholt werden, wo sie mit ihren individuellen Voraussetzungen stehen.

ITM: *Setzen Sie sich bereits mit Technologien wie Machine Learning (ML) oder Künstliche Intelligenz (KI) auseinander?*
EVERTS: Wir machen uns Gedanken über die Nutzungsmöglichkeiten. Beispielsweise ermitteln wir bereits aus unserer Business Intelligence (BI), inwieweit sich relevante Trends herauskristallisieren. Gerade wurde in Nürnberg eine neue Universität gegründet – mit dem ersten Lehrstuhl für KI praktisch gegenüber. Hier wollen wir mit der Forschung zusammenarbeiten.

ITM: *Wie wichtig sind Agilität und Flexibilität heute für Ihr Unternehmen? Wie zeigt sich das in Prozessen, Projektmethoden und IT-Systemen?*
EVERTS: Agilität ist elementar wichtig, ganz einfach, weil die Geschwindigkeit zunimmt, mit der wir reagieren müssen. In der Corona-Krise haben wir einen starken Wandel gelebt. In dieser Zeit ist die größte Anzahl von Neuprodukten entstanden, die wir bisher – einschließlich des Zertifizierungsaufwands – auf den Markt gebracht haben. Das war nur mit agilem Projektmanagement zu schaffen. Mit traditionellen Methoden wäre das schlicht nicht möglich.

ITM: *Dann sind Ansätze wie Scrum oder DevOps relevant für Ihr Unternehmen?*
EVERTS: Wir setzen uns vor allem sehr stark mit der Scrum-Methodologie auseinander. Ich habe selbst eine Ausbildung zum Scrum Master gemacht, um besser zu verstehen und nachzuvollziehen, wie uns agile Methoden ans Ziel führen können.

> **„Die IT hat aus meiner Sicht eine sehr wichtige Rolle als Enabler für alle Prozesse und ein gesundes, ertragreiches Wachstum. Die Datenqualität und -integrität sind dafür ebenso entscheidend wie ein durchgängiges IT-System.“**
>
> *Michael Everts*

ITM: *Welche Herausforderungen ergeben sich durch den zunehmenden Druck auf Lieferketten? Hat Ihr Unternehmen daraus Konsequenzen gezogen?*
EVERTS: Wir sind sicherlich heute ebenfalls von den größeren Herausforderungen in der Lieferkette betroffen. Allerdings konnten wir das gut abfedern, weil wir unsere partnerschaftlichen Beziehungen meist in Multisource-Ansätzen auslegen. Wir konnten unsere Umsatzziele übertreffen, auch wenn es hin und wieder eine Verschiebung um ein, zwei Wochen gab. Wir hatten allerdings keine Ausfälle, gerade weil wir so eng mit den Lieferanten zusammenarbeiten. Das gilt auch IT-seitig, da wir einen kontinuierlichen Datenaustausch über EDI und unsere Kundenplattform pflegen. ›

ITM: *Welchen Stellenwert hat die Zusammenarbeit mit den Fachbereichen? Wie setzen Sie neue Anforderungen IT-seitig um?*
WEINBERGER: Wir legen als IT spezifisch den Fokus darauf, die Fachabteilungen in ihrer Zusammenarbeit mit dem Kunden und im Sinne des Kunden zu unterstützen. Ein Beispiel: Oft gehen mehr Abrufe in digitaler Form ein, die zuvor manuell eingetragen wurden. Dann setzen wir Lösungen um, die wiederkehrende Aufgaben automatisieren, damit der Fachbereich intern schneller handlungsfähig ist. Aber wir arbeiten auch eng mit den Ingenieuren in den Fachabteilungen zusammen, die mit der Digitalisierung unserer Produkte befasst sind und die Expertise rund um das Maschinen-Engineering einbringen. Nur so entstehen gute, praxisnahe Lösungen. Denn klar ist: Digitalisierte Produkte sind sinnvoll für die Kunden.

> **„Die Bedeutung datenbasierter Services wird aus unserer Sicht exponentiell wachsen. Virtuelle Inbetriebnahme, Predictive Maintenance und virtueller Support sind erst der Anfang."**
> *Michael Everts*

ITM: *Welchen Beitrag leisten Ihre Technologien zu mehr Nachhaltigkeit?*
EVERTS: Praktisch alle Produkte zahlen bei unseren Kunden auf die Nachhaltigkeit ein – ob bei der Triebwerkstechnologie oder den Pumpen, die einen um 30 Prozent höheren Wirkungsgrad mit einem erheblich geringerem Energieverbrauch haben. Im Bereich „Sondermaschinen" setzen wir keine traditionellen Kühlschmiermittel ein, sondern arbeiten mit trockener Zerspanung, sodass kein schwer zu entsorgender Schlamm entsteht. Im Recycling-Bereich leisten wir mit Maschinen, die von „Flake to Bottle" recyceltes Kunststoffgranulat in neue Produkte verwandeln, einen ganz direkten Beitrag.

ITM: *Wie aufwendig ist es, im eigenen Unternehmen Nachhaltigkeit voranzutreiben und zu priorisieren, gerade für kleine und mittlere Unternehmen (KMU)?*
EVERTS: Das fällt gleichermaßen leicht als auch schwer. Leicht, weil wir schnellen Zugang zu den Mitarbeitern haben und jeder das Thema „Nachhaltigkeit" für sich verstanden hat. Schwierig ist es für Mittelständler hingegen, die Ressourcen wie Arbeitszeit und finanzielle Mittel für das Thema zur Verfügung zu stellen. Da weiß ich aufgrund meiner früheren Tätigkeit in einem großen, innovativen Konzern, wie Großunternehmen ganze Abteilungen dafür bereitstellen und vieles experimentell erproben. Bei KMU muss es sich immer auch schnell wirtschaftlich rechnen – das ist der wesentliche Unterschied.

ITM: *Wie wichtig ist Ihnen Nachhaltigkeit – auch mit Blick auf die Versorgungssicherheit?*
EVERTS: Für uns hat das Thema einen sehr hohen Stellenwert, das zeigt sich nicht nur in unseren Produkten. Wir kaufen zu 100 Prozent grünen Strom und dort, wo wir es benötigen, grünes Gas. Alle Dächer, die wir derzeit in unserer Infrastruktursanierung überholen, werden für Solarenergie vorbereitet. Die meisten sind bereits fertig und werden mit Photovoltaik ausgestattet.

ITM: *Wie haben Sie Ihre IT auf den Nachhaltigkeitsfokus ausgerichtet? Spielt möglichst hohe Nachhaltigkeit im RZ-Betrieb eine Rolle? Was leistet der Outsourcing-Partner hier?*
WEINBERGER: Bei der Besichtigung haben uns die effizienten Kühlkonzepte positiv beeindruckt. Dass der Anbieter viel Aufwand in seine Planung gesteckt hat und es schafft, Energie effizient zu nutzen und selbst bei großen Flächen Warm- und Kaltbereiche trennt, war ein Pluspunkt. Gerade der neu gebaute Abschnitt, in dem unsere Systeme stehen, zeichnet sich durch gut durchdachte Lösungen aus.

ITM: *Wie schätzen Sie die Entwicklung angesichts der Klimaziele in den nächsten Jahren ein? Sehen Sie in Ihrem Markt bereits mehr Druck auf Ihre Kunden, sich nachhaltiger aufzustellen?*
EVERTS: Alle großen Kunden fragen danach. Sie wollen wissen, welchen CO_2-Fußabdruck unser Produkt in der Kette verursacht. Diesen Druck verspüren wir mehr und mehr und wir sind darauf vorbereitet.

ITM: *Welchen Beitrag kann – neben nachhaltigen Produkten – die Digitalisierung im Kontext der Kreislaufwirtschaft und beim Re- und Upcycling leisten?*
EVERTS: Die Bedeutung der Kreislaufwirtschaft wird stark zunehmen. Dabei spielt die Nutzung der Kundendaten aus dem Betrieb der Produkte eine wesentliche Rolle, um beispielsweise aktiv ein Refit oder Upcycling für Maschinen anzubieten, die wir in den vergangenen Jahren auf den Markt gebracht haben. Wir haben uns hier gemeinsam mit den Kunden über unser CRM-System eine gute Datentransparenz erarbeitet.

ITM: *Haben sich Compliance-Vorgaben verändert oder haben diese in den letzten Jahren in Ihrer Branche zugenommen? Wie setzen Sie Compliance IT-seitig um? Spielt das Outsourcing dabei eine Rolle?*
EVERTS: Das ganze Thema „Datensicherheit", ob im Bereich „personenbezogener Daten" mit der DSGVO oder seitens der Kunden in Branchen wie Luft- und Raumfahrt mit sehr starker Regulierung, hat massiv an Bedeutung gewonnen. Wir nehmen die Anforderungen, die unsere Kunden an uns stellen, sehr ernst. Dem Thema begegnen wir u.a. durch interne Prozesse und Ressourcen. So haben wir Mitarbeiter, die sich primär um Dokumentation und Prozesssicherheit kümmern, auch gestützt durch die IT-Systeme.

ITM: *Welche Ziele will Ihr Unternehmen mittel- und langfristig erreichen und welche Rolle spielt die IT bei Ihrer Strategie?*
EVERTS: Wir setzen weiterhin auf Innovation als Wachstumsmotor, und die IT ist der Enabler für profitables Wachstum. Die IT unterstützt uns einerseits bei den Innovationsprozessen selbst, andererseits auch durch qualifizierte, aussagekräftige Daten. Ohne das entsprechende Backbone wird es nicht funktionieren.

WEINBERGER: Wir arbeiten aktiv an der Beseitigung von Systembrüchen. Bisher haben unterschiedliche ERP-Systeme viele Herausforderungen gebracht, Daten manuell oder automatisch zu konsolidieren. Ziel ist eine zentrale Plattform in der Private Cloud als Grundlage für ein zentrales Datenmanagement, um Daten übergreifend nutzen zu können.

DANIELA HOFFMANN

SPECIAL

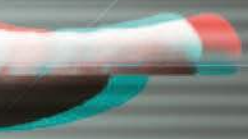
Die Bedrohung wächst

ZUGRIFF AUS DEM NETZ

Wie sicher sind Unternehmen in Deutschland? Eine Frage, die dieser Tage immer häufiger gestellt wird. Der Russland-Ukraine-Krieg und massive Hackerangriffe sorgen vielerorts für Unsicherheit. Es ist also an der Zeit, einen Blick auf mögliche Lösungen zu werfen.

Der deutschen Wirtschaft entsteht ein jährlicher Schaden von rund 203 Mrd. Euro durch Diebstahl von IT-Ausrüstung und Daten, Spionage und Sabotage.

Quelle: Bitkom



AUS DEM INHALT

Wie in vielen Fällen gibt es auch beim Thema „Cybersecurity" zwei Seiten der Medaille. Auf der einen Seite ist über die Medien zu hören, dass sich Hackerangriffe mehren, Ransomeware und Phishing-Mails nach wie vor ein massives Problem für Unternehmen sind und sich die Cyberbedrohungslage durch den Ukraine-Krieg deutlich verschärft hat – zumindest laut einer IT-Sicherheitsumfrage des Verbands der Internetwirtschaft Eco. 94 Prozent der befragten IT-Experten sind sich sicher, dass die Bedrohungslage wächst.

Auf der anderen Seite stehen die Unternehmen und ihre Cyberabwehr. Laut einer Bitdefender-Studie attestieren sich 61 Prozent der befragten Firmen weltweit eine verbesserte Cybersicherheit. Befragt wurden rund 1.700 überwiegend kleine und mittelständische Unternehmen – doch gerade diesen wird häufig nachgesagt, dass im Bereich der IT-Security noch nachgebessert werden muss. Vor allem das menschliche Fehlverhalten von Mitarbeitern scheint für viele Unternehmen – egal ob groß oder klein – die größte Sorge zu sein.

Wie genau also stehen Deutschlands Unternehmen wirklich da? „Die Unternehmen in Deutschland geben beim Thema ‚IT-Security' ein sehr heterogenes Bild ab. Das lässt sich auch nicht pauschal an Unternehmensgrößen oder Branchenzugehörigkeit knüpfen", sagt Helge Schroda, Business Lead Cybersecurity bei Microsoft Deutschland. Generell lasse sich jedoch festhalten, dass die erfolgreichen Cyberangriffe der jüngeren Vergangenheit und die teils begleitende Berichterstattung das Bewusstsein für die IT-Sicherheit in vielen Unternehmen deutlich geschärft habe.

Angespannte Bedrohungslage

Auch Fabian Glöser, Team Leader Sales Engineering bei Forcepoint, betont: „Die Unternehmen sind sich der angespannten Bedrohungslage bewusst. Wir stellen fest, dass das Thema ‚IT-Security' auf immer mehr Akzeptanz und Verständnis stößt, die Investitionen steigen entsprechend." Dennoch: Mit ihren oft noch klassischen IT-Sicherheitsarchitekturen seien deutsche Unternehmen nicht optimal gerüstet. ›

SPECIAL

Die Liste der größten Sicherheitssorgen führt laut Gisa Kimmerle, Head of Cyber bei Hiscox, nach wie vor der Einsatz von Ransomware an – „und wir gehen nicht davon aus, dass sich dies in naher Zukunft ändern wird“. Der Terminus „Cyberangriff“ klinge für manche nach einer kompliziert geplanten Attacke – dabei seien auch die breit gestreuten Phishing-Mails mit Schadsoftware nach wie vor lukrativ für Hacker.

Das „A und O“ der Cyberresilienz

Die Herausforderung „IT-Security“ hat also viele Facetten und muss auf mehreren Ebenen angegangen werden. Die IT-Expertin rät Unternehmen daher, ganz konkrete Schritte im Kampf gegen Angreifer zu gehen: „Die erste hilfreiche Maßnahme zur Prävention eines Cyberangriffs betrifft ein gut aufgestelltes Patch Management. Darüber hinaus sind Ransomware-sichere Backups das ‚A und O‘ beim Thema Cyberresilienz. Wir erleben in der Praxis immer wieder, dass diese Basiselemente der IT-Sicherheitsstrategie nicht erfüllt werden.“

Schroda rät zu fünf Maßnahmen, die dazu beitragen sollen, Systeme erfolgreich gegen einen Großteil aller Gefahren zu wappnen: „Zu der Basishygiene gehören neben der Multi-Faktor-Authentifizierung zeitnahe Updates zum Schließen von Sicherheitslücken, der Einsatz von XDR/SIEM-Lösungen, Netzwerksegmentierung und das regelmäßige Erstellen von Backups.“ Was es darüber hinaus jedoch brauche – und das gelte heute mehr als jemals zuvor –, sei der Aufbau einer ganzheitlichen Sicherheitsinfrastruktur. Eine zentrale Rolle für mögliche Lösungsansätze spielen seiner Ansicht nach moderne Endpoint-Systeme, sogenannte Extended-Detection-and-Response-Lösungen. „Diese sind der moderne Ersatz herkömmlicher Anti-Malware-Lösungen und können Angriffe entdecken, ohne dass die Sicherheitshersteller vorab diese intensiv analysiert und durch Signaturen aktualisiert haben“, erklärt er.

Für Fabian Glöser bietet ein Zero-Trust-Ansatz das höchste Schutzniveau. Dieser misstraue grundsätzlich allem und jedem und verlange, dass der komplette Datenverkehr geprüft wird und dass sich Nutzer, Geräte, Anwendungen und andere Einheiten bei jedem Zugriff auf Systeme oder Daten authentifizieren müssen. Zwei gute Beispiele für Zero-Trust-Lösungen seien Remote Browser Isolation sowie Content Disarm and Reconstruction. „Beide Lösungen gehen davon aus, dass grundsätzlich alle Inhalte aus dem Internet Schadsoftware enthalten, und misstrauen ihnen deshalb per se.“

Helge Schroda, Microsoft:

„Die IT-Landschaft eines Unternehmens führt in der Praxis mitunter ein Eigenleben.“

Schatten-IT und der Faktor „Mensch“

Zu einem Problem wird die Suche nach Sicherheitskonzepten und -lösungen, wenn Mitarbeiter sie – bewusst oder unbewusst – umgehen, um eigene Geräte, Tools und Services, die sie als benutzerfreundlicher, zielführender o.Ä. ansehen, zu nutzen. Unbemerkt von IT-Teams bildet sich so die sogenannte Schatten-IT – ein Phänomen, das vielen Firmen bekannt ist, gegen das teilweise aber nur wenig getan werden kann.

„Die IT-Landschaft eines Unternehmens führt in der Praxis mitunter ein Eigenleben“, fasst Helge Schroda das Problem zusammen. „Wir sehen in unserer Arbeit immer wieder IT-Lösungen, die nicht den jeweiligen Compliance-Vorgaben oder einem offiziellen Standard entsprechen – und wohl bisweilen auch extra darauf ausgelegt sind, sich der Compliance zu entziehen.“ Allerdings gebe es inzwischen gute Discovery-Lösungen, die IT-Abteilungen dabei helfen, solche versteckten Infrastrukturen zu entdecken, um der Schatten-IT wahlweise den Stecker zu ziehen oder um aus ihr „durch entsprechende Kontrollen und Maßnahmen Compliance-gerechte Lösungen zu machen, die Anforderungen der Anwender aufzunehmen und sicher umzusetzen“.

Um der Schatten-IT einen Schritt voraus zu sein, können zudem Schulungen und Fortbildungen helfen. Gerade weil der Faktor „Mensch“ oft das Zünglein an der Waage der IT-Security eines Unternehmens – egal ob groß oder klein – ist, müssen Mitarbeiter und Führungskräfte gleichermaßen ausreichend informiert und geschult sein. „Das kontinuierliche Training im Bereich der IT-Sicherheit sollte genauso selbstverständlich sein wie die regelmäßigen Brandschutzübungen“, betont Schroda und auch Fabian Glöser rät: „Die Schulungen müssen in ihrer Häufigkeit angemessen sein, dürfen von den Mitarbeitern aber auch nicht als Last empfunden werden. Sie sollten aber auf jeden Fall regelmäßig über aktuelle Bedrohungen und Gegenmaßnahmen aufgeklärt werden, um ihre Wachsamkeit hochzuhalten.“

Trainings für mehr Awareness

Auch für Gisa Kimmerle ist die Sensibilisierung von Mitarbeitern ein essenzieller Teil der IT-Sicherheitsstrategie. Sie verweist zudem auf den aktuellen Hiscox Cyber Readiness Report, aus dem hervorgeht, dass die Einfallstore für Cyberattacken in Deutschland in vielen Bereichen liegen, die mit Remote-Arbeit verknüpft sind, wie Remote-Zugriff auf das Unter-

Gisa Kimmerle, Hiscox:

„Ransomware-sichere Backups sind das ‚A und O‘ beim Thema Cyberresilienz.“

nehmensnetzwerk (VPN) mit 42 Prozent. 35 Prozent der Cyberangriffe entstanden über E-Mail-Kompromittierung, aber auch mobile Geräte aus dem Privatbesitz von Mitarbeitern führten in 33 Prozent zu Cyberschäden. „Jeder Mitarbeiter sollte professionell geschult werden. Regelmäßige Updates sind ideal, um das Bewusstsein aufrechtzuerhalten. Wir empfehlen mindestens jährliche, besser halbjährliche Awareness-Trainings“, hebt sie hervor.

Fabian Glöser, Forcepoint:

„Der bisherige Kampf der IT-Sicherheitsbranche gegen Cyberkriminalität gleicht mit seinem signaturbasierten Ansatz dem sprichwörtlichen Kampf gegen Windmühlen.“

Diverse Hürden und die Bedeutung von KI

Doch auch wenn Mitarbeiter künftig besser geschult werden, gibt es für Unternehmen noch einige Hürden zu meistern – denn die Bedrohungslage wird sich voraussichtlich in nächster Zeit nicht entspannen. „Wir müssen leider sogar vom Gegenteil ausgehen“, sagt Glöser. Der bisherige Kampf der IT-Sicherheitsbranche gegen Cyberkriminalität gleiche mit seinem signaturbasierten Ansatz dem sprichwörtlichen Kampf gegen Windmühlen. Da Sicherheitssysteme immer nur Bedrohungen entschärfen könnten, die sie schon kennen, hätten Cyberkriminelle einen entscheidenden Vorsprung. „Dieser aussichtslose Wettlauf wird durch die Übernahme des Zero-Trust-Prinzips über kurz oder lang beendet werden“, ist er sicher. Einen etwas anderen Blick in die Zukunft offeriert Helge Schroda. Er vermutet: „Die höhere Qualifikation der Mitarbeiter sorgt dafür, dass Angriffe zunächst weniger effektiv sind. Wir erleben also das sogenannte Angreiferdilemma: Die Kosten für Angriffe steigen so weit, dass sie sich zum Teil nicht mehr lohnen.“ Allerdings würden die Angreifer sich damit nicht langfristig zufriedengeben, sondern kreativ bleiben und neue Wege finden, um ihre Attacken mit einem geringeren Aufwand und größerem Erfolg dennoch durchführen zu können. Auf der anderen Seite gebe es das Zusammenspiel von Versicherern, die Cyberinsurance anbieten, und IT-Sicherheitsabteilungen, die das allgemeine Sicherheitsniveau verbessern. Darüber hinaus gewinne Künstliche Intelligenz eine immer größere Bedeutung. „Schon heute können unsere Anwendungen 97 Prozent der Routineaufgaben automatisiert ausführen und damit eine synchronisierte Verteidigung über alle Plattformen gewährleisten.“

Kimmerle sieht indes eine erhöhte Gefahr durch Insider-Täter: „Das heißt, wir gehen davon aus, dass, je mehr Menschen unter finanziellen Druck kommen, auch die Motivation steigt, Daten zu stehlen. Außerdem könnte die Unzufriedenheit der Mitarbeiter wegen stagnierender Löhne oder drohender Entlassungen zu Datenextraktion und -schmuggel führen.“

Ricarda Müller

Cybersicherheit

KEINE ANGST – HACKER BEISSEN NICHT

Im Kommentar erläutert Dr. Karsten Nohl, IT-Sicherheitsexperte und Gründer von Autobahn Security, warum es für Unternehmen höchste Zeit ist, den Mythos um Hacker aufzulösen.

In seiner Rolle als Hacking-Experte ist Karsten Nohl daran interessiert, Innovation und Sicherheit in Einklang zu bringen.

Auf der Kinoleinwand werden Hacker zu den Superhelden unserer Zeit. Der deutsche Hacking-Blockbuster „Who am I“ lockte knapp eine Million Menschen in die Kinos. Doch die Kinofantasie von unbesiegbaren Super-Nerds spiegelt sich in der Realität nicht wider.

Wenn Unternehmen ernsthaft gegen die von kriminellen Hackern ausgehende Gefahr vorgehen wollen, wird es höchste Zeit, irrationale Ängste abzulegen. Hacker bleiben ein Mythos, solange wir über sie sprechen anstatt mit ihnen. Der direkte Kontakt zu ethischen oder „White Hat“-Hackern ist essenziell, um zu verstehen, wie Cyberkriminelle arbeiten. Nur so haben Firmen eine Chance, Schwachstellen zu erkennen und anzugehen.

Nicht länger im Dunkeln stochern

Ein wichtiger Schritt zu dieser Selbsterkenntnis ist es, Hacking-Angriffe regelmäßig zu simulieren. Die erste Erkenntnis solcher Simulationen ist meist, dass Hacking länger dauert als gedacht. Selbst bei schwach geschützten Firmen sind mehrere Schritte nötig, um auf wertvolle Daten zuzugreifen. Im ersten Schritt wird meist versucht, mithilfe einer E-Mail-Malware, Kontrolle über einen einzelnen Computer zu gewinnen, oft ein unkritisches System. Im zweiten Schritt suchen die Hacker ungestört in internen Anwendungen und Servern nach weiteren Schwachstellen. Bis auf diese Weise das gesamte IT-Netz einer Firma gehackt ist, dauert es in der Regel mehrere Tage bis Wochen. Schwachstellen, die während dieses Prozesses von „White Hat“-Hackern identifiziert wurden, können strukturiert angegangen werden.

Das Wissen darüber, wo genau Schwächen liegen, ist aber nur die halbe Miete. Mindestens ebenso wichtig ist es, Schwachstellen priorisieren zu können. Das Aufstellen zielführender KPIs ist für Unternehmen deshalb unabdingbar. Nur so sind sie in der Lage, ihr tatsächliches Risiko zu verstehen und mit anderen zu vergleichen, um Security-Budgets effizient zum Einsatz zu bringen. Für Unternehmen gibt es keinen Grund, länger im Dunkeln zu stochern. Sie können Hacker mit ihren eigenen Waffen schlagen.

SPECIAL

Fehlende Prioritäten

WENN DAS OFFENSICHTLICHE ÜBERSEHEN WIRD

Deutsche Unternehmen und Institutionen stehen seit Ausbruch des Russland-Ukraine-Kriegs mehr denn je im Fadenkreuz von Cyberkriminellen. Doch IT-Sicherheit hat bei zu vielen Unternehmen noch immer keine oberste Priorität.

Die Daten sprechen für sich: Laut dem Trellix Advanced Research Center war die Anzahl der Ransomware-Angriffe auf deutsche Ziele im dritten Quartal 2022 um 32 Prozent höher als im Vergleich zum zweiten Quartal. Deutschland ist damit derzeit weltweit ein Topziel in dieser Angriffskategorie.

Dasselbe gilt für sogenannte Advanced Persistent Threats (APTs), also mehrstufige, langfristiger angelegte, gezielte Angriffe auf ganz bestimmte Unternehmen oder Personen. Das Ziel dabei ist, dort Informationen zu erlangen oder anderweitigen Schaden zu verursachen. 29 Prozent der weltweiten APT-Attacken entfielen auf Deutschland.

Der Frust ist groß

Eine aktuelle PwC-Studie zeigt, dass rund 29 Prozent der deutschen CEOs Cyberrisiken zwar als größte Sorge für die Wirtschaftslage sehen. Dennoch fehlt in vielen Fällen weiterhin die Priorisierung der IT-Sicherheit in ihren Unternehmen. Diesen Schluss induziert eine weitere Studie aus dem Jahr 2022, an der 9.000 Cybersicherheitsexperten teilnahmen – 500 davon aus Deutschland.

Denn einerseits sagen 95 Prozent der Befragten aus Deutschland, dass es bei Vorstand und Geschäftsführung eine klare Zuweisung der IT-Sicherheitsverantwortung gibt. Andererseits geben 28 Prozent der Teilnehmer an, dass in ihrem Unternehmen der Schutz vor Cyberangriffen bei Vorstand und Entscheidungsträgern keine Top-Priorität genießt. 54 Prozent meinen, die Geschäftsleitung schenke der digitalen Sicherheit nicht ausreichend Aufmerksamkeit. Und 36 Prozent benennen die fehlende Wertschätzung durch ihre Chefs als eine der größten Frustrationsquellen.

> ***Auch externe Partner lassen sich in eine XDR-basierte Sicherheitsarchitektur einbinden.***

Ein paar Tage?

Auch wenn reale Angriffe passieren, zeigt sich, wie dünn die Sicherheitsdecke ist: Rund 33 Prozent der deutschen Studienteilnehmer sagten, dass es mindestens ein paar Tage oder länger dauere, bis eine Attacke bemerkt wird. Ein paar Tage? Bis dahin können Produktion, Stromnetz oder lebenswichtige Krankenhausinfrastrukturen längst zusammengebrochen sein.

Anscheinend werden Investitionen und Bemühungen in Sachen IT-Sicherheit bei zu vielen Akteuren vor allem als kostenträchtiges Feigenblatt betrachtet, nicht als notwendige und oft genug überlebenssichernde Maßnahme. Dabei sollte die erhebliche Erweiterung des Kreises der Unternehmen, deren Infrastruktur laut dem erneuerten KRITIS-Gesetz als kritisch für das Funktionieren der Gesellschaft gilt, eigentlich Warnschuss genug sein.

Was aber tun? Möglicherweise ist die Indolenz in einigen deutschen Chefetagen auch auf eine gewisse Hilflosigkeit zurückzuführen: Cyberexperten sind rar und teuer, die Angriffe werden mehr und raffinierter. Zudem wächst die Angriffsfläche beispielsweise durch mobiles Arbeiten, Homeoffice und die unternehmensübergreifende Vernetzung von Lieferketten. Das führt u.a. zu immer mehr Sicherheits-Tools, die immer mehr Meldungen erzeugen. IT-Experten können hier oft nicht mehr mithalten.

Einen Schritt voraus

Ein Ansatz, diesen gordischen Knoten zu durchschlagen, ist Extended Detection and Response (XDR). XDR erkennt mittels lernfähiger Künstlicher Intelligenz auch Frühsymptome digitaler Angriffe und blockt diese ab, noch bevor sie Schaden anrichten können. XDR-Systeme binden die vorhandenen Sicherheitssysteme, deren vielfältige Meldungen für das IT-Team einzeln kaum noch zu bewältigen sind, unter einem Dach zusammen und priorisieren sie übergreifend.

Auch externe Partner lassen sich in eine XDR-basierte Sicherheitsarchitektur einbinden. XDR-Lösungen können neben den Informationen aus allen Verästelungen und allen Endpunkten des jeweiligen Informationssystems auch externe Informationsquellen einbinden. Zudem ist die Benutzerschnittstelle einer guten XDR-Lösung so gestaltet, dass nicht nur IT-Sicherheitsspezialisten mit langjähriger Erfahrung sie bedienen können. So kann man internes Personal für IT-Sicherheitsaufgaben weiterbilden oder Quereinsteiger anwerben, was wiederum Personalkosten spart. Kurz: XDR bringt IT-Sicherheitsteams und das IT-Management zu vertretbaren Kosten wieder vor die Angriffswelle. Das ist dringend nötig, denn die Hacker dieser Welt schlafen nicht.

Fabien Rech

Die Sicherheitsdecke *ist dünn: Teilweise dauert es Tage oder noch länger, bis eine Attacke überhaupt bemerkt wird. Die Hacker freut es.*

With secure supply chain...

or without?

Gemeinsam die Supply Chain für die Geschäftskontinuität sichern

Cyberangriffe können sich auf weltweite Supply Chains auswirken und die Geschäftskontinuität beeinträchtigen. Sie brauchen einen Partner mit dem richtigen Fachwissen, der richtigen Technologie und dem richtigen Ansatz, um bewährte Maßnahmen für die Cybersicherheit zu erzielen. Gemeinsam für nachhaltige Cybersicherheit

www.withsecure.com

WITH™ secure

SPECIAL

Cybersecurity-Politik

„WAS UNTERNEHMEN WISSEN SOLLTEN“

Warum es Datenschutz nicht zum Nulltarif gibt und welche Verbesserungen Unternehmen in diesem Bereich noch offenstehen, erläutert Dr. Christoph Bausewein, Assistant General Counsel, Data Protection & Policy bei Crowdstrike.

Eine starke Cybersecurity *und ausgefeilte Datenschutzlösungen sind für Unternehmen heutzutage nicht mehr optional.*

Herr Bausewein, die Datenschutz-Grundverordnung (DSGVO) wird in der öffentlichen Debatte nicht selten als bürokratisches Monster dargestellt. Außerdem wird bemängelt, dass Datenschutz und Datensicherheit nicht als Ganzes betrachtet werden. Was sagen Sie zu dieser Kritik?

BAUSEWEIN: Ich bin der Überzeugung, dass es Datenschutz nicht zum Nulltarif gibt und er immer zwangsläufig mit Aufwand verbunden ist. Dies betrifft Unternehmen und Organisationen jeder Größe gleichermaßen, weshalb ich die pauschale Kritik an der Datenschutz-Grundverordnung nicht teilen kann. Dennoch gibt es wie überall Verbesserungsmöglichkeiten, über die es sich zu reden lohnt. Dementsprechend möchte ich dafür werben, gute Datenschutzpraktiken als Investitionen in die Zukunft zu verstehen und nicht auf die lange Bank zu schieben.

Die Ansicht, dass Datenschutz und Datensicherheit oftmals nicht als Ganzes betrachtet werden, teile ich indes uneingeschränkt. Nicht selten sehe ich in meiner Praxis, wie Datenschutz- und Informationssicherheitsbeauftragte nur unzureichend zusammenarbeiten. Dies ist absolut kontraproduktiv, weil Datenschutz und Datensicherheit einander bedingen und nicht isoliert voneinander betrachtet werden können und sollten. Dies belegt nicht nur die DSGVO, sondern ist auch Grundpfeiler der Privacy-by-Design-Lehre nach Ann Cavoukian. Diese spricht davon, dass Datenschutz bei voller Funktionalität gewährleistet werden muss, was für mich auch Sicherheit beinhaltet. Im Übrigen verbietet sich denklogisch jede andere Auslegung, weil Sicherheitsdefizite ihrerseits Eingriffe in die Grundfreiheiten der Menschen begründen können, wie sie der Europäische Gerichtshof in der Rechtssache Schrems II mit Blick auf den Datenschutz eingefordert hat.

> **„Datenschutz und Datensicherheit können und sollten nicht isoliert voneinander betrachtet werden.“**

Dr. Christoph Bausewein *hat einen ausgeprägten technologischen Fokus. Insbesondere beschäftigt er sich mit rechtlichen Fragen der Künstlichen Intelligenz und Cybersicherheit.*

Wo stehen wir aktuell in Europa hinsichtlich der Gesetzeslage im Bereich Cybersicherheit und wohin entwickelt sich diese? Welche Trends beobachten Sie?

BAUSEWEIN: Ich halte es für legitim zu behaupten, dass Cybersecurity zu den Schwerpunkten der EU-Digitalstrategie gehört. Begründet wird diese Annahme durch eine Vielzahl von Gesetzesvorhaben, wie etwa den Cybersecurity Act, Cyber Resilience Act, die Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors sowie die Richtlinie über die Resilienz kritischer Einrichtungen. Sogar der äußerst relevante Data Act sowie der AI Act haben wesentliche Auswirkungen und Bezüge zur Cybersicherheit.

Bei aller damit einhergehenden Bemühung um eine Verbesserung der Cyberresilienz und -resistenz der Europäischen Union beobachte ich, dass damit gleichzeitig widersprüchliche Trends einhergehen, die die Cybersicherheit zu reduzieren drohen. So gibt es etwa immer mehr Vorschläge, die Fortschritt und Harmonisierung im Bereich der Cyberresilienz zu untergraben drohen. Besonders kritisch sehe ich Bestrebungen zur Datenlokalisierung, die den Zugriff auf Daten und damit auch die Nutzung von Cloud Services nicht unerheblich einzuschränken versuchen. Im schlimmsten Fall kann dies zur Herabsetzung der Cybersicherheit durch die Nichtnutzbarkeit von Cloud-basierten, weltumspannenden Cybersicherheitsservices führen, deren Zweck es ist, Sicherheit rund um die Uhr an 365 Tagen optimal sicherzustellen.

Was sollten Unternehmen tun, um diese Trends zu navigieren und nicht auf Basis hypothetischer Risiken zu agieren?

BAUSEWEIN: Cybersicherheit ist heutzutage nicht mehr optional für Unternehmen. Angesichts der Tragweite der aktuellen Cyberattacken und der eingesetzten Techniken müssen sich Unternehmen die Frage stellen, ob die in ihrem Netzwerk eingesetzten Sicherheitstechnologien dem Risiko angemessen sind, den heutigen rechtlichen Standards entsprechen und die gängigen Best Practices beinhalten. Generell ist es empfehlenswert, die Cybersicherheit zu stärken, um nicht nur resistent, sondern auch resilient zu sein, was diverse Cybergefahren anbelangt. Um sich bestmöglich aufzustellen, ist es wichtig, den Anbieter wohl überlegt auszuwählen. Hier lohnt es sich, in Hinblick auf die aktuellen Debatten verschiedene Blickwinkel einzunehmen und den ganzheitlichen Datenschutz nicht aus den Augen zu verlieren.

Ricarda Müller

CISOs unter Druck

WIE DIE RICHTIGE STRUKTUR VERANTWORTLICHE ENTLASTET

Die Gefahr durch Cyberangriffe steigt und mit ihr der Druck, der auf CISOs lastet. Wer die Sicherheit seines Unternehmens nicht aufs Spiel setzen möchte, muss anfangen, sein Security-Personal zu entlasten.

Die Verantwortung der Sicherheitsexperten ist enorm. Zunehmende mentale Belastung der Chief Information Security Officers (CISOs) ist die Folge. Inzwischen verlässt sogar immer mehr Security-Fachpersonal das Feld, um dem Burnout zu entgehen.

Für Bosch Cybercompare liegt der Hauptgrund für die zunehmende Belastung im rasanten Wachstum des Security-Markts der vergangenen Jahre. Das hat dazu geführt, dass der Cybersecurity-Markt ineffizient und intransparent geworden ist. Unzählige Hersteller bieten Sicherheitslösungen für Unternehmen an. Doch je mehr Tools im Einsatz sind, desto komplexer wird die Infrastruktur. Zwar haben die meisten dieser Produkte ihre Daseinsberechtigung, doch nicht jede Lösung entspricht den individuellen Anforderungen jedes Unternehmens. Es gilt also, Struktur und Übersicht ins Chaos der unzähligen Optionen zu bringen.

> ***Es gilt, Struktur und Übersicht ins Chaos der unzähligen Optionen zu bringen.***

Ein einheitliches Regelwerk

Man sollte sich zunächst bewusst sein, dass es keinen 100-prozentigen Schutz vor Cyberangriffen gibt. Das Pareto-Prinzip kann jedoch bei der Orientierung helfen: Bereits mit 20 Prozent des Aufwands können Unternehmen einen guten Schutz aufbauen. Nun sollten Unternehmen nicht unbedingt „nur“ 80 Prozent Sicherheit anpeilen, doch gerade zu Beginn und für kleinere Organisationen ist dies ein guter Richtwert. Security-Mitarbeitern kann so Druck von den Schultern genommen werden, da sie nun einfacher priorisieren können. Dafür sollte im ersten Schritt eine Bestandsaufnahme stattfinden.

Dabei hilft die Einführung eines Informationssicherheitsmanagementsystems (ISMS). Dieses besteht aus einer Reihe von Vorgaben und Richtlinien, die sowohl einheitliche Standards für die Informationssicherheit festlegen als auch die Einhaltung von Compliance-Regeln gewährleisten. Ein ISMS funktioniert dabei auf drei Ebenen: Richtlinien, Prozesse und Prozeduren.

Richtlinien definieren organisationsweite Ziele für die Sicherheit. Prozesse wiederum sind die Schritte, die das Unternehmen durchführt, um diese Ziele zu realisieren. Auf der untersten Ebene stehen die Prozeduren, die konkrete Anweisungen beinhalten, wie bestimmte Aufgaben und Verfahren sicher durchgeführt werden können. Darüber hinaus setzt ein ISMS auch auf standardisierte Testverfahren und sorgt so dafür, dass CISOs die Sicherheit der eigenen Infrastruktur stets ohne großen Arbeitsaufwand im Blick behalten. Gleichzeitig dient das Regelwerk auch dazu, die Awareness der Mitarbeiter zu erhöhen und Sicherheitsrisiken im täglichen Ablauf zu minimieren.

Ordnung entlastet

Der beste Weg, um die eigenen Security-Mitarbeiter zu entlasten, ist die richtige Struktur. Dafür kann ein ISMS ein stabiles Grundgerüst bilden. Damit haben Verantwortliche eine Richtschnur, anhand derer sie bewerten können, welche Maßnahme auf die übergeordneten Ziele einzahlt und für die aktuelle Situation des Unternehmens passend ist. Sie haben also eine Basis, auf der sie ihr System und den Einkauf strukturiert aufbauen können und mit der sie nicht mehr hilflos den rasanten Entwicklungen in Markt und Technologie ausgesetzt sind. Denn auf dieser Grundlage können sie passende Angebote einholen, die exakt auf die individuellen Anforderungen zugeschnitten sind. Externe Partner können dabei helfen, den Aufbau der eigenen Sicherheitsmaßnahmen und den Einkauf strukturiert und Schritt für Schritt anzugehen und das Security-Personal so noch weiter zu entlasten.

Simeon Mussler

Die Verantwortung der Sicherheitsexperten *ist enorm – kein Wunder also, dass sich bei steigender Cyberkriminalität eine zunehmende mentale Belastung bei Chefs und Mitarbeitern bemerkbar macht.*

SPECIAL

Internationale Fahndung

DER CYBERDIEB IM LAMBORGHINI

Vermehrt ist seit Beginn des Russland-Ukraine-Kriegs von Cyberangriffen auf deutsche Unternehmen zu hören. Dabei fällt oft der Name einer russischen Hackergruppe: „Indrik Spider“. Der mutmaßliche Anführer: Maksim Yakubets. Nach ihm wird international gefahndet.

Der Mann, der in russischen Medien als der „100-Mio.-Dollar-Dieb“ tituliert wurde, wird bereits seit 2019 gesucht. Damals schrieb die US-Bundespolizei den Hacker zur internationalen Fahndung aus. Auf dem digitalen Steckbrief sind 5 Mio. US-Dollar für seine Ergreifung ausgesetzt.

Im Jahr 2020 kamen verschiedene Firmennetzwerke in Deutschland zum Erliegen, darunter die Uniklinik in Düsseldorf. Die Folge war u.a. der Tod einer Frau, da der Zwischenfall die Abmeldung der Notfallaufnahme notwendig gemacht hatte. Das Ziel der Hacker war offenbar Lösegeld für das Entfernen der genutzten Schadsoftware.

Zahl der Angriffe steigt

Nach Medienberichten gelang es Ermittlern in Deutschland vor Kurzem, die Hintermänner zu enttarnen: Yakubets, dem nachgesagt wird, dass er einen extravaganten Lebensstil führt und eine Vorliebe für Sportwagen der Marke Lamborghini hat, soll die Gruppe angeführt haben. Ihm werden zahlreiche Cyberangriffe vorgeworfen. Sein Landsmann Igor Turashev soll als Chefadministrator involviert gewesen sein. Das Landeskriminalamt NRW vermutet zudem Igor Garshin als einen der Hauptverantwortlichen. Die Justizbehörden mutmaßen, dass sich die Gesuchten in Russland befinden.

Klar ist: Die Zahl der staatlich gelenkten russischen Cyberangriffe steigt noch immer deutlich an. Laut Digitalverband Bitkom gehen 36 Prozent der Online-Attacken auf deutsche Unternehmen im Jahr 2022 auf Cyberkriminelle russischer Herkunft zurück. Die Bedrohungslage in Deutschland ist also unverändert hoch.

„Im vergangenen Jahr haben 84 Prozent aller Unternehmen in Deutschland mit zehn oder mehr Beschäftigten angegeben, dass sie innerhalb von zwölf Monaten Opfer von Datendiebstahl, Spionage oder Sabotage geworden sind. Das heißt: Jedes Unternehmen kann Opfer einer Cyberattacke werden – ganz unabhängig von Größe oder Branche“, warnt Simran Mann, Referentin Sicherheitspolitik beim Digitalverband Bitkom. Die zu Kriegsbeginn vor einem Jahr befürchtete massive Angriffswelle im Cyberraum auf Unternehmen oder staatliche Institutionen westlicher Staaten sei zwar bislang ausgeblieben, dennoch nehmen Cyberattacken seit Jahren zu. „Dabei werden die Angriffe immer professioneller durchgeführt und lassen sich häufiger nach Russland und China zurückverfolgen.“

Zuständigkeit klären

Unternehmen und Behörden müssten „unbedingt ihre Informationssicherheit ernst nehmen“ und entsprechende Abwehrmaßnahmen ergreifen, die notwendigen Investitionen durchführen sowie einen Notfallplan aufstellen. Damit das gelinge, müsse Cybersicherheit Sache von Geschäftsführung oder Vorstand sein und alle Mitarbeiter müssten regelmäßig geschult werden.

Dem mutmaßlichen Cyberkriminellen Yakubets wird nachgesagt, dass er ein extravagantes Leben führt und eine Vorliebe für Lamborghini-Sportwagen hat.

2020 starb eine Frau wegen eines Angriffs von Hackern – Maksim Yakubets soll einer von ihnen gewesen sein.

Dem schließt sich eine Sprecherin des Bundesamts für Sicherheit in der Informationstechnik (BSI) an. Die Unternehmensleitung sei gefragt, Sicherheitsrisiken zu erkennen, Zuständigkeiten zu klären und passende Maßnahmen zu ergreifen. „Am Anfang steht in der Regel eine Inventur der im Unternehmen vorhandenen Daten und die Identifikation der sogenannten Kronjuwelen: Diese für das Geschäft und die Betriebsabläufe unverzichtbaren Daten sollten den höchsten Schutz genießen“, betont die BSI-Sprecherin.

Sie rät Unternehmen dazu, sich regelmäßig einen Überblick über die genutzten Programme zu verschaffen und dafür zu sorgen, dass Sicherheitsupdates so rasch wie möglich eingespielt werden. Unternehmen sollten zudem Sicherungskopien ihrer Daten anlegen und Back-ups regelmäßig testen, um auf der sicheren Seite zu sein, wenn Computer von Viren befallen oder gestohlen werden. „Insbesondere können auf diese Weise auch Schäden durch Erpressungstrojaner – die sogenannte Ransomware – vermieden werden, die sich aktuell bei Cyberkriminellen besonderer Beliebtheit erfreuen.“

Ricarda Müller

BCI-Report 2023

RESILIENZ GANZ OBEN
AUF DER AGENDA

Im Kommentar erläutert Benjamin Jansen, Senior Vice President Sales ENS/CM bei F24, Erkenntnisse aus dem kürzlich veröffentlichten BCI Emergency & Crisis Communications Report 2023.

Benjamin Jansen hat mehr als 23 Jahren Erfahrung in verschiedenen Management-Positionen im Vertrieb und über 16 Jahren Erfahrung in den Bereichen „SaaS-Lösungen“, „Internet of Things“ und „Cloud-Technologie“.

Im Februar dieses Jahres hat eine globale Welle von Ransomware-Cyberattacken Einrichtungen und Unternehmen angegriffen. Weltweit war die Schadsoftware nach Angaben der Medien auf etwa 84.000 Servern installiert, in Deutschland allein auf etwa 7.000. Die Folgen waren unterschiedlich stark zu spüren, deutlich macht dieser Vorfall aber vor allem eins: Effektives Krisen- und Risikomanagement ist ein Marathon, kein Sprint.

Glücklicherweise haben viele Betriebe dies bereits erkannt, darauf deuten die Zahlen des im Februar erschienenen BCI Emergency & Crisis Communications Report 2023 hin. Es zeigte sich: Die zentralen Anforderungen sind Flexibilität und Verfügbarkeit.

Im Notfall schnell sein

Deshalb setzen 81 Prozent der befragten Organisationen, die digitale Tools im Einsatz haben, eine SaaS-Lösung für die Notfallkommunikation ein. Der Bericht zeigt auch, dass durch digitale Krisenmanagementlösungen eine schnellere Reaktionsgeschwindigkeit und Aktivierung von Krisenkommunikationsplänen erreicht wird: 33 Prozent der Organisationen, die digitale Tools verwenden, konnten ihre Notfallkommunikationspläne innerhalb von fünf Minuten aktivieren, wohingegen es bei Unternehmen, die keine digitalen Tools im Einsatz haben, lediglich 7 Prozent waren. An diesen Zahlen zeigt sich die Stärke von SaaS-Lösungen. Sie sind der Goldstandard, da durch ihren Einsatz sichergestellt werden kann, dass schnelle und ausfallsichere Kommunikation jederzeit möglich und damit Teamkoordination auch im Ernstfall machbar bleibt.

Digitale Krisenmanagementlösungen ermöglichen automatisierte Alarmierung auf der Basis eines umfassenden Krisenmonitorings und setzen die vorab für den jeweiligen Fall festgelegten Aktivitäten in Gang – je nach Programmierung so lange, bis eine Rückmeldung auf die Alarmierung erfolgt ist. Außerdem sind sie individuell für das vorliegende Szenario anpassbar – ein kaum zu unterschätzender Vorteil, denn IT- oder Telekommunikationsvorfälle sind bei Weitem nicht alleinige Hauptauslöser für die Aktivierung von Notfallkommunikationsplänen. Zwar kommen sie laut BCI-Report mit 43 Prozent auf Platz zwei, aber auch Faktoren wie widrige Wetterbedingungen (49 Prozent) und Krankheitsausbrüche (28 Prozent) stellen weiterhin ein großes Risiko für Unternehmen dar.

Unter dem Strich machen die Erkenntnisse aus dem Report Mut, zeigen sie doch, dass mehr Unternehmensverantwortliche sich für die frühzeitige Implementierung von Krisenmanagementlösungen und damit für die Resilienz des eigenen Betriebs entscheiden.

SPECIAL

Security Operations Center

HACKER HABEN HÄUFIG LEICHTES SPIEL

Die aktuelle Cybersicherheitslage ist turbulent: Ransomware as a Service im Aufwind, zunehmende Kompromittierungen von Geschäfts-E-Mails und ungepatchte Schwachstellen bedeuten ein enormes Risiko für Unternehmen jeder Größe und Branche.

Insbesondere kleine und mittelständische Unternehmen stehen angesichts knapper Budgets und des IT-Fachkräftemangels vor Herausforderungen. Laut Digitalverband Bitkom fehlen in Deutschland rund 137.000 IT-Experten. Das verschärft die Fachkräftesituation für den Mittelstand, der im Wettlauf um qualifizierte Mitarbeiter hinter großen Unternehmen und Konzernen nicht selten das Nachsehen hat. Stattdessen sind deren IT-Teams vor allem mit Generalisten besetzt, die fachlich zwar breit aufgestellt sind, denen jedoch die nötige Kompetenz bei Cybersicherheitsfragen fehlt.

Das ist riskant, denn angesichts der aktuellen Bedrohungslage wird diese Expertise dringend gebraucht: So stellte das BSI in seinem Lagebericht zur IT-Sicherheit 2022 fest, dass sich die Cybersicherheitssituation angesichts geopolitischer und ökonomischer Unsicherheit weiter verschärft. Und obwohl die Fälle von Ransomware-Attacken

> ***„Der Unterhalt eines eigenen SOC ist teuer und nur für große Konzerne rentabel.“***

insgesamt leicht zurückgegangen sind, haben Cyberkriminelle schon das nächste Cyber-Cash-Modell entwickelt. So ergaben die Auswertungen des Arctic Wolf Labs Threat Report 2023 einen deutlichen Anstieg der Fälle von Business-E-Mail-Compromise, durch die sich Cyberkriminelle finanziell bereichern. Generell haben Hacker häufig leichtes Spiel, denn noch immer gehen 45 Prozent der Sicherheitsvorfälle auf bekannte, aber ungepatchte Schwachstellen wie Log4Shell zurück. Vielfach fehlt schlicht die Zeit zur Behebung. Dass es eine umfassende Sicherheitsstrategie und entsprechende Security-Maßnahmen braucht, daran zweifelt heute niemand mehr. Doch wie ist das auch für den Mittelstand umsetzbar?

Aufgrund bekannter, *aber ungepatchter Schwachstellen haben Cyberkriminelle häufig leichtes Spiel.*

Sicherheit im Abomodell

Security Operations Center (SOC) bilden die Zentrale für alle Sicherheitsmaßnahmen eines Unternehmens und sind damit das Herzstück moderner IT-Sicherheit. Der Unterhalt eines eigenen SOC ist jedoch teuer und nur für große Konzerne rentabel. Eine Alternative ist ein Security-Operations-Center-as-a-Service-Modell (SOCaaS), bei dem ein Sicherheitspartner alle Security-Maßnahmen übernimmt. Die Budgets sind hier transparent und flexibel, die Implementierung erfolgt schnell. Die Services reichen von der Bestandsaufnahme der Sicherheits-Assets, einem 24/7-Threat-Monitoring, über Detection und Response, Managed Risk und die Reaktion auf Sicherheitsvorfälle bis hin zu einer kontinuierlichen Verbesserung der Sicherheitslage des Unternehmens.

Im besten Fall bildet der externe Security-Partner die „verlängerte Werkbank“ der IT-Abteilung und verfügt dabei über fundiertes Sicherheitswissen und aktuelle Bedrohungsdaten. So können Anpassungen an neueste Cyberrisiken reaktionsschnell gemeinsam vorgenommen werden. Ein direkter Ansprechpartner steht dabei jederzeit für Rückfragen und zur Beratung zur Verfügung.

Um festzustellen, ob SOCaaS für ein Unternehmen infrage kommt, bedarf es einer genauen Evaluation der Umsetzbarkeit und Kosten für eine Inhouse-Sicherheitslösung inklusive ausreichend qualifizierten Personals, im Vergleich zu einem externen Security-Provider. Ganz egal, für welche Option ein Unternehmen sich entscheidet, ist am Ende vor allem eines wichtig: dass die Sicherheit langfristig verbessert und Cyberrisiken minimiert werden.

Dr. Sebastian Schmerl

Ein zweischneidiges Schwert

KANN SICHERHEIT BENUTZERFREUNDLICH SEIN?

Dr. Dominik Schürmann, Gründer und CEO der Heylogin GmbH, erklärt im Kommentar, warum sich Komfort und Sicherheit beim Zugriff auf IT-Ressourcen nicht ausschließen müssen.

Die betriebliche IT entwickelt sich mit großer Dynamik. Mitarbeiter beziehen wichtige Informationen für ihre tägliche Arbeit aus dem Web, sie buchen das Hotelzimmer für ihre Dienstreise bei einem Online-Portal oder sie bestellen wichtige Vorprodukte auf einer Handelsplattform – die Zahl webgestützter Anwendungsfälle wächst schneller, als man „Passwort“ sagen kann.

Dass man betriebliche Ressourcen – etwa Konstruktions- und Personaldaten, Bankkonten oder Bestellvorgänge – gegen den Zugriff Unbefugter schützen muss, ist eine Binsenweisheit. Unbefugte: Das können Mitarbeiter der eigenen Firma sein, aber auch Angreifer aus der Tiefe des Cyberspace. Gerade letztere Kategorie nimmt ständig zu. Kriminelle dringen in die Unternehmens-IT ein und entwenden wettbewerbsrelevante Daten oder verschlüsseln die Datenbestände des Unternehmens, um Lösegeld zu erpressen. Laut Branchenverband Bitkom summiert sich der volkswirtschaftliche Schaden durch solche Aktivitäten auf mehr als 200 Mrd. Euro pro Jahr.

Gegensätzliche Anforderungen

Damit kommen wir zum Schutz der betrieblichen IT. Das Authentisierungsverfahren der Wahl in den meisten Unternehmen ist eine Kombination aus einer User ID und einem Passwort. Doch deren Einsatz ist ein zweischneidiges Schwert, denn sie muss zwei gegensätzliche Anforderungen erfüllen: Einerseits sollen Passwörter sicher sein – d.h., sie sollen aus komplexen Zeichenfolgen bestehen und zudem möglichst lang sein, damit sie nicht leicht zu erraten sind. Andererseits soll sich der Benutzer an den Arbeitsplatzrechnern diese Passwörter leicht merken können. Das ist schon deshalb wichtig, weil nach den Regeln der Cybersicherheit für jeden Account ein separates Passwort zu benutzen ist. Wer sich an diese Regel halten will, sieht sich mit einer anspruchsvollen Denksportaufgabe konfrontiert: Im Durchschnitt setzt jeder User mehr als 150 verschiedene Passwörter ein.

Doch es gibt ja Passwort-Manager – zum Glück, oder? Der Passwort-Manager merkt sich all diese verschiedenen Passwörter und speichert sie auf einem Server oder in der Cloud. Der Mitarbeiter an seinem Arbeitsplatzrechner braucht sich dann nur noch ein Master-Passwort zu merken. Aber man sollte genau hinschauen: Diese Lösung verschiebt letztlich das Problem an eine andere Stelle. Der Server ist möglicherweise besser gesichert als der Laptop des Sachbearbeiters im Homeoffice. Aber dafür speichert er nicht nur ein Passwort, sondern gleich viele davon. Damit wird er zum bevorzugten Ziel für Hacker – und das häufig mit Erfolg, wie den Medien regelmäßig zu entnehmen ist. Aus diesen Gründen sind Passwörter als Instrument für die IT-Sicherheit etwas in Verruf geraten.

> ***„Nach den Regeln der Cybersicherheit ist für jeden Account ein separates Passwort zu benutzen.“***

Dr. Dominik Schürmann *hat in IT-Sicherheit promoviert und während seiner Zeit an der TU Braunschweig über 15 wissenschaftliche Publikationen veröffentlicht.*

Sicherheit ohne Abstriche

Erfreulicherweise gibt es Alternativen, die ohne Abstriche an der Sicherheit komfortabel einzusetzen sind. Der Blick ist dabei vor allem auf Sicherheits-Hardware aktueller Smartphones zu richten. Unter Namen wie „Secure Enclave“ (Apple) oder „Knox Vault“ (Samsung) besitzen die Mobiltelefone Hardware-Inseln, die nach heutigem Ermessen als Hacker-resistent gelten können – niemand kommt da rein außer dem Besitzer selbst. Ein guter Platz für die Ablage von Master-Passwörtern und ähnlichen sicherheitsrelevanten Daten. Damit lassen sich die Handys der Mitarbeiter zur Authentisierung heranziehen: Einmal bestätigt und Fingerabdruck gescannt, und schon hat sich der User eingeloggt. Und ein Handy hat heute praktisch jeder. Natürlich muss das Gerät auf dem Unternehmensserver registriert sein, aber dafür gibt es geeignete Software. Es ist zu vermuten, dass dieser elegante und dennoch sichere Ansatz schnell eine Anhängerschaft in den Unternehmen finden wird.

SPECIAL

Sicherheit im Netz

„DEN CYBERKRIMINELLEN IMMER EINEN SCHRITT VORAUS“

Im Interview erläutern Daniel Hofmann, Gründer und CEO von Hornetsecurity, und Christian Stein, Managing Director bei PSG Equity Equity, wie sich Unternehmen gegen Cyberkriminalität schützen können.

Herr Hofmann, Herr Stein, was sind aktuell die häufigsten Angriffstypen, denen Unternehmen ausgesetzt sind?

HOFMANN: E-Mails sind weiterhin das wichtigste Kommunikationsmittel, entsprechend ist das sogenannte Phishing mit 39,6 Prozent aller Attacken eine der häufigsten Bedrohungen. Allerdings variieren die Angriffstypen, ebenso wie die Häufigkeit der Attacken von Branche zu Branche. Angriffe auf Markenidentitäten nehmen weiter zu. So nutzen Cyberkriminelle Plattformen wie Linkedin, um Informationen über die Arbeitsstelle ausfindig zu machen und sich durch Social Engineering Zugang zu Unternehmensressourcen zu verschaffen. Dabei können sie gefälschte E-Mails oder Stellenanzeigen verwenden oder sich als potenzielle Kunden oder Partner ausgeben. In diesem Zusammenhang werden auch sogenannte Deepfakes, also durch Künstliche Intelligenz (KI) abgeänderte oder gefälschte Medieninhalte, immer häufiger, die eine wachsende Bedrohung für die Sicherheit von Unternehmen darstellen.

Christian Stein:

„Es ist für mich sehr vielversprechend zu sehen, dass sich Unternehmen der Bedeutung von ganzheitlichen Security-Strategien bewusst werden.“

STEIN: Eine ebenso wachsende Bedrohung ist das Feld des Wohltätigkeitsbetrugs. Dieser tritt meist in Zusammenhang mit größeren Ereignissen und Krisen auf der Welt auf, etwa während der Covid-19-Pandemie oder des Kriegs in der Ukraine. Auch wenn Wohltätigkeitsbetrug zu den ältesten Betrugsarten gehört, hat sich auch dieser Bereich durch Technologien wie E-Mails und soziale Medien digitalisiert. Die Versuche von Kriminellen, von Katastrophenereignissen zu profitieren, werden sich vermutlich durch die Folgen des Klimawandels weiter fortsetzen.

Welche Firmen bzw. Branchen sind für Cyberkriminelle besonders attraktiv und warum?

HOFMANN: Grundsätzlich sind alle Branchen und Firmen durch Cyberangriffe bedroht, die meisten kriminellen Attacken sind nicht auf bestimmte Branchen oder Unternehmen ausgerichtet. Jedoch gehört die Automobilindustrie zurzeit zu den am stärksten bedrohten Branchen. Das liegt u.a. an den finanziellen Mitteln der Unternehmen, also der Fähigkeit, gefordertes Lösegeld zu zahlen. Aber auch die Sektoren „Bildung“ und „Forschung“ sind häufige Ziele von Bedrohungsakteuren. Nicht zu vernachlässigen ist in dem Zusammenhang auch der Umfang der vorhandenen Technologien, die angegriffen werden können. Beispielsweise verfügen Krankenhäuser über eine Vielzahl medizinischer Geräte mit eingebetteten Computern. Da sich auf diesen oft alte Betriebssysteme befinden, die nur vom Hersteller aktualisiert werden können, ist es schwieriger, sie vor Cyberangriffen zu schützen.

STEIN: Mit der steigenden Bedrohung durch Cyberkriminalität glauben wir, dass die Nachfrage nach innovativen Lösungen zur Stärkung der Cyberabwehr immer größer wird. Firmen, die sich umfassend gegen Cyberangriffe schützen, sind daher auch attraktivere Partner für Investoren. Wir sehen große Wachstumschancen im Security-Bereich, da neue Bedrohungen die Nachfrage nach fortschrittlichen Sicherheitslösungen erhöhen.

Inwieweit setzen Unternehmen bereits innovative Security-Lösungen zur Abwehr der Angriffe ein oder planen aktuell, in den Security-Bereich zu investieren?

HOFMANN: Es gibt eine breite Palette an innovativen Security-Lösungen, die Unternehmen verwenden können, um ihre Systeme und Daten zu schützen. Einige der gängigen Lösungen sind:

1. Unternehmen setzen zunehmend auf KI und Maschinelles Lernen (ML), um Anomalien im Systemverhalten zu erkennen und zu bekämpfen. Diese Technologien ermöglichen es, verdächtige Aktivitäten schnell aufzuspüren und zu blockieren.
2. Die Automatisierung von Sicherheitsprozessen kann dazu beitragen, die Effektivität und Effizienz von Sicherheitsmaßnahmen zu verbessern. Dazu gehören etwa regelmäßige Updates von Sicherheits-Software oder das automatische Durchführen von Scans auf Schwachstellen.
3. Cloud-Services sind in den letzten Jahren immer beliebter geworden, vor allem wegen ihrer Flexibilität und Zuverlässigkeit. Unternehmen, die Cloud-Services wie Microsoft 365 nutzen, müssen ihre Daten und Systeme allerdings vor Angriffen schützen. Solche Cloud-Sicherheitslösungen umfassen etwa Firewall-Technologien, Intrusion Detection & Prevention, Verschlüsselung, Datensicherung und -wiederherstellung sowie Zugangskontrollen.
4. Das Verwalten von Benutzeridentitäten und Zugriffsrechten kann dazu beitragen, unautorisierte Zugriffe zu verhindern. Identity-and-Access-Management-Lösungen umfassen Single Sign-on, Zwei-Faktor-Authentifizierung, rollenbasierte Zugriffskontrollen, Identitätsmanagement und Berechtigungsverwaltung.

Wir sehen, dass eine wachsende Zahl von Unternehmen in diese innovativen Sicherheitslösungen investiert, um sich vor Angriffen zu schützen. Sie haben erkannt, dass traditionelle Sicherheitslösungen nicht ausreichen, um sich gegen ausgefeilte Angriffe zu verteidigen. Daher ist unserer Meinung nach auch zu erwarten, dass der Markt für innovative Sicherheitslösungen in den kommenden Jahren weiterwachsen wird.

Daniel Hofmann:

„Nicht zu vernachlässigen ist auch der Umfang der vorhandenen Technologien, die angegriffen werden können."

STEIN: Die Verwendung von KI und ML zur Erkennung von Anomalien im Systemverhalten sowie die Automatisierung von Sicherheitsprozessen sind nur einige Beispiele für die fortschrittlichen Technologien, die Unternehmen heute einsetzen. Cloud-Sicherheitslösungen und Identity-and-Access-Management-Lösungen sind ebenfalls wichtige Bereiche in der Cybersecurity-Branche. Ich denke, dass der Markt für innovative Sicherheitslösungen weiterwachsen wird, was viele Möglichkeiten bietet.

Welche Entwicklungen zeichnen sich für den Rest des Jahres ab? Worauf sollte sich die Cybersecurity-Branche in den kommenden Monaten einstellen?

HOFMANN: Unternehmen sollten robuste E-Mail-Sicherheitsstrategien implementieren und innovative Lösungen wie Maschinelles Lernen und Multi-Faktor-Authentifizierung integrieren, um den Cyberkriminellen immer einen Schritt voraus zu sein. Daher wird auch der Einsatz von Künstlicher Intelligenz und Cloud-basierten Sicherheitslösungen weiter an Bedeutung gewinnen. Für Unternehmen ist es wichtig, mit IT-Dienstleistern zusammenzuarbeiten und eigene Cybersicherheitsmaßnahmen zu implementieren, wie z.B. regelmäßige Software-Updates und Mitarbeiterschulungen. Denn nur, wenn alle Angestellten informiert sind und proaktiv handeln, können sich Unternehmen effektiv vor Cyberangriffen schützen und langfristig erfolgreich sein.

STEIN: Es ist für mich sehr vielversprechend zu sehen, dass sich Unternehmen der Bedeutung von ganzheitlichen Security-Strategien bewusst werden und innovative Lösungen integrieren. Ein umfassendes Verständnis und eine proaktive Haltung gegenüber Cybersicherheit sind dabei der Schlüssel, um die Sicherheit von Unternehmen langfristig zu gewährleisten. Ich bin optimistisch, dass Unternehmen in diesen Bereich investieren und noch umfassendere Sicherheitsmaßnahmen implementieren, um sich gegen Cyberangriffe zu schützen – und dies auch zunehmend von Investoren wertgeschätzt wird. ✔

Lea Sommerhäuser

SPECIAL

Insider-Bedrohungen

GEFAHREN IM INNEREN

Bei Cyberangriffen denken viele an Kriminelle, die Unternehmen von außen „hacken", während das größte Risiko von Insider-Angriffen ausgeht.

Dabei ist ein Insider nicht immer ein böswilliger Mitarbeiter. Zwei von drei Insider-Vorfällen werden durch Nachlässigkeit verursacht. Diese Angriffe sind deshalb so gefährlich, da sich die Cyberkriminellen scheinbar legitim in den Unternehmenssystemen befinden und dort über bestimmte Zugriffsrechte verfügen. Wie der aktuelle Software-as-as-Service-Datenrisiko-Report (SaaS) von Varonis gezeigt hat, sind in einem durchschnittlichen Unternehmen einer von zehn (auch sensitiven) Datensätzen für alle Mitarbeiter – und damit auch für Insider – zugänglich. Sicherheitsverantwortliche sollten sich bei den Abwehrmaßnahmen vor allem auf fünf Bereiche konzentrieren und sich folgende Fragen stellen.

Welche Daten müssen besonders geschützt werden? Die Basis sämtlicher Schutzmaßnahmen bildet die Identifizierung der wertvollsten und schützenswerten Daten. Hierzu müssen die Daten entsprechend bestimmter Richtlinien identifiziert und klassifiziert werden, um darauf basierend die Datensicherheitsstrategie zu priorisieren. Aufgrund der schieren Menge an Dateien kann dies nur automatisiert erfolgen.

Wer benötigt wirklich Zugang zu sensitiven Informationen? Um den Explosionsradius, also den Schaden, den ein kompromittiertes Konto verursachen kann, so klein wie möglich zu halten, sollte jeder Mitarbeiter nur auf die Daten zugreifen können, die für die Arbeit auch tatsächlich benötigt werden.

Gibt es auffälliges Nutzerverhalten? Insider können nur durch auffälliges Verhalten identifiziert werden. Sicherheitsteams müssen also bewerten, welches Verhalten für welchen Mitarbeiter „normal" ist.

Sind die Mitarbeiter ausreichend sensibilisiert? Nur wenn die Arbeitnehmer über den Wert von Daten sensibilisiert sind, werden sie langfristig Warnsignale erkennen und melden, damit diese vom Sicherheitsteam untersucht werden können.

Sind sämtliche nicht mehr aktive Konten deaktiviert? Veraltete, aber nicht deaktivierte Nutzerkonten sind für Angreifer ideal, da ihre Nutzung nicht weiter auffällt. Deshalb sollten Unternehmen ihren Off-Boarding-Prozessen große Aufmerksamkeit schenken und so sicherstellen, dass ehemalige Partner und Mitarbeiter keinen Zugang mehr besitzen. ✔

Michael Scheffler

SPECIAL

Bewusstsein für Sicherheit

DAS PASSWORTPUZZLE IST GELÖST

Die internationale Gruppe Ravensburger AG mit mehreren renommierten Spielzeugmarken setzt auf professionelle Passwortsicherheit.

Laut Benjamin Zwaka hat sich das Bewusstsein für Sicherheit im Unternehmen allgemein erhöht.

Wie in vielen anderen Unternehmen auch benötigte der Helpdesk von Ravensburger viel Zeit, um Support-Tickets für Passwörter und Benutzerauthentifizierung zu bearbeiten. Trotz klarer IT-Richtlinien lag die Nutzung von Passwörtern und deren Aufzeichnung im Ermessen der Mitarbeiter. Die Herausforderung war, dass einige Mitarbeiter die Passwörter auf Papier notierten und gelegentlich vergaßen. Andere wiederum verwendeten den Passwort-Manager des Browsers mit dem Nachteil von Sicherheitslücken, einschließlich des Risikos einer Exfiltration der unverschlüsselten Zugangsdaten. Zudem war die Produktivität globaler Teams mit gemeinsamen Konten beeinträchtigt. Beispielsweise verwendet das Social-Media-Team gemeinsame Unternehmensprofile. Das Fehlen einer technischen Lösung zur Standardisierung und Erleichterung rollenbasierter Zugriffsrechte stellte eine Herausforderung für die Sicherheit und für die Bildung einer ganzheitlichen Verteidigung gegen Cyberbedrohungen dar.

Das Unternehmen möchte in einer schnelllebigen Gesellschaft, in der wenig Zeit für- und miteinander ist, Momente für Gemeinsamkeit und persönliche Entwicklung bieten.

Klare Anforderungen

Der Spielzeugspezialist hatte klare Vorstellungen für die Sicherheit von Passwörtern. Die Lösung für die Passwortverwaltung musste in Microsoft Azure integriert werden, das zusammen mit einem Active Directory zur Verwaltung der Benutzerauthentifizierung verwendet wird. Entscheidend war auch die Verfügbarkeit auf verschiedenen Browsern. „Es war aus technischer Sicht wichtig, die Lösung in unsere Satellitensysteme zu integrieren. Außerdem musste die Software einfach zu bedienen sein, damit sie von jedem Mitarbeiter genutzt werden kann“, sagt Benjamin Zwaka, leitender Systemadministrator bei der Ravensburger AG.

Nachdem die Entscheidung für Keeper Security gefallen war, wurde die Lösung erst dem IT-Team und anschließend allen anderen Abteilungen zur Verfügung gestellt. Die Passwortlösung etablierte sich schnell als ein wichtiges Werkzeug für Produktivität, Zusammenarbeit und für die Sicherheit. Die integrierte Multi-Faktor-Authentifizierung und die Single-Sign-on-Optionen ermöglichen beispielsweise den Social-Media- und Marketing-Managern, sicher auf gemeinsamen Konten zusammenzuarbeiten. Gleichfalls erachten es auch technisch versiertere Benutzer als nützlich, etwa die Entwicklungsabteilungen, die sich Passwortdatensätze und SSL-Zertifikate teilen. Das Resultat: Die Funktionalität und die Sicherheit haben die Anzahl der passwortbezogenen Support-Tickets reduziert.

> ***„Wir haben eine Software, die jedem hilft, das Unternehmen zu schützen.“***

Mehr Sicherheit

Ravensburger greift für eine noch höhere Sicherheit auf eine zusätzliche Sicherheitsfunktion des Anbieters zurück: Das Tool Breachwatch überwacht die Passwörter und prüft, ob diese im Darkweb auftauchen. Es benachrichtigt die Administratoren und Anwender, wenn ein Passwort möglicherweise im Darkweb entdeckt wurde, um Maßnahmen zum Schutz des Unternehmens einzuleiten. Zudem werden Risikobewertungen zur Verfügung gestellt, um schwache Passwörter aktiv durch starke zu ersetzen.

Die intuitive Benutzeroberfläche führte zu einer schnellen Akzeptanz. Benjamin Zwaka bestätigt, dass die Passwortverwaltung bei Ravensburger verbessert und das Bewusstsein für Sicherheit im Unternehmen allgemein höher ist: „Vor der Passwortlösung war das IT-Team für die Sicherheit zuständig. Jetzt ist jeder für die IT-Sicherheit verantwortlich. Wir haben eine Software, die jedem hilft, das Unternehmen zu schützen.“

Pawel Jankowski

DIE RAVENSBURGER AG ...

[→ ... ist eine internationale Unternehmensgruppe mit mehreren renommierten Spielwarenmarken. Die bedeutendste Marke des Unternehmens, das Ravensburger blaue Dreieck, ist eine der führenden europäischen Marken für Spiele, Puzzles und Kreativprodukte sowie für deutschsprachige Kinder- und Jugendbücher. Das Familienunternehmen erwirtschaftete 2022 mit 2.534 Mitarbeitern einen Umsatz von 598 Mio. Euro. ←]

www.ravensburger.de

SPECIAL

Um erfolgreich zu sein, *müssen Sicherheitslösungen u.a. bedienungsfreundlich sein, damit Mitarbeiter sie akzeptieren und möglichst keine Fehler passieren können.*

Remote Work

„BERUFLICHES UND PRIVATES TRENNEN“

Remote Work ist aus dem Arbeitsalltag nicht mehr wegzudenken. Christian Pohlenz, Security-Experte bei Materna Virtual Solution in München, erklärt die Sicherheitsrisiken im Homeoffice und beim mobilen Arbeiten – und wie Unternehmen sich davor schützen können.

Herr Pohlenz, durch den zunehmenden Einsatz mobiler Endgeräte zur privaten und beruflichen Nutzung ist auch die Gefahr von Cyberangriffen auf diesen Geräten gestiegen. Warum ist ultramobile Kommunikation besonders anfällig für Ransomware-Attacken?

POHLENZ: Ziel von Ransomware-Attacken ist es, Lösegeld für die Freischaltung der Daten respektive des Geräts zu erpressen. Mobilgeräte sind für Cyberkriminelle dabei ein reizvolles Ziel, weil sie damit vergleichsweise leichtes Spiel haben. Smartphones und Tablets sind einfacher zu attackieren, denn sie sind oft „always-on“ mit dem Internet verbunden. Zudem sind sie meist schlechter vor Malware oder Angriffen geschützt als ein stationärer, besser in die interne Sicherheitsstruktur eingebundener Rechner. Cyberkriminelle können daher Schadprogramme mit geringerem Aufwand einschleusen, um die Geräte zu überwachen oder sensible Daten abzugreifen. Und auf Mobilgeräten sind häufig viele persönliche und geschäftliche Daten gespeichert, darunter auch wertvolle Nutzeridentitäten für Anwendungen oder Portale, die für Cyberkriminelle hochinteressant sind.

Wie können sich Mitarbeiter und Unternehmen besser vor Hackerangriffen schützen?

POHLENZ: Zu den generischen Maßnahmen zur Absicherung der Kommunikation zählen Verschlüsselung, Firewalls, Antivirusprogramme, Spamfilter und Multi-Faktor-Authentifizierung. Das alleine aber reicht als Prophylaxe nicht aus. Gefährlich wird es vor allem dann, wenn auf einem Smartphone berufliche wie private Apps parallel eingesetzt werden. Das passiert millionenfach sowohl auf Firmen- als auch auf Privat-Handys.

Viele private Apps aber haben einen unstillbaren Appetit auf Daten aller Art – und sind damit ein latentes Sicherheitsrisiko. Mit Verboten allein lässt sich dieses Problem jedoch nicht in den Griff bekommen. Also muss es so gelöst werden, dass eine parallele Nutzung beruflicher und privater Apps grundsätzlich möglich ist, eine gegenseitige Beeinflussung dabei aber auf technischer Ebene von vornherein ausgeschlossen wird. Dafür haben sich Container-Lösungen als besonders geeignet erwiesen. Sie trennen berufliche und private Daten strikt voneinander und sorgen u.a. dafür, dass dem Zugriff privater Apps auf berufliche Informationen ein unknackbarer Riegel vorgeschoben wird.

Christian Pohlenz *hat langjährige Erfahrungen als Consultant für Infrastruktur- und Software-Projekte.*

> ***„Auch die besten Sicherheitslösungen sind nur dann erfolgreich, wenn Mitarbeiter sie akzeptieren und ordnungsgemäß anwenden.“***

Welche Rolle spielt die Mitarbeiterfortbildung für die Sicherheit von Unternehmen?

POHLENZ: Die Sicherheitsrichtlinien, die sich ein Unternehmen gibt, müssen für alle transparent sein und entsprechend geschult werden. Das Vertrauen darauf, dass solche Verhaltenskodizes und praktischen Anweisungen auch eingehalten werden, reicht als Security-Mechanismus jedoch nicht aus. Auch die besten Sicherheitslösungen sind nur dann erfolgreich, wenn Mitarbeiter sie akzeptieren und ordnungsgemäß anwenden. Die Software muss so bedienungsfreundlich wie möglich sein, darf Fehlbedienungen erst gar nicht zulassen und die Arbeit nicht blockieren. Deshalb ist der Bedienungskomfort so wichtig. Aufwendige Lösungen mit komplizierten, zeitfressenden Prozessen sind daher tabu. Die beste Sicherheitslösung nützt wenig, wenn sie im Arbeitsalltag immer wieder umgangen wird.

Ricarda Müller

GELUNGENE ERP-MODERNISIERUNG

WENN DER SIMPLE RELEASE-WECHSEL NICHT MEHR REICHT

Was bei der ERP-Einführung seinerzeit noch modern war, wird irgendwann altbewährt oder gar altbacken. Modernisierung ist daher gefragt, um die Integration, Erweiterbarkeit, Automatisierung und Sicherheit beim Betrieb laufend zu verbessern.

ZENTRALE GESCHÄFTSFUNKTIONEN WIE BUCHHALTUNG, Warenwirtschaft oder Fertigung hängen oft schon lange von einem gut funktionierenden Enterprise-Resource-Planning-System (ERP) ab. Was aber, wenn die bewährte Software den Anforderungen von heute nicht mehr gerecht wird, etwa weil es an der Integration mit externen Systemen und Anbietern hapert? Die dann nötige manuelle Eingabe durch die Belegschaft bremst die Prozesse aus, erhöht die Fehlerwahrscheinlichkeit und verdoppelt den Aufwand.

Typisch für ältere ERP-Systeme sind auch Performance-Probleme, keine Verfügbarkeit auf mobilen Geräten oder eine „angestaubte" Bedienoberfläche. All das kann zu Frustration der Mitarbeiter und zu Produktivitätsverlusten führen. Auch die Skalierbarkeit des ERP-Systems kann, z.B. aufgrund eines schlechten Anwendungsdesigns, problematisch werden, insbesondere bei rasch wachsenden Unternehmen. Oft fehlt dem ERP-System dann auch die Unterstützung für innovative Technologien, wie z.B. Künstliche Intelligenz (KI) und Machine Learning (ML).

Wer mit diesen Problemen konfrontiert ist, wird ein Upgrade der ERP-Software auf eine neue Version oder sogar einen vollständigen Austausch in Betracht ziehen. Upgrades gelten jedoch als kostspielige, zeitaufwendige und riskante Projekte, und ein Ersatz noch viel mehr. Der Entscheidungsprozess muss die richtigen Führungskräfte einbeziehen und kann einen externen Berater erfordern.

Kleine Trippelschritte statt großer Sprünge

Allerdings geht es auch anders, erklärt Stefan Müssemann, Prozessmanager Release-Management beim ERP-Anbieter Ams.Solution. Kleinere Release-Schritte sorgen seiner Meinung nach dafür, dass die Anwender einen besseren Überblick über funktionale Veränderungen behalten. Also tragen häufigere Release-Wechsel entscheidend dazu bei, von neuesten technischen Entwicklungen profitieren zu können und ein besseres Gesamtverständnis für die Software-Prozesse zu entwickeln. „Wir veröffentlichen unsere Haupt-Releases und die größeren Feature-Packs seit einiger Zeit in einem verbindlichen Turnus", erklärt Müssemann die Vorgehensweise. „Die Haupt-Releases erscheinen jeweils am 1. April jedes Jahres und die Feature-Packs sechs Monate später am 1. Oktober. Die Anwender können die Aktualisierung ihrer Systeme auf dieser Basis zu jedem Zeitpunkt exakt und vorausschauend planen. In den Perioden zwischen den fixen Terminen erscheinen dem aktuellen Bedarf entsprechend und in etwas unregelmäßigeren Zeitabständen sogenannte Service-Packs. Der Support für ältere Versionen endet in der Regel drei Jahre nach Freigabe der jeweils nächsten Hauptversion."

Viele ERP-Anwender beherzigen aber aufgrund ihrer Erfahrungen noch das Motto „Never change a running system“, weil in der Vergangenheit dem Release-Wechsel eine intensive Planungsphase vorausging und der spätere Organisations- und Testaufwand immens hoch und zeitraubend war, was wiederum zu langen Umstellungsphasen führte. Es wurden damit insgesamt sehr viele Ressourcen über längere Zeiträume hinweg gebunden, insbesondere in den IT-Teams. Das eigentliche Problem war jedoch der anfängliche „Blindflug“, so Müssemann, „weil Störungen erst dann sichtbar wurden, wenn das System in den Echtbetrieb ging. Hier wirken wir mit unserer von uns selbst entwickelten Testautomation entgegen, die den Testaufwand immens reduziert“.

Das Problem: Längst nicht jeder ERP-Hersteller ist technisch und organisatorisch so weit, dass er regelmäßig kleine Release-Wechsel mit wenig Impact auf Infrastruktur, Geschäftsprozesse und Belegschaft anbieten kann. Erschwerend kommt hinzu, dass so manches Mal gar kein Upgrade mehr möglich ist, etwa weil der Hersteller insolvent wurde oder die Weiterentwicklung eingestellt hat.

EINEN AUSWEG AUS DIESEM DILEMMA VERSPRECHEN LOW-CODE-PLATTFORMEN.

Letzteres kommt häufiger vor, als man denkt – selbst der ERP-Marktführer SAP hat seine bewährte Software für 2027 abgekündigt, um sie durch den 2015 vorgestellten Nachfolger S/4 Hana abzulösen. Das heißt für die Kunden: Sie müssen das ERP-System neu erwerben, obwohl sie einen gültigen Wartungsvertrag mit dem Hersteller haben, die Software neu installieren und konfigurieren – und all das mit der Randbedingung, dass S/4 Hana auch acht Jahre nach der Markteinführung nicht die volle Funktionalität des Vorgängers hat. Sebastian Westphal, Technologievorstand der DSAG, fordert daher „schnellstmöglich eine klare Perspektive und entsprechende Migrationsszenarien“.

Rückkehr zur Individual-Software

Einen Ausweg aus diesem Dilemma zwischen Upgrade und Austausch versprechen Low-Code-Plattformen, mit denen Fachabteilungen selbst passgenaue Lösungen entwickeln können. Die Idee: eine neue App entwickelt von der Buchhaltung, Dashboards angepasst von der Logistik und Workflows konzipiert vom Marketing. All das muss die IT-Abteilung nicht mehr programmieren, sondern das können auch diejenigen, die diese Apps täglich nutzen. Software entsteht dabei nicht mehr durch das Schreiben von Quellcode, sondern mithilfe vorgefertigter Bausteinen, die sich grafisch per Klick zusammenstellen lassen.

Ein neues Diskussionspapier des Branchenverbands Bitkom mit dem Titel „Programmieren für Dummies: Bedeutet Low Code das Ende von ERP?“ beleuchtet, wie sich Low-Code-Plattformen auf die klassische ERP-Welt auswirken und wie sich diese integrieren lassen. „Die klassische ERP-Welt wird durch Low-Code-Plattformen nicht ersetzt, sondern ergänzt“, sagt Nils Britze, Bereichsleiter Digitale Geschäftsprozesse beim Bitkom. „Und die ERP-Anbieter haben die Chance, sich wieder stärker auf die Entwicklung und Optimierung der Kernfunktionen zu konzentrieren.“

Nicht überall, wo Low Code draufsteht, ist auch Low Code drin, warnt Markus Schindler, CTO bei Step Ahead. Manches Produkt werde zwar als Low Code vermarktet, doch unter der schicken Oberfläche verbergen sich oft nur die herkömmlichen starren Programme. „Das volle Potenzial einer Low-Code-Entwicklungsplattform – insbesondere Flexibilität, Benutzerfreundlichkeit und einfache Wartung – lässt sich jedoch nur dann vollständig nutzen, wenn das System von Grund auf und durchgängig in Low Code programmiert ist“, gibt Schindler zu bedenken.

Ernst zu nehmende ERP-Systeme auf Low-Code-Basis beinhalten seiner Meinung nach sämtliche Bausteine, aus denen auch traditionelle Systeme bestehen. Dies beginnt bei der Anwendungslogik für die Arbeitsabläufe, dem Datenmodell, APIs für die Integration externer Ressourcen und setzt sich fort bis hin zur Benutzerschnittstelle. „Nur wenn jene Systeme komplett in einer Low-Code-Umgebung entwickelt wurden, lassen sich die Vorteile hinsichtlich Flexibilität, Benutzerkomfort und Updates vollständig nutzen“, so Schindler. „Dies gilt vor allem für Datenbankmodelle, die Speicherprozesse und die Businesslogik. Immerhin müssen sie komplexe Geschäftsaufgaben zuverlässig erfüllen.“ Deshalb sei durchgängiger Low Code „deutlich mehr als nur ein hübsches ERP-Make-up“.

BERTHOLD WESSELER

*Laut **Stefan Müssemann** von Ams. Solution sorgen kleinere Release-Schritte dafür, dass die Anwender einen besseren Überblick über funktionale Veränderungen behalten.*

***Sebastian Westphal,** DSAG, fordert von SAP „schnellstmöglich eine klare Perspektive und entsprechende Migrationsszenarien“.*

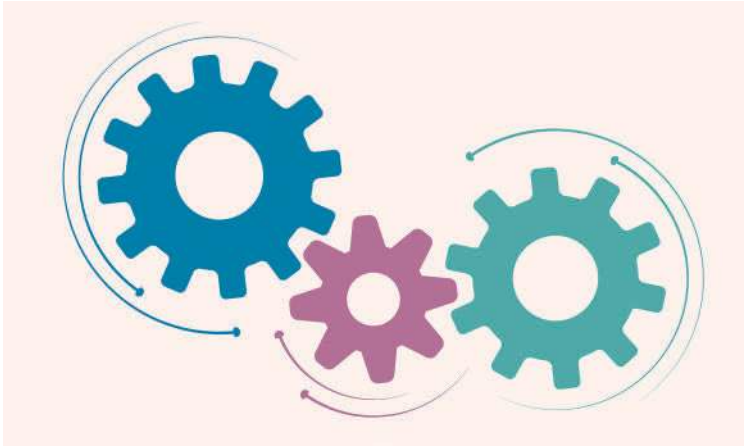
***Nils Britze,** Bitkom: „Die klassische ERP-Welt wird durch Low-Code-Plattformen nicht ersetzt, sondern ergänzt.“*

***Markus Schindler,** Step Ahead, warnt: „Nicht überall, wo Low Code draufsteht, ist auch Low Code drin.“*


„Personalarbeit ist wie ein Puzzle. Toll, wenn alles zusammenpasst.“
Cheri, Personalleiterin
Sage HR Cloud Software ermöglicht einen optimalen Workflow, um ein stimmiges HR Puzzle zusammenzusetzen.
Besuchen Sie Sage.com
Sage
helping business flow

STANDARD- ODER INDIVIDUAL-SOFTWARE?

EINE CHANCE FÜR INTERNE PROZESSE



Kaum ein IT-System ist derart eng mit den Prozessabläufen eines Unternehmens verbunden wie das *ERP-System*. Die Migration auf eine neue Software-Version stellt somit die perfekte Gelegenheit dar, interne Prozesse zu analysieren, zu hinterfragen und – bei Bedarf – einer Generalüberholung zu unterziehen, meint Ralf Bachthaler, Vorstand bei Asseco Solutions, im Kommentar.

Ralf Bachthaler *war lange Jahre beim ERP-Hersteller Infor bzw. bei den Vorgängerfirmen Rembold+Holzer und später Brain tätig.*

Wird die Belegschaft bei Veränderungen des Enterprise-Resource-Planning-Systems (ERP) eingebunden, steigt nicht nur die Effizienz der Lösung, auch das Unternehmen an sich profitiert. Am Anfang stehen nicht wenige IT-Verantwortliche, die mit der Modernisierung ihrer Lösung betraut sind, vor der Frage: Soll sich ein ERP-System an das Unternehmen anpassen oder das Unternehmen an das System? Die richtige Antwort auf diese Frage ist besonders dann wichtig, wenn der Sprung zwischen alter und neuer Version besonders groß ist und die Modernisierung quasi einer Neueinführung gleichkommt.

Altlasten ausräumen

Auch wenn die Versuchung groß sein mag, im Kontext einer Migration alles beim Alten zu belassen: In nahezu allen Unternehmen finden sich Prozesse, die ineffizient ablaufen oder durch die Weiterentwicklung des Unternehmens bereits obsolet geworden sind. Die neue ERP-Version daran anzupassen, würde nicht nur unnötigen Zeit- und Kostenaufwand nach sich ziehen, sondern im schlimmsten Fall sogar die Effizienz des modernisierten Systems schmälern. Statt diese Altlasten mitzunehmen, sollten Unternehmen besser die Gelegenheit nutzen, auch die eigenen Prozesse unter die Lupe zu nehmen und effizienter zu gestalten.

Um eine solche Optimierung vorzunehmen, ist im ersten Schritt eine Offenlegung der bisherigen praktischen Abläufe vonnöten. Nicht selten stößt diese jedoch auf Widerstand in der Belegschaft. Detaillierte Auskunft über die eigene Arbeitsweise zu geben, geht oft mit der Angst einher, persönliches Spezialwissen preiszugeben und sich damit ersetzbar zu machen. Außerdem gehen die eingespielten Prozesse leicht von der Hand, während Neuerungen oft auf den ersten Blick eher als Verschlechterung wahrgenommen werden.

Ohne die Rückendeckung der Belegschaft sind Modernisierungsvorhaben jedoch von Anfang an zum Scheitern verurteilt. Im schlimmsten Fall bildet sich dann interner Widerstand gegen die Maßnahmen, überarbeitete Prozesse werden nach Möglichkeit umgangen oder gar boykottiert.

Die Karten auf den Tisch legen

Um ein solches Szenario zu vermeiden, ist es entscheidend, eine ERP-Modernisierung von Beginn an als gemeinsames Projekt von Management und Belegschaft zu begreifen und Fachkräfte aus allen Abteilungen in die Planung und Umsetzung der Neuerungen miteinzubeziehen. Eine transparente Kommunikation sorgt dabei zu jeder Zeit für die Nachvollziehbarkeit der erforderlichen Prozessanpassungen.

„OHNE DIE RÜCKENDECKUNG DER BELEGSCHAFT SIND MODERNISIERUNGSVORHABEN VON ANFANG AN ZUM SCHEITERN VERURTEILT."

Hilfreich kann zudem sein aufzuzeigen, wie ein zusätzlicher Arbeitsschritt auf einer folgenden Prozessstufe zu einer deutlichen Erleichterung führt. So sehen die Mitarbeiter nicht nur ihren eigenen Mehraufwand, sondern werden sich darüber bewusst, wie ihre Kollegen im Folgeschritt ganz konkret davon profitieren und der Gesamtprozess an sich effizienter wird. Das Ziel der ERP-Umstellung besteht ja in der Regel darin, durch neue Funktionen und verbesserte Abläufe für mehr Effizienz im Tagesgeschäft zu sorgen. Veraltete interne Prozesse werden dabei schnell zum Flaschenhals. Entsprechend sollte eine entsprechende Systemmodernisierung stets Hand in Hand mit der kritischen Betrachtung der eigenen Unternehmensabläufe gehen.

Wer die Vorteile einer solchen Prozessgeneralüberholung offen kommuniziert und frühzeitig für Verständnis wirbt, schafft eine bestmögliche Basis für die Unterstützung der Belegschaft. Und diese ist der eigentliche Erfolgsfaktor: Denn nur wenn auch die späteren Endanwender mit an Bord sind, stellt eine Modernisierung tatsächlich die Weichen für ein effizientes Arbeiten in der Zukunft.

Das besondere Fahrgefühl *der Boote wird hervorgerufen durch die „dem Wasser weitgehend enthobene Trimmlage" – oder wie der ehemalige Firmenchef Walter Boesch es nannte: „Horizon Gliding".*

Boesch Motorboote AG

Branche: Holzsportboote und küstentaugliche Cruiser
Gründungsjahr: 1920
Hauptsitz: Kilchberg bei Zürich (Schweiz)
Mitarbeiterzahl: 35 (Stand 2020)

www.boesch.swiss/de/

VOLLE KRAFT VORAUS

ERP-SOFTWARE MIT FOKUS AUF LOSGRÖSSE 1+

Um ihre Marktposition auszubauen, haben sich die Verantwortlichen bei Boesch Motorboote für die Implementierung der Multiprojektmanagement-Software Ams.erp entschieden – vor allem, weil die ERP-Standard-Software auf die speziellen Erfordernisse der Losgröße 1+ zugeschnitten ist.

Der Name Boesch Motorboote besitzt unter Bootseignern und Wassersportlern einen exzellenten Ruf. Das traditionsreiche, 1920 gegründete Schweizer Unternehmen gehört zu den renommiertesten Konstrukteuren und Baumeistern von Holzsportbooten und küstentauglichen Cruisern. Bislang setzten die Schweizer zwei parallel laufende Software-Produkte mit unterschiedlichen Schwerpunkten ein. Zum einen handelte es sich um eine Software für die Finanzbuchhaltung, die Arbeitszeiterfassung und die allgemeine Projektverwaltung, zum anderen um eine in die Jahre gekommene PPS-Software, die im Laufe der Zeit stark an die Abläufe bei Boesch angepasst worden war.

Vor allem Letztere konnte den auf allen Ebenen wachsenden Ansprüchen seitens der Kunden und Lieferanten immer weniger gerecht werden. „Mit unserer alten Systemlandschaft war die Realisierung der heute geforderten kürzeren Liefer- und Projektlaufzeiten nicht mehr vollumfänglich möglich, vor allem nicht vor dem Hintergrund der zunehmender kundenspezifischer Produktanforderungen", beschreibt ERP-Projektleiter Marcel Stricker die Ausgangslage, die zur Suche nach einem ERP-System führte. Schnell war klar, dass künftig nur noch mit einem integrierten Gesamtsystem anstelle des bisherigen „Doppelpacks" gearbeitet werden sollte.

Materialbewirtschaftung gefragt

Ein Berater brachte den Anbieter ins Spiel. Die Entscheidungsträger im Unternehmen folgten seiner Einschätzung, dass die Software für den umrissenen Anwendungsbereich am besten geeignet war: „Bei den Präsentationen und im Rahmen eines Vorprojekts vermochte uns das System schnell zu überzeugen", bestätigt Stricker. Die Fokussierung des gewählten ERP-Systems auf die Einzel-, Auftrags- und Variantenfertigung spielte dabei die entscheidende Rolle, denn es sollte die enorme Fertigungstiefe, die zahlreichen kundenbezogenen Spezialitäten und die vielen Boesch-spezifischen Artikel flexibel abbilden können. In diesem Zusammenhang bezeichnet Stricker die Möglichkeit, alle Warenbestände und Liefertermine stets tagesaktuell und in Echtzeit einsehen zu können, als eines der wichtigsten funktionalen K.-o.-Kriterien, denn Kontrollgänge durch das Lager, die aufgrund der Arbeit mit veralteten Daten bislang notwendig waren, entfallen künftig.

Auf prozesstechnischer und betriebswirtschaftlicher Ebene versprechen sich die Schweizer Bootsbauer vor allem immense Einsparungen bei den Materialrüstzeiten infolge des Wegfalls der Lagerbestandskontrollen unter dem Jahr. Außerdem soll die Aufnahme der Inventurbestände massiv optimiert werden können, sodass den Mitarbeitern im Bereich der Material- und Lagerbewirtschaftung durch die Entlastung mehr Zeit für wertschöpfende Aufgaben bleibt.

GUIDO PIECH

DREI FRAGEN AN ...

Bernd Rech, *Vertriebsleiter bei Nissen & Velten*

Wolfgang Kobek, *General Manager International Business bei Infor*

Das altbewährte Enterprise-Resource-Planning-System (ERP) beizubehalten, kann durchaus die richtige Entscheidung sein, selbst wenn es modernisiert werden muss, damit das Unternehmen in der Branche wettbewerbsfähig bleibt. Entscheidend bei der Modernisierung ist die Wahl des passenden Ansatzes, denn die Modernisierung von Legacy-ERP erfordert mehr als nur ein paar kleinere Upgrades und Erweiterungen.

Es gilt abzuwägen, ob der Austausch oder eine grundlegende Überholung die Unterbrechung des Geschäftsbetriebs wert ist. Dabei dürfen auch die Stärken des bisherigen ERP-Systems nicht übersehen werden, beispielsweise die eingespielten Abläufe im Unternehmen und der souveräne Umgang der Belegschaft mit dem System. Bei der Entscheidung lohnt sich auch der Fokus darauf, welche Eigenschaften am Legacy-ERP am dringendsten einer Verbesserung bedürfen. Auch die Modernisierungskosten müssen berücksichtigt werden. Es gilt abzuwägen, ob man sich die Kosten für einen bestimmten Modernisierungsansatz leisten kann. Falls beispielsweise die Performance des Altsystems nicht stimmt, kann schon ein simples „Rehosting" reichen. Refactoring oder Rebuild sind andere etablierte Alternativen. Am kostspieligsten, zeitaufwendigsten und riskantesten ist die Strategie des Ersatzes einiger und aller Komponenten des alten ERP-Systems (Replace), falls diese ineffektiv sind und die heutigen Anforderungen nicht mehr erfüllen. IT-MITTELSTAND hat zwei Kenner des Markts gefragt, welche Punkte ein Mittelständler bei der Auswahl des für ihn passenden Konzepts zur ERP-Modernisierung im Auge behalten sollte.

ITM: *Herr Rech, Herr Kobek, wenn Sie einen Blick in die ERP-Landschaft des deutschen Mittelstands werfen: In welchen Bereichen sehen Sie den dringendsten Modernisierungsbedarf?*

„Aus unserer Sicht ist Modernisierung idealerweise kein großes Projekt, sondern ein kontinuierliches Mitgehen des Anwenders mit den Release-Wechseln des Herstellers."

Bernd Rech

RECH: Darauf gibt es zwei Antworten. Die eine ist eher struktureller Natur: In vielen Unternehmen laufen nach wie vor recht alte ERP-Systeme. Es kommt gar nicht so selten vor, dass wir 20 Jahre alte Lösungen ablösen. Da ist es zum Teil schon so, dass sowohl der Hersteller-Support nicht mehr gewährleistet ist als auch die Know-how-Träger im Unternehmen vor dem Ruhestand stehen. In diesen Fällen ist der Modernisierungsbedarf im Unternehmen also flächendeckend. Da ist es dann manchmal schon fünf vor zwölf. Auf der funktionalen Seite sind die Schmerzen oft im Bereich fehlender Schnittstellen bzw. mangelnder Kommunikationsfähigkeit über die Unternehmensgrenzen hinweg zu finden. Speziell im B2B-Handel gibt es Herausforderungen bei E-Commerce und Vertriebskanalintegration. In vielen Fällen wird auch noch kein Lagerverwaltungssystem eingesetzt. Gerade vor dem Hintergrund der Erfahrung der Verwundbarkeit von Lieferketten in der Corona-Pandemie hat das eigene Lager enorm an Bedeutung für die Lieferfähigkeit gewonnen.

Fragen von **Berthold Wesseler**

„Als Faustregel sollte gelten, dass nur etwa die Hälfte bis zwei Drittel aller existierenden Prozesse unverändert übernommen und weitere gut 30 Prozent mittels einfacher Rekonfigurationen angepasst werden sollten."

Wolfgang Kobek

KOBEK: Letztlich lässt sich der verbliebene Modernisierungsbedarf in Unternehmen nicht zwingend an einzelnen Bereichen festmachen, sondern an der Art und Weise, wie modernisiert wird. Entscheiden sich Unternehmen etwa für den Schritt in die Cloud, so tun sie dies zu häufig noch mit der Absicht, ihre bestehenden Prozesse aus dem analogen Zeitalter möglichst unangetastet in die Cloud zu transferieren. Diese Prozesse werden also einzeln digitalisiert, aber nicht das gesamte Unternehmen an sich und auf eine kohärente Weise. Entscheidungsträger scheuen davor zurück, lieb gewonnene Abläufe – gerade in einem komplexeren Kontext – zugunsten einer vollständigen Transformation ihres Geschäfts fallen zu lassen, die ihnen jedoch ganz neue Möglichkeiten eröffnen würde. Gerade im Hinblick auf Datenanalysen, idealerweise voll automatisiert und unter Einbindung beispielsweise von Zulieferern und anderen Partnern, besteht ein riesiges Potenzial zur Wertschöpfung.

ITM: *Anhand welcher Kriterien lässt sich entscheiden, ob eine Modernisierung oder die Ablösung des altbewährten ERP-Systems mehr Sinn macht?*

KOBEK: Hierfür muss auf innerbetriebliche und externe Faktoren geachtet werden. Kann die existierende IT-Landschaft noch Kapazitäten aufbringen für weiteres Geschäftswachstum, ist sie insgesamt in der Lage, alle benötigten Funktionen und Prozesse abzubilden, ohne dass wesentliche Nachbesserungen erforderlich sind? Falls Ja, ist das auf jeden Fall ein gutes Zeichen. Aber gerade die letzten Jahre haben auch gezeigt, dass im Härtefall sehr schnell von alten Gewissheiten Abstand genommen werden muss. Wir sehen deutliche Trends hin zu mehr Volatilität in den Lieferketten, aber auch zu neuen Arbeitsweisen – etwa aus dem Homeoffice heraus – sowie zu mehr Nachhaltigkeit. Auch darf die Sicherheit des eigenen IT-Systems nicht mehr vernachlässigt werden. Allein aus rein rechtlichen Gründen ist es nicht mehr möglich, diese Entwicklungen einfach zu ignorieren – und spätestens, wenn rechtlichen Anforderungen nicht mehr ohne größere Mühen entsprochen werden kann, ist es höchste Zeit für einen vollständigen Wechsel. An der Cloud führt dann allerdings kein Weg mehr vorbei, denn der Markt entwickelt sich zu schnell weiter, um noch aus eigener Kraft immer auf dem neuesten Stand bleiben zu können.

RECH: Die erste Frage aus Anwendersicht ist sicher, inwiefern eine gangbare Modernisierungsoption des bestehenden Software-Anbieters zur Verfügung steht. Und die zweite Frage lautet, was aus der Substanz des aktuellen Systems dabei mit welchem Aufwand übernommen werden kann – also etwa Datenbanken, Logik und Prozesse. Je teurer und aufwendiger sich die Kalkulation eines solchen Projekts darstellt und je näher es damit de facto an eine Software-Neueinführung rückt, desto interessanter wird es für das Anwenderunternehmen sein, auch aktuelle, alternative ERP-Lösungen anderer Software-Häuser am Markt in Betracht zu ziehen und zu bewerten. Für uns ist das nicht selten auch eine Konstellation, in der es zu Neukundengewinnen kommt.

ITM: *Worauf kommt es bei einem Projekt zur Modernisierung des ERP-Systems vor allem an, damit es erfolgreich abgeschlossen werden kann?*

KOBEK: Wie immer im Projektmanagement steht die Frage im Zentrum, welches konkrete und messbare Ziel ich überhaupt erreichen will. Den Weg dahin sollten dann Provider, Partner und Kunden gemeinsam bestimmen und gehen – je enger die Abstimmung, desto besser lassen sich etwa unerwartete Hindernisse aus dem Weg räumen. Als Faustregel sollte gelten, dass nur etwa die Hälfte bis zwei Drittel aller existierenden Prozesse unverändert übernommen und weitere gut 30 Prozent mittels einfacher Rekonfigurationen angepasst werden sollten. Die verbliebenen Abläufe gilt es einzeln zu betrachten und gegebenenfalls zu ersetzen oder ganz fallen zu lassen.

RECH: Aus unserer Sicht ist Modernisierung idealerweise kein großes Projekt, sondern ein kontinuierliches Mitgehen des Anwenders mit den Release-Wechseln des Herstellers. Wir sehen als Anbieter im Mittelstand auch, dass gerade kleinere Unternehmen ungern jährliche Updates durchführen. Aus diesem Grund bieten wir in unserer Release-Planung regelmäßig sogenannte Long-Term-Releases an, die dann für jeweils drei Jahre unterstützt werden. Wir haben allerdings den Vorteil, dass kundenspezifisches „Customizing" problemlos von Release zu Release mitgenommen werden kann. Das ist in unserer Systemarchitektur so angelegt. Der Anreiz, ein aktuelles Update schnell durchzuführen, ist erfahrungsgemäß dann besonders groß, wenn neue Features für den jeweiligen Kunden einen großen Mehrwert schaffen. Eine weitere, unterschätzte Facette des Themas „Modernisierung" ist neben dem Umsetzen von Updates die Vertiefung des Nutzungsgrads der bereitgestellten Funktionen der ERP-Software. Ein Projekt erfüllt beim Echtstart definierte Leistungsumfänge und Ziele. Unternehmen verändern sich aber und Funktionsumfänge der Software wachsen. Es ist deshalb vernünftig, die Unternehmensprozesse kontinuierlich zu überprüfen und die zur Verfügung stehenden Funktionen der Software auszuschöpfen, um die eigene Unternehmens-Performance immer wieder zu optimieren. Falls sich allerdings ein Modernisierungsprojekt von Aufgaben und Umfang her einem Neuprojekt annähert, dann ist es sinnvoll, es auch wie eines anzugehen – d.h., ein Projektmanagement mit einem Projektteam, Key Usern und Meilensteinen bietet sich an.

VORSCHAU AUF HEFT 5/2023

STRATEGIE

WEITERBILDUNG IM IT-BEREICH

DAS THEMA „IT-WEITERBILDUNG“ IST IN ALLER MUNDE und wird doch viel zu oft sträflich vernachlässigt. Gerade im Mittelstand muss sich in diesem Bereich noch einiges tun, damit Mitarbeiter nicht zum Ziel von z.B. Cyberangriffen werden. Doch wie genau können abwechslungsreiche E-Learnings und Co. in der heutigen von Krisen geprägten Zeit Unternehmen unterstützen und dafür sorgen, dass sie langfristig erfolgreich bleiben?

WEITERE THEMEN

- IT-Dienstleistungen, Outsourcing
- Logistik

ERSCHEINUNGSTERMIN

22. Mai 2023

REDAKTIONSSCHLUSS

27. April 2023

ANZEIGENSCHLUSS

27. April 2023

IT MITTELSTAND
IT-BUSINESS IM MITTELSTAND

IMPRESSUM

Herausgeber: Klaus Dudda

Redaktion: Lea Sommerhäuser (LS, verantwortlich für den Inhalt), Berthold Wesseler (WE), Ricarda Müller (RM), Alexander Lorber (AL)

E-Mail Redaktion: redaktion@itmittelstand.de

www.itmittelstand.de

Ständige Mitarbeit: Siegfried Dannehl (SD), Daniela Hoffmann (DH), Ingo Steinhaus (IS), Markus Strehlitz (MST)

Autoren dieser Ausgabe: Ralf Bachthaler, Dr. Christopher Jahns, Pawel Jankowski, Benjamin Jansen, Luzia Langhans, Simeon Mussler, Dr. Karsten Nohl, Guido Piech, Fabien Rech, Michael Scheffler, Dr. Sebastian Schmerl, Dr. Dominik Schürmann, Benjamin Springub

VERLAG

MEDIENHAUS Verlag GmbH
Bertram-Blank-Str. 8 · 51427 Bergisch Gladbach
Tel.: 02204/9214-0 · Fax: 02204/9214-30

E-Mail Verlag: info@medienhaus-verlag.de

Geschäftsführer: Klaus Dudda

Grafik/Layout: Karoline Birkert, Kathrin Pohl, Katharina Schwadorf (medienzentrum süd, www.mzsued.de), Gerhard Samland

Titelfoto: Claus Uhlendorf

Bildnachweis: Boesch Motorboote (47), Claus Uhlendorf (Titel, 4, 18-25), Daimani (4, 16+17), Detecon (7), Gabal Verlag (15), Getty Images/iStock/Getty Images Plus (3-6, 8-10, 14+15, 26+27, 29+30, 32-37, 39, 41-43, 46, 48-50), Getty Images/OJO Images (38+39), Heide Velten (40), Ionos (6) sowie Produkt-, Schmuck- und Personenfotos der genannten Anbieter/Hersteller.

WISSEN, WAS ZÄHLT
Geprüfte Auflage
Klare Basis für den Werbemarkt

LAC/2011
Mitglied

ANZEIGENVERKAUF/MEDIABERATUNG

Gesamtanzeigenleiter: Thomas Büchel

Leiter Verkauf: Hendrik Dreisbach

Assistenz: Susanne Rosenbaum

Anzeigenverwaltung: Jutta Herkenrath

E-Mail Anzeigen: anzeigen@medienhaus-verlag.de

Anzeigenpreise: Es gilt die Anzeigenpreisliste vom 1.1.2023

ABONNEMENT

Jahresbezugspreis: Inland 75,- EUR
inkl. Versand und MwSt., Europa 99,- EUR inkl. Versand

Erscheinungsweise: 10 x jährlich

Abonnenten-Service: +49(0)2204/9214-0

Druck/Druckunterlagen:
L.N. Schaffrath GmbH & Co. KG DruckMedien
www.schaffrath.de

Gedruckt auf chlorfrei gebleichtem Papier

presserat
IT-MITTELSTAND unterstützt die freiwillige Selbstkontrolle der deutschen Presse.

Hinweis:
In unseren Publikationen verwenden wir ausschließlich das generische Maskulinum und berichten „diskriminierungssensibel“. Auf Sonderzeichen wie Genderstern, Unterstrich und Doppelpunkt, die auch nicht-binäre Geschlechtsidentitäten abbilden sollen, verzichten wir im Sine der Prägnanz und Verständlichkeit der Texte generell.

IT-ZOOM
WORLD OF TECHNOLOGY

JEDEN TAG NEU!

TECHNOLOGIE-NEWS MIT FORMAT

PSI Software: flexibel und zukunftssicher

ERP-System als Taktgeber für die smarte Fabrik

www.psi-automotive-industry.de

LogiMAT

Lernen Sie uns kennen
und besuchen Sie uns in
Halle 8 | Stand A41.

Intelligent Production

PSI