Jagd nach Black Hats · Transparente Lieferketten · Optimierte Kauferlebnisse

ÖSTERREICH: 4,70 EUR
LUXEMBURG: 4,95 EUR
SCHWEIZ: 8,40 SFR
**DEUTSCHLAND: 4,30 EUR**

4 | 2023

BUSINESS · PEOPLE · COMPANIES

# IT DIRECTOR

G 31227 I WWW.IT-DIRECTOR.DE

Nº 4

**TITELINTERVIEW**

# Die Supply Chain sicher im Griff

## Im Interview erläutert Klaus Jetter,

Regional Vice President DACH von WithSecure, wie Unternehmen mit Outcome-based Security ihre Geschäftsziele einhalten können.

**Seite 18**



MEDIENHAUS VERLAG
Postfach 30011l · 51411 Bergisch Gladbach
»Entgelt bezahlt«

**SPECIAL: IT-SECURITY**

**Unternehmen im Visier der Cyberkriminellen** Seite 26

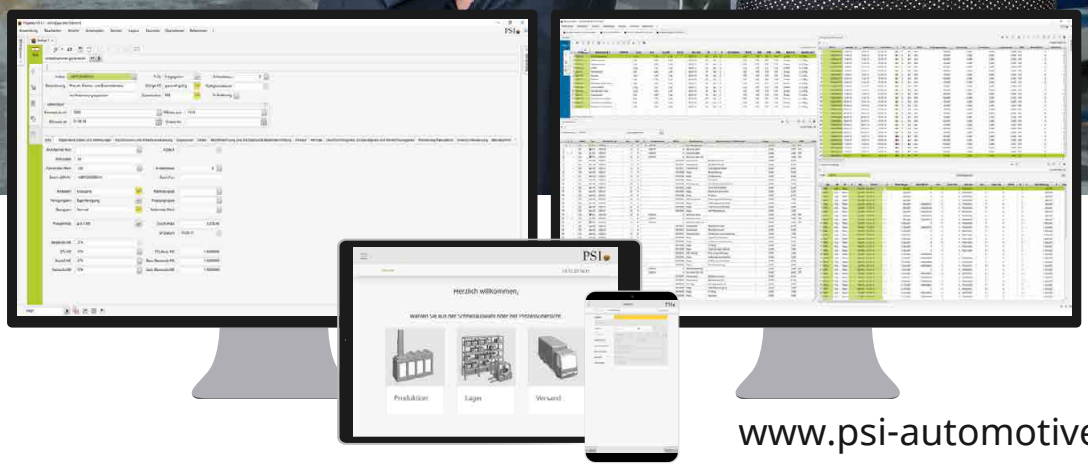
**DIGITALISIERUNG**

**Der Wandel in den Köpfen** Seite 42

4 195039 104303 04

Mehr als Software

**Wir stehen nicht nur für exzellente Software, sondern auch für kompetente Beratung und Know-how-Transfer**



www.psi-automotive-industry.de

LogiMAT

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

# Intelligent Production

PSI

# Wie sicher sind Deutschlands Unternehmen?

*> Die Bedrohungslage wächst – zumindest nach Ansicht von 93 Prozent der IT-Experten, die in einer Studie des Eco-Verbands befragt wurden. Diese Einschätzung wird von diversen Medienberichten unterstützt. Immer häufiger ist von Cyberattacken, Erpressungen und Datendiebstahl zu hören. Einer der möglichen Faktoren für diese Entwicklung ist der Russland-Ukraine-Krieg. Das belegt u.a. eine Umfrage im Auftrag des Digitalverbands Bitkom. Sie zeigt, dass insgesamt rund 84 Prozent der Unternehmen im vergangenen Jahr von Cyberangriffen betroffen waren, weitere 9 Prozent gehen davon aus. Dabei sind die Angriffe aus Russland und China zuletzt 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).*

**von Ricarda Müller,**
*Redaktion IT-DIRECTOR*

*Erst kürzlich forderte die Gewerkschaft der Polizei (GdP) einen besseren Schutz der kritischen staatlichen Infrastruktur. Dies resultierte aus zahlreichen Cyberattacken auf Polizeibehörden und Websites mehrerer Landesregierungen. Die Polizei in Bund und Ländern benötige einen „gemeinsamen und starken Schutzschild gegen Cyberangriffe", sagte der stellvertretende GdP-Bundesvorsitzende, Alexander Poitz.*
*Auch die Experten, die in unserem IT-Security-Special ab Seite 26 zu Wort kommen, berichten von einer wachsenden Bedrohungslage – und geben Tipps, wie Unternehmen dieser begegnen können. <*

*Viel Spaß beim Lesen dieser Ausgabe!*

*Ricarda Müller*

# INHALT

2023 > APRIL

## 26 ZUGRIFF AUS DEM NETZ

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



**Die Höhen und Tiefen der Digitalisierung:** *Wie kommt die Digitale Transformation in der Praxis voran?*

## 42

### STRATEGIE > DIGITALISIERUNG



### STANDARDS

## Neue Geschäftsführerin ernannt

> Seit dem 1. April 2023 ist Alexandra Hiendlmeier – neben CEO Stefan Hansen und COO Ralf Malter – neues Mitglied der Geschäftsführung von NTT Data in der DACH-Region. Hansen und Malter arbeiten mit Alexandra Hiendlmeier in ihrer Rolle als CFO bereits seit Jahren eng und erfolgreich zusammen. Als neue Geschäftsführerin übt sie diese Rolle weiterhin aus und verantwortet die Bereiche „Finance", „Controlling", „Purchasing" sowie „Workplace & Mobility". Alexandra Hiendlmeier ist seit 16 Jahren in unterschiedlichen Positionen für den IT-Dienstleister tätig. Ursprünglich kam sie von einer Managementberatung und hat bei dem Unternehmen zunächst die Business Unit Finance Transformation mit aufgebaut und geführt. Anschließend war sie im Business Development sowie im Marketing tätig. 2017 wechselte Hiendlmeier zurück zu den Finanzen, erst als Leiterin Controlling, dann im Jahr 2021 als CFO für Deutschland, Österreich und die Schweiz. Gemeinsam mit ihren Kollegen will sie den erfolgreichen Wachstumskurs des Unternehmens nun weiter vorantreiben. <

*Mit ihrer Sachkenntnis und Führungsstärke wird* **Alexandra Hiendlmeier** *die Zukunft des Unternehmens gestalten.*

**Im Internet:** https://de.nttdata.com

# Verstärkung für Technologie-Entwicklung

**Stuttgart wird im Bereich „Automotive-IT" noch stärker: Im vergangenen Quartal eröffnete Cognizant Mobility in der Großstadt einen Standort für IT-Entwicklung.**

> Das Unternehmen gehört zum Cognizant-Konzern, der mit 355.000 Mitarbeitern einer der größten IT-Dienstleister weltweit ist. Schwerpunkt in Stuttgart soll die Technologie-Entwicklung rund um das Software-definierte Fahrzeug sein. Als neuer Arbeitgeber in der Region wird das Unternehmen besonders für Entwickler mit ersten Berufserfahrungen in den Bereichen „Software" und „Elektronik" attraktiv sein.
„Einen neuen Standort aufzubauen, ist immer eine besondere und spannende Aufgabe. Neue Mitarbeiter können sich dabei besonders viel einbringen. Zum einen sind sie in der Lage, sich dadurch selbst weiterzuentwickeln und ihr Skillset auszubauen. Zum anderen wirken sie so auch direkt an der Entwicklung des Standorts mit – auch wenn wir einer der Arbeitgeber waren, die in Bezug auf den Arbeitsstandort der Mitarbeiter schon sehr früh die Möglichkeit für Full-Remote-Work geschaffen haben", so Niederlassungsleiter Mohamed Lüdke. <

*In* **Stuttgart** *will das IT-Unternehmen die Automobilindustrie mit entsprechenden Technologien und Skills unterstützen.*

**Im Internet:** www.cognizant.com

# Neuer Name für T-Systems MMS

**Im Rahmen einer strategischen Neuausrichtung wechselt die T-Systems Multimedia Solutions GmbH ab sofort zur Deutschen Telekom AG.**

> Daher erhält das Unternehmen einen neuen Namen und firmiert nun unter Deutsche Telekom MMS GmbH. Mit rund 2.200 Digitalexperten an neun Standorten in Deutschland bringe die Firma weiterhin ihr Know-how für die Umsetzung digitaler Strategien für ihre Kunden ein. Auf Personal und Kunden habe die Umfirmierung keine weiteren Auswirkungen.
„Wir verankern uns tief in die Digitalstrategie der Deutsche Telekom und haben so noch besser die Chance, Kunden durch Digitalisierung voranzubringen und dabei den Konzern auf seinem Weg zur Leading Digital Telco zu unterstützen. Das fühlt sich gut an und ich freue mich auf die gemeinsamen Erfolge", so CEO Ralf Pechman. <

**Im Internet:** www.telekom-mms.com

# Speichern und sparen mit Hybrid Storage

**Im Kommentar** erklärt **Stefan Käser,** Solution Architect bei Doublecloud, ob Hybrid Storage der optimale Weg für den Umgang mit Big Data ist.

> Auch in der Cloud-Ära und trotz neuer Speichertechnologien wie NVMe (Non-Volatile Memory Express) müssen sich Unternehmen heute immer noch zwischen schnellem Daten-Handling oder kostengünstiger Speicherung entscheiden. Hybrid Storage ist gerade dabei, sich auch in Sachen „Datenspeicherung" als optimale Lösung für viele Anforderungen durchzusetzen. Es ist ein Ansatz, welcher sowohl Cloud-native als auch lokale Ressourcen nutzt. Ziel ist es, das Beste aus beiden Welten in einer gemeinsamen Speicherarchitektur zu kombinieren.

*„Hybrid Storage verspricht Kosteneinsparungen, ist aber trotzdem in der Lage, die Datenbewegungen im Hintergrund sehr schnell zu bewerkstelligen", sagt* **Stefan Käser.**

## Was im Kleinen funktioniert, geht auch im Großen

Im Kleinen hat sich ein ähnlicher Ansatz bereits bei sogenannten Hybridfestplatten (SSHD) etabliert, einer Kombination aus herkömmlicher Festplatte (HDD) mit einer schnellen SSD im selben Gehäuse. Der integrierte Controller verschiebt die Daten zwischen den verschiedenen Teilen der Hardware auf der Grundlage von Regeln wie der Häufigkeit der Zugriffe oder der Zeit seit dem letzten Zugriff. Für Benutzer läuft dies automatisch im Hintergrund ab, während sie die Hybridfestplatte einfach als einen einheitlichen Speicher nutzen.
Im größeren Stil – bei Hybrid Storage – bedeutet dies, kostengünstigen, aber langsamen S3-Objektspeicher mit schnellem, aber teurem lokalen GP2-Speicher zu kombinieren. GP2 ist der Standard-EBS-Volume-Typ für Amazon EC2-Instances. Diese auf SSDs gesicherten Volumes eignen sich für eine breite Palette von Transaktionsarbeitslasten, einschließlich Entwicklungs- bzw. Testumgebungen, interaktiver Anwendungen mit niedriger Latenz und Boot-Volumes.

Benutzer können ihre Daten einfach in eine Tabelle schreiben und müssen sich nicht darum kümmern, alte Daten nach S3 zu verschieben und ihre Anwendung zu ändern, um andere Zugriffsmuster zu nutzen. Dies erfolgt alles automatisiert auf einer Managed-Database-Plattform. Dieser Ansatz soll wirtschaftlicher sein, indem Unternehmen einen Teil der Kosten für das Hinzufügen und die Wartung von lokalem Speicher in die Cloud verlagern. Die Unternehmen greifen dann auf S3-Ressourcen zurück, wenn sie diese benötigen, was eine flexible Skalierbarkeit bietet.

Eines der häufig diskutierten Probleme bei Hybrid Storage ist, dass er bei falscher Architektur sowohl teuer als auch langsam sein kann. Dies gilt sowohl für die Hardware vor Ort als auch für unerwartete Cloud-Kosten. Eine elegante Lösung ist eine Managed Database im Rahmen eines modernen Data-Stacks für End-to-End-Analytik, um Datenanalysen mit SSD-Speichergeschwindigkeiten zu nutzen – auf dem Preisniveau von S3. Mit einem verwalteten Open-Source-basierten Datenbank-Management-System wie Clickhouse können Unternehmen ihre neuesten oder am häufigsten genutzten Daten automatisch direkt auf SSD verwenden, während die weniger häufig genutzten Daten automatisch auf S3 landen. Auf diese Weise lässt sich mehr als das Fünffache an Kosten einsparen. Ansätze wie dieser tragen dazu bei, die typischen Herausforderungen der Datenspeicherung auf sehr effiziente Weise dauerhaft in den Griff zu bekommen. <

> „Hybrid Storage ist ein Ansatz, welcher sowohl Cloud-native als auch lokale Ressourcen nutzt."

# „Termine müssen eingehalten werden“

**Interview** mit **Eva Neumann,** Geschäftsführerin der Neumann & Neumann Software und Beratungs GmbH, über hybride Arbeitsweisen in Großunternehmen

**ITD:** *Frau Neumann, inwieweit dürfen Mitarbeiter in Großunternehmen anno 2023 selbst entscheiden, wann und wo sie arbeiten?*

**Neumann:** Bei uns sieht es so aus: Nicht erst seit der Corona-Zeit merkten wir, dass viele Mitarbeiter zumindest einen Teil der Arbeitszeit im Homeoffice verbringen möchten. Das hat uns vor die Frage gestellt: Ist es überhaupt noch sinnvoll und zeitgemäß, feste Bürozeiten für jeden einzelnen Mitarbeiter festzulegen? Wir trauen jedem bei uns im Unternehmen ein hohes Maß an Eigenverantwortung zu. Insofern soll auch jeder selbst entscheiden, wo er arbeiten möchte und zu welcher Zeit. Wer am Abend produktiver ist und dafür gern länger schläft, soll das tun. Und umgekehrt darf auch jeder Frühaufsteher schon früh am Morgen loslegen. Wichtig ist nur: Vereinbarte Termine, z.B. bei Kundenprojekten, müssen eingehalten werden.

**Eva Neumann** *ist gelernte Hotelmeisterin und führt mit ihrem Bruder Oswald seit 31 Jahren das Unternehmen.*

„Wir haben im Sommer 2021 unser Innovationszentrum eröffnet – mit Almhüttencharme und Blick auf das Voralpenland.“

**ITD:** *Welche Tools und Lösungen sind für hybride Arbeitsmodelle unverzichtbar?*

**Neumann:** Wichtig ist für uns, dass sich jedes Team klare Regeln gibt und sinnvoll organisiert. Das heißt beispielsweise festzulegen, was bis zu welchem Zeitpunkt abgearbeitet sein muss oder wann gemeinsame Meetings stattfinden. Dann ist es wichtig, dass mit den gleichen Tools gearbeitet wird, um Brüche an Schnittstellen zu vermeiden. Wir haben unsere internen Prozesse seit vielen Jahren digitalisiert und das ganze Team arbeitet einheitlich auf dieser Basis. Natürlich gehören zur Kommunikation auch persönliche Treffen.

**ITD:** *Worin sehen Sie die Vorteile, dass Ihre Mitarbeiter zwischen Büro und Homeoffice wählen können?*

**Neumann:** Da wäre zunächst die leichtere Vereinbarkeit von Familie und Beruf vom Homeoffice aus. Uns ist das sehr wichtig, schließlich sind wir als familienfreundliches Unternehmen ausgezeichnet worden. Dass jeder seine Arbeitszeiten am besten selbst festlegt, hatte ich schon erwähnt. Es kommt aber noch ein weiterer Punkt hinzu: Je nachdem, an welcher Aufgabe man gerade arbeitet, passt eine bestimmte Arbeitsumgebung besser oder schlechter. Deshalb haben wir im Sommer 2021 unser Innovationszentrum eröffnet – mit Almhüttencharme und Blick auf das Voralpenland. Hier ist Raum für Kreativität und innovative Ideen. Jeder Mitarbeiter, der gern hier arbeiten möchte, kann das tun – oder eben an unserem altbewährten Standort ein paar Kilometer weiter oder von zu Hause aus.

**ITD:** *Wie gestaltet sich die Arbeitszeiterfassung, wenn die Mitarbeiter „mal hier, mal da“ arbeiten?*

**Neumann:** Was für die freie Wahl des Arbeitsorts gilt, gilt auch für die Arbeitszeit unserer Mitarbeiter. Wir halten das Prinzip der Vertrauensarbeitszeit hoch. Wichtig ist uns, dass vereinbarte Kundentermine und interne Meetings eingehalten werden. <

LEA SOMMERHÄUSER

# Althergebrachten Workflows das Handwerk legen

**Noch hinkt die Baubranche in Sachen „Digitalisierung" hinter anderen Wirtschaftszweigen her, doch zunehmend beweisen smarte Workflows, wie sich Herausforderungen lösen lassen und dem drohenden Fachkräftemangel der Traditionsbranche entgegengewirkt werden kann. Strabag und Dropbox liefern Beweise aus der Praxis.**

> Die Mitarbeiter und Projekte des in Europa ansässigen Technologiekonzerns für Baudienstleistungen sind über verschiedene Standorte verstreut, was sich für eine einfache und effektive Zusammenarbeit als schwierig erweisen kann. Unternehmen dieser Größenordnung kämpfen mit komplexen, verwaltungsintensiven Prozessen, die oftmals zu unnötigen Verzögerungen führen. Strabag ist schon seit 2017 Kunde von Dropbox und konnte in den vergangenen Jahren einige entscheidende Veränderungen in der Arbeitsweise feststellen. Seit August 2017 ist Hans-Jörg „Hajo" Klingelhöfer Kopf der Digitalisierung des Technologiekonzerns und seit Juli 2020 Head of BIM 5D. Er treibt mit seinem Team die Digitalisierung des Unternehmens mit Siebenmeilenstiefeln erfolgreich voran.

## Herausfordernde Aufgaben bewältigen

Wer dachte, es wird leichter in der Baubranche, der irrt sich. Mehr als 15.000 Bauprojekte pro Jahr managt der Konzern und muss die Herausforderung der weltweiten Pandemie, politischer Krisenherde, eingeschränkter Lieferketten, steigender Energiepreise und strenger ESG-Vorschriften einhalten. Gleichzeitig gilt es zu versuchen, die immer schmerzhafter aufklaffende Wunde, die der Fachkräftemangel in die Baubranche reißt, zu schließen. Dabei erwarten Kunden die Realisierung immer größerer Bauvorhaben in immer kürzerer Zeit. „Große Probleme verursachten in der Vergangenheit verschiedene Versionen von Bauplänen, bei denen niemand wusste, welche die aktuellere war, veraltete Informationen und mangelhafte Abstimmung oder Freigabeprozesse im Bauverlauf. Griffen die Workflows nicht nahtlos ineinander, weil die Tools nicht miteinander verzahnt sind, waren unnötige Verzögerungen und ein Chaos im Arbeitsablauf der beteiligten Gewerke absehbar. Ohne die Vernetzung aller Beteiligten über digitale Tools und Cloud-Lösungen wäre effizientes Bauen heute gar nicht mehr realisierbar", so Klingelhöfer.

**Für die Baubranche** *ist die digitale Abbildung von Handgriffen und Abläufen ganzer Projekte ein Riesenfortschritt, der vor zehn oder 15 Jahren noch undenkbar war.*

*Zusammen mit seinem Team treibt* **Hans-Jörg Klingelhöfer** *die Digitalisierung bei Strabag voran.*

Um Prozesse zu beschleunigen, die Effizienz zu steigern und letztlich die Zusammenarbeit von Mitarbeitern und Lieferanten bei oft komplexen Projekten zu erleichtern, entschied sich der Konzern für die Dropbox-Technologie. Sie mache es einfach, wichtige Inhalte wie Fotos, Videos, DWG-Dateien und Dokumente zu erstellen, zu aktualisieren, zu teilen und sicher zu speichern. So ließen sich zeitraubende Papierwege vermeiden und die Mitarbeiter könnten sich auf ihr eigentliches Kerngeschäft konzentrieren. „Mit Dropbox Transfer beispielsweise können wir remote auf die neueste Version eines Dokuments zugreifen und es sofort freigeben und aktualisieren. Wir sehen, wer was gesehen hat. Dank der fortschrittlichen Freigabefunktionen kann sichergestellt werden, dass diese Dokumente sicher sind und dass die richtigen Personen zur richtigen Zeit Zugriff darauf haben", berichtet Klingelhöfer. Darüber hinaus benötigen Partner keine eigenen Konten für die entsprechende Lösung, da alles über sichere Links abgewickelt werden kann.

Mit den eingesetzten Technologielösungen wird schlussendlich die digitale Zusammenarbeit gefördert und die Anforderungen digitaler Arbeitsbedingungen werden erfüllt. Nutzer können verschiedene Medienformate gemeinsam bearbeiten, von zu Hause, vom Büro oder von unterwegs aus. <

**Im Internet:** www.dropbox.com

# Cybersecurity als Geschäfts- und Umsatztreiber

**Aus einer aktuellen Studie von Trend Micro geht hervor, dass 63 Prozent der befragten Unternehmen planen, ihre Budgets für IT-Security im Jahr 2023 zu erhöhen.**

> Die Studie zeigt jedoch auch kritische Verständnislücken der Führungsebene zur Bedeutung der Cybersecurity für andere Unternehmensbereiche auf. So sagt mehr als die Hälfte der Befragten (56 Prozent), IT-Sicherheit sei ein notwendiger Kostenfaktor, trage aber nicht zur Umsatzgenerierung bei. Ein ähnlich hoher Anteil der Befragten (55 Prozent) argumentiert, ihr Wert beschränke sich darauf, Angriffe oder Bedrohungen abzuwehren. Fast die Hälfte (45 Prozent) sieht die IT-Security sogar eher als Hindernis denn als Business Enabler an. Das negative Verständnis der deutschen Führungsebene für Cybersecurity fällt im globalen Vergleich deutlich auf. Weltweit sehen lediglich 38 Prozent die Cybersecurity als „Verhinderer" an. Darüber hinaus sind 87 Prozent der befragten deutschen Unternehmen besorgt, dass mangelnde Cybersecurity die Gewinnung von Neukunden beeinträchtigen könnte. 15 Prozent geben sogar zu, dass dies bereits der Fall ist. Ein Anteil von 81 Prozent räumt ein, dass sie bei Verhandlungen mit potenziellen Kunden und Lieferanten nach ihrem IT-Sicherheitsniveau gefragt werden. <


*Unternehmen investieren zwar in ihre* **IT-Sicherheit**, *aber deutsche Unternehmensvorstände unterschätzen noch die Bedeutung von Cybersecurity.*

**Im Internet:** www.trendmicro.com

# Auf der Jagd nach Black Hats

**Hacker ist nicht gleich Hacker: Einige von ihnen sind unverzichtbare Verbündete im Kampf gegen Cyberkriminalität. Das IT-Systemhaus Sievers-Group setzt deshalb ab sofort auf die Zusammenarbeit mit zwei „guten" Hackern – sogenannten White Hats.**


*Hat der feindliche* **Hacker** *Spuren hinterlassen, die auf ihn zurückführen können, startet eine Jagd nach dem Systemeindringling.*

> Als Penetrationstester für IT-Systeme (Pentester) und aktive Berater für Sicherheitsvorfälle begleiten sie ab sofort Kunden auf dem gesamten Lösungsweg. So muss Sievers nicht bei Sicherheits-Audits mit einem Abschlussbericht stoppen, sondern unterstützt das jeweilige Unternehmen, bis es wieder den normalen Betrieb aufnehmen kann. Besonders Vor-Ort-Einsätze können den Arbeitstag dabei je nach Hackeraktivität deutlich in die Länge ziehen und eine spannende Jagd nach dem Schuldigen beinhalten.

Das Aufgabengebiet eines White Hats bei einem IT-Systemhaus ist vielschichtig. Ein Pentester muss sich beispielsweise auch an normalen Bürotagen ab und zu in die Rolle eines boshaften Hackers (Black Hat) hineinversetzen können. Sein Aufgabengebiet besteht nämlich u.a. darin, die Systeme eines Unternehmens in der Tiefe zu untersuchen und das Schadenspotenzial von möglichen Schwachstellen zu demonstrieren. Dazu bedient er sich der gesamten Palette an Hackerwerkzeugen, die auch von Systemeindringlingen genutzt wird. Mithilfe der Simulation eines typischen Cyberangriffs kann er so die tatsächlichen Gefahren aufzeigen, ohne dass ein realer Schaden entsteht. Daraus entwickelt er anschließend entsprechende Maßnahmen, um diese Sicherheitslücken auch gegen echte Angriffe abzuschirmen. <

**Im Internet:** www.sievers-group.com

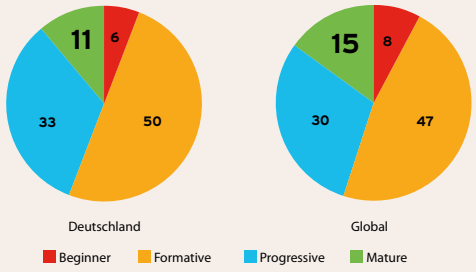
# Weltweit im Mittelfeld

**Wie gut sind deutsche Unternehmen auf IT-Angriffe vorbereitet? Weltweit liegen sie nur im Mittelfeld, doch in Europa auf einem guten zweiten Platz hinter Großbritannien.**

> Die Anforderungen an Cybersicherheit haben sich durch die Covid-19-Pandemie deutlich verändert. Statt eines festen Arbeitsorts mit statischem Unternehmensnetzwerk kommen bei Hybrid Work und virtueller Kollaboration nun mehrere Geräte an diversen Standorten zum Einsatz. Unternehmen müssen daher nicht nur ihre Security-Strukturen umbauen, sondern sich auch gegen neue und ständig weiterentwickelnde Gefahren schützen.

## Vier Reifegrade

Der Cisco Cybersecurity Readiness Index 2023 hat ermittelt, wie weit Unternehmen diesen neuen Herausforderungen gewachsen sind. Auf Basis von 6.700 Expertenbefragungen wurden die Unternehmen in vier Reifegrade eingeteilt: Anfänger (Beginner), Gestalter (Formative), Fortgeschrittene (Progressive) und Reife (Mature). Den höchsten Reifegrad (Mature), der bestmöglich vor modernen Sicherheitsrisiken schützt, erreichen weltweit nur 15 Prozent der Unternehmen, in Deutschland sogar nur 11 Prozent. Damit liegen deutsche Unternehmen weltweit nur im Mittelfeld von 27 untersuchten Ländern. In Europa belegen deutsche Unternehmen einen guten zweiten Platz hinter Großbritannien. Am besten schneiden deutsche Unternehmen bei der Endgerätesicherheit mit dem weltweit zehnten Platz (Mature und Progressive) ab. Der Schutz von Netzwerken ist in Deutschland am besten ausgeprägt (Platz 11), was u.a. an einem vergleichsweise häufigen Einsatz von Firewalls mit integriertem Intrusion-Prevention-System (IPS) liegt. Der Schutz von Anwendungen (Platz 13) und Identitäten (Platz 15) nimmt bereits ab, und beim Thema „Datensicherheit“ hinkt Deutschland klar hinterher (Platz 20). <




*Der* **Cybersecurity Readiness Index 2023** *basiert auf einer Doppelblindumfrage unter 6.700 Führungskräften in 27 Ländern, die in ihren Unternehmen für Cybersicherheit zuständig sind. Die Untersuchung wurde zwischen August und September 2022 mittels Online- und Telefoninterviews durchgeführt.*

**Im Internet:** www.cisco.com

# Zusammenschluss für mehr Sicherheit

**Der Managed-Service-Provider Spacenet nimmt die Google Cloud Chronicle Security Operations Suite in sein Portfolio auf und möchte es so Unternehmen im DACH-Raum ermöglichen, Cyberattacken schneller feststellen und abwehren zu können.**

> IT-Abteilungen überwachen und schützen heute immer komplexere, teils hybride Multi-Cloud-Strukturen. Die Anzahl, Raffinesse und der zunehmende Automatisierungsgrad bei Cyberangriffen machen es jedoch unmöglich, Bedrohungen ohne automatisierte Kontrollmechanismen zu entdecken. Denn große Datenmengen zu erheben, in auswertbaren Formaten zu speichern und die anfallenden Log-Daten zu analysieren, kann kosten- und zeitintensiv werden. Hinzu kommt, dass IT-Sicherheitsfachkräfte und -lösungen in vielen Unternehmen fehlen.

Durch die Partnerschaft von Spacenet mit Google Cloud können Unternehmen ihre IT-Sicherheit erhöhen und sich vor Phishing-Angriffen, Verschlüsselungen oder dem Zusammenbruch ihrer IT-Systeme durch Cyberangriffe schützen. Besonders relevant soll das für Firmen sein, die stark vom Funktionieren der Unternehmens-IT abhängig sind, deren Prozesse wie Auftrag, Einkauf, Produktion, Lieferung und Abrechnung voll elektronisch sind oder die sensible Kundendaten verwahren. <

**Im Internet:** www.space.net

# Transparenz in der Lieferkette

**Laut einer aktuellen Studie von TCS und Microsoft haben die meisten Großunternehmen noch keine Ziele für Emissionen in der Lieferkette festgelegt.**

> Anfang des Jahres trat in Deutschland das Lieferkettensorgfaltspflichtengesetz in Kraft. Doch die Unternehmen haben im Bereich „Lieferkettentransparenz" noch einiges nachzuholen, so das Ergebnis einer neuen Studie: Mit 84 Prozent hat eine deutliche Mehrheit der Großunternehmen noch keine wissenschaftlich fundierten Ziele zur Verringerung der direkten betrieblichen Emissionen festgelegt. Demgegenüber hat sich sogar ein noch kleinerer Teil (11 Prozent) zu wissenschaftlich fundierten Ziele zur Verringerung der Emissionen in ihren Lieferketten verpflichtet.


**Die Studie** *macht deutlich, dass noch viel Arbeit geleistet werden muss, damit die globale Wirtschaft nachhaltiger wird.*

## Noch viel innovative Arbeit ist zu leisten

Die Analyse zeigt, dass die meisten Unternehmen noch Schwierigkeiten haben, ihre Daten zu validieren und ihre Dekarbonisierungsanstrengungen genau zu messen. Sie unterstreicht außerdem die Bedeutung eines regelmäßigen Engagements mit erweiterten Geschäftsökosystemen – einschließlich Kunden, Lieferanten und anderen Stakeholdern –, um die Transparenz der Lieferkette zu verbessern und den $CO_2$-Fußabdruck zu reduzieren. Die Ergebnisse machen deutlich, wie viel innovative Arbeit noch zu leisten ist, um die globale Wirtschaft nachhaltig zu gestalten, betonen die Autoren der Studie. <

**Im Internet:** www.tcs.com/de

# Innovative IT-Lösungen für die Logistik

**Mit neuen Software-Lösungen will Siemens Digital Logistics Unternehmen helfen, Herausforderungen im globalen Lieferketten-Management nachhaltig zu meistern.**

> Zum Repertoire gehören u.a. eine zertifizierte Lösung zur Berechnung und Visualisierung von $CO_2$-Emissionen in Logistiknetzwerken, der Einsatz des Digital Twin als Optimierungsinstrument sowie ein Control Tower, mit dem sich Produktions- und Lieferprozesse in Echtzeit synchronisieren lassen.

Mit dem Digital Twin liefert der Anbieter z.B. Antworten auf die aktuellen, krisenbedingten Lieferengpässe in Industrie und Handel. Durch die Einbindung in das konzerneigene Ökosystem verfügt das Unternehmen über natürliche Verbindungen zum Industriesektor und ein Portfolio von Tools, die Unternehmen auf der ganzen Welt dabei helfen, ihre Produkte, Produktion und Kapazitäten erfolgreich zu planen und sie auf die Bedürfnisse von Supply-Chain-Managern beim Aufbau widerstandsfähigerer Wertschöpfungsketten auszurichten. Lösungen wie der Control Tower sollen nicht nur Supply-Chain-Transparenz in Echtzeit ermöglichen, sondern auch Visibilität über alle Produktions- und Logistikprozesse liefern, indem sie Daten systemübergreifend konsolidieren. Möglich wird dadurch auch die Synchronisation von Produktions- und Logistikprozessen in der Fertigung. <

**Im Internet:** www.sw.siemens.com/de-DE/

**Siemens** *stellt neue Innovationen vor, darunter das Sustainability Dashboard, das vollständige Transparenz über $CO_2$-Emissionen in Logistiknetzwerken bietet.*

# Daten als Schlüssel für mehr Nachhaltigkeit

**Rechenzentren sind das Rückgrat der Digitalisierung, aber auch große Stromverbraucher. Ein datenbasierter Ansatz hilft, die Anlagen effizienter zu betreiben.**

> Auf der einen Seite tragen digitale Lösungen zu mehr Nachhaltigkeit bei: Videokonferenzen machen z.B. viele Dienstreisen überflüssig. Auf der anderen Seite erfordert der Betrieb der Lösungen viel Strom: Allein die Rechenzentren (RZ),

**Mit energieeffizienten Rechenzentren** *leisten Unternehmen nicht nur einen wichtigen Beitrag zum Klimaschutz, sondern senken auch ihre Betriebskosten.*

in denen ein Großteil der digitalen Daten lagert und die meisten Anwendungen laufen, verschlingen in Deutschland jährlich 16 Milliarden Kilowattstunden. Um hier die Umweltbilanz zu verbessern, gibt es laut Dell Technologies viele Stellschrauben.

**Verbrauchs- und andere Daten erfassen:** Betreiber von Rechenzentren benötigen Echtzeiteinblicke in die Auslastung und den Stromverbrauch ihrer IT-Systeme. Nur so können sie realistisch einschätzen, wie effizient die Server, Storage-Arrays und Netzwerkgeräte arbeiten. Eine moderne Plattform für das System-Management erlaubt es, die Leistungs- und Verbrauchswerte detailliert zu erfassen und das Energie- und Wärmemanagement zu automatisieren.

**Design des Rechenzentrums optimieren:** Ein großer Teil des Stromverbrauchs entfällt auf die RZ-Kühlung. Weniger Systeme bedeuten weniger Hitzeentwicklung und damit einen geringeren Kühlaufwand – durch eine Konsolidierung der IT-Infrastruktur und eine bessere Auslastung der Systeme lässt sich daher viel Strom sparen.

**Veraltete Systeme und Technologien ablösen:** Moderne Server sind weit leistungsstärker als ältere Systeme und senken den Stromverbrauch im Rechenzentrum deutlich. Zum einen kann ein einzelner Server der aktuellen Generation die Aufgaben gleich mehrerer Legacy-Systeme übernehmen, zum anderen besitzt er effizientere Hardware-Komponenten und optimierte Stromsparfunktionen. Auf Storage-Seite wiederum helfen fortschrittliche Kompressions- und Deduplizierungsalgorithmen, den Speicherplatz der Arrays besser auszunutzen und eine Überprovisionierung zu vermeiden. <

**Im Internet:** www.delltechnologies.com

# Kontrollverlust oder Vertrauen

**Zum Vorschlag eines sechsmonatigen Moratoriums für die Weiterentwicklung bzw. das Training besonders leistungsfähiger Künstlicher-Intelligenz-Systeme (KI) äußert sich Dr. Joachim Bühler, Geschäftsführer des Tüv-Verbands, im Kommentar.**

> Weltweit führende KI-Experten, Wissenschaftler und KI-Unternehmer weisen eindringlich darauf hin, dass die gesellschaftlichen und wirtschaftlichen Folgen mächtiger KI-Systeme noch nicht beherrschbar sind. Dieser Appell zeigt den politischen Handlungsbedarf: für eine klare gesetzliche Regulierung Künstlicher Intelligenz. Nur so können wir die Risiken besonders leistungsfähiger KI-Systeme in den Griff bekommen. Gleichzeitig schaffen wir mit einer solchen Gesetzgebung die Grundlage, um die immensen Chancen dieser Technologie ausschöpfen zu können.

**Dr. Joachim Bühler** *ist promovierter Politikwissenschaftler und war vor seiner jetzigen Stelle beim Digitalverband Bitkom tätig.*

## Fatale Folgen

Die Experten warnen vor einer Flut von Propaganda und Fake News, der Vernichtung vieler Arbeitsplätze und einem generellen Kontrollverlust. Gleichzeitig ist klar, dass KI-Systeme verstärkt in der Medizin, in Fahrzeugen oder anderen sicherheitskritischen Bereichen eingesetzt werden. Fehlfunktionen können fatale Folgen haben. Hier braucht es rechtliche KI-spezifische Leitplanken, an denen sich die Anbieter orientieren können. Das schafft Vertrauen und fördert innovative Angebote statt sie auszubremsen.

## Keine Zeit verlieren

Europa hat mit dem Gesetzgebungsverfahren für den AI Act die Chance, weltweit den ersten Rechtsrahmen für Künstliche Intelligenz zu schaffen. Mit dem Wissen um die Fähigkeiten mächtiger Systeme wie ChatGPT darf Europa jetzt keine Zeit mehr verlieren und muss zügig den gesetzlichen Rahmen schaffen. Wie von den Unterzeichner des Appells vorgeschlagen, sollten unabhängige Prüfungen und Zertifizierungen eine wichtige Rolle für Vertrauen und Akzeptanz von KI-Systemen spielen und damit dem Recht in der Praxis Geltung verschaffen. <

# Mit KI Blutvergiftungen verhindern

**Die Telekom und das Start-up Telehealth Competence Center Analytics wollen mithilfe von KI das Risiko einer Sepsis reduzieren.**

> Die Lösung soll auf Intensivstationen eingesetzt werden. Der Algorithmus lernt permanent dazu. So soll die Künstliche Intelligenz (KI) die Ärzteschaft vor einer drohenden Sepsis bei einem Patienten warnen können. Über Standardschnittstellen werden die Vitaldaten der Intensivpatienten im Krankenhaus erfasst und in der Open Telekom Cloud vom KI-Algorithmus analysiert. Er soll rund zehn Stunden vor dem Ausbruch einer Sepsis das individuelle Risiko vorhersagen können und so die Möglichkeit eröffnen, diese zu verhindern. Ein Dashboard zeigt den Ärzten auf einen Blick das Sepsisrisiko an, sodass sie schnell handeln können. Über die üblichen Vitaldaten hinaus müssen die Kliniken keine weiteren Parameter erfassen. Die Lösung ist marktreif und wird aktuell in zwei Krankenhäusern pilotiert. Weitere Krankenhäuser sind im Gespräch. <

**Im Internet:** www.telekom.de

# ChatGPT: Viele Nutzer finden Fehler

**Eine aktuelle Studie zeigt: Die meisten Nutzer des Chatbots ChatGPT sind mit der Qualität der Ergebnisse zufrieden und vertrauen diesen. Gleichzeitig entdeckten viele in den Antworten Fehler.**

> Im Auftrag von Prof. Tobias Kollmann, Universität Duisburg-Essen, hat Civey über 5.000 Bundesbürger sowie rund 1.500 Nutzer von ChatGPT befragt. Demnach findet es rund ein Viertel der über 18-Jährigen (23 Prozent) grundsätzlich positiv, dass Menschen mit Künstlicher-Intelligenz-Anwendungen (KI) kommunizieren können. Bereits 17 Prozent haben den Bot schon einmal genutzt.

Einmal ausprobiert, wird das Tool durchaus intensiver in Anspruch genommen: 5 Prozent verwenden es täglich, 23 Prozent wöchentlich und weitere 21 Prozent monatlich. Die Qualität der Antworten bewerten 44 Prozent der Befragten mit gut oder sogar sehr gut. Demgegenüber befand nur etwa jeder Zehnte die Qualität als eher schlecht bzw. sehr schlecht.

## Kein blindes Vertrauen

Immerhin rund drei Viertel der Nutzer überprüfen die Antworten der KI. Offenbar zu Recht: Deutlich über die Hälfte der Befragten (59 Prozent) hat schon einmal Fehler in den Antworten von ChatGPT gefunden. <

**Im Internet:** www.uni-due.de

**Die Qualität der Antworten** *von ChatGPT wird durchaus als positiv wahrgenommen.*



# Endgerätesicherheit zeitgemäß gestalten

> Früher konnte man sich für den Schutz von Endgeräten weitestgehend auf Windows-basierte Systeme fokussieren und hier waren auch noch klassische Technologien wie „Musteranalysen", die zur Erkennung bzw. Abwehr von Schadsoftware eingesetzt wurden, ausreichend. Heute treffen wir auf eine Vielzahl von Betriebssystemen bzw. Embbeded Systems und eine große Bandbreite von Anwendungsfällen.

**Michael Huber,**
*Consultant bei der PROFI Engineering Systems AG*

Ein zeitgemäßer Management-Ansatz sollte zum Ziel haben, ganzheitlich zu agieren, und zwar sowohl was das Auffinden von Auffälligkeiten betrifft als auch die Bekämpfung/Eindämmung dieser.

Was es jedoch zu beachten gilt, ist, dass eine „Endpoint Detection & Response"- oder auch „Xtended Detection & Response"-Lösung nur so gut ist wie die Daten, die sie von den beteiligten Endpoints erhält. Nur so kann gewährleistet werden, dass ein Unternehmen Einblick in bzw. Informationen über etwaige Sicherheitsvorkommnisse bekommt und eine umgehende Schadensanalyse möglich ist.

Der Anspruch an ein umfassendes Endpoint-Security-Konzept sollte sein, dass es eine nahezu vollständige Übersicht über alle Teilnehmer/Endpoints und deren Aktivitäten im Netzwerk bietet, die vorhandenen fortschrittlichen Abwehrfunktionen nutzt und Routineaufgaben automatisiert.

Nur in einer ausgewogenen Kombination zwischen Tools und entsprechend ausgebildetem Personal kann die Grundlage zur effektiven Bekämpfung komplexer Cyberangriffe und damit zur Aufrechterhaltung des Geschäftszweckes geschaffen werden. Was wiederum dafür sorgt, dass Unternehmen in die Lage versetzt werden, ihre knappen Ressourcen gezielt einzusetzen und sich auf ihre eigentlichen Kernthemen zu fokussieren – ohne sich Sorgen um den Schutz ihrer IT machen zu müssen. <

**Im Internet:** www.profi-ag.de

PROFI
Wir entwickeln mehr als IT

# Das goldene Ticket – oder nicht?

**Nach dem Krisenjahr 2022 sehen die Wachstumsprognosen für den E-Commerce-Sektor besser aus. Kein Wunder, denn Technologie und Investitionen in die Customer Experience machen Kunden das personalisierte Shoppen leichter denn je.**

> Nahezu alle wichtigen E-Commerce-Branchen haben im vergangenen Jahr eine Rückgang der Umsatzentwicklung hinnehmen müssen. Am schlimmsten hat es dabei laut Statista (02/2023) den Handel mit Elektronik getroffen, aber auch den Klassiker, die Fashion-Segmente, hat es mit rund 10 Prozent weniger Umsatz hart erwischt. Nach dem kurzen Schock der Konsumenten sehen die Prognosen für die kommenden Jahre jedoch wieder deutlich zuversichtlicher aus und rechnen bis 2027 mit einem beachtlichen Umsatz von 167 Mrd. Euro für den gesamten Sektor.

**Beim Online-Handel** *ist – neben der Ware selbst – vor allem die Customer Experience entscheidend.*

Das ist auch wenig verwunderlich, wenn man die Investitionen in Marketing und Customer Experience betrachtet. Beim Online-Handel sind neben der Ware vor allem Kauferlebnis und Zugänglichkeit entscheidend. Das beginnt beim Targeting der richtigen Zielgruppen und endet beim bequemen Check-out im Webshop. An nahezu allen Zwischenstationen der Customer Journey müssen die großen E-Commerce-Player dafür sorgen, dass die Kunden nicht aussteigen.

## Optimierte Kauferlebnisse

Höchst personalisierte Kauferlebnisse machen auch deshalb großen Sinn, da das Generieren eines neuen Kunden im Schnitt das sechs- bis siebenfache Invest der Erhaltung eines Bestandskunden kostet. Aber wie bei einer Beziehung zwischen Menschen wird dieses gute Verhältnis häufig erst dann wirklich auf die Probe gestellt, wenn es mal kracht und die Zahlung eines Kunden ausfällt. Und die Scheidung kommt meist dann, wenn der Kunde das Hoheitsgebiet des Webshops verlassen hat und z.B. an einen Inkassodienstleister weitergeleitet wird.

## Mit der Kundenbrille

Man nehme an, der Kunde ist im Markt für ein neues Mobiltelefon. Vielleicht hat er schon ein bestimmtes Modell im Auge – also beginnt er die Recherche nach dem besten Preis. Das Targeting nimmt ihn natürlich sofort ins Visier und alle möglichen Anbieter versprechen auf jedem Kanal die besten Preise. Auch die eigenen Social-Media-Feeds sind nun gefüllt mit Inhalten, die die Kaufentscheidung erleichtern sollen. Dann kommt der Moment, an dem der Kunde sein goldenes Ticket einlösen möchte. Die Wahl auf einen Anbieter ist gefallen, denn dort waren die Inhalte besonders hilfreich und der Preis stimmt auch. Doch es gibt eine letzte Frage zum Versand. Kein Problem, der Chatbot des Shops beantwortet alles rund um die Uhr. Der Kunde bezahlt – praktischerweise in Raten – und das Gerät ist bereits einige Tage später bei ihm. Der Service scheint gut zu sein.

Doch dann passiert etwas, das statistisch gar nicht so unwahrscheinlich ist: Eine der Raten fällt durch, und der Kunde landet im Mahnwesen oder Inkasso. Jetzt gibt es Briefe in bürokratischer Tonalität und alles ist wenig transparent. Von den vielen nützlichen Websites mit Hilfestellungen, Chatbots oder sonstigen Informationen fehlt jede Spur. Das goldene Ticket des Kunden ist nichts mehr wert und er wird fallen gelassen. Mahn- und Inkasso-Anbieter wie Troy haben sich darauf spezialisiert, den hohen Level der Customer Experience auch gerade dort aufrechtzuerhalten, wo es sonst gerne weh tut. So werden nicht nur die noch offenen Rechnungen bearbeitet, sondern gleichzeitig auch teure Investitionen in Customer Acquisition Costs (CAC) gerettet. <

JOCHEN SCHÜSSLER

# Von Metaverse bis New Learning

**Auf der Learntec in Karlsruhe präsentieren vom 23. bis 25. Mai 2023 nationale und internationale Aussteller neue Technologien zum digitalen Lernen und Arbeiten.**

> Der begleitende Fachkongress bietet einen Blick in die Zukunft des digitalen Bildungsmarkts und verknüpft diese mit dem Ausstelleranagebot 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. 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". <

**Im Internet:** www.learntec.de

*Auf der Learntec werden Themen wie Metaverse und Künstliche Intelligenz auf der Agenda stehen.*

## Zukunft Personal Süd

**Termin:** 9. und 10. Mai 2023
**Veranstalter:** Spring
**Info:** www.zukunft-personal.de

Am 9. und 10. Mai 2023 trifft sich die HR-Community auf der ZP Süd in Stuttgart. Das heißt: zwei Tage Produktneuheiten und Trends der Arbeitswelt live erleben, plus Austausch und Networking, interaktive Sessions und inspirierende Insights von erfahrenen HR-Experten. Fokus der Veranstaltung sind die Trends der Arbeitswelt von heute und morgen. Für alle relevanten Personalfragen zeigt die Fachmesse in Stuttgart Produktinnovationen, Entwicklungen und Trends auf. Renommierte Experten aus der Praxis sprechen in spannenden Vorträgen über die aktuellen Fragen aus der Welt der Arbeit.

## BME-E-Lösungstage

**Termin:** 23. und 24. Mai 2023
**Veranstalter:** BME
**Info:** www.bme.de

Auf den BME-E-Lösungstagen im 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 um eine Analyse und Optimierung der Einkaufsorganisation. Auf der Veranstaltung erwartet die Interessierten ein umfangreiches Fachprogramm mit Fachvorträgen, Workshops, Round Tables und Solution Foren sowie mehr als 80 Aussteller und Partner.

## New Work Evolution

**Termin:** 23. bis 25. Mai 2023
**Veranstalter:** Messe Karlsruhe
**Info:** www.newworkevolution.de

Die New Work Evolution ist eine unverzichtbare Veranstaltung für alle, die sich mit der Zukunft der Arbeitswelt beschäftigen. Sie bietet eine umfangreiche Plattform für Unternehmen, Planer und Berater, um die neusten Entwicklungen und Innovationen im Bereich „New Work" zu präsentieren und zu diskutieren. Besucher haben in zahlreichen Vorträgen und Workshops die Möglichkeit, sich über die neusten Trends und Entwicklungen zu informieren und von Experten zu lernen. Die Fachmesse findet erstmals zusammen mit der Learntec vom 23. bis 25. Mai 2023 in Karlsruhe statt.

18

# DIE SUPPLY CHAIN SICHER IM GRIFF

**Im Interview erläutert Klaus Jetter, Regional Vice President DACH von WithSecure, wie Unternehmen mit Outcome-based Security ihre Geschäftsziele und -prozesse einhalten können.**

> Cyberkriminalität ist attraktiv, denn hier lässt sich mit geringem Aufwand das große Geld machen. So verwundert es wohl kaum, dass die Zahl der Hackerangriffe stetig wächst. Doch das ist nicht alles: Russlands Krieg gegen die Ukraine und weitere politische Spannungen werden auch digital ausgefochten. Die aktuelle Situation wirkt sich natürlich auf die IT-Sicherheit aus, doch viele Unternehmen unterschätzen das Risiko nach wie vor. →

Fotokonzept, Layout und Produktion:
**Medienhaus Verlag GmbH**

**Klaus Jetter**

**Alter:** 54 Jahre

**Familienstand:** verheiratet

**Derzeitige Position:** Regional VP DACH von WithSecure

**Interessen:** alles, was der Erholung dient

Text: **Ingo Steinhaus** Fotos: **Claus Uhlendorf**

20

# „Wenn ein Land oder eine Region von einer Krise betroffen sind, kann dies Auswirkungen auf die globale Lieferkette haben.“

**ITD:** *Herr Jetter, auf welche Weise hat die aktuelle Situation die Sicherheitslage verändert – vor allem mit Blick auf die Supply Chain?*
**Klaus Jetter:** Die Absicherung der Supply Chain war noch nie einfach. Und die aktuellen Krisen machen die Situation nicht besser. Doch erinnern wir uns an die Malware Notpetya, die uns 2016 lange Zeit in Atem gehalten hat. Über eine Schwachstelle in einer Software für die Steuererklärung gelangte das Schadprogramm in Unternehmensnetze. Es infizierte die Systeme von Reckitt-Benckiser, Beiersdorf, Mars und Mondelez, blockierte Kassen bei Handelsfilialisten in der Ukraine, befiel Rechner der Metro und legte die Hafenterminals der weltweit größten Reederei Maersk lahm. Mit einem geschätzten Schaden von rund 10 Mrd. US-Dollar handelte es sich damals um einen der weltweit teuersten Cyberangriffe.
**ITD:** *Wie gehen Cyberkriminelle gerne vor?*
**Jetter:** Sie suchen sich innerhalb des Lieferantennetzwerks die schwächste Stelle für ihre Angriffe aus. Das sind häufig kleinere Zulieferer, die wie bei der Steuersoftware nicht einmal im Kerngeschäft tätig sind. Dort ist die Chance am größten, in IT-Systeme einzudringen und sich anschließend zum eigentlichen Ziel vorzuarbeiten. Daran zeigt sich, wie verletzlich Lieferketten wirklich sind. Aktuell sind Unternehmen angreifbarer denn je, denn die Schließung von Grenzen, Unterbrechungen im Transportwesen und Lieferkettenstörungen haben dazu geführt, dass viele Unternehmen Schwierigkeiten haben, ihre Produkte und Dienstleistungen bereitzustellen. Ein weiterer Aspekt, der die Sicherheitslage beeinflusst, ist die Abhängigkeit von bestimmten Ländern und Regionen für die Lieferung von kritischen Waren und Dienstleistungen. Wenn ein Land oder eine Region von einer Krise betroffen sind, kann dies Auswirkungen auf die globale Lieferkette haben und zu Engpässen und Störungen führen.
**ITD:** *Wie sollten Unternehmen vorgehen, um ihre Supply Chain abzusichern? Eine ausschließliche Produktion in Deutschland kann ja nicht die Antwort sein.*
**Jetter:** Leider gibt es keinen 100-prozentigen Schutz und die Frage lautet nicht ob, sondern wann ein Unternehmen angegriffen wird. Unternehmen und Organisationen müssen ihre Lieferketten entsprechend diversifizieren und widerstandsfähiger gestalten, um besser auf zukünftige Krisen vorbereitet zu sein. Darüber hinaus müssen sie ihre Cybersicherheitsmaßnahmen verstärken, um sich vor Hackerattacken zu schützen.
**ITD:** *Wie geht das am besten?*
**Jetter:** Planvoll, um es kurz auszudrücken. Das ist für Unternehmen eigentlich Alltag. Jedes Unternehmen hat strategische Pläne für die Geschäftsentwicklung in den nächsten drei oder vier Jahren. Doch wenn wir die Sicherheitsstrategie für die nähere Zukunft erfahren wollen, schauen wir häufig in fragende Gesichter. Wir sehen da


21

22

„Ausgaben für Security stehen in keinem Verhältnis zum Schaden. Natürlich trifft es nicht jeden, aber die Unternehmen sollten das Risiko trotzdem berücksichtigen."

gleich mehrere Hürden: So müssen die Unternehmen zunächst ein Risikobewusstsein aufbauen. Inzwischen ist es leider so, dass auch kleinere Unternehmen ein lukratives Ziel sind. Es ist für Cyberkriminelle technisch möglich, mit sehr wenig Aufwand eine enorme Menge an Geld einzustreichen – über Ransomware oder Distributed-Denial-of-Service-Angriffe (DDoS) auf Webserver. Die Unternehmen müssen sich also auf den Fall vorbereiten. Eine weitere Hürde ist das mangelnde Verständnis für die Bedeutung von Security für das Geschäftsergebnis. Sie ist nämlich sehr hoch, auch wenn sie auf den ersten Blick nach einer lästigen Investition aussieht. Wir plädieren deshalb für die sogenannte ergebnisbasierte Sicherheit – Outcome-based Security.

**ITD:** *Was ist das Besondere an diesem Ansatz?*

**Jetter:** Er spricht die Sprache der Unternehmen, also die Sprache der Effizienz. Denn genau das benötigen Unternehmen. Seit Jahrzehnten steigen in Deutschland die Ausgaben für Cybersicherheit, ohne dass die Zahl erfolgreicher Cyberangriffe nach unten geht. Regelmäßig berichtet der Bitkom-Verband über Milliardenschäden für betroffene Unternehmen. Die Verantwortlichen sind in einer Zwickmühle: Sie erhöhen jedes Jahr ihre IT-Sicherheitsausgaben, sehen aber keine Verbesserung ihrer Cybersicherheit – im Gegenteil. Die Unternehmensleitungen stempeln Cybersicherheit deshalb häufig als reinen Kostenfaktor ab. Sie bekommt den schlechten Ruf, nichts zu den Unternehmenszielen beizutragen. Das rächt sich natürlich. Ein typischer Fall ist ein von uns im Schadenfall unterstütztes Industrieunternehmen. Ein Ransomware-Angriff hat einen Produktionsausfall von zwei Wochen bewirkt. Der Schaden lag alles in allem bei 10 Mio. Euro für den Stopp der Fertigung und die vollständige Rekonstruktion von insgesamt 800 IT-Systemen. Demgegenüber steht eine nicht umgesetzte Investition von etwa 50.000 Euro für die entsprechenden Sicherheitsvorkehrungen. Das zeigt deutlich: Ausgaben für Security stehen in keinem Verhältnis zum Schaden. Natürlich trifft es nicht jeden, aber die Unternehmen sollten das Risiko trotzdem berücksichtigen.


**ITD:** *Wie geht Ihr Ansatz konkret vor?*
**Jetter:** Wir messen den Nutzen von Cybersicherheit. Dafür verknüpfen wir Security mit den Unternehmenszielen. Bei Outcome-based Security handelt es sich um ein Konzept, bei dem der Fokus auf der Einhaltung der Geschäftsziele und aller damit verbundenen Prozesse liegt. Letztlich geht es darum, wie die Ziele erreicht werden und wie Cybersicherheit dafür einen Beitrag leistet. Wir verstehen diese Art der ergebnisorientierten Cybersicherheit nicht als Gegenmodell zu den etablierten strategischen Ansätzen der IT-Sicherheit. Wir bauen vielmehr darauf auf. Der Ansatz der Outcome-based Security ändert nicht nur die Haltung des Sicherheitsverantwortlichen, sondern auch sein Standing im Unternehmen. Dadurch ist der Chief Information Security Officer (CISO) nicht mehr nur der Nein-Sager. Stattdessen sagt er: Ja, wir können diese Geschäftsergebnisse ermöglichen und auf diese Art können wir es sicher machen. Auf einmal spricht er die Sprache der Strategie und der Ergebnisse – auf Augenhöhe mit denjenigen, die am Ende auch über das Budget für die IT-Security entscheiden. So verstehen die Stakeholder endlich, welchen positiven, aktiven Beitrag die Cybersecurity zum Erfolg des Unternehmens leistet.

**ITD:** *Im Zusammenhang mit Sicherheit ist häufig von Datensouveränität die Rede. Was bedeutet dieser Begriff?*
**Jetter:** Datensouveränität bezieht sich in erster Linie auf das Recht und die Fähigkeit eines Unternehmens, die Kontrolle über die eigenen Daten zu haben. Es geht darum, welche Daten gesammelt, gespeichert, verarbeitet und geteilt werden dürfen. Datensouveränität ist somit ein wichtiger Aspekt der Sicherheit, insbesondere in einer Welt, in der Daten zunehmend digital gespeichert und übertragen werden. Die Idee der Datensouveränität ist eng mit den Konzepten der Informationssicherheit und des Datenschutzes verbunden und wird oft als eine grundlegende Voraussetzung für eine erfolgreiche und vertrauenswürdige Digitale Transformation angesehen. Doch dafür müssen auch Staaten die rechtlichen und regulierenden Voraussetzungen schaffen. Schon seit 2019 versucht auch die Welthandelsorganisation (WTO) Regeln für den grenzüberschreitenden Datenverkehr auszuhandeln. Die weit verbreitete Besorgnis über Störungen durch frei fließende Daten hat jedoch dazu geführt, dass sich bisher die Hälfte der 184 Mitgliedsstaaten gegen eine Teilnahme an den Verhandlungen entschieden hat. Diese Länder sind also nicht bereit, gemeinsame Regeln zu entwickeln. Der internationale Datenverkehr wird dennoch weitergehen, aber solange es keinen globalen Ansatz für die Regulierung von Datenschutz und Datenaustausch gibt, müssen wir uns mit einem Flickenteppich konkurrierender Vorschriften herumschlagen. Trotzdem sollte jedes Unternehmen seine eigene Datensouveränität schützen. Dafür ist es z.B. wichtig, dass Unternehmen die Bedingungen und Vereinbarungen mit Dienstleistern sorgfältig prüfen und klären, wer die Kontrolle über die eigenen Daten hat und wie diese geschützt werden.

> „Solange es keinen globalen Ansatz für die Regulierung von Datenschutz und Datenaustausch gibt, müssen wir uns mit einem Flickenteppich konkurrierender Vorschriften herumschlagen."

**ITD:** *Das betrifft dann beispielsweise auch Cloud-Provider. Wie sieht da die Sicherheitslage aus? Oder anders gefragt: Ist die Cloud wirklich sicher?*
**Jetter:** Cloud-Provider haben dieselben Sicherheitsrisiken wie jedes

➞

24

„Die Umsatzentwicklung zeigt uns klar, dass Security aus der Cloud im Aufschwung ist. Das ist in anderen Branchen ähnlich. Die Vorteile sind einfach zu verführerisch."

→ andere Unternehmen. Doch sie sind viel schneller, als es die IT-Organisationen in den meisten Firmen sein können. Die Provider überwachen ihre Infrastruktur engmaschig und achten genau darauf, dass Sicherheitsaktualisierungen unmittelbar und ohne Verzögerung umgesetzt werden. Zudem setzen sie möglichst immer die besten Tools ein und beschäftigen sich intensiv mit neuen Entwicklungen sowohl in der Cyberkriminalität als auch in der Security-Technologie. Das macht Cloud-Services deutlich sicherer als die meisten On-Premises-Installationen. Generell ist die Cloud im Aufschwung, das merken wir beispielsweise auch an unseren eigenen Umsätzen. Natürlich bieten wir sowohl On-Premises-Lösungen als auch Managed Services in der Cloud an. Doch die Umsatzentwicklung zeigt uns klar, dass Security aus der Cloud im Aufschwung ist. Das ist in anderen Branchen ähnlich. Die Vorteile sind einfach zu verführerisch.

**ITD:** *Ein typisches Argument gegen die Cloud ist ja immer der Schutz geschäftskritischer Daten. Wie gehen Sie damit um?*

**Jetter:** Um mit geschäftskritischen Daten umzugehen, verfügen wir über robuste Sicherheitsmaßnahmen, die den Datenschutz und die Datensicherheit gewährleisten. Hierzu gehört u.a. die Speicherung der Daten innerhalb der Europäischen Union mit all den damit verbundenen gesetzlichen Bestimmungen sowie die Nutzung von Verschlüsselungstechnologien, um sicherzustellen, dass Daten während der Übertragung geschützt sind.

**ITD:** *In diesem Zusammenhang: Wie sind Ihre Erfahrungen mit der Datenschutz-Grundverordnung (DSGVO)? Hat sie sich bewährt oder muss sie überarbeitet werden?*

**Jetter:** Die Datenschutz-Grundverordnung ist ein wichtiger Schritt zur Stärkung der Datenschutzrechte von Personen und hat den Datenschutz in der Europäischen Union deutlich verbessert. Die Unternehmen sind dazu gezwungen, sich intensiver mit ihren Datenverarbeitungsprozessen auseinanderzusetzen und Sicherheitsmaßnahmen umzusetzen. Damit ist das Bewusstsein für Datenschutz und Datensicherheit gestiegen und der Schutz personenbezogener Daten besser geworden. Allerdings ist die Umsetzung der DSGVO nicht immer einfach verlaufen. Zu viele Unternehmen haben nach wie vor Schwierigkeiten, sie zu verstehen und umzusetzen. Denn die DSGVO ist sehr komplex und erfordert ein hohes Maß an Fachwissen. Zudem hat die Umsetzung hohe Kosten verursacht, insbesondere für kleinere Unternehmen. Es ist jedoch wichtig zu betonen, dass der Schutz personenbezogener Daten eine Herausforderung ist, die sich ständig weiterentwickelt. Auch die Bedrohungen unterliegen einem ständigen Wandel. Deshalb sollten Unternehmen und Politik sicherstellen, dass die 2018 wirksam gewordene DSGVO mit der Zeit geht. Sie muss auf neue Entwicklungen und Herausforderungen bei Datenschutz und Datensouveränität reagieren.

**ITD:** *Seien wir ehrlich: Ein Problem für die Datensouveränität ist das Quasi-Monopol von IT-Riesen aus den USA und die gleichzeitig völlig andere Auffassung von Datenschutz, vor allem bei Behörden. Wie schätzen Sie die aktuelle Situation ein?*

**Jetter:** Der IT-Markt ist in der Tat von US-Unternehmen beherrscht. Das US-Datenschutzrecht besteht aus einem Flickenteppich von sektor- und bundesstaatsspezifischen Gesetzen. Nach jahrzehntelanger Arbeit wurde im Juni 2022 der Entwurf eines Bundesgesetzes zum Datenschutz verabschiedet. Er ähnelt in seinem generellen Anspruch der DSGVO, auch wenn er Schlupflöcher und Ausnahmen enthält. Selbst wenn das Gesetz beschlossen wird, muss sich erst zeigen, ob es tatsächlich DSGVO-konform ist. Dasselbe gilt hinsichtlich des Dekrets für ein neues Datenschutzabkommen zwischen den USA und der EU, das Präsident Joe Biden im Oktober 2022 erlassen hat. Ein globaler Ansatz ist entscheidend, beispielsweise ein weltweites Abkommen über Datenschutzstandards für den internationalen Datenverkehr. Doch die Fortschritte dabei vollziehen sich in fast geologischen Zeiträumen. Der Datenverkehr zwischen der EU und den USA wird also noch viele Jahre lang schwierig sein. Solange sollten Unternehmen die Notwendigkeit internationaler Datenübertragungen hinterfragen und zu einer stärker lokalisierten Datenverarbeitung übergehen. <

# 25

Das Interview mit Klaus Jetter finden Sie auch auf www.it-director.de

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*

# Die Höhen und Tiefen der Digitalisierung

**Alle reden vom digitalen Wandel. Unternehmen jeder Größe bis hin zu Behörden spüren den zunehmenden Veränderungsdruck. Doch wie kommt die Digitalisierung in der Praxis voran?**

von Alexander Lorber,
*Redaktion IT-DIRECTOR*

> Laut einer DIHK-Umfrage von Ende 2022 unter mehr als 4.000 Betrieben bleiben die Unternehmen in Deutschland wie schon im Vorjahr bei ihrer durchwachsenen Selbsteinschätzung in puncto „Digitalisierung“ und bewerten ihren Digitalisierungsgrad im Durchschnitt mit der Schulnote „befriedigend“ (2,9). Aber spiegelt diese Sichtweise den echten Fortschritt wider? Marc Oliver Hugger, Chief Executive Officer (CEO) bei Tresonus: „Die Definition von Digitalisierung ist kein klar umrissener Standard, sondern bietet viel Spielraum. Für die einen ist Digitalisierung nur das Arbeiten mit Office, für die anderen, manuelle Tätigkeiten stringent in einem Workflow mit KI umzusetzen.“ Die größte Herausforderung sei daher, eine klare und konsequente Digital-Only-Unternehmensstrategie zu schaffen.

Während die Digitalisierung im privaten Umfeld rasant voranschreitet, kommt sie in vielen Unternehmen und in der öffentlichen Verwaltung eher schleppend voran. Bei vielen Unternehmen fehle schlicht das echte Verständnis für ihr Kerngeschäft und wie sie es durch die Möglichkeiten der Digitalisierung verändern, gestalten und ausbauen könnten, meint Christian Rauch, Vice President Transformation Consulting Services bei der iTSM Group. „Bei der Mehrheit der Unternehmen drängt sich der Eindruck auf, man müsse Digitalisierung betreiben, weil es irgendwie ja alle anderen auch tun.“ Dies sei eher ein Mitschwimmen, als dass es einem klaren strategischen Geschäftsziel folge.

## Digitalisierung ist kein Selbstzweck

Auch Hugger betont, die Digitalisierung sei kein Selbstzweck und dürfe nicht um der Digitalisierung willen erfolgen. „Im Vordergrund steht die Effizienz des Gesamtprozesses – auch wenn eine hybride Strategie das erreicht.“ Das heißt, wo analoge Prozesse Sinn machen, können sie durchaus bestehen bleiben. Dort komme man aber nur hin, wenn man eine Digital-Only-Strategie anstrebe – sonst würden alte analoge Strukturen per se nicht ersetzt. „Leider kommt bei zu

**Die Digitalisierung** *hilft Unternehmen dabei, Kosten zu senken und Arbeitsabläufe effizienter zu gestalten, um innovativ und wettbewerbsfähig zu bleiben.*

vielen Unternehmen der Druck nur seicht von außen, geschweige denn überhaupt von innen", meint Hugger. „Es fehlt der Druck, weil auch die objektive Vergleichbarkeit zu Wettbewerbern fehlt." Gleichzeitig gehe es den Unternehmen noch zu gut, um einen Digitalisierungsdruck von innen aufzubauen. „Die größte Herausforderung ist aber in meinen Augen der Generationenwandel", sagt Sirko Schneppe, Chief Customer Officer (CCO) bei Diva-e. Heutzutage würden die meisten Leitungspositionen noch Menschen besetzen, die zwar mit dem PC aufgewachsen sind, die aber das Internet nur als E-Mail-Postfach verstehen. „Sie unterschätzen die Möglichkeiten und fokussieren auf die Risiken, um sich dieser Herausforderung nicht mehr stellen zu müssen."

## Know-how ist eine wichtige Komponente

Zwar haben Russlands Krieg gegen die Ukraine, Probleme in den weltweiten Lieferketten sowie die weiterhin hohe Inflation Unternehmen aus fast allen Branchen zugesetzt, laufende Digitalisierungsvorhaben bremsen die aktuellen Krisen aber kaum aus. „Solche Projekte im Kerngeschäft sind nicht von Budgetkürzungen oder Ähnlichem betroffen und werden auch nicht verschoben", sagt Christian Rauch, denn „durch Digitalisierung erwartet man sich in der Regel mehr Unabhängigkeit, Kostensenkungen und höhere Flexibilität, um auf Veränderungen am Markt sowie gesellschaftlicher Art zu reagieren".

Damit werde die Digitalisierung eher als Notwendigkeit gesehen, diesen aktuellen Veränderungen zu begegnen. „Digitalisierung ist auf allen Ebenen zu wichtig geworden, um sie aufzuschieben, und viele allgemeine Investitionen benötigen digitale Komponenten und eine entsprechende IT-Architektur, um überhaupt zu funktionieren", betont Sirko Schneppe. Dabei ist klar, dass der digitale Wandel nicht ohne versierte Fachkräfte gelingen kann. Doch inwieweit stellt der branchenweite Fachkräftemangel in diesem Kontext ein Problem dar? „Kaum, wenn die Unternehmen neue, kreative Wege finden, Fachkräfte zu gewinnen und zu →

**Christian Rauch,** *iTSM Group: „Wer die Digitalisierung als Möglichkeit versteht, Zusammenarbeits- und Entscheidungsmodelle neu zu gestalten, wird auch in Zeiten des Fachkräftemangels bestehen können."*

**Sirko Schneppe,** *Diva-e: „Digitalisierung ist auf allen Ebenen zu wichtig geworden, um sie aufzuschieben, und viele allgemeine Investitionen benötigen digitale Komponenten, um überhaupt zu funktionieren."*

**Marc Oliver Hugger,** *Tresonus: „Wer glaubt, Corona hätte die Prozesse beschleunigt, wird vom Gegenteil überzeugt. Behörden haben beim Thema ‚Digitalisierung' vollkommen versagt."*

binden", ist Rauch überzeugt. „Lokalität, formale Ausbildung und Ähnliches spielen eine immer untergeordnetere Rolle. Wer intelligentes Sourcing im Personalstamm betreibt, kann seine Digitalisierungsvorhaben mit Geschwindigkeit umsetzen."

Hugger hingegen sieht im Fachkräftemangel gewisse Risiken für Digitalisierungsinitiativen: „Auf der einen Seite entsteht heute ein Engpass, wenn Fachleute nicht bei Digitalisierungsaufgaben unterstützen können. Auf der anderen Seite werden durch dieses Versäumnis Potenziale bei der Digitalisierung morgen nicht genutzt werden können, z.B. bei der Automatisierung von Prozessen. Das bedeutet, dass Unternehmen perspektivisch der Herausforderung entgegentreten, auch für solche Aufgaben Personal zu finden." Schneppe ist überzeugt, dass sich personelle Engpässe weniger auf Vorhaben auswirken als vermutet, denn der Arbeitsmarkt sei durchlässig. Aber: „Nach meiner Erfahrung beginnt der Arbeitskräftemangel eher beim angestammten Personal, welches innerbetrieblich die digitalisierten Projekte steuern soll. Hier gibt es schlicht zu wenig qualifizierte Fachkräfte, die Betriebliches mit Digitalem in Einklang bringen", mahnt Schneppe und stellt fest: „Je mehr die Technologie zum Wettbewerbsfaktor wird, umso gezielter sollte man hier auch intern personell nachrüsten und sich informiert halten – insbesondere auf der Management-Ebene und bei Strategieentscheidungen."

## Der Wandel in den Köpfen

Die Experten sind sich überwiegend einig, dass heute niemand mehr den Anforderungen, die die Digitalisierung an Wirtschaft und Gesellschaft stellt, aus dem Weg gehen kann – und es gibt noch eine Menge zu tun: „Wer glaubt, Corona hätte die Prozesse beschleunigt, wird vom Gegenteil überzeugt. Behörden haben beim Thema ‚Digitalisierung' vollkommen versagt", sagt Marc Oliver Hugger. Statt echter Digitalisierung würden die meisten Behörden noch immer auf das Verständnis der Gesellschaft setzen. Darauf sollten sich Unternehmen bei ihren Kunden und Mitbewerbern lieber nicht verlassen. „Selbst der Bau einer Lagerhalle ist heutzutage ohne digitale Ansätze nicht mehr möglich", so Schneppe. „Jedes Unternehmen, jede Organisation sollte sich eine eigene Strategieabteilung oder ein Team leisten, welches die technologische Entwicklung ‚außerhalb' der Kernwertschöpfung beobachtet und daraus eigene Strategien und Investitionsprojekte ableitet, oder bei Bedarf eine externe Beratung hinzuholen." Woran es aus seiner Sicht meistens fehlt, sei der Blick auf die indirekten Einflüsse auf das Unternehmen. „Die Frage etwa, wie und wann KI ihre betrieblichen Prozesse beeinflussen wird, können nur wenige Unternehmer zielführend beantworten. Doch für Ansätze, wie KI für die eigenen Produkte und deren Weiterentwicklung eingesetzt werden kann, gibt es fast überall Experten und Produktmanager, die darauf sehr gute Antworten haben", meint der Experte.

Nicht zuletzt geht es bei der Digitalisierung immer auch darum, innovativ und wettbewerbsfähig zu bleiben und noch mehr Effizienz in die Arbeitsabläufe zu bringen. „Wer die Digitalisierung als Möglichkeit versteht, Zusammenarbeits- und Entscheidungsmodelle im Unternehmen neu zu gestalten, wird auch in Zeiten des Fachkräftemangels als attraktiver Arbeitgeber und erfolgreiches Unternehmen bestehen können", resümiert Christian Rauch. <

Das E-3 Magazin

## SUMMIT DER SAP-COMMUNITY

# COMPETENCE CENTER

## Salzburg, 1. und 2. Juni 2023


**April 2023:**

**Das Magazin zum Competence Center Summit 2023**

In dieser Ausgabe befindet sich das E-3 Extra zum Summit mit dem Beitrag zur SAP-Keynote von Uwe Grigoleit sowie weiteren Wissensbeiträgen der Aussteller und Sponsoren über Automatisierung, SolMan und ALM, Monitoring, Lizenzmanagement und natürlich Steampunk als zweite Keynote auf dem Summit in Salzburg.

### Conversion, ALM, Lizenzen und Steampunk,

die SAP-Basis-Funktionen und damit das CCC, Customer Competence Center, und CCoE, Customer Center of Expertise, sind sowohl für die Private (On-prem) als auch für die Public Cloud die Garantie für nachhaltigen Erfolg. Wir greifen die Tradition des erfolgreichen CCC-Forums auf und präsentieren den Competence Center Summit 2023.

Auf dem Weg nach Hana und S/4 entstehen viele Fragen hinsichtlich Betriebsmodell, Architektur, Lizenzen und natürlich Basissupport. Viele dieser Fragen werden am 1. und 2. Juni in Salzburg auf dem Summit 2023 beantwortet.

Der Summit liefert die On-prem- und Cloud-Antworten zu SolMan und ALM sowie Maintenance, Monitoring, System- Updates, Applikationsbetreuung, Programmdokumentation, DevOps und API, Change Management, ITSM und 1st/2nd Support, Sourcing-Strategien, Automatisierung und Modifikationen, DB-Management und Berechtigungsmanagement etc.

Jetzt anmelden: Die Teilnahmegebühr zum Summit exkl. USt. beträgt 590,– Euro.

Alle Infos unter e-3.de/summit-cc

E-3 Summit **COMPETENCE CENTER** wird gesponsert von:

DATA MIGRATION INTERNATIONAL · itesys · new relic

**e-3.de/summit-cc/**

KOMMENTAR



# Wie sich Digitalisierungshürden überwinden lassen

**Im Kommentar** plädiert **Andreas Eichhorn,** Managing Partner der Beratungssparte „Business Design" der Cosmo-Consult-Gruppe, im Rahmen von Digitalisierungsprojekten für Ansätze wie Living Organisation, um gemeinschaftlich agiler zu werden.

> In der Praxis unterschätzen Geschäftsleitung und C-Level immer wieder, dass sich Veränderung nicht erreichen lässt, indem eine fertige Digitalstrategie per Powerpoint präsentiert wird. Erst wenn Menschen die Informationen in den persönlichen Kontext setzen und praktische Erfahrungen machen, wird die Transformation greifbar. Dazu braucht es geeignete Räume und Formate, damit die Mitarbeiter in Gruppen diskutieren und mitmachen können.

*Echte Transformation erfordert laut* **Andreas Eichhorn** *eine Neuaufstellung – gemeinsam mit den Mitarbeitern.*

## Vorbereitet auf Veränderungsdruck?

Wir sehen, dass Geschwindigkeit, Komplexität und Dynamik zunehmen. Unternehmen sollten deshalb Veränderung anders denken, als es bisher üblich war: Es geht nicht um ein Change-Management-Projekt, das irgendwann abgeschlossen ist. Stattdessen müssen eine dauerhafte, kontinuierliche Change-Kompetenz und eine flexiblere, agilere Organisationsstruktur aufgebaut werden, die Veränderung aus sich heraus erzeugt und von außen aufgreifen. Dafür eignet sich das Konzept der Living Organisation besonders gut: Lebende Organismen passen sich auch immer weiter evolutionär an wechselnde Umstände an.

## Mehr Verantwortung an die Teams geben

Bisher werden Entscheidungen meist zentral an wenigen Stellen getroffen, die weit weg von der eigentlichen Situation sind. Hier ist ein Wandel wichtig: Die Entscheidungskompetenz sollte dezentral in autonome Teams gebracht werden. Arbeitet also ein Team direkt mit dem Kunden zusammen, dann sollte es nicht zuletzt aus Zeitgründen selbst Entscheidungen treffen können. New Leadership wird im Modell der Living Organisation zur Teamkompetenz: Die Führungsverantwortung hängt nicht mehr an einer Position, sondern verteilt sich auf unterschiedliche Rollen.

## Neue Führungsqualitäten entwickeln

New Leadership bedeutet, dass klassische Führungskräfte auch Macht und Kontrolle abgeben. In manche Rollen werden Mitarbeiter in neuen Konzepten hineingewählt, manche Rollen werden auf Zeit vergeben. Das bedeutet letztlich einen Wandel von Macht- hin zu Kompetenzhierarchien. Auch hier gibt es gewichtige Rollen, die mit einem hohen Reifegrad einhergehen. Gerade für Menschen, die stark an traditionellen Karrierepfaden orientiert waren, ist das nicht einfach. Die Praxis zeigt aber, dass die Akzeptanz erstaunlich hoch ist. So verließ bei der Tochter eines Automobilkonzerns, die sich innerhalb eines knappen Jahres auf die neue Organisationsform umgestellt hat, nur ein Prozent der Beschäftigten das Unternehmen – trotz umfassender Veränderungen. Die meisten haben schnell passende Aufgaben für sich gefunden. Wichtig ist aber auch für Sponsoren und Treiber der Transformation, einen langen Atem mitzubringen – schließlich geht es nicht um kleine Veränderungen, sondern um das Erreichen einer neuen Entwicklungsstufe. <

„Unternehmen sollten Veränderung anders denken, als es bisher üblich war."

# FÜR MEHR DIGITALKOMPETENZ

# DER NEWSLETTER

**IMMER AUF DEM AKTUELLEN STAND!**
**FÜR IHREN ERFOLGREICHEN IT-EINSATZ IM UNTERNEHMEN**


**JETZT ANMELDEN:**
***it-director.de***

**FOLGEN SIE UNS AUCH BEI**

**HIER ANMELDEN**

# „Digitalisierung geht immer mit Veränderungen einher“

Über die größten Herausforderungen bei der Digitalisierung berichtet **Maria Truong,** Standortleitung der CNT Management Consulting in Mainz, **im Interview.**

**ITD:** *Frau Truong, die Corona-Pandemie hat Deutschland einen Digitalisierungsschub verliehen – aber wo „stottert“ der Digitalisierungsmotor derzeit noch?*
**Truong:** Da gibt es unterschiedliche Gründe, warum es an manchen Ecken noch etwas langsamer geht, und vor allem gibt es Unterschiede zwischen den Branchen. In vielen Unternehmen stehen sich Entscheidungsträger manchmal selbst im Weg. Oft wurden oder werden unterschiedliche IT-Projekte unkoordiniert aus der Taufe gehoben. Abstimmungen dazu fehlen teilweise. Darüber hinaus warten manche Firmen auch noch ab – Digitalisierung geht immer mit Veränderungen einher; und dazu sind noch nicht alle bereit. Man greift natürlich auf bestehende Prozesse zurück und deckt viele Verbesserungspotenziale auf. Oft wird das fälschlicherweise mit einem Ersetzen von Stellen oder Mitarbeitern gleichgesetzt. Aber eigentlich ist es klar das Gegenteil. Die gewonnene Zeit etwa können die Mitarbeiter viel besser an anderer Stelle einsetzen. Klassisches Beispiel: die manuelle Abarbeitung von Eingangsrechnungen. Nach der Automatisierung bei unseren Kunden bleibt der Fachabteilung viel mehr Zeit, um eine Qualitätskontrolle intern sowie extern zu betreiben, das Stammdatenmanagement zu optimieren und Prozesse zu standardisieren. Die Mitarbeiter sind nicht mehr einfach Sachbearbeiter, sondern tragen zur Verbesserung der gesamten Wertschöpfungskette bei, indem sie Prozesse besser verstehen lernen und stetig verbessern. Wichtig ist dabei, alle Beschäftigten in die Digitalisierungsprojekte zu integrieren und ihre Sichtweise zu berücksichtigen.

*Die 1982 geborene Österreicherin* **Maria Truong** *studierte Betriebswirtschaft und Informationsmanagement an der FH Salzburg und startete ihre SAP-Karriere als Inhouse-Logistik-Beraterin in Salzburg.*

**ITD:** *Wie wirken sich die aktuellen Krisen (Russland-Ukraine-Krieg, steigende Energiekosten, Inflation etc.) auf die Digitalisierungsvorhaben aus?*
**Truong:** Wir können derzeit eigentlich keinen Negativtrend bei unseren Kunden erkennen. Zu Beginn der Pandemie wurden tatsächlich einige Vorhaben verschoben – aber die derzeit geplanten Projekte laufen weiterhin. Die Unternehmen sehen natürlich auch die Chance, aus Krisen gestärkt herauszukommen. Gerade bei steigenden Energiekosten oder der Inflation sehen sie die Vorteile von Digitalisierung – wo man aufgrund einfacherer Prozesse oder durch IT-Unterstützung überflüssige Arbeitsschritte oder langwierige manuelle Tätigkeiten einsparen kann und die Durchlaufzeiten somit verkürzen kann.

**ITD:** *Welche Ängste und Bedenken äußern Ihre Kunden in Bezug auf die Digitalisierung?*
**Truong:** Kosten, Sicherheit, Mitarbeiter – das sind sicherlich die drei Hauptthemen, die immer wieder zur Diskussion stehen. Viele sehen natürlich nicht sofort den Mehrwert einer Investition in die Digitalisierung. Aber um wettbewerbsfähig zu bleiben, gibt es mittel- bis langfristig keine Alternativen. Wir sehen das bei einigen Unternehmen bereits, wie sie vielerorts hinterherhinken und aufgrund der komplexen Arbeitsweisen viel langsamer agieren als ihre Konkurrenten. Auch die Betreuung der alten Systemlandschaften bzw. die Systembrüche bergen viele Fehlerpotenziale, erschweren den täglichen Arbeitsablauf und verursachen immense Mehrkosten. Diese Kosten sollte man lieber in die Digitalisierung und Vereinfachung über-

> „Viele sehen natürlich nicht sofort den Mehrwert einer Investition in die Digitalisierung.“

holter Prozesse investieren. Und hat man auch bezüglich der IT-Sicherheit Bedenken, dann sei hier klar gesagt, dass mit einer vernünftig aufgesetzten Systemlandschaft auch die Sicherheit gewährleistet ist. Viele veraltete Systeme und Netzwerke haben einen hohen Wartungs- und Sicherheitsaufwand bzw. sind anfälliger für Angriffe von außen. Der Gang in die Cloud gewährleistet darüber hinaus zusätzlichen Schutz. Man lagert das Datensicherheitsthema aus und überlässt die Arbeit Experten, die darauf spezialisiert sind.

Die Ängste und Bedenken der Mitarbeiter aus den Fachbereichen sind mitunter eine der größten Herausforderungen in einem Digitalisierungsprojekt. Diese Herausforderung ist nicht sofort zu Beginn erkennbar und entwickelt sich meistens im Laufe des Projekts. Viele Projektmanager und Entscheidungsträger erkennen zu spät, dass die betroffenen Mitarbeitenden zu wenig oder viel zu spät in das Projekt integriert wurden. Die Motivation und vor allem die Vorbereitung der Fachbereiche und deren Teams auf die kommenden Änderungen sind das A und O eines solchen Projekts.

**ITD:** *Was geben Sie den Entscheidern als Handlungsempfehlungen mit auf den Weg?*

**Truong:** Entscheider müssen sich mit den unternehmensinternen Prozessen, Herausforderungen und Potenzialen auseinandersetzen, um zu erkennen, was das Unternehmen wirklich benötigt und vor allem auch verkraftet. Es muss nicht auf Biegen und Brechen die teuerste und neueste Software angeschafft werden. Die Mitarbeiter müssen von Beginn an eingebunden werden – wenn möglich sogar schon bei der Auswahl der Software. In sogenannten Pre-Studies, die wir Kunden ebenfalls anbieten, erarbeitet man einerseits die bestehenden Prozesse, hat aber andererseits die Möglichkeit, sich von der bestehenden Systemlandschaft und Datenstruktur ein Bild zu machen. Das erleichtert Beratungshäusern wie uns zu erkennen, welcher Bedarf besteht, aber auch, wie viel Potenzial und Aufwand hinter einem Digitalisierungsprojekt stecken. Darüber hinaus können wir damit besser abschätzen, was die Organisation in der Lage wäre zu verdauen – das schließt die Fachbereiche und deren Mitarbeitenden sowie die interne IT und das Management mit ein. Entscheider müssen von Beginn an ein aktives Change Management betreiben, offen für Änderungen sein und am Ende des Tages diese Änderung selbst aktiv mittragen. <

*Oft sind bei* **Digitalisierungsvorhaben** *die Ängste und Bedenken der Mitarbeiter im Unternehmen die größte Herausforderung.*

ALEXANDER LORBER

# Wachsendes Digitalgeschäft

**Die Digitale Transformation von Giesecke+Devrient (G+D) hat sich als Erfolgsgarant erwiesen. Der Technologiekonzern verzeichnete ein starkes Geschäftsjahr 2022.**

> Besonders stark entwickelte sich das Geschäft mit dem Internet of Things (IoT), dem elektronischem Bezahlen und der Cybersecurity. Damit stellte das breit gefächerte Portfolio seine Resilienz auch in einem Jahr mit zahlreichen weltweiten Krisen unter Beweis. Trotz der Corona-Pandemie, Russlands Krieg gegen die Ukraine, weltweiter Logistikschwierigkeiten, mangelnder Verfügbarkeit von Chips und Energieknappheit konnten die Geschäftsaktivitäten weiter ausgebaut werden.

## Digitalisierung als Wachstumsmotor

Als starker Treiber des Geschäftserfolgs erwies sich die erfolgreiche Digitale Transformation des Unternehmens. Der Konzern erwirtschaftet einen relevanten Teil seines Umsatzes mit digitalen Produkten und Lösungen. Mit seinen vier Kernfeldern „Bezahlen“, „Konnektivität“, „Identitäten“ und „Digitale Infrastrukturen“ adressiert das Unternehmen wichtige Zukunftsmärkte und blickt zuversichtlich auf das Geschäftsjahr 2023. <

**Im Internet:** www.gi-de.com/de

## Vorschau auf Heft 5/2023

Erscheinungstermin:
22. Mai 2023
Redaktions- & Anzeigenschluss:
27. April 2023

**Themen:** IT-Dienstleistung und Managed Services, Automatisierung im Lager- und Logistikbereich sowie reibungsloser IT-Betrieb dank Hochverfügbarkeit

Special: Logistik

# Nachhaltige Lieferketten

*> Innovative Technologien werden im Zuge der Digitalisierung und des steigenden Zeit- und Kostendrucks immer wichtiger für die Lager- und Transportlogistik. In der kommenden Ausgabe erfahren Sie, wie Unternehmen ihre Prozesse mithilfe von Rugged Devices, Drohnen, Datenbrillen, Robotern oder Künstlicher Intelligenz automatisieren und nachhaltig gestalten können. <*

IT DIRECTOR
BUSINESS · PEOPLE · COMPANIES
vereinigt mit Client/Server-magazin

## 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@it-director.de

**Internet:** www.it-director.de

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

**Autoren dieser Ausgabe:** Dr. Joachim Bühler, Andreas Eichhorn, Pawel Jankowski, Benjamin Jansen, Stefan Käser, Simeon Mussler, Dr. Karsten Nohl, Fabien Rech, Michael Scheffler, Dr. Sebastian Schmerl, Dr. Dominik Schürmann, Jochen Schüssler

**Grafik/Layout:** Gerhard Samland

**Titelfoto:** Claus Uhlendorf

**Bildnachweis:** Claus Uhlendorf (Titel, 4, 18-23, 25), CNT (48), Doublecloud (7), Dropbox (9), Getty Images / iStock / Getty Images Plus (Titel, 3-6, 10, 12-17, 26+27, 29+30, 32-37, 39, 41-43, 49+50), Getty Images / OJO Images (38+39), Heide Velten (5, 40), iTSM (44), Lea Sommerhäuser (3), Sievers Group (10), Strabag (9), Tobias Koch (14), Tresonus (44) sowie Produkt-, Schmuck- und Personenfotos der genannten Anbieter/Hersteller.

**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:**

**Jahresbezugspreise**
**Inland:** EUR 75,- inkl. Versand u. MwSt.
**Europa:** EUR 99,- inkl. Versand

**Erscheinungsweise:** 10 x jährlich

**Abonnenten-Service:** Tel.: 0 22 04 / 92 14 - 0

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

Gedruckt auf chlorfrei gebleichtem Papier

**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 Sinne der Prägnanz und Verständlichkeit der Texte generell.

**Verlag:**

MEDIENHAUS Verlag GmbH
Bertram-Blank-Straße 8 · 51427 Bergisch Gladbach
Tel.: 0 22 04/92 14-0 · Fax: 0 22 04/92 14-30

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

**Geschäftsführer:** Klaus Dudda

WISSEN, WAS ZÄHLT
Geprüfte Auflage
Klare Basis für den Werbemarkt

LAC/2011
Mitglied

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

MEDIENHAUS VERLAG

# IT-ZOOM
WORLD OF TECHNOLOGY


## JEDEN TAG NEU!

# TECHNOLOGIE-NEWS MIT FORMAT


**1** connect Mobilfunk- und 5G-Netztest, Heft 01/2023: „sehr gut" (894 Punkte) für $O_2$; insgesamt wurden vergeben: 2x „sehr gut" (915 und 894 Punkte) und 1x „überragend" (952 Punkte). 5G ist für geeignete Endgeräte an immer mehr Standorten verfügbar. Weitere Informationen unter: o2.de/netz

**2** Mobilfunk-Studie 2022 durchgeführt vom Marktforschungsinstitut SWI Finance für Handelsblatt, Veröffentlichung Handelsblatt am 28.9.2022: „sehr gut" (87,4 Punkte) für $O_2$ Business; insgesamt wurden vergeben: 2x „sehr gut" (87,4 und 85,3 Punkte) und 4x „gut".