Juli '25

GENIUS THINKERS

think about

# Digital Future

**Impulse, Strategien und Lösungen für die Wirtschaft von morgen**

**Künstliche Intelligenz**

Gamechanger für die Wirtschaft

**Cyber Security**

Schutzschild in einer vernetzten Welt

**Digitalisierung**

Treiber für Resilienz & Wachstum

**Digitale Souveränität**

Europas Antwort

**Smart Factory**

Effizienz durch Automatisierung

# Mit KI in die Zukunft: Deutschlands Chance im globalen Wettlauf

Bild: Luke Jones/Unsplash

Wir erleben derzeit eine KI-Revolution, die eine enorme Dynamik entfacht und insbesondere ein großes Potenzial besitzt, unsere Wirtschaft wieder in Schwung zu bringen. Attraktive Anwendungsfelder entstehen zum Beispiel im Gesundheitssektor, in der Mobilität, im Bereich Luft- und Raumfahrt, auf dem Gebiet der Energiesysteme oder in der Modellierung des Klimawandels.

Der internationale Wettbewerb in der KI-Entwicklung ist massiv und wird derzeit von den USA und China dominiert. Dennoch verfügt Deutschland über hervorragende Voraussetzungen, um in diesem Wettlauf eine führende Rolle einzunehmen und wesentliche Anwendungsgebiete eigenständig zu erschließen. Entscheidend für den Erfolg ist ein Schulterschluss zwischen Wissenschaft, Wirtschaft, Anwendern, Kapitalgebern und weiteren Akteuren, um auf Schlüsselfeldern entscheidende Fortschritte zu erzielen.

In der Forschung sind Foundation-Modelle längst ein unverzichtbares Werkzeug. Sie sind in der Lage, hochkomplexe wissenschaftliche Fragestellungen auf einem bislang unvorstellbaren Niveau zu lösen. Bei der Entwicklung komplexer Foundation-Modelle ist die Helmholtz-Gemeinschaft führend, da wir über umfangreiche Datensätze, leistungsstarke Rechenkapazitäten, herausragende KI-Expert:innen sowie exzellente Wissenschaftler:innen aus verschiedenen Fachdisziplinen verfügen. Was fehlt, sind die richtigen politischen Weichenstellungen, um KI-gestütztes Wissen schneller in die Praxis zu überführen.

Die aktuelle Legislaturperiode bietet eine einmalige Chance, Deutschland als Innovationsstandort nachhaltig zu stärken. Als einer der führenden Akteure auf dem Gebiet innovativer Künstlicher Intelligenz setzen wir uns für eine nationale Initiative zum Aufbau regionaler KI-Kompetenzzentren ein. Diese sollen Spitzenforschung, Wirtschaft und weitere Schlüsselakteure gezielt vernetzen, um zentrale Anwendungsfelder voranzutreiben.

Bild: Helmholtz/Phil Dera

***Otmar D. Wiestler, Präsident der Helmholtz-Gemeinschaft***


## Impressum

Redaktion (verantwortlich):
Rüdiger Schmidt-Sodingen

Layout (verantwortlich):
Andrea Caduff

Coverfoto:
FlashMovie/iStockphoto

Distribution & Druck:
Die Welt, Axel Springer SE

Die Inhalte mit dem Label »Genius Partner« in dieser Veröffentlichung wurden in enger Zusammenarbeit mit unseren Kunden entwickelt und sind Anzeigen.

Herausgegeben von:
Genius Thinkers GmbH
Egzona Gashi
Grienbachstrasse 36
6300 Zug, Schweiz

Tel.: +41 58 510 99 39
E-Mail: info@genius-thinkers.com
Web: www.genius-thinkers.com


Inhalt: **04** Regulierung **06** AI Panel **12** Cyber Security **18** Digitalisierung **20** Digitale Souveränität **26** Smart Factory

Bild: Michael Schuff

4 **Regulierung der KI**

12 **Cyber Security**

26 **Smart Factory**


## Genius Partner • anacision GmbH

*think about: Künstliche Intelligenz*

# Kompetenz statt KI-Show: Warum Weiterbildung über den Erfolg von KI entscheidet

**Ein Gespräch mit Dr. Frank Oechsle, Geschäftsführer der auf KI-Beratung und Umsetzung spezialisierten anacision GmbH, über den Mehrwert von KI in der öffentlichen Verwaltung und warum Lösungen erst dann wirken, wenn Menschen sie verstehen.**

**Herr Dr. Oechsle, künstliche Intelligenz wird vielerorts als Effizienzbringer gefeiert. Wo sehen Sie den tatsächlichen Nutzen in der öffentlichen Verwaltung?**
KI bietet ein enormes Potenzial – gerade in der öffentlichen Verwaltung. Ob es um Prognosen, Automatisierung oder bessere Entscheidungsgrundlagen geht: Richtig eingesetzt, kann KI-Verwaltungsprozesse spürbar verbessern. Aber: Technologie allein bringt keine Wirkung. Entscheidend ist, dass sie in den richtigen fachlichen und organisatorischen Kontext eingebettet wird. Und genau da setzen wir bei anacision an.

***Dr. Frank Oechsle, Geschäftsführer anacision GmbH***

**Was unterscheidet erfolgreiche KI-Projekte von solchen, die im Pilotstatus verharren?**
Es ist das Zusammenspiel aus Fachlichkeit, Technologie und Organisation. In vielen Projekten wird die Technologie getestet – aber der Transfer in den Alltag bleibt aus. Erfolgreich sind die Projekte, bei denen die Fachbereiche von Anfang an eingebunden sind und selbst Anwendungsfälle mitgestalten. Dann entsteht nicht nur Akzeptanz, sondern auch echter, messbarer Nutzen.

**anacision bietet neben technischen Lösungen auch Schulungen an. Warum?**
Unsere Kernleistungen sind individuelle KI-Lösungen, die auf konkrete Herausforderungen zugeschnitten sind – insbesondere im öffentlichen Sektor. Damit diese Lösungen wirken, müssen die Beteiligten verstehen, was KI kann – und was nicht. Deshalb bieten wir Schulungen als gezielte Ergänzung an. Sie befähigen Projektverantwortliche, Führungskräfte und Fachabteilungen, KI einzuordnen, kritisch zu begleiten und sinnvoll in bestehende Abläufe zu integrieren. Das erhöht die Umsetzungsfähigkeit erheblich. Diese Schulungen sind im Übrigen nicht nur hilfreich, sondern laut EU AI Act auch verpflichtend: Anbieter und Betreiber von KI-Systemen müssen sicherstellen, dass ihr Personal ausreichend KI-Kompetenz besitzt – abgestimmt auf Einsatzkontext und Zielgruppe.

**Worauf kommt es bei der Kompetenzentwicklung an?**
Es geht nicht darum, alle zu Datenwissenschaftler:innen auszubilden. Viel wichtiger ist ein grundlegendes Verständnis: Welche Daten brauche ich? Wie entstehen Ergebnisse? Wo sind Grenzen? Wer das versteht, kann mit KI souverän arbeiten – und Entscheidungen fundiert treffen.

**anacision.de**

anacision

### Genius Tip

»**Technologie** verändert **Prozesse**. Doch **Kompetenz** verändert **Organisationen** – nachhaltig. Wer **beides** zusammen denkt, schafft echten **Mehrwert**.«

# Industrie digital denken heißt: Zusammenarbeit neu denken

**Wie sieht die Zukunft der Fertigung aus und was bedeutet digitale Exzellenz wirklich? Ob Engineering, Produktion oder Supply Chain – echte digitale Transformation gelingt nur, wenn alle an einem Strang ziehen. Dr. Florian Harzenetter, Global Industry Advisor bei PTC, erklärt, warum die Zukunft der Industrie in der Zusammenarbeit liegt.**

**Herr Dr. Harzenetter, wenn Sie an die Zukunft der Industrie denken, was sehen Sie vor sich?**
Eine vernetzte Welt, in der Ideen quasi in Echtzeit Realität werden. Eine Fertigung, in der Entwicklung, Produktion, Zulieferer und Kunden nicht getrennt nebeneinanderher arbeiten, sondern als digitales Ökosystem agieren. Der Weg dorthin führt aber nicht allein über Technologien, sondern erfordert auch die Fähigkeit, Menschen, Systeme und Prozesse intelligent zu verbinden.

**Das klingt groß gedacht. Wo stehen die Unternehmen heute wirklich?**
Viele Unternehmen sind weiter, als sie selbst glauben. Daten liegen vor, Prozesse laufen – aber nicht integriert. Entwicklung und Produktion arbeiten oft in Silos, Änderungen werden zu spät erkannt, die Qualität leidet. Digitalisierung muss mehr sein als nur »ein Tool mehr«. Es geht um Durchgängigkeit, Transparenz und Vertrauen in die Datenbasis.

**Also: Es geht nicht nur um neue Systeme – sondern um ein neues Denken?**
Ganz genau. Technologie ist wichtig, aber wer heute digital führend sein will, muss Silos aufbrechen, Zusammenarbeit neu organisieren und Verantwortung teilen. Digitale Transformation ist ein Mannschaftssport. Die Tools sind da – Cloud, KI, CAD, AR, PLM, MES, ERP – aber erst das Zusammenspiel macht sie wirksam. Der Kulturwandel ist dabei genauso entscheidend wie die Wahl der Technologie.

**Was bedeutet das für die Strategie von Unternehmen?**
Sie müssen weg vom Projektdenken. Digitale Exzellenz entsteht nicht aus einzelnen Leuchttürmen, sondern aus einer konsistenten Architektur, die Entwicklung, Fertigung, Qualität und Supply Chain verbindet. Das gelingt nicht auf Knopfdruck, sondern mit einem klaren Zielbild, skalierbaren Ansätzen und einem starken Partnernetzwerk. Besonders wichtig: Digitale Initiativen müssen im gesamten Unternehmen verankert sein, nicht nur in der IT-Abteilung.

**Welche Rolle spielt PTC in diesem Netzwerk?**
Wir sehen uns als Brückenbauer. Wir liefern das digitale Rückgrat, etwa mit unserer PLM-Plattform, die Entwicklung, Produktion und Service verbindet. Aber wichtiger noch: Wir bringen Know-how, Methoden und Partner zusammen. Unsere Mission ist es, Kunden zu befähigen, ihre eigene digitale Zukunft zu gestalten – pragmatisch, nachhaltig und zukunftssicher. Um flexible und erweiterbare Systeme zu schaffen, setzen wir auf Interoperabilität, offene Standards und enge Zusammenarbeit.

Wir arbeiten mit Reifegradmodellen, die Unternehmen helfen, ihren Standpunkt zu bestimmen und eine Roadmap für die nächsten Schritte zu entwerfen. Dabei ist entscheidend: Nicht der Vergleich mit anderen zählt, sondern die eigene Entwicklung entlang der strategischen Ziele. Wer sich konsequent weiterentwickelt, erreicht mit der Zeit echte Exzellenz.

Hierfür sind sowohl digitale Skills erforderlich als auch interdisziplinäres Denken – wir registrieren eine zunehmende Nachfrage nach Schulungen für die Weiterentwicklung dieser Kompetenzen. Unternehmen, die in Weiterbildung und Lernkultur investieren, sind langfristig klar im Vorteil – auch im Wettbewerb um Talente. Hinzu kommt: Digitale Technologien wie Augmented Reality oder virtuelle Schulungsumgebungen ermöglichen es, Wissen praxisnah und skalierbar zu vermitteln, selbst in komplexen, sicherheitskritischen Bereichen.

> » Technologie ist wichtig, aber wer heute **digital führend** sein will, muss **Silos aufbrechen**, **Zusammenarbeit** neu **organisieren** und **Verantwortung teilen.** «

*Dr. Florian Harzenetter*
*Global Industry Advisor*
*PTC*

**Wie verändert sich die Zusammenarbeit mit Partnern – und welche Rolle spielt Interoperabilität in der Industrie von morgen?**
Partnerschaftliche Zusammenarbeit wird zum strategischen Erfolgsfaktor. Früher war ein klarer Lieferant-Kunde-Gegensatz prägend; heute brauchen wir Ökosysteme, in denen Know-how, Daten und Innovationen gemeinsam wachsen. Kein Unternehmen kann die digitale Transformation allein stemmen. Entscheidend ist, wie gut Systeme und Prozesse verschiedener Partner miteinander kommunizieren. Interoperabilität ist dabei kein technisches Randthema, sondern Voraussetzung für Agilität, Resilienz und Wachstum.

Ein oft unterschätzter Aspekt dabei ist die Standardisierung von Schnittstellen. Unternehmen, die frühzeitig in offene und skalierbare Plattformarchitekturen investieren, sichern sich langfristige Flexibilität. Das ermöglicht nicht nur schnellere Innovation, sondern auch eine bessere Anpassung an regulatorische oder marktspezifische Veränderungen. Zudem wird durch gemeinsame Standards die Innovationsgeschwindigkeit im gesamten Netzwerk erhöht. Unternehmen können neue Partner, Produkte und Services nahtlos integrieren und dabei von einer deutlich schnelleren Time-to-Value profitieren.

**Was sind aktuell die größten Herausforderungen, die Sie bei Ihren Kunden sehen?**
Drei Themen tauchen immer wieder auf: Erstens, wie man schneller wird – Stichwort Time-to-Market. Zweitens, wie man Komplexität beherrscht – Stichwort Variantenvielfalt, Regularien und global verteilte Werke. Und drittens, wie man trotz Fachkräftemangel und Kostendruck innovativ bleibt. All das braucht digitale Lösungen, aber auch ein neues Mindset, das Fehler erlaubt, Lernen fördert und Verantwortung verteilt. Auch die Fähigkeit, dezentrale Teams effektiv zu steuern und zu motivieren, spielt eine zunehmend wichtige Rolle in der neuen Arbeitsrealität.

**Haben Sie ein konkretes Beispiel, wo das schon heute gelingt?**
Ja, etwa bei einem globalen Maschinenbauer, mit dem wir zusammenarbeiten. Früher hat es Wochen gedauert, bis Änderungen in der Entwicklung in der Fertigung ankamen. Heute läuft das durchgängig digital, Änderungen, Stücklisten, 3D-Arbeitsanweisungen sind in Echtzeit synchronisiert. Das Ergebnis: schnellere Anläufe, weniger Ausschuss, mehr Agilität und ein Team, das über Kontinente hinweg als Einheit agiert.

**Und die großen Trends, wie etwa KI, Nachhaltigkeit, Resilienz?**
Das sind keine Buzzwords mehr, das sind strategische Imperative. KI kann Prozesse automatisieren, Entscheidungsqualität steigern, Fehler vermeiden. Aber nur, wenn die Daten stimmen. Nachhaltigkeit wird zur Voraussetzung des Wirtschaftens und erfordert Transparenz über den gesamten Produktlebenszyklus. Und Resilienz beginnt nicht beim Risikomanagement, sondern bei der Fähigkeit, schnell und flexibel zu reagieren. Auch hierfür braucht es digitale Vernetzung.

**Was raten Sie Unternehmen, die 2025 den nächsten Schritt machen wollen?**
Drei Dinge: Erstens – starten! Beginnen Sie mit einem klar abgegrenzten Use Case und skalieren Sie dann. Zweitens – vernetzen! Holen Sie alle mit ins Boot: Engineering, Fertigung, IT, Qualität, Lieferanten. Digitalisierung ist keine Abteilung, sondern ein Kulturwandel. Und drittens – dranbleiben! Wir reden nicht von einem Sprint, sondern einem Marathon. Es braucht Ausdauer, Anpassungsfähigkeit und die Bereitschaft, aus Erfahrungen zu lernen. Unternehmen, die dies verinnerlichen, schaffen die Grundlage für kontinuierlichen Fortschritt.

**Und was wünschen Sie sich für die Industrie als Ganzes?**
Mut. Mut, neu zu denken, neu zu gestalten. Deutschland und Europa haben enormes Potenzial – technologische Stärke, industrielle Exzellenz, kreative Köpfe. Wenn wir das digital bündeln und gemeinsam handeln, dann gestalten wir nicht nur den Wandel, wir führen ihn an. Und genau das sollte unser Anspruch sein.

ptc

# Deutschlands KI-Zukunft

## Wie Deutschland den Anschluss im globalen KI-Wettbewerb schafft

**KI hat in den letzten Jahren einen beispiellosen Aufschwung erlebt und Einzug in nahezu alle Bereiche unserer Gesellschaft und Wirtschaft gehalten. Die Technologie hat die nächste globale Innovationswelle ausgelöst und wird diese maßgeblich prägen. Allerdings haben die politischen und wirtschaftlichen Rahmenbedingungen in Deutschland und der EU mit der technologischen Entwicklung nicht Schritt gehalten. Dieser Rückstand muss unbedingt aufgeholt werden. Dafür braucht es jetzt eine gemeinsame Kraftanstrengung durch Politik und Wirtschaft, um nicht weiter in der globalen KI-Entwicklung zurückzufallen, sondern ganz vorne mitzumischen.**

**Text** Daniel Abbou, Geschäftsführer KI Bundesverband

**Wo stehen wir aktuell?**
Das deutsche Wirtschaftswachstum stagniert seit geraumer Zeit, unser digitaler Rückstand nimmt im globalen und europäischen Vergleich zu, das Investitionsvolumen in KI- und Digitalunternehmen bleibt weit hinter vergleichbaren Wirtschaftsnationen zurück und der Einsatz von KI in der Industrie nimmt nur schleppend zu. Für den KI Bundesverband ist klar: Deutschland darf auf keinen Fall eine weitere Transformations- und Innovationswelle verpassen.

Das Zeitfenster, um zu handeln, schließt sich aber immer schneller. Während in Deutschland in den letzten Jahren nahezu digitalpolitischer Stillstand herrschte, haben andere Nationen milliardenschwere Innovationspakete verabschiedet. Erst kürzlich haben die USA die größte KI-Infrastrukturinitiative der Geschichte angekündigt und wollen in den kommenden Jahren bis zu 500 Millionen US-Dollar in die KI-Infrastruktur investieren.

**Wie kann eine Antwort Deutschlands und Europa aussehen?**
Angesichts dieser Ausgangslage ist die Frage, ob Deutschland und Europa eine Antwort auf solche KI-Initiativen geben sollten, eindeutig mit »Ja« zu beantworten.

KI-(Rechen-)Infrastruktur wird sich in den kommenden Jahren zweifellos zu einem Teil unserer Kritischen Infrastruktur entwickeln. Gemeinsame Investitionen von Politik und Wirtschaft sind daher unerlässlich, um wirtschaftliche Wettbewerbsfähigkeit und digitale Souveränität langfristig zu sichern.

Eine leistungsfähige KI-Infrastruktur ist von zentraler Bedeutung, der Zugang dazu ist derzeit jedoch stark eingeschränkt. Zwar gibt es in Deutschland Höchstleistungsrechenzentren, doch stehen diese primär der Forschung zur Verfügung. Gerade für deutsche KI-Startups wird die Entwicklung dadurch erschwert. Damit Innovationen nicht ins Ausland abwandern, bedarf es deshalb einer koordinierten Strategie von Wirtschaft und Politik, um entsprechende Infrastrukturprojekte zu realisieren und der deutschen Industrie und KI-Entwicklung eine leistungsfähige KI-Infrastruktur zur Verfügung stellen zu können.

Ein weiterer Wettbewerbsnachteil zeigt sich in der geringen Nutzung von KI-Anwendungen durch deutsche Unternehmen. Vor allem kleineren und mittleren Unternehmen (KMU) fehlt es an Know-how, Fachkräften und Ressourcen, um KI-Projekte zu realisieren. Hierfür müssen z.B. über ein KI-Voucher-Programm die entsprechenden Investitionsanreize geschaffen werden.

Ein weiterer Schwachpunkt ist die Finanzierung von KI-Unternehmen in Deutschland. Deutsche Start-ups sind im internationalen Vergleich stark unterfinanziert. Programme wie der Wachstumsfonds haben erste Fortschritte gebracht, aber weitere Maßnahmen sind dringend notwendig.

**Und nun: Quo vadis?**
Einmal entstandene Abhängigkeiten lassen sich oft nicht oder nur mit großem Aufwand wieder reduzieren. So wie Anfang 2022 die Wende in der deutschen Sicherheits- und Verteidigungspolitik eingeläutet wurde, bedarf es nun einer ebensolchen gemeinsamen Kraftanstrengung von Politik, Wirtschaft und Forschung, um Europas digitale Souveränität und strategische Unabhängigkeit zu sichern. Deutschland und Europa haben dafür die besten Voraussetzungen - jetzt gilt es, sie endlich zu nutzen.

### Über den KI Bundesverband

Der Bundesverband der Unternehmen der Künstlichen Intelligenz in Deutschland e.V. vernetzt die innovativsten KI und Deep Tech Unternehmen mit der etablierten Wirtschaft und Politik und ist mit rund 450 KI-Unternehmen das größte KI-Netzwerk Deutschlands. Die Mitglieder des KI Bundesverbands setzen sich dafür ein, dass diese Technologie im Sinne europäischer und demokratischer Werte Anwendung findet und Europa digitale Souveränität erreicht. Dafür muss die Bundesrepublik Deutschland und die EU ein attraktiver KI-Standort für Unternehmerinnen und Unternehmer werden, in dem Risikobereitschaft gewürdigt wird und Innovationsgeist auf die besten Voraussetzungen trifft.


Bild: Michael Schuff

### Zur Person

Daniel Abbou ist seit dem 1. Mai 2020 Geschäftsführer des KI Bundesverbandes.
Er war Pressesprecher in verschiedenen Finanz- und Wirtschaftsministerien, u.a. als Sprecher des ehemaligen Finanzsenators und späteren Staatssekretärs im Bundeswirtschaftsministerium Ulrich Nußbaum. Im ersten baden-württembergischen Kabinett Kretschmann bekleidete er die Funktion des stellvertretenden Regierungssprechers. Seine Begeisterung für Digitalisierung und Innovation begleitet ihn seit seiner Zeit als Fernseh- und Hörfunkjournalist für neue Technologien.

---

**Genius Partner • Santiago Advisors**

*think about: Künstliche Intelligenz*

# »Wer KI will, muss seine Organisation neu denken«

**Die meisten Unternehmen haben Künstliche Intelligenz längst auf der Agenda. Doch der große Durchbruch bleibt oft aus. Wieso das häufig nichts mit Technologie zu tun hat, erläutert Dr. Juan Rigall, Geschäftsführer der Strategie- und Organisationsberatung Santiago Advisors.**

**Herr Dr. Rigall, was beobachten Sie bei der Einführung von KI-Lösungen im Unternehmensalltag?**
Viele Unternehmen starten mit großem Enthusiasmus, aber die Wirkung bleibt aus. Ein häufig übersehener Grund: Sie versuchen, KI in bestehende Strukturen einzupassen – in klassische Hierarchien, starre Prozesse, isolierte Abteilungen. Doch KI braucht neue Formen der Zusammenarbeit, Entscheidungsfindung und Verantwortungsverteilung, um wirksam zu werden.

**Was heißt das konkret für die Organisation?**
Wettbewerbsvorteile entstehen nicht durch einzelne KI-Tools, sondern durch das Zusammenspiel von Technologie, Organisation und Menschen. Wer bestehende Rollen und Prozesse einfach digitalisiert, verpasst das eigentliche Potenzial. Es braucht vernetzte, lernfähige Einheiten statt funktionaler Silos und neue Rollenprofile, etwa für übergreifende Optimierung oder datenbasierte Entscheidungen.

**Welche Rolle spielt dabei der demografische Wandel?**
Eine zentrale. In Europa werden wir den Wettlauf um nachhaltige Wettbewerbsfähigkeit nur bestehen, wenn wir intelligent automatisieren. Herausforderungen gerade in für uns wichtigen Industrien wie Automotive, Chemie und Maschinenbau lassen keine andere Wahl. Repetitive Tätigkeiten müssen durch KI-gestützte Systeme ersetzt werden – nur so bleiben wir trotz schrumpfender Belegschaften leistungsfähig und gleichen künftig fehlendes Know-how aus.

**Ist KI dann noch ein Wettbewerbsvorteil?**
Tatsächlich werden immer mehr KI-Tools zur verfügbaren Regalware. Der Wettbewerbsvorteil entsteht woanders: Durch die gezielte Verknüpfung von Technologie mit dem sogenannten Domain Knowledge, dem unternehmensspezifischen Wissen über Materialien, Produkte und Prozesse. Wenn ich etwa in der Produktion ein KI-basiertes Kamerasystem zur Qualitätskontrolle einsetze, ist das allein keine Differenzierung. Erst wenn ich weiß, worauf es bei den Bauteilen ankommt, wie ich die Systeme sinnvoll trainiere und einbette, entsteht echter Mehrwert.

**Was raten Sie Unternehmen, die KI erfolgreich nutzen wollen?**
KI wird niemals in alten Strukturen skalieren. Wer die Chancen von KI wirklich nutzen will, muss daher sich selbst neu denken: Strukturen, Rollen und Kompetenzen müssen sich gemeinsam mit der Technologie entwickeln. Wer es heute schafft, seine Wettbewerbsvorteile in die digitale Welt zu überführen, wird sich auch morgen behaupten können.

### Genius Tip

**Drei Stellhebel für wirksame KI-Nutzung:**

1. Domain Knowledge – wissen, wie sich das eigene Know-how durch KI skalieren lässt.

2. Beurteilungskompetenz – verstehen, was sich technologisch tut, und was die Firma wirklich nach vorne bringt.

3. Strukturen – neue Rollen schaffen, alte Routinen loslassen, Organisation aktiv umbauen.

# »Der AI Act schafft vertrauenswürdige KI – und Chancen«

**KI »Made in Germany« steht für Qualität, Transparenz und digitale Souveränität. Ralf Pechmann, CEO Deutsche Telekom MMS, erklärt im Interview, warum eine starke Datenstrategie das zentrale Fundament für vertrauenswürdige KI bildet – und wie Unternehmen regulatorische Anforderungen wie den EU AI Act in Innovationschancen verwandeln.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Pechmann, Sie begleiten Unternehmen seit vielen Jahren bei der digitalen Transformation. Wie sehen Sie die aktuelle Dynamik rund um KI?**
Künstliche Intelligenz verändert zentrale Geschäftsprozesse – schneller, effizienter, intelligenter. Aber damit sie sinnvoll und verantwortungsvoll eingesetzt werden kann, braucht es ein stabiles Fundament. Daten sind dabei der Schlüssel. Die entscheidende Frage lautet: Haben wir die richtigen, sicheren und nutzbaren Daten, um KI überhaupt sinnvoll zu trainieren und einzusetzen?

**Viele Unternehmen sammeln Daten – aber haben keine echte Strategie. Warum ist das so kritisch?**
Weil Daten ohne Kontext, Struktur und klare Regeln zur Nutzung keine Wirkung entfalten. Eine moderne Datenstrategie ist nicht nur ein technisches Konzept, sondern ein unternehmerischer Steuerungsrahmen: Sie definiert, welche Daten wie gesammelt, verarbeitet, genutzt und geschützt werden – unter Einhaltung von Sicherheit, Transparenz und Compliance. Das ist entscheidend, um gesetzlichen Anforderungen wie der DSGVO gerecht zu werden – und künftig KI-Anwendungen im Sinne des EU AI Acts rechtskonform zu entwickeln und zu betreiben. Erst wenn diese Basis stimmt, kann KI im Unternehmen skalierbar, verantwortungsvoll und wirtschaftlich sinnvoll eingesetzt werden. Ohne diese Klarheit bleiben viele Potenziale ungenutzt – oder laufen ins Leere.

**Welche Verantwortung tragen dabei die Mitarbeitenden – und warum ist ihre Datenkompetenz so entscheidend für den Erfolg?**
Ohne ein grundlegendes Verständnis für den Wert von Daten – Data Literacy – wird jede Strategie zur Theorie. Mitarbeitende müssen verstehen, woher Daten kommen, wie sie verarbeitet werden und welche Verantwortung damit einhergeht. Nur so entsteht ein nachhaltiger Kulturwandel, der Innovation trägt und Vertrauen schafft.

**Was verstehen Sie persönlich unter KI »Made in Germany«?**
Es geht nicht um Herkunftssiegel, sondern um Werte: Qualität, Nachvollziehbarkeit, Datenschutz und digitale Souveränität. Unternehmen, die KI im Sinne europäischer Standards aufbauen – also fair, nachvollziehbar und sicher – schaffen Vertrauen bei Kunden, Partnern und Mitarbeitenden. Das ist ein echter Wettbewerbsvorteil, gerade im globalen Vergleich. Wenn wir diesen Anspruch ernst nehmen, müssen wir entsprechende Voraussetzungen schaffen. Dazu gehört, dass Unternehmen ihre Daten souverän managen, KI nicht nur einkaufen, sondern strategisch steuern, und sich unabhängig von einzelnen Technologieanbietern machen. Es braucht also nicht nur Infrastruktur, sondern ein eigenes Verständnis davon, wie Wertschöpfung in einer KI-getriebenen Wirtschaft funktioniert.

*Ralf Pechmann, CEO Deutsche Telekom MMS*

Für mich bedeutet KI »Made in Germany« deshalb vor allem Gestaltungswillen. Es geht darum, eine klare Haltung zu zeigen – für wirtschaftlich nachhaltige Innovation.

**Der EU AI Act wird in vielen Unternehmen vor allem als neue regulatorische Hürde und Innovationsbremse wahrgenommen. Welche Chancen sehen Sie dennoch?**
Die KI-Verordnung bringt vor allem eines: Planungssicherheit. Die Anforderungen sind hoch, aber klar definiert – und genau das schafft die Grundlage für verantwortungsvolle Innovation. Unternehmen, die frühzeitig auf Transparenz, dokumentierte Prozesse und ein aktives Risikomanagement setzen, können sich gezielt vorbereiten und Wettbewerbsvorteile sichern. Wir unterstützen sie dabei, auditierbare und rechtskonforme KI-Systeme aufzubauen – und regulatorische Vorgaben nicht als Bremse, sondern als Katalysator für nachhaltige Digitalisierung zu nutzen.

**Was sind aus Ihrer Sicht die wichtigsten Schritte, damit Unternehmen KI erfolgreich und verantwortungsvoll einsetzen können?**
Unternehmen brauchen dafür mehr als eine gute Idee oder starke Tools. Entscheidend ist ein systematisches Vorgehen – wir empfehlen sieben Maßnahmen, um wirklich »KI-ready« zu werden:

1. **Status-Quo analysieren:** Datenlandschaft, Prozesse, IT-Infrastruktur und Kompetenzen der Mitarbeitenden erfassen.

2. **Datenstrategie entwickeln:** Ziele, Verantwortlichkeiten, Governance und passende Architekturen (z. B. Data Mesh, Lakehouse) definieren.

3. **KI-Strategie etablieren:** Festlegen, in welchen Geschäftsbereichen KI wie eingesetzt werden soll – mit klaren Prioritäten, Prinzipien und Umsetzungsrahmen.

4. **Technologische Basis schaffen:** Cloud, Datenplattform und KI-Tools auswählen und skalierbar implementieren – mit Blick auf Sicherheit und AI-Act-Konformität.

5. **Organisation befähigen:** Mitarbeitende schulen, verantwortungsvollen Umgang mit Daten und KI fördern und Kulturwandel aktiv begleiten.

6. **Use Cases priorisieren:** Relevante Pilotprojekte mit messbarem Impact starten und skalieren.

7. **Strukturen schaffen und Regeln einhalten:** Damit KI sicher und verantwortungsvoll eingesetzt werden kann, braucht es klare Abläufe, Zuständigkeiten und Rollen. Gleichzeitig müssen gesetzliche Vorgaben wie der EU AI Act erfüllt, Risiken bewertet und Kontrollmechanismen etabliert werden.

Diese Schritte helfen Unternehmen, KI nicht nur sicher, sondern auch nachhaltig und wirksam einzuführen.

**Der letzte Punkt spricht ein entsprechendes Compliance-Risikomanagement an. Was müssen Unternehmen hier besonders beachten?**
Transparenz ist der Schlüssel. Es ist wichtig, dass die KI bei kritischen Themen ausschließlich unterstützend und vorbereitende wirkt und ein Mensch dann auf dieser Vorarbeit eine informierte Entscheidung treffen kann. Unternehmen müssen deshalb wissen, welche ihrer KI-Anwendungen als »Hochrisiko« eingestuft werden – und wie sie diesen gerecht


Bild: Deutsche Telekom AG / Westend61

werden. Das klingt nach Aufwand, ist aber vor allem: Risikominimierung und Zukunftssicherung.

Compliance-Risikomanagement bedeutet aber nicht nur, Gesetze einzuhalten – sondern frühzeitig zu erkennen, wo Risiken entstehen könnten. Es ist daher entscheidend, klare Standards und Zuständigkeiten zu definieren – beispielsweise für Trainingsdaten, Modellentscheidungen oder Zugriffsrechte. Wer überwacht? Wer dokumentiert? Wer greift ein, wenn etwas schiefläuft? Ein gutes Risikomanagement funktioniert wie ein Frühwarnsystem – es schützt nicht nur vor regulatorischen Folgen, sondern auch vor Reputationsschäden und Vertrauensverlust.

**Viele Unternehmen haben strategische Ambitionen – aber kämpfen in der Umsetzung. Wie helfen Sie konkret?**
Genau da liegt unsere Stärke. Wir kennen erfolgreiche Anwendungen, beraten technologieunabhängig, verfügen über tiefes Know-how in Datenarchitekturen und begleiten Projekte von der ersten Konzeption bis zur produktiven Anwendung. Als Teil der Deutschen Telekom bieten wir hochverfügbare Netze, zertifizierte Rechenzentren und datenschutzkonforme Plattformen. Das schafft Vertrauen – und ermöglicht skalierbare, rechtskonforme KI-Lösungen, die wirklich produktiv gehen.

**Ihr Ausblick – wohin geht die Reise?**
Wer jetzt investiert, kann in Europa Maßstäbe setzen. Die nächsten 12 bis 18 Monate entscheiden darüber, wer KI wirklich strategisch nutzt – und wer im Wettbewerb zurückfällt. Mit einer klaren Datenstrategie, verantwortungsvoller Umsetzung und einem starken Partner an der Seite kann »KI Made in Germany« nicht nur Realität, sondern ein Qualitätsversprechen werden.

*Weitere Informationen via QR-Code:*

## Genius Tip

»**KI** kann nur so gut sein wie die **Daten**, auf denen sie basiert. Wer heute **verantwortungsvoll handeln** und morgen **innovativ** sein will, muss **Datensouveränität**, **Transparenz** und **Compliance** von Anfang an **mitdenken**.«

# KI als Gamechanger: So sichern Unternehmen ihre Zukunft

**Künstliche Intelligenz gilt als Schlüsseltechnologie für die Zukunft der Wirtschaft. Doch viele Unternehmen stehen vor der Herausforderung, KI nicht nur als Trendthema zu betrachten, sondern nachhaltig und wirkungsvoll in ihre Prozesse zu integrieren. Worauf kommt es dabei wirklich an? Vier führende Experten geben ihre zentrale Handlungsempfehlung.**

Welche **zentrale Handlungsempfehlung** geben Sie Unternehmen, die **KI erfolgreich** in ihre **Geschäftsprozesse integrieren** möchten?

### David Parry-Jones

*Chief Revenue Officer, DeepL*

»Während sich die KI-Adoption in Unternehmen enorm beschleunigt, wollen diese nun vom Hype zum Impact: Unternehmen wollen messbare Resultate sehen. Am besten gelingt dies mit dem Wechsel hin zu spezialisierten KI-Lösungen. Denn diese sind darauf trainiert, spezifische Use Cases zu meistern, um die hohen Qualitätsstandards von Unternehmen zu erfüllen. Zudem lassen sie sich an Geschäftsanforderungen anpassen und personalisieren. Die Einführung und Skalierung von KI lässt sich weiter vereinfachen, indem die Tools über APIs in den bestehenden Tech-Stack integriert werden.«

### Walter Sun

*Global Head of AI, SAP SE*

»Stellen Sie den KI-Erfolg sicher, indem Sie nicht nur Technologie implementieren, sondern fundamental Ihre Geschäftsprozesse transformieren und Daten intelligent einsetzen.

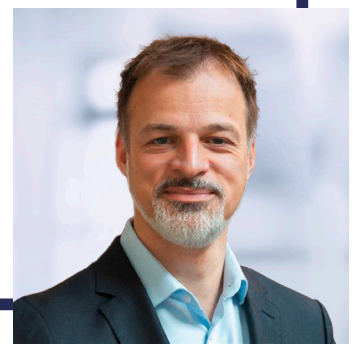
Legen Sie den Fokus auf klaren Geschäftswert, bauen Sie eine solide Datenbasis auf, vernetzen Sie Prozesse durchgängig und nehmen Sie Ihre Mitarbeitenden aktiv auf dieser Transformationsreise mit.«

### Benno Blumoser

*Head of AI Lab, Siemens*

»Neben einer guten Datenstrategie (und ihrer ehrlichen Umsetzung!) braucht es einen sich selbst verstärkenden Innovations-Kreislauf, der wie folgt aussehen kann:
1. KI-Tools allen Mitarbeitenden bereitstellen und zu ihrer Nutzung einladen
2. Die besten Ideen und Anwendungsfälle schnell umsetzen und ihren Wert zeigen
3. Erfolgsbeispiele im Unternehmen teilen (Meetups / Podcasts / Communities)

Dies motiviert weitere Kolleginnen, eigene Anwendungen zu entwickeln. Dann kann eine Kultur aus Neugier und Fokus entstehen.«



### Dr. Björn Bringmann

*Managing Director, Deloitte AI Institute - The Garage*

»Mehrwert mittels KI entsteht durch Change, nicht durch Code. Statt immer wieder dem jüngsten AI-Modell hinterherzujagen, denken Sie Ihre Prozesse neu: gesteuert durch klare Erfolgskriterien, getragen von Entscheidern mit GenAI-Fluency und vorangetrieben durch schnelle, iterative Umsetzung, die aus Pilotprojekten Profite erzeugt. Nur so wird sich die Transformation in der Realität auch rechnen.«

---

## Genius Partner • msg industry advisors ag



# »Wir müssen KI-Lösungen vom Prozess her denken«

**Dr. Dennis Janning, Verantwortlicher für KI-Transformation bei msg industry advisors, erklärt, warum erfolgreiche KI-Projekte immer bei klar definierten Prozessen beginnen und wie Unternehmen echten Business Value erzielen.**

**Herr Dr. Janning, immer wieder ist von enttäuschten Erwartungen im Zusammenhang mit KI zu lesen – warum scheitern so viele KI-Initiativen?**
Das Problem liegt oft im Ansatz: Unternehmen starten mit spektakulären Leuchtturmprojekten statt mit praxisrelevanten Anwendungen. Dabei werden drei Faktoren übersehen: KI wird wie normale Software behandelt, obwohl sie neue Arbeitsweisen erfordert, schlechte Prozesse werden nicht automatisch besser und ohne Change-Management bleiben Erfolge aus.

***Dr. Dennis Janning***
***Head of Artificial Intelligence***
***msg industry advisors***

**Wie unterscheidet sich Ihr Ansatz?**
Wir denken KI-Lösungen vom Prozess her, nicht von der Technologie. Unsere Branchenexpertise hilft, die KI-Einführung mit unserem »AI-FIRST Framework« systematisch zu strukturieren. Wir sehen KI als Enabler, um nachhaltig und fokussiert zu skalieren.

**Wie adressieren Sie die besonderen regulatorischen Anforderungen der Life-Sciences-Branche?**
Im regulierten Umfeld ist unser prozessorientierter Ansatz entscheidend. Er hilft, die Balance zwischen Innovation und Compliance zu finden, etwa durch das »Human in the Loop«-Prinzip: KI prüft Dokumente automatisiert, während Fachexpert:innen die finale, audit-sichere Freigabe erteilen.

**Welche Voraussetzungen müssen Unternehmen schaffen, um ihr KI-Potenzial zu heben?**
Drei Faktoren entscheiden über den Erfolg: hochwertige Prozesse und Daten als Basis, interne »KI-Champions« als Treiber und systematisches Change-Management. Ohne diese Grundlage scheitert die Lösung, ohne Fürsprecher bleibt KI nebensächlich und ohne Akzeptanz gelingt die Integration nicht.

**Können Sie ein Erfolgsbeispiel nennen?**
Ein Life-Sciences-Unternehmen hat KI in seiner Quality- & Compliance-Abteilung eingeführt. Die Ergebnisse sind beeindruckend: 24 % schnellere Bearbeitung, 12 % mehr abgeschlossene Prüfprozesse und 37 % weniger Nacharbeiten durch bessere Erstqualität. Wer jetzt zögert, riskiert seine Wettbewerbsfähigkeit, da die Lücke zu Vorreitern täglich wächst.

.msg advisors

### Genius Tip

»Beginnen Sie mit einem **kleinen, klar abgrenzbaren Pilotprojekt**. Ein **messbarer Erfolg** überzeugt **interne Skeptiker** nachhaltiger als jede Strategiepräsentation.«

# »Die Differenzierung liegt nicht mehr im Produkt, sondern erfolgt über Daten und Services«

**»Cloud is not a location. It's a mindset.« Dr. Karsten Kötter, AI Lead und Leiter Geschäftsfeld Cloud Platform bei cbs Corporate Business Solutions, klärt im Interview über die Kraft von KI auf, die in der Fertigungsindustrie von der Automatisierung bis zur Prozesssicherheit alle Bereiche betrifft und voranbringt.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Dr. Kötter, wie sehr ist die Fertigungsindustrie besonders von den Entwicklungen und Möglichkeiten im Bereich KI betroffen?**
Die Fertigungsindustrie war lange – salopp gesagt – der »digitale Spätzünder«. Doch heute steht sie unter massivem Transformationsdruck: Globale Lieferkettenrisiken, ESG-Vorgaben, geopolitische Instabilitäten und ein rasant beschleunigter Innovationszyklus zwingen produzierende Unternehmen, ihre Wertschöpfung neu zu denken. Wenn ein physisches Produkt mit jedem 3D-Drucker gefertigt oder global eingekauft werden kann, liegt die Differenzierung nicht mehr im Produkt selbst, sondern erfolgt über Daten und Services. KI wirkt dabei wie ein Brandbeschleuniger und befähigt Unternehmen, Planung, Fertigung, Logistik und After-Sales in Echtzeit zu vernetzen und datenbasiert zu steuern. Bei unseren Kunden sehen wir, wie sich das klassische Effizienz-Mantra - »schneller, günstiger« – zu einem neuen Dreiklang wandelt: Resilienz, Agilität und Innovationsfähigkeit. Das physische Produkt liefert nur noch den Rohstoff, die Wertschöpfung entsteht durch die intelligenten Datenströme dahinter. Bei der cbs Corporate Business Solutions sehen wir diese Entwicklung schon bei vielen unserer Kunden und begleiten sie ganzheitlich in diesem Wandel: Mit transformationssicheren SAP-Architekturen, global harmonisierten End-to-End Prozessen und KI-gestützten Optimierungsszenarien entlang der Wertschöpfungskette. Das klare Zielbild sind zukunftsfähige Geschäftsarchitekturen mit maximaler Wirkung auf die Effizienz, Flexibilität und Innovationskraft. Kurz gesagt: Wir helfen Industrieunternehmen, nicht nur digitaler, sondern auch zukunftsfähiger zu werden und – technologisch, organisatorisch und strategisch.

**Einerseits wollen Unternehmen innovativ und automatisiert arbeiten, andererseits sollen sämtliche Prozesse eine maximale Verfügbarkeit und Stabilität haben. Wie geht das?**
Das ist der klassische Spagat der Ambidextrie – also die Fähigkeit, effizient und innovativ zugleich zu sein. Bei IT-Systemen für Unternehmensprozesse ist das vereinfacht ein stabiler Kern ergänzt um eine »agile Schale« – nach dem einfachen Prinzip: Stabilität im Kern, Agilität an der Peripherie. Konkret heißt das, der stabile Kern, meist auf Basis von SAP S/4HANA, bildet klar definierte, hochverfügbare End-to-End Prozesse ab. Mit einem Clean-Core Ansatz sorgen wir bei cbs dafür, dass diese Prozesse sicher, konsistent und releasefähig bleiben. Parallel etablieren wir gemeinsam mit unseren Kunden einen flexiblen Innovationslayer in der Cloud, typischerweise auf Basis der SAP Business Technology Platform (BTP) oder in hybriden Architekturen. Dort können neue Ideen, Technologien und KI-Services pilotiert, validiert und bei Erfolg in den Standardprozess integrieren werden. Wir nennen das »reflektierte Innovation«: Schnelle Experimentierrunden, aber mit klaren Guardrails in Bezug auf Sicherheit, Compliance und wirtschaftliche Tragfähigkeit. Unsere Erfahrung aus über 3.000 erfolgreichen Projekten zeigt: Wer diesen dualen Ansatz konsequent verfolgt, kann die scheinbaren Gegensätze von Stabilität und Innovation in eine produktive Balance bringen.

*Dr. Karsten Kötter, AI Lead und Leiter Geschäftsfeld Cloud Platform bei cbs Corporate Business Solutions*

> » Wer heute auf die **Cloud verzichtet**, verliert nicht nur **Geschwindigkeit**, sondern **Zugang** zu den **Innovationen von morgen.** «

**Warum ist die Cloud heute Grundvoraussetzung für datengestützte, automatisierte Prozesse und den Einsatz von KI-Agenten?**
Ganz einfach: Weil Innovation heute in der Cloud entsteht. Die Fortschritte im Bereich KI, Automatisierung und Datenverarbeitung sind atemberaubend. Es ist schlicht nicht mehr möglich, diese Technologien On-Premise eigenständig zu betreiben – weder fachlich noch wirtschaftlich. Viele der leistungsfähigsten KI-Modelle, etwa im Bereich Natural Language Processing, Bildverarbeitung oder semantischer Prozessautomatisierung sind ausschließlich cloudbasiert verfügbar. Dazu kommt: Die Cloud ist heute mehr als nur reine Infrastruktur. Sie bietet sofort nutzbare Services, Sicherheitsstandards und Skalierbarkeit, die als Innovationsbeschleuniger wirken! Mit Plattformen wie der BTP entsteht ein Innovationslayer, der sich nahtlos mit dem ERP-Kern verbindet. Hier lassen sich KI-Agenten, Automatisierungsszenarien oder Data-Driven Services schnell aufsetzen, iterieren und – bei Reife – produktiv in Geschäftsprozesse integrieren. Bei cbs setzen wir bereits seit 2016 auf hybride und cloud-native Architekturen, um betriebswirtschaftliche Prozesse innovativ zu transformieren. Unsere Kunden profitieren von vorgefertigten Templates, Architektur-Blueprints und erprobten Integrationsmodellen. Wer heute auf die Cloud verzichtet, verliert nicht nur Geschwindigkeit, sondern Zugang zu den Innovationen von morgen.

**Ist Unternehmen klar, zu was sie KI-Agenten alles einsetzen können?**
Noch nicht vollständig. In vielen Unternehmen ist das Verständnis von KI noch stark auf isolierte Use Cases beschränkt, etwa Chatbots oder Prognosemodelle. Aber KI-Agenten sind viel mehr: Sie agieren wie digitale Kollegen, die selbstständig Aufgaben übernehmen, mit anderen Systemen interagieren und Entscheidungen treffen und sich dabei an Ziel, Kontext und verfügbare Tools anpassen können. Ich erkläre es gerne so: Ein KI-Agent ist wie ein digitaler Trainee mit allen Bachelor-Abschlüssen gleichzeitig, polyglott, rund um die Uhr einsatzbereit, aber noch ohne »Firmen-DNA«. Der Trick ist: Wie beim Menschen definiert man das Ziel, Kontext und gibt die passenden Werkzeuge, sogenannte Skills. Der Agent findet dann selbst seinen Weg.

**Wie unterstützen KI-Agenten Unternehmen dabei, große Datenmengen eigenständig zu bewerten und wie ein digitaler Mitarbeiter zu agieren?**
Lange galt das Paradigma: »Garbage in, garbage out« – erst wenn alle Daten perfekt strukturiert, bereinigt und klassifiziert sind, kann KI sinnvoll eingesetzt werden. Das trifft auf klassische Machine-Learning-Modelle nach wie vor zu. Moderne KI-Agenten funktionieren anders: Sie haben ein semantisches Verständnis und sind deutlich robuster. Menschen arbeiten auch mit unvollkommenen Daten, weil sie auf Kontextwissen und Prozessverständnis zurückgreifen. Genau das lässt sich heute auch auf KI-Agenten übertragen. Damit können Prozesse automatisiert werden, selbst wenn die Datenlage nicht perfekt ist. Das revolutioniert viele IT- und Business-Prozesse. Bei cbs kombinieren wir diese Fähigkeit mit tiefem SAP und Prozess-Knowhow. Dadurch ermöglichen es unsere Lösungen, KI gezielt in produktive End-to-End-Prozesse einzubetten. Unsere Agenten sind heute schon in der Lage eingehende Dokumente (wie z.B. Langzeitlieferantenerklärungen, Steuerformulare oder Qualitätszertifikate) eigenständig zu verarbeiten und wiederzuverwerten. Dadurch liefern sie einen echten Beitrag auf operativer Ebene.

**Welche Rolle spielt der Mensch in Zukunft noch – und wie realistisch ist das Ziel, dass nur noch ein Prozent der Prozesse manuell gesteuert werden müssen?**
Der Mensch bleibt zentral. Nicht als Dateneingabekraft, sondern als Architekt, Supervisor und Impulsgeber. Das Ziel »1 % manuelle Steuerung« ist kein Dogma, sondern ein Nordstern – eine Vision, in der Menschen nur dort eingreifen, wo Urteilskraft, Empathie oder Kreativität gefragt ist. In Serienfertigung ist 99 % Automation vielleicht machbar, im Projektgeschäft wird dies deutlich geringer sein. Entscheidend ist: Wer Routine abgibt, gewinnt Freiraum für Strategie, Kundennähe und Innovation. Letztlich ist KI kein Ersatz für den Menschen, sondern ein Verstärker seiner Stärken, wenn man den richtigen Rahmen dafür schafft.

## Genius Tip

»Statt ›Produkt verkaufen‹ heißt es **›Mehrwert liefern‹**. Also: **Plattform** bauen, **Daten** monetarisieren, **PartnerÖkosystem** orchestrieren. Wer das beherrscht, sitzt nicht mehr im Keller, sondern auf dem **Fahrersitz**.«

# »Nur wer intern Kompetenzen entwickelt, wird langfristig unabhängig und erfolgreich transformieren«

**Innovation gelingt nur, wenn Unternehmen und ihre Mitarbeitenden wissen, wohin die Reise geht. Tim Strohschneider, Head of Generative AI bei adesso, über Künstliche Intelligenz, Innovationsstau und den überfälligen Wandel in Unternehmen.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Strohschneider, welche praktischen Schritte sind erforderlich, um den Change zu Künstlicher Intelligenz erfolgreich zu meistern?**
Change zu KI ist kein Selbstläufer – er braucht Struktur, Richtung und Geschwindigkeit. Dabei ist entscheidend: Eine klare Strategie mit messbarem Zielbild, eine technologische Plattform, die skalierbar ist, und vor allem: der Faktor Mensch. Der Dreh- und Angelpunkt sind dabei immer konkrete, industriespezifische Use Cases. Wir denken in drei Phasen: Innovate – Design – Transform. Also erst die Potenziale strategisch erkennen, dann nutzerzentrierte Anwendungsfälle entwickeln und schließlich die Organisation durch Enablement und Führung mitnehmen. Mein praktischer Tipp: ein Aufbau eigener AI-Growth-Modelle. Nur wer intern Kompetenzen entwickelt, wird langfristig unabhängig und erfolgreich transformieren.

**Wie können Unternehmen ihre Mitarbeitenden befähigen und motivieren, KI als unterstützendes Werkzeug zu verstehen und nicht als Bedrohung?**
Der Schlüssel zur Akzeptanz von KI ist: Verständnis, Transparenz und konkreter Nutzen im Alltag. Mitarbeitende müssen wissen, wie sich ihr Beitrag zum Unternehmenserfolg durch KI verändert – nicht ob. Das beginnt mit klarer Kommunikation: Was übernimmt die KI, was gehört zu den Aufgaben der Menschen? Dann geht es um Erlebbarkeit: Wir starten mit Lösungen, die die größtmögliche Nutzeranzahl haben – z. B. Wissensagenten oder Service-Anwendungen – und die schnell entlasten, statt zu überfordern. Ein konkretes Beispiel: Bei einem Versicherungskunden haben wir KI-Tools im Kundenservice eingeführt – und 1.200 Mitarbeitende profitieren jetzt von spürbarer Entlastung und mehr Raum für echte Beratung. Genau das motiviert – weil der Nutzen greifbar ist.

**Welche Rolle spielen Leadership und Unternehmenskultur bei der Umsetzung von KI-Initiativen?**
Leadership und Kultur sind die beiden Faktoren, mit denen jede KI-Initiative steht oder fällt. Gerade die mittlere Führungsebene ist entscheidend – sie kennt die operativen Prozesse und erkennt, wo KI wirklich Mehrwert stiftet. Viele relevante Use Cases bleiben heute unentdeckt, weil Entscheidungen zu weit weg vom Alltag getroffen werden. Deshalb: Fachbereiche frühzeitig einbinden – nicht nur anhören, sondern mitverantwortlich machen. Das sorgt für höhere Akzeptanz, realistische Lösungen und nachhaltige Umsetzung. Gleichzeitig braucht es Führung, die Raum für Experimente, Lernen durch Ausprobieren und klare Verantwortung für Ergebnisse vorlebt. KI ist ein Werkzeug – und das muss aktiv geführt werden. Ohne diese Kultur bleibt jede noch so gute Lösung Stückwerk.

**Sie werben auch für passende Schulungsformate, um alle Mitarbeitenden zu fördern. Welche sind das?**
Pflichtschulungen nach dem EU AI Act sind ein Anfang – aber das ist noch kein echter Kompetenzaufbau. Wer seine Mitarbeitenden wirklich befähigen will, muss zielgruppenspezifisch denken. Wir unterscheiden zwischen Management, Anwendern und IT – jede Gruppe braucht andere Inhalte und Formate. Das Management muss strategisch verstehen, was mit KI möglich ist. Anwender brauchen Schulungen zu konkreten Tools und Fähigkeiten. Die IT muss wissen, wie Modelle integriert und verantwortungsvoll betrieben werden. Unser Tipp: Generative KI direkt im Training einsetzen, z. B. für Live-Demos, automatische Übersetzungen oder Textgenerierung. Das macht KI greifbar – und zeigt Mitarbeitenden, was heute schon alles möglich ist.

**Die Regulierungen und gesetzlichen Vorgaben nehmen zu. Inwieweit kann KI schneller und genauer bestehende Inhouse-Prozesse oder Verträge mit Dienstleistern, beispielsweise entsprechend der DORA-Anforderungen, überprüfen?**
Regulatorische Vorgaben wie sie durch DORA etc. entstehen sind komplex, aber mit KI gut beherrschbar. Moderne KI kann Verträge, Notfallpläne oder interne Prozesse automatisiert auf regulatorische Anforderungen prüfen und das schnell, zuverlässig und wiederholbar. Besonders relevant ist dabei der sogenannte »RAG-Ansatz«, Retrieval-Augmented Generation. Dabei sucht die KI zuerst gezielt in den eigenen Dokumenten nach relevanten Passagen (Retrieval) und generiert dann auf Basis dieser Inhalte eine verständliche Antwort (Generation). So lassen sich Fragen stellen wie: »Wo fehlen Regelungen zur Ausfallsicherheit?« oder »Welche Dienstleisterverträge enthalten bereits DORA-relevante Klauseln?« Das reduziert manuelle Prüfaufwände, erhöht die Frequenz und Qualität der Reviews – und sorgt dafür, dass regulatorische Anforderungen wie DORA sicher eingehalten werden.

**Sie weisen auch nachdrücklich auf die Bedeutung souveräner Lösungen im Bereich KI hin. Wie lassen die sich herstellen?**
Souveränität in der KI bedeutet: Kontrolle über Betrieb, Modelle und Expertise – alles, was langfristig erfolgskritisch ist. Gerade in den letzten Monaten hat das Thema wieder deutlich an Relevanz gewonnen. Es geht dabei nicht um »alles selbst machen«, sondern um bewusste Entscheidungen: Welche Kompetenzen bauen wir intern auf – und wo setzen wir kontrolliert auf Partner? Technisch heißt das: Datenhoheit sichern, etwa durch Hosting in der EU. Offene, lokal betreibbare Modelle nutzen, um sensible Daten im Unternehmen zu halten. Und: eigene Teams befähigen, statt sich dauerhaft abhängig zu machen. Souveräne Lösungen entstehen dort, wo Unternehmen Technologie, Betrieb und Know-how gezielt selbst gestalten – oder mit Partnern, die dieses Prinzip mittragen. Immer angepasst auf das jeweilige Szenario.

**Wie sieht denn ein Modell aus, bei dem Unternehmen wirklich souverän agieren?**
Ein souveränes KI-Modell heißt: Kontrolle behalten – technisch, fachlich und organisatorisch. Das gelingt, wenn Unternehmen drei Perspektiven systematisch adressieren:

**1. Interoperabilität und Infrastruktur:** Skalierbare Hardware ermöglicht den flexiblen Einsatz von Sprachmodellen, sei es lokal, hybrid oder in zertifizierten europäischen Rechenzentren. Wichtig ist: Datenverarbeitung muss GDPR-konform sein. Der Einsatz von Open-Source-Modellen oder von DSGVO-konformen Anbietern schafft einen höheren Grad von Unabhängigkeit.

**2. Entwicklungskompetenz:** Souveränität heißt auch: verstehen, was im Modell passiert. Es können eigene Applikationen entwickelt werden – auf Basis von lokalen Modellen, aber auch unter Einbindung externer APIs mit voller Transparenz über Datenflüsse und Systemzugriffe.

**3. Governance:** Ohne klare Regeln keine Verantwortung. Das umfasst nicht nur AI- und Data-Governance-Strukturen, sondern auch Training und Rollenmodelle. Wer KI einführt, muss gleichzeitig Vertrauen, Kontrolle und Sicherheit mitdenken.

**Best Practice:** Der Aufbau interner »Communities of Practice« bringt Fachbereiche und Technik zusammen, vermeidet Redundanzen – und macht aus KI-Projekten souveräne Wertschöpfung.

**Wo liegen jetzt und in den kommenden Jahren die Herausforderungen bei Generativer KI?**
Wir stehen mitten in der zweiten Welle der Generativen KI – Agentic AI – und das Tempo zieht weiter an. KI assistiert nicht mehr nur, sie handelt eigenständig. Sie startet Workflows, bereitet Entscheidungen vor. Viele Unternehmen sind darauf weder technisch noch organisatorisch vorbereitet. Vier Herausforderungen zeichnen sich jetzt schon ab:

1. Geschwindigkeit managen – ohne Organisationschaos.
2. Schatten-IT verhindern – Mitarbeitende nutzen längst externe Tools.
3. Explainability & Datenschutz – wer KI nicht erklären kann, darf sie nicht produktiv einsetzen.
4. Kulturwandel schaffen – Testumgebungen, sichere Freiräume und klare Governance statt Blockade.

Nur wer diese Punkte adressiert, ist bereit für die nächsten Wellen: Autonome und eingebettete KI. Und das wird schneller Realität, als viele heute glauben.

*Tim Strohschneider, Head of Generative AI, adesso*

## Genius Tip

»KI ist kein Tool, das man einfach einführt – sie verändert **Rollen**, **Prozesse** und **Verantwortung**. Wer echte Wirkung will, braucht **klare Leitplanken**, **eigene Kompetenz** und die **Menschen im Zentrum**. Nur so wird aus Hype **nachhaltiger Fortschritt**.«

# »Künstliche Intelligenz darf kein Selbstzweck sein – sie muss echte Geschäftsprobleme lösen«

**Ein Interview mit Dr. Christian Wesp, Partner bei EY-Parthenon für Künstliche Intelligenz.**

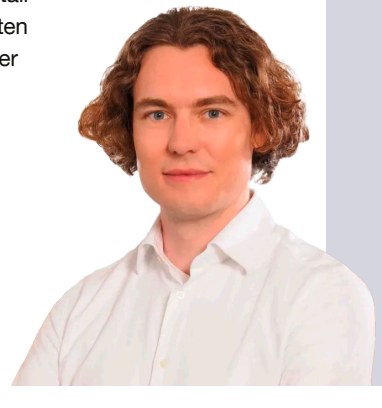
**Herr Dr. Wesp, wie sollten Unternehmen ihre Business-strategie anpassen, um eine nachhaltige KI-Strategie zu entwickeln?**
KI sollte nicht isoliert als IT-Thema betrachtet werden, sondern als Teil der Gesamtstrategie. Unternehmen müssen sich fragen: Wo kann KI heute und in Zukunft einen Unterschied machen? Welche technischen und organisatorischen Fähigkeiten sind nötig, um wettbewerbsfähig zu bleiben? Welcher technische Reifegrad existiert in der Organisation heute? Mit einem strukturierten Ansatz lassen sich diese Fragen beantworten. Denn nur wenn die KI-Anwendungen aus dem Piloten ins operative Geschäft überführt werden, lassen sich ihre Wertpotentiale realisieren.

**Welche konkreten Use Cases sehen Sie aktuell als besonders relevant?**
Relevanz ergibt sich immer aus dem geschäftlichen Mehrwert. Wachstumsorientierte Unternehmen profitieren von anderen Use Cases als solche, die auf Effizienz setzen. Besonders wertstiftend sind Anwendungen entlang der Wertschöpfungskette: automatisierte Angebots- und Preisgestaltung im Vertrieb, KI-gestützte Bedarfsprognosen und dynamische Lieferkettenoptimierung in der Logistik oder intelligentes Dokumentenmanagement in Legal und Compliance.

Ein stark wachsender Bereich sind KI-Agenten, die Aufgaben autonom ausführen. Hier lassen sich vor allem Prozesse massiv beschleunigen oder völlig neu denken. Entscheidend ist, KI dort einzusetzen, wo Komplexität, Datenvielfalt und Entscheidungsgeschwindigkeit hoch sind.

**Welche strukturellen und organisatorischen Veränderungen sind nötig, um KI erfolgreich zu implementieren?**
Für mich gibt es drei zentrale Faktoren, die alle mit Zusammenarbeit zu tun haben. Denn KI entfaltet das größte Potential, wenn Business mit IT verbunden wird. Erstens, interdisziplinäre Teams, bestehend aus Technikexpert:innen, Fachbereichen und Prozessverantwortlichen. Zweitens agile Governance-Strukturen mit klarem Use Case-Ownership. Drittens Change Management: Mitarbeitende müssen verstehen, wie KI ihre Arbeit verändert und sie entlastet, nicht ersetzt. Dazu gehören gezielte Weiterbildungen und eine Innovationskultur.

**Wie sieht es beim technischen Unterbau aus – insbesondere im Datenmanagement?**
Schlechte Daten führen zu schlechten Ergebnissen – besonders bei KI. Viele Unternehmen kämpfen mit schwer zugänglich und qualitativ schwachen Daten. Zwar gibt es viele KI Use Cases, die keine eigenen Daten brauchen, der echte Wettbewerbsvorteil kommt aber nur aus der gezielten Nutzung der eigenen Daten. Hier wird klar:
KI ist die nächste Stufe der Digitalisierung – und technische Altlasten wiegen besonders schwer. Daher müssen die Unternehmen ihre Datenhausaufgaben leider weiterhin machen.



***Dr. Christian Wesp***
***Experte für Künstliche Intelligenz, AI-Lead EY-Parthenon Deutschland.***

**Wie verhindern Unternehmen, dass KI-Implementierungen zum reinen Hype verkommen?**
Unternehmen sollten KI-Software nicht blind kaufen oder ungerichtet selbst entwickeln. Jede KI-Initiative sollte mit einer klaren wirtschaftlichen Zielsetzung verknüpft und der Erfolg dieser Ziele messbar gemacht werden. Ohne KPIs laufen Unternehmen Gefahr, viel Geld in technologisch spannende, aber wirtschaftlich irrelevante Projekte zu stecken. Und nicht zuletzt: KI muss zur »gelebten Realität« werden – nicht nur für Technolog:innen, sondern für alle Mitarbeitenden. Nur so lässt sich echte Transformation erreichen. Klar ist: KI ist gekommen, um zu bleiben und wird normaler Teil des digitalen Werkzeugkastens werden.

EY Parthenon
Shape the future with confidence

## Genius Tip

»KI entfaltet ihr **volles Potenzial** nur, wenn sie klar definierte, messbare **Ziele** verfolgt und als integraler **Bestandteil** der **Unternehmensstrategie** und -kultur verankert wird. Entscheidend ist, dass sie unternehmerisch sinnvoll, **zielgerichtet** und im Zusammenspiel mit **menschlicher Intelligenz** eingesetzt wird. So wird KI vom Selbstzweck zum **Werkzeug** für **nachhaltige Wettbewerbsfähigkeit**.«



# »Digitale Zukunft? Ist jetzt.«

**Dr. Martina Burgetsmeier ist Geschäftsführerin und Managerin des Bereichs KI bei eXXcellent solutions. Im Interview spricht sie über KI als neue Infrastruktur, die Renaissance der Individualentwicklung und warum jetzt keine Zeit mehr zu verlieren ist.**

**Individualentwicklung galt lange als aufwendig und ressourcenintensiv. Was hat sich durch KI konkret verändert – und in welchen Fällen lohnt sie sich besonders?**
Individualentwicklung war nie Luxus – sie war immer dort notwendig, wo Standardlösungen an ihre Grenzen stoßen: bei kritischen Kernprozessen, bei speziellen Schnittstellen, bei echten Differenzierungsmerkmalen. Genau da setzen wir an. Was sich durch KI verändert hat, ist das »Wie«: Wir entwickeln heute schneller, effizienter und noch zielgerichteter. Das senkt nicht nur Aufwand und Kosten, sondern macht Individualsoftware auch für mittelständische Unternehmen zu einer wirtschaftlichen Option. In vielen Fällen ist sie nicht nur sinnvoll, sondern strategisch notwendig.

**Also ein Aufbruchssignal an den Mittelstand?**
Absolut. Aber es geht um mehr als nur Software. Wir verstehen KI als Infrastruktur. Ein Unternehmen kann sich heute keine KI-Abstinenz mehr leisten. Von Vertrieb über HR bis Logistik: Jeder Bereich sollte befähigt werden, KI sinnvoll zu nutzen. Erst wenn diese Basis gelegt ist, sprechen wir über spezialisierte Lösungen und Prozessautomatisierungen. Und das muss schnell gehen. Die Innovationsgeschwindigkeit nimmt weiter zu – wer abwartet, riskiert den Anschluss zu verlieren. Wir helfen dabei, diesen Wandel strukturiert und pragmatisch umzusetzen.

***Dr. Martina Burgetsmeier***
***Geschäftsführerin***
***Managerin Bereich KI***
***eXXcellent solutions***

> »Was sich durch **KI verändert** hat, ist das **Wie**.«

**Und wie geht schnell starten mit KI?**
Wir setzen auf Tempo und Machbarkeit statt endloser Theorie. Für unsere Kunden heißt das, wir definieren KI-Richtlinien und Governance, schaffen ein sicheres Umfeld in der zentralen KI-Plattform, und wenn diese Infrastruktur steht, folgen Use-Cases für die Anwendung und deren Umsetzung. Damit ermöglichen wir allen Mitarbeitenden unmittelbaren und gewünschten Zugang. Keine Schatten-KI. Kein Sicherheitsrisiko. Denn Datenschutz ist von Anfang an mitgedacht. Wer heute KI richtig integriert, kann das völlig regelkonform und sicher tun. Uns ist wichtig, die Hemmungen abzubauen.

**Was macht eXXcellent solutions zum idealen Partner in diesem Wandel?**
Wir bringen Erfahrung mit: Über zwei Jahrzehnte in der klassischen Softwareentwicklung. Diese kombinieren wir mit KI-Kompetenz. So entstehen ganzheitliche Lösungen, die nicht nur technisch passen, sondern auch zur Unternehmenskultur. Uns geht es darum, Individualität und Unabhängigkeit zu fördern – genau das, was viele Mittelständler heute wieder stärker suchen.

**Wagen wir einen Blick in die Zukunft: Wo steht der Mittelstand in fünf Jahren – mit oder ohne KI?**
Mit KI ist er innovativ, resilient und wettbewerbsfähig. Ohne wird es schwierig. KI ist keine Spielerei mehr, sie ist Bestandteil der Realität. Unsere Botschaft lautet: Jetzt aktiv werden. Wer den Wandel mitgestaltet, gewinnt. Und wir zeigen, wie das konkret funktioniert.

Weitere Informationen:
**www.eXXcellent.de**

oder via QR-Code

eXXcellent solutions

# »Wenn der digitale Informationszwilling für Unternehmen zum Digitalisierungsmotor wird«

**Effiziente Prozesse sind heute ein entscheidender Faktor für den Unternehmenserfolg, die Digitalisierung ist das Werkzeug mit dem größten Potential. Doch viele Digitalisierungsinitiativen scheitern bereits an der Grundlage: den Unternehmensdaten. Nur wenn Informationen konsistent, strukturiert und systemübergreifend nutzbar gemacht werden, lassen sich daraus belastbare Prozessoptimierungen und neue Services entwickeln.**

**Interview** Rüdiger Schmidt-Sodingen

Welche Rolle digitale Zwillinge und Plattformtechnologien dabei spielen und wie Unternehmen ihre fragmentierten Datenströme in ein tragfähiges Informationsmodell überführen können, erläutert Dr. Jörg Nagel, Geschäftsführer der Neoception GmbH. Das Unternehmen wurde 2017 als industrienaher IT-Lösungsanbieter innerhalb der Pepperl+Fuchs Gruppe gegründet und unterstützt Unternehmen inzwischen mit einem eigenen Produktportfolio dabei, aus verteilten Datenstrukturen ein stabiles digitales Fundament für Automatisierung und Innovation zu schaffen.

**Herr Dr. Nagel, viele Unternehmen sprechen vom digitalen Zwilling. Sie verwenden bewusst den Begriff digitaler Informationszwilling. Was unterscheidet ihn vom klassischen Verständnis?**
Der digitale Informationszwilling umfasst sämtliche relevante Informationen rund um ein Produkt oder Asset. Dazu gehören technische Merkmale, Handbücher, Zertifikate, Simulationsmodelle, Nutzungsdaten und vieles mehr. Stellen Sie sich vor: Für jedes Asset existiert ein digitaler Ort mit allen Informationen – unabhängig von der Quelle.

**Welche Rolle spielen Plattformtechnologien und digitale Zwillinge bei der Umsetzung datengetriebener Anwendungsfälle in Unternehmen?**
Digitalisierungsprojekte erfordern oft Informationen aus verschiedenen Quellen wie ERP-Systemen, Produktdatenbanken, usw. Für jeden weiteren Anwendungsfall müssen diese Schnittstellen neu umgesetzt werden. Schnell wird durch die Aufwandsspirale der wirtschaftliche Nutzen aufgefressen. Digitale Informationszwillinge schaffen hier eine Entkopplung von unstrukturierten und vielfältigen Datenquellen und den einzelnen Anwendungsfällen.

Dr. Jörg Nagel, Geschäftsführer der Neoception GmbH

So können Daten systemübergreifend bereitgestellt und wiederverwendet werden. Um diese Potenziale im Unternehmensalltag tatsächlich zu heben, braucht es jedoch mehr als ein Konzept, nämlich eine Plattform, die solche Zwillinge nicht nur bereitstellt, sondern ihre Erstellung und Pflege vereinfacht.

Genau vor diesem Hintergrund haben wir die Digital Twin Infrastructure (DTI) entwickelt. Sie ermöglicht es, Inhalte aus bestehenden Systemen bedarfsgerecht in ein einheitliches, maschinenlesbares Datenmodell zu überführen und damit technische Komplexität zu reduzieren. So werden Anwendungsfälle skalierbar und Fachbereiche können auf verlässliche Informationen zugreifen, ohne auf individuelle Schnittstellen oder IT-Unterstützung angewiesen zu sein.

**Wie schwer ist es, bestehende Datenquellen oder -systeme in Ihre Plattform zu überführen und digitale Zwillinge zu erstellen?**
Exakt dieser Herausforderung haben wir uns gestellt. Viele am Markt verfügbare Tools zur Erstellung digitaler Zwillinge setzen voraus, dass die zugrunde liegenden Daten bereits standardisiert und vollständig strukturiert vorliegen. Doch die reine Zurverfügungstellung solcher Inhalte macht in der Praxis nur den letzten Schritt des Gesamtaufwands aus. Die eigentliche Arbeit, und damit auch die Grundlage für den wirtschaftlichen Gesamterfolg, liegt darin, die Aufbereitung und Standardisierung von Informationen aus unterschiedlichen Quellen skalierbar und bedarfsgerecht zu ermöglichen. Unsere Digital Twin Infrastructure wurde genau dafür entwickelt. Sie unterstützt Unternehmen nach einmaliger Integration in die eigene Infrastruktur dabei, bestehende Daten ohne Programmieraufwand so aufzubereiten. Ganz nach dem Motto: Es muss nicht immer einfach sein, aber es muss sich lohnen. Als technologische Grundlage dient dabei die Asset Administration Shell (AAS), ein internationaler Standard zur strukturierten Beschreibung von Produkten und Assets.

**Sie sprechen von Standards. Wieso sind Standards relevant für digitale Zwillinge?**
Erst durch Standards lassen sich digitale Zwillinge wirtschaftlich und über System- oder Unternehmensgrenzen hinweg nutzen. Sie sorgen dafür, dass Informationen nicht nur intern konsistent strukturiert sind, sondern auch extern eindeutig verstanden werden, unabhängig davon, aus welchem System sie stammen oder mit welchem Partner sie geteilt werden. Mit der AAS steht ein offener Industriestandard zur Verfügung, der eine einheitliche Struktur für digitale Zwillinge bietet. In Kombination mit semantischen Standards wie ECLASS, die Begriffe, Merkmale und Klassifikationen eindeutig definieren, wird eine durchgängige und maschinenlesbare Beschreibung von Produkten, Komponenten oder Maschinen möglich. Das ist die Grundlage für automatisierten Datenaustausch, regulatorische Nachweise und neue digitale Geschäftsmodelle.

**Demnächst müssen Unternehmen einen digitalen Produktpass anbieten. Welche Rolle kann dabei der digitale Informationszwilling spielen?**
Der digitale Produktpass wird in den kommenden Jahren zur Pflicht, und die Anforderungen an Transparenz, Nachverfolgbarkeit und Aktualität von Produktinformationen steigen erheblich. Unternehmen, die heute bereits digitale Informationszwillinge nutzen, schaffen dafür bereits die optimale Basis. Die AAS erfüllt als technologischer Rahmen alle Anforderungen, die von der EU formuliert wurden.

**Lohnt es sich also, auf dem Weg zum digitalen Produktpass seine manuellen Prozesse schon zu automatisieren?**
Auf jeden Fall. Die Einführung des digitalen Produktpasses ist nur ein Beispiel für eine Entwicklung, die längst begonnen hat. Informationen werden zunehmend zum strategischen Faktor in der industriellen Wertschöpfung. Wer frühzeitig beginnt, seine Daten systematisch zu organisieren und unternehmensweit nutzbar zu machen, erschließt unmittelbar Mehrwerte wie effizientere Serviceprozesse oder digitale Produktdokumentation. Darüber hinaus können Unternehmen auf dieser Basis neue datenbasierte Angebote entwickeln, direkte Kundenbeziehungen stärken und ihre Position im Markt ausbauen. So wird aus einem oft vernachlässigten IT-Thema ein konkreter Wettbewerbsvorteil.

» Wer seine Daten **strukturiert** und **unternehmensweit nutzbar** macht, erschließt **unmittelbar Mehrwerte.** «

**Künstliche Intelligenz gilt als Schlüsseltechnologie für die Automatisierung. Welche Rolle spielt Künstliche Intelligenz im Zusammenhang mit digitalen Informationszwillingen?**
Künstliche Intelligenz kann nur dann zuverlässig funktionieren, wenn sie auf strukturierte, konsistente und maschinenlesbare Daten zugreifen kann. In vielen Unternehmen fehlt dafür noch die Grundlage. Genau hier kommen digitale Informationszwillinge ins Spiel: Sie machen Informationen in deutlich höherer Qualität für KI nutzbar. Ein digitaler Informationszwilling schafft somit die Voraussetzung dafür, dass KI-gestützte Analysen, Vorhersagen oder Entscheidungslogiken überhaupt sinnvoll eingesetzt werden können. Wer heute in eine saubere Datenbasis investiert, macht nicht nur erste Automatisierungsschritte möglich, sondern legt auch den Grundstein für einen erfolgreichen KI-Einsatz im operativen Alltag. In dieser Rolle wird der digitale Informationszwilling zum Digitalisierungsmotor, zur zentralen Instanz für datengestützte Entscheidungen und nachhaltige Wettbewerbsvorteile.

NEOCEPTION
Pepperl+Fuchs

**Jetzt Daten in Assets verwandeln!**
Mit der Digital Twin Infrastructure von Neoception machen Sie Ihr Unternehmen fit für KI, Automatisierung und den digitalen Produktpass. Mehr Informationen und persönlicher Support unter: **www.neoception.com**

## Genius Tip

»Erstellen Sie heute **digitale Informationszwillinge** – das spart **Geld**, schafft **Vorteile** und bereitet auf **KI** und den **Digitalen Produktpass** vor.«

# »Embedded-Module bringen KI in smarte Geräte«

**Seit zwei Jahrzehnten fördert congatec mit Embedded-Lösungen Visionen, Innovationen und Technologien – und schafft eine agilere Produktentwicklung bei Unternehmen. Konrad Garhammer, Managing Director und COO & CTO der congatec Group, über das Embedded Computing der Gegenwart und Zukunft.**

**Herr Garhammer, was kann Embedded Computing in Unternehmen bewirken?**
Embedded Computing sorgt für die Intelligenz in modernen Geräten – kompakt, leistungsstark und direkt auf die jeweilige Aufgabe zugeschnitten. In der Anwendungsentwicklung der Unternehmen sorgt diese Technologie für effizientere Prozesse, bessere Qualität und schnellere Innovationen. Unsere Aufgabe bei congatec ist es, diese Intelligenz über modulare Embedded-Plattformen so bereitzustellen, dass sie leicht integrierbar, skalierbar und zukunftssicher ist. Unternehmen müssen sich nicht mit der komplexen Entwicklung von Computertechnik beschäftigen, sondern können sich auf ihre Kernkompetenzen konzentrieren. Das verkürzt Entwicklungszeiten, senkt Kosten und schafft echte Wettbewerbsvorteile.

**Wie können Unternehmen KI in Embedded Systems integrieren, um ihre Systeme smarter und effizienter zu machen?**
Künstliche Intelligenz (KI) macht nicht nur Prozesse effizienter, sondern erweitert den Einsatzbereich und die Fähigkeiten von smarten Geräten immens. Damit Unternehmen KI in ihren Geräten oder Anlagen nutzen können, sind spezialisierte, leistungsfähige Recheneinheiten nötig – und genau hier kommen wir ins Spiel. Unsere Computer-on-Modules liefern genau die passende Rechenleistung. Sie sind robust, energieeffizient und lassen sich flexibel in unterschiedlichste Anwendungen integrieren. Unternehmen können damit KI-Anwendungen in ihren Produkten schnell umsetzen und sich ganz auf ihre Lösungen konzentrieren, ohne sich tief in die Embedded-Hardware einarbeiten zu müssen.

**Welche Herausforderungen bestehen allgemein bei der Implementierung von KI in Embedded Systems, und wie hilft congatec bei der Lösung dieser Herausforderungen?**
Die größten Herausforderungen sind technische Komplexität, hohe Entwicklungskosten, Cybersicherheit, das richtige Leistungsniveau zu wählen und die Fähigkeit, neue Lösungen skalierbar weiterzuentwickeln. Embedded-Systeme müssen gleichzeitig leistungsstark, energiesparend, robust und sicher sein – und sich dennoch flexibel anpassen lassen. Mit unseren modularen Plattformen liefern wir anwendungsfertige Hardware- und Softwarepakete, die genau darauf ausgerichtet sind. Wir nennen sie aReady, application ready. Unternehmen erhalten damit ein solides technisches Fundament, auf dem sie ihre KI-Anwendungen schnell, sicher und wirtschaftlich realisieren können – ohne sich durch die komplette Systemarchitektur arbeiten zu müssen.

**Es geht auch darum, dass sich Unternehmen dank Lösungen wie aReady wieder auf ihre Kernkompetenzen konzentrieren können, während die Basistechnologien im Unternehmen sicher weiterlaufen?**
Genau. Unsere modularen aReady-Plattformen bieten die benötigten Basistechnologien. Dazu gehören nicht nur das eigentliche Modul, sondern auch Workload-Consolidation, installierte und lizenzierte Betriebssysteme sowie Tools für die Anbindung an das Internet der Dinge (IoT), um Anwendungen zu monitoren, managen und zu aktualisieren. Das bedeutet: Ein einzelnes Modul kann mehrere Anwendungen gleichzeitig sicher betreiben, inklusive KI-Funktionalitäten und kann so mehrerer Systeme ersetzen. Unternehmen sparen dadurch nicht nur Kosten, sondern gewinnen auch Flexibilität. Dank der langjährigen Verfügbarkeit der Module und ihrer Standardisierung lassen sich ganze Produktfamilien durch einen einfachen Modultausch einfach entwickeln, ganz ohne Herstellerbindung. Außerdem unterstützen wir unsere Kunden mit umfassendem Design-in-Support und engen Technologiepartnerschaften. So helfen wir dabei, Entwicklungszeiten zu verkürzen, Risiken zu minimieren und KI zuverlässig in Maschinen und Geräte zu bringen.

**aReady verwandelt Applikationen auch in agile Innovationstreiber. Wie funktioniert das?**
aReady beschleunigt Innovationsprozesse gleich mehrfach: Erstens erhalten Kunden eine sofort einsatzfähige Technologieplattform, was die Markteinführungszeiten verkürzt. Innovationen können so viel schneller auf den Markt gebracht werden. Zweitens können mit unseren Plattformen die Lösungen effizient angepasst oder skaliert werden– ohne langwierige Neuentwicklungen. Und drittens ermöglichen wir mit dem modularen Aufbau, neue Technologien schnell zu integrieren. Kommt beispielsweise ein neuer Prozessor mit besseren KI-Funktionen auf den Markt, kann einfach das Computermodul ausgetauscht werden – ohne das Systemdesign zu verändern. Innovationen lassen sich so selbst in bestehenden Designs sehr schnell und kostengünstig umsetzen und zügig auf den Markt bringen. Das verlängert die Nutzungsdauer, erhöht die Nachhaltigkeit und maximiert den Return on Investment.

**Wie wichtig ist die Auswahl der richtigen Hardware für den Erfolg von KI-gestützten Embedded-Lösungen?**
Die Wahl der richtigen Hardware ist entscheidend. Das brandneue Whitepaper »Empowering Industrial Vision AI« vom Marktforschungsunternehmen VDC Research zeigt: 47 Prozent der Ingenieure nennen die Hardwarekosten als größten Kostentreiber bei KI-Anwendungen. Gleichzeitig sind Rechenleistung, Softwareökosysteme und optimierte Hardwarenutzung die drei größten Herausforderungen. Unsere aReady-Plattformen sind genau auf diese Anforderungen abgestimmt: Sie liefern bedarfsgerechte Performance, greifen auf ein umfangreiches Software-Ökosystem zurück und unterstützen Workload-Consolidation. Durch unsere Technologiepartnerschaften mit führenden Prozessorherstellern wie Intel, AMD, NXP und Texas Instruments bieten wir zukunftssichere Lösungen, die wirtschaftlich überzeugen.

**Welche Anwendungsfälle von Embedded Systems mit KI haben sich als besonders erfolgreich herausgestellt?**
Besonders erfolgreich ist der Einsatz dort, wo schnelle, verlässliche Entscheidungen direkt im Gerät getroffen werden müssen. In der Medizintechnik verbessern sie die Diagnostik, etwa durch automatisierte Bildauswertung. In der Industrie erkennen KI-Systeme frühzeitig Verschleiß oder Abweichungen und verhindern so Ausfälle. In autonomen mobilen Robotern und Fahrzeugen sorgt KI für mehr Sicherheit, zum Beispiel durch automatische Objekterkennung und intelligente Navigation. Ein weiteres stark wachsendes Feld ist die Smart City: Kameras mit KI werten Verkehrsflüsse aus oder erkennen Gefahrensituationen. Und in Smart Cities analysieren sie Verkehrsflüsse oder erkennen Gefahrensituationen. Gemeinsam ist all diesen Anwendungen: Sie bringen Effizienz, Sicherheit und Kostenersparnis – weil die Intelligenz dort sitzt, wo sie gebraucht wird.

**Sie konnten gerade Kontron als weiteren Partner zur Herstellung von Computer-on-Modules gewinnen. Wie wichtig ist oder wird der Local-for-Local-Ansatz von congatec?**
Der »Local-for-Local«-Ansatz ist für uns von zentraler Bedeutung – eine lokale Fertigung und Präsenz in allen Weltregionen wird in Zukunft immer wichtiger. Kunden staatlicher Auftraggeber setzen die Produktion vor Ort nicht selten zwingend voraus. Oder nehmen Sie die Cyberresilienz-Verordnung: Das Label »Designed AND manufactured in Europe« wird für die Einhaltung von Vorschriften immer wichtiger. Natürlich hilft die lokale Produktion auch dabei, Importzölle zu vermeiden, die eine Bedrohung für globale Lieferketten darstellen können. Außerdem lassen sich geopolitische Herausforderungen oder Naturkatastrophen mit lokalisierten Lieferketten viel leichter abfedern – was wir bereits während der COVID-Pandemie erlebt haben. Und nicht zuletzt trägt die lokale Produktion dazu bei, den ökologischen Fußabdruck unserer Produkte noch weiter zu verkleinern, da die Transportwege deutlich verkürzt werden.


Das oben zitierte VDC Whitepaper »Empowering Industrial Vision AI« können Sie bei congatec hier herunterladen:

**Mehr Informationen über congatec via QR-Code oder auf www.congatec.com**

congatec

## Genius Tip

»Setzen Sie bei der **Entwicklung** Ihrer KI-beschleunigten Embedded Systeme von Anfang an auf **anwendungsfertige, modulare Plattformen** – sie bieten die nötige Rechenleistung, Sicherheit und Energieeffizienz, um **KI agil** und **zukunftssicher** ins Gerät zu bringen. Das spart **Entwicklungszeit**, senkt **Kosten** und steigert die **Innovationskraft**. Mit standardisierten Computer-on-Modules **starten Sie heute smart** und können **morgen groß skalieren**.«

## Zur Person

Konrad Garhammer ist COO & CTO bei congatec und leitet seit über acht Jahren erfolgreich Technologie und operative Abläufe. Zuvor war er CTO bei Saab Medav Technologies, Senior Business Consultant bei msg systems sowie Geschäftsbereichsleiter bei a:k:t:. mit Fokus auf Telekommunikation. Weitere Stationen führten ihn zur Mühlbauer Group und in den öffentlichen Dienst. Sein technisches Fundament legte er mit einem Diplom in Elektrotechnik mit Schwerpunkt Nachrichtentechnik.

# Hinter Schloss und Siegel

## Cybersecurity zwischen Angriffen von unten und Regulierung von oben

Bild: RoonZ nl/Unsplash

**Kriminelle Angreifer, die Unternehmen lahmlegen und Lösegeld fordern, und regulatorische Anforderungen, die länderübergreifend Kooperationen und die Auswahl der Partner oder Zulieferer beeinflussen: Das Thema Cybersecurity bahnt sich mit Macht seinen Weg in die Unternehmen.**

**Text** Rüdiger Schmidt-Sodingen

Abriegeln unmöglich. Übersehen fatal. Geht aufgrund eines Cyberangriffs plötzlich nichts mehr, hat das eine psychologische Komponente, die gerne übersehen wird: Mitarbeitende haben plötzlich Angst, sind verunsichert, fürchten sich vor alltäglichen Tätigkeiten. Wer als Unternehmen keine souveräne Abwehr bietet, könnte demnächst keine souveränen Mitarbeitenden mehr haben. Experimentierlust? Freiheit? Dazulernen? Alles weit weg, wenn Computer nicht mehr funktionieren, Maschinen stillstehen und eine »fremde Macht« gegen die eigene Firma und den eigenen Arbeitsplatz opponiert.

Anfang des Jahres skizzierte Grant Waterfall, Cyber Security Leader bei PwC in Deutschland und EMEA, die »sechs wichtigsten Cyber-Security-Trends 2025«. Als ersten Punkt nannte er KI-Agenten mit ihren Chancen und Risiken. Viele Unternehmen setzen KI-Agenten ein – oder planen es zumindest. Öffnen diese automatisierten Dienste das Tor für Angreifer, täuschend echte Phishing-Mails oder unerwünschte Dateneinsichten? Laut der globalen Cyber-Studie Digital Trust Insights sagen »67 Prozent der deutschen Befragten, dass generative KI die Angriffsfläche in den letzten 12 Monaten erhöht hat«. Gleichzeitig ist klar, dass KI selbst zum besten Bekämpfer hochtechnisierter Angriffe werden kann. Doch dazu muss sie mit Verstand und allgemeiner Akzeptanz bei den Mitarbeitenden installiert werden. KI als Partner.

**»Regulations« und »Acts« fordern: »Security First«**

Neben den regulatorischen Anforderungen der Politik, Punkt 2 der Liste, geraten auch die Lieferketten und -partner, Punkt 3, zwangsläufig ins Visier der Unternehmen. Denn wenn Unternehmen darlegen müssen, wie sie sich und ihre Daten oder Produkte schützen, betrifft das auch diejenigen, die nur Teile, die ebenfalls mit Software ausgestattet sind, liefern oder weitersenden. Die Themen werden mehr, der Blickwinkel der Betroffenen weitet sich indes nur bedingt. Dass demnächst Produktpässe eingeführt werden und Sicherheitslücken in verbauter Software sofort gemeldet werden müssen, lässt die Nervosität bei denjenigen, die sich nur rudimentär beraten lassen oder informieren, steigen. Die DSGVO bekommt mit der General Product Safety Regulation (GPSR) und dem Cyber Resilience Act (CRA), der ab 2027 EU-weite Mindestanforderungen für die Sicherheit vernetzter Geräte festlegt, zwei strenge Geschwister.

Von der Post-Quanten-Kryptographie als Lösung für immer mehr benötigten Speicherplatz, Punkt 4, schwenkt die Liste der Cyber-Security-Trends zur dringend benötigten Digitalen Souveränität, um sich gegen die Willkür von Großkonzernen oder autoritären Regimen, die das Netz und seine Funktionen zum perfekten Nebenkriegsschauplatz erkoren haben, zu wehren. Auch hier müssen noch Missverständnisse ausgeräumt werden – denn Unabhängigkeit bedeutet nicht, dass allein der Staat das Problem löst. Jedes Unternehmen kann sich aktiv unabhängig machen und seine Strukturen entsprechend überprüfen und umstellen. Sorgen bereitet auch der abschließende Klassiker unter den Sicherheitsmissverständnissen: »Die überwiegende Mehrheit der Ausgaben für Cybersicherheit entfällt immer noch auf die IT und nicht auf OT und IIoT«, so PwC-Mann Waterfall. Nicht der Aktenschrank, sprich die Verzeichniswelten und Adressen, sind der Goldschatz eines Unternehmens, sondern die konkrete physische Betriebstechnik und die Zusammenarbeit der Maschinen und Produktionsstätten.

---

**Genius Partner • Sophos**

*think about: Cyber Security*

# Moderne Cyberabwehr: Hybrides Team, Struktur, Training

Cyberangriffe gehören längst zum Alltag von Unternehmen – mit teils drastischen Folgen. Während Cyberkriminelle ihre Methoden stetig weiterentwickeln, müssen sich Unternehmen fragen: Sind wir wirklich ausreichend vorbereitet? Die Antwort liegt in der richtigen Kombination aus Technologie und menschlichem Urteilsvermögen. Denn selbst modernste künstliche Intelligenz (KI) kann nicht alle Bedrohungen allein bewältigen. Erst das Zusammenspiel aus intelligenter Automatisierung, vorausschauendem Training und menschlicher Expertise schafft ein Sicherheitsniveau, das Angriffen standhält.

Die Erwartungen an die KI in der IT-Sicherheit sind dabei hoch: Sie soll Schutz verbessern, Analysen effizienter machen und Arbeitslasten reduzieren. Doch es gibt auch Vorbehalte – die größten betreffen mögliche Funktionsmängel, überhöhtes Vertrauen in KI-gestützte Security, unklare Einsparpotenziale und die Gefahr einer zu starken Abhängigkeit von der Technologie.

**Zeit und Struktur**

In der IT-Security kann jede Minute zählen. Eine effektive Sicherheitsstrategie kombiniert daher künstliche Intelligenz (KI) mit menschlichem Urteilsvermögen. Ein integriertes Sicherheits-Ökosystem, wie es etwa 600.000 Sophos-Kunden weltweit nutzen, bringt alle relevanten Schutzmechanismen unter einen zentralen Schutzschirm: von Endpoints, Servern und Mobilgeräten bis hin zu Cloud-Diensten, Firewalls und sicherem Netzwerkzugriff. Die zentrale Steuerung der gesamten IT-Sicherheitsarchitektur minimiert Reaktionszeiten sowie das Risiko, dass Cybervorfälle unentdeckt bleiben.

**Der Mensch bleibt unverzichtbar**

Automatisierung und KI leisten wertvolle Hilfe, doch im Ernstfall ist menschliche Intuition oft unersetzlich. Unternehmen sollten ihre Mitarbeitenden daher auf Cyberangriffe vorbereiten. Ein bewährtes Mittel sind Tabletop-Übungen, bei denen realistische Bedrohungsszenarien simuliert werden. Dies soll helfen, blinde Flecken zu identifizieren, Kommunikationswege zu optimieren und die Reaktionsfähigkeit zu verbessern.

**Drei wesentliche Szenarien haben sich bewährt:**

*Rapid-Fire-Übungen:* Schnelle, interaktive Szenarien, die ohne große Vorbereitung auskommen und Mitarbeitende aus verschiedenen Abteilungen einbeziehen.

*Technische Szenarien:* Detaillierte Analysen komplexer Cyberangriffe zur Vorbereitung spezialisierter IT-Teams.

*Interdisziplinäre Szenarien:* Abteilungsübergreifende Übungen mit Stakeholdern aus IT, Recht, Kommunikation und Management zur Verbesserung der Reaktionskoordination.

**Externe Expertise**

Nicht immer stehen Firmen die personellen Ressourcen für eine starke Cyberabwehr zur Verfügung. Hier können externe Managed Detection and Response (MDR)-Teams wertvoll unterstützen. Sie helfen Unternehmen, Bedrohungen rund um die Uhr zu erkennen, zu untersuchen und darauf zu reagieren. Echtzeit-Incident-Response (IR)-Dienste bieten zudem sofortige Hilfe, wenn ein Angriff bereits stattgefunden hat.

Durch die Kombination aus einer intelligenten Sicherheitsarchitektur, praxisnahen Schulungen und professionellen Security-Dienstleistungen entsteht ein Sicherheitsniveau, das Cyberbedrohungen effektiv entgegenwirkt.

SOPHOS

# Täuschung als Verteidigung: So funktioniert Cybersecurity 2025

**Mit einem eigenen Entwicklungsteam im Herzen Wiens verfolgt CyberTrap ein klares Ziel: Cyberangriffe nicht nur erkennen, sondern ihnen einen entscheidenden Schritt voraus sein. CEO und Mitbegründer Adi Reschenhofer sowie CTO Dr. René Heinzl erklären im Interview, warum herkömmliche Sicherheitsarchitekturen angesichts zunehmend automatisierter Angriffe an ihre Grenzen stoßen – und wie moderne Cybersecurity durch aktive Täuschung, KI-gestützte Analyse und adaptive Digital Twins neu gedacht werden muss. Dabei sprechen sie nicht nur über technologische Durchbrüche, sondern auch über den wachsenden Druck auf CISOs – und warum immer mehr von ihnen an ihre Grenzen kommen.**

**Herr Reschenhofer, Herr Dr. Heinzl, welche strategischen Herausforderungen kommen auf Unternehmen zu, wenn sie ihre Cyber Defense wirklich zukunftssicher gestalten wollen?**
*Dr. René Heinzl:* Die größte strategische Herausforderung besteht darin, mit der Geschwindigkeit der Angreifer Schritt zu halten – oder ihnen sogar einen Schritt voraus zu sein. Denn die Bedrohungsakteure von heute nutzen bereits KI: von automatisierten Phishing-Kampagnen über KI-generierte Malware bis hin zu adaptivem Verhalten in kompromittierten Netzwerken. Klassische, rein reaktive Sicherheitsansätze kommen da schlichtweg an ihre Grenzen.

*Adi Reschenhofer:* Cyberabwehr der nächsten Generation ist vorausschauend – sie erkennt Muster, bevor daraus Angriffe werden, und nutzt Täuschung gezielt als strategisches Werkzeug. Wer Sicherheit nicht als Limit, sondern als vorausschauende Intelligenz begreift, legt die Basis für digitale Souveränität und öffnet Räume für echte Innovation. Unser Motto: anders denken.

**Angesichts rasant wachsender Cloud-Abhängigkeit und der EU-Regulierung (NIS2, DORA, CRA): Warum muss Cybersicherheit heute Chefsache sein, noch bevor die erste Code-Zeile geschrieben wird?**
*Dr. René Heinzl:* Sicherheit ist heute ein zentraler Bestandteil moderner Systemarchitektur und muss bereits in der Planungsphase mitgedacht werden. Unsere Plattform verfolgt einen technologiegetriebenen Ansatz, bei dem Schutzmechanismen von Anfang an intelligent integriert sind. Gerade mit Blick auf Cloud-Komplexität und Vorgaben wie NIS2 zeigt sich, wie entscheidend eine stabile und zugleich adaptive Architektur ist.

**KI kann Angriffe automatisieren, tarnen und skalieren. Welche realen Szenarien ergeben sich daraus für Unternehmen und ihre Sicherheitsstrategien?**
*Adi Reschenhofer:* Cyberabwehr von morgen erkennt Gefahren, bevor sie Form annehmen – sie lernt, täuscht, lenkt und antizipiert. In einer Welt, in der Angreifer mit KI arbeiten, müssen Verteidiger Räume schaffen, in denen der Angriff zur Illusion wird. Wahre Sicherheit entsteht nicht durch Mauern, sondern durch Intelligenz, die das Unbekannte sichtbar macht – und dem Angreifer immer einen Gedanken voraus ist.

*Dr. René Heinzl:* KI verändert die Spielregeln – und zwar zugunsten der Angreifer. Sie erlaubt es, Schwachstellen automatisiert zu analysieren und Angriffe in Echtzeit anzupassen – schneller, als menschliche Analysten reagieren können. Das Grundproblem bleibt: Der Angreifer muss nur einmal durchkommen, die Verteidiger müssen jeden einzelnen Angriff erkennen und abwehren.

***Dr. René Heinzl, CTO***

**KI-gestützte Bots generieren Phishing-Kampagnen, schreiben Exploits und testen Passwörter. Welche realen Szenarien haben Sie 2024/25 bereits beobachtet, und wie trennt man Hype von akuter Gefahr?**
*Dr. René Heinzl:* Seit 2024 sehen wir eine starke Professionalisierung von Angriffen durch generative KI – etwa durch automatisch erstellte Phishing-Mails oder angepasste Exploits. Was früher Tage dauerte, geschieht heute in Minuten – oft vollautomatisch. Unsere Plattform reagiert darauf mit KI-gestützter Anomalieerkennung und verhaltensbasierten Decoys, die Angreifer frühzeitig enttarnen, noch bevor Schaden entsteht.

**Wenn Angreifer KI einsetzen – mit welchen Mitteln kann sich die Verteidigung überhaupt noch behaupten?**
*Dr. René Heinzl:* Wenn Angreifer KI nutzen, bleibt als eine wirksame Antwort nur, selbst KI einzusetzen – aber intelligenter, schneller und vorausschauender. Statt statischer Regeln braucht es lernende Systeme, die auch versteckte Muster erkennen und automatisiert darauf reagieren. Genau das ist die Stärke moderner proaktiver Cyber Defense: Sie erkennt Bedrohungen, bevor sie zum Vorfall werden.

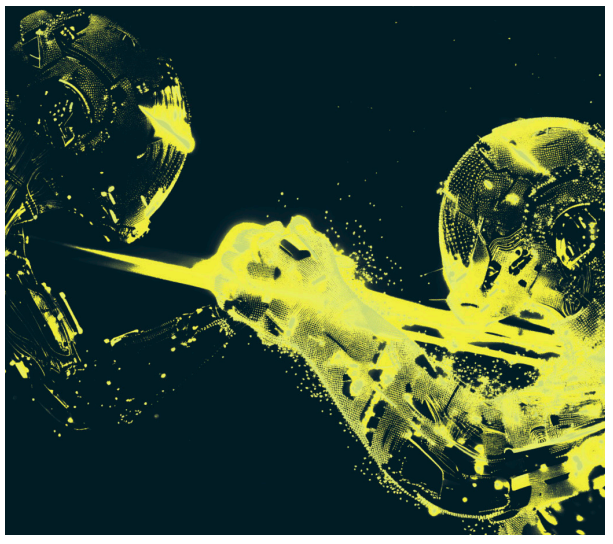
*Adi Reschenhofer:* In einer automatisierten Bedrohungswelt muss Verteidigung klüger und irreführender sein, um bestehen zu können. KI zwingt uns, Cybersecurity – wie viele andere Bereiche – komplett neu zu denken.

**Deepfake-Voicemails, CEO-Fraud, Erpressung im Homeoffice – wie unterstützen Sie Unternehmen dabei, nicht nur Technik, sondern auch Menschen resilienter zu machen?**
*Dr. René Heinzl:* Angriffe wie Deepfake-Anrufe oder CEO-Fraud zielen direkt auf die Verunsicherung von Mitarbeitenden. Deshalb setzen wir nicht nur auf Awareness-Trainings, sondern integrieren täuschungsbasierte Szenarien in den Arbeitsalltag – etwa durch simulierte E-Mails oder Decoy-Zugriffe. So schaffen wir einen sicheren Lernraum, der auf Verständnis und Handlungssicherheit statt Angst basiert.

**Welche Rolle spielen täuschungsbasierte Sensoren und automatisierte SOAR-Playbooks, um KI-getriebene Angriffe in Minuten statt Stunden einzudämmen?**
*Dr. René Heinzl:* Täuschungstechnologien wie Honey-Tokens oder Decoy-VMs sind heute hochpräzise Sensoren in Bereichen, die klassische Sicherheitslösungen oft übersehen. Unsere Plattform platziert diese Artefakte dynamisch und verhaltensbasiert – je nach Aktivität im Netzwerk. Kombiniert mit KI-Agenten und SOAR-Systemen entsteht so eine automatisierte Echtzeit-Reaktion, die Angriffe sofort erkennt, isoliert und neutralisiert.

**Wie sieht eine Sicherheitsarchitektur aus, die nicht nur schützt, sondern Angreifer aktiv in die Irre führt und daraus lernt – und welche Technologien braucht es dafür?**
*Dr. René Heinzl:* Sicherheitsarchitektur muss heute mehr leisten als nur Abschottung – sie muss Angreifer gezielt fehlleiten und beobachten können. Dafür kombinieren wir Täuschungstechnologien, KI-gestützte Verhaltensanalyse und dynamische Angriffserkennung. Konkret heißt das: Digitale Zwillinge produktiver Systeme werden als Decoys eingebunden, die Angreifer anziehen und deren Verhalten in Echtzeit sichtbar machen – ohne dass sie es bemerken.

***Adi Reschenhofer, CEO und Mitbegründer***



**Zum Abschluss eine persönliche Frage: Viele CISOs stehen heute unter massivem Druck – kurze Reaktionszeiten, hohe Verantwortung, permanente Alarmbereitschaft. Warum geraten so viele in Richtung Burnout – und was müsste sich strukturell ändern, damit Cybersecurity nicht zur psychischen Dauerbelastung wird?**
*Adi Reschenhofer:* Das Thema wurde zu lange ignoriert. CISOs sind heute nicht nur für den Schutz hochkomplexer digitaler Infrastrukturen verantwortlich, sondern müssen gleichzeitig zwischen Management, Regulatorik, IT und Fachabteilungen vermitteln – oft rund um die Uhr und unter enormem Erwartungsdruck. Viele arbeiten im Reaktionsmodus, ständig alarmbereit, ohne die nötige strategische Unterstützung oder klare Entscheidungsbefugnisse. Was es braucht, ist ein Umdenken: Wer CISOs entlasten will, muss ihnen genügend Personal und moderne, automatisierte Werkzeuge zur Seite stellen – und klare Rückendeckung aus der Führungsebene geben. Nur so lässt sich der Druck mindern, bevor er krank macht.

*Weitere Informationen via QR-Code:*

CYBERTRAP

## Genius Tip

»Welchen einen Schritt sollten CISOs morgen früh zuerst setzen, um ihre **Angriffsfläche** kurzfristig um mindestens 30 Prozent **zu reduzieren**? Beginnen Sie mit einer **systematischen Kartierung Ihrer digitalen Assets** – nicht aus Sicht der IT, sondern aus Sicht eines potenziellen Angreifers. Platzieren Sie gezielt **Decoys und Honey-Tokens** an sensiblen Punkten, um unerlaubte Zugriffe sichtbar zu machen. Schon diese eine Maßnahme **schafft Transparenz**, erhöht die **Reaktionsgeschwindigkeit** und **reduziert die Angriffsfläche** spürbar.«

# »Präventive IT-Forensik wehrt Cyberangriffe aktiv ab«

**Die Bedrohungen durch Cyber-Kriminelle nehmen zu. Joanna Lang-Recht, Director IT Forensics der intersoft consulting services AG, erklärt, wie Unternehmen sich im Falle eines Cyberangriffs richtig verhalten – und wie präventive IT-Forensik und schnelle Reaktionsmaßnahmen Schäden begrenzen.**

**Interview** Rüdiger Schmidt-Sodingen

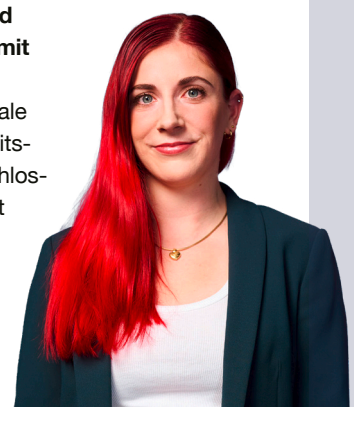
**Frau Lang-Recht, warum ist präventive IT-Forensik heute ein entscheidender Bestandteil jeder Sicherheitsstrategie?**
Präventive IT-Forensik oder auch »Forensic Readiness« hat zum Ziel, sich auf mögliche IT-Sicherheitsvorfälle und deren Bewältigung vorzubereiten. Im Fokus stehen Maßnahmen, um IT-Sicherheitsvorfälle zu vermeiden und ihre Auswirkungen zu minimieren. Unter dem Begriff versteht man auch, eine IT-Landschaft so aufzustellen, dass eine IT-forensische Analyse durchgeführt werden kann und ausreichend Spurenmaterial zur Verfügung steht, um Vorfälle aufzuklären.

**Sie suchen mit ihrem Team gezielt nach digitalen Spuren, um diese auch vor Gericht verwerten zu können?**
Genau. In der IT-Forensik geht es darum, digitale Beweise gerichtsfest zu sichern – also lückenlos dokumentiert, manipulationssicher und nachvollziehbar. Das erfordert spezielles Know-how, standardisierte Prozesse und den Einsatz von Tools, die eine dauerhafte Reproduktion der Ergebnisse garantieren, um die Integrität der Daten und die Beweiskraft vor Gericht zu gewährleisten. Wenn ich einen Datendiebstahl analysiere und die Ergebnisse aufbereite, muss ein zweites unabhängiges IT-Forensik-Team mit den gleichen Tools zum exakt gleichen Ergebnis kommen.

**Wie läuft eine strukturierte Incident Response ab?**
Eine strukturierte Incident Response gliedert sich typischerweise in mehrere Phasen: Vorbereitung, Erkennung und Analyse, Eindämmung, Beseitigung, Wiederherstellung und schließlich die Nachbearbeitung. In jedem Schritt ist es entscheidend, systematisch und dokumentiert vorzugehen. Am wichtigsten ist eine gute Vorbereitung, in der alle Prozesse dokumentiert und regelmäßig auf die Probe gestellt werden. Zum Beispiel durch das Durchführen von Notfallübungen, die sich an realen Szenarien orientieren.

**Wie hilft ein mobiles IT-Forensik-Labor dabei, Schwachstellen oder Anomalien schnell zu identifizieren und entsprechend zu handeln?**
Mit unserem mobilen IT-Forensik-Labor DEVIL können wir direkt beim Kunden vor Ort schnell und effizient arbeiten. Das Labor ist ausgestattet mit allem, was für die Sicherung, Analyse und Auswertung von Daten notwendig ist. Dadurch verkürzt sich die Zeit bis zur ersten fundierten Einschätzung erheblich – ein kritischer Faktor, um weiteren Schaden zu verhindern und effektive Gegenmaßnahmen einzuleiten.

**Welche Rolle spielt Patch Management bei der Risikominimierung – und was tun, wenn Verhandlungen mit Hackern nötig werden?**
Patch Management ist eine zentrale Präventionsmaßnahme: Sicherheitslücken müssen konsequent geschlossen werden, bevor sie ausgenutzt werden können. Dies muss in Unternehmen eine hohe Priorität besitzen, gerade für Systeme, die von außen erreichbar sind. Diese bilden oft den einfachsten Weg in eine IT-Infrastruktur. Kommt es dennoch zu einem Angriff und stehen Verhandlungen mit Hackern im Raum, ist äußerste Vorsicht geboten. Hier sollten spezialisierte Krisenteams oder erfahrene Incident-Responder eingebunden werden. Mit einer strategischen Herangehensweise lassen sich einige Ziele in der Verhandlung realisieren, Zeit gewinnen, oder auch ein geringeres Lösegeld aushandeln.



*Joanna Lang-Recht, Director IT Forensics der intersoft consulting services AG*

**it-forensik.de**
**0180 622 124 6** (24/7-IT-Notfallhilfe)

intersoft consulting

## Genius Tip

»Eine gute **Incident Response** ist wie ein **Feueralarm**: Je **schneller und klarer** alle reagieren, desto **kleiner bleiben die Schäden**. Präventive IT-Forensik hilft dabei, **kritische Schwachstellen** schon im Vorfeld zu erkennen. So wird aus reaktiver Schadensbegrenzung **aktive Verteidigung**.«



# »Durchgängige Überwachung ist unverzichtbar«

**Immer mehr Unternehmen kämpfen mit Cyberangriffen. Thomas Meier, CEO von InfoGuard, sorgt mit 350 Sicherheitsexpert:innen im DACH-Raum dafür, dass Unternehmen rund um die Uhr geschützt sind. Im Interview plädiert er für umfassende Sicherheitsstrategien – und ein dediziertes Security Operations Center (SOC) mit 24/7 Betrieb.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Meier, warum reicht aus Ihrer Sicht eine reine Cyberabwehr heutzutage nicht mehr aus?**
Weil klassische Abwehrmechanismen dem Tempo und der Raffinesse heutiger Angriffe nicht mehr gewachsen sind. Cyberattacken werden immer ausgeklügelter und durch den Einsatz von Künstlicher Intelligenz immer gezielter. Klassische, präventive Schutzmaßnahmen wie Firewalls, MFA oder Patch-Management greifen längst zu kurz. Eine 360-Grad-Cybersicherheit ist deshalb unverzichtbar: Sie kombiniert Prävention, 24/7-Monitoring, Echtzeit-Erkennung und professionelle Vorfallreaktion inklusive forensischer Analysen – für einen optimalen Schutz.

**Welche Rolle spielt die Geschwindigkeit, mit der Angriffe erkannt werden müssen?**
Sie ist absolut entscheidend. Je schneller ein Angriff erkannt wird, desto geringer der Schaden. Dabei sprechen wir heute von Minuten. Genau hier kommen dedizierte SOCs (Security Operations Center) ins Spiel. Unsere SOC- und CSIRT-Fachkräfte analysieren für Kunden 24/7 Bedrohungen, erkennen Anomalien in Echtzeit und leiten Sofortmaßnahmen ein, damit das Sicherheitsdispositiv nachhaltig optimiert wird.

**Was passiert, wenn doch einmal ein Angriff erfolgreich ist?**
Dann zählt jede Sekunde. Professionelle Incident Response macht den Unterschied. Im Ernstfall steht unser hochspezialisiertes Computer Security Incident Response Team (CSIRT) rund um die Uhr einsatzbereit. Erfahrene Experten dämmen die Auswirkungen ein, stellen kompromittierte Systeme und Daten umgehend wieder her und sorgen dafür, dass der Geschäftsbetrieb schnellstmöglich weiterläuft. Was mich besonders freut: Bei all unseren SOC-Kunden konnten wir schwerwiegende Business-Impacts durch Cyberangriffe verhindern.

**Welche Erfolgsfaktoren sehen Sie für ein externes Security Operations Center – auch mit Blick auf KMU?**
Gerade der Mittelstand braucht heute Schutz auf höchstem Niveau. Unsere Erfahrung zeigt: Die Notwendigkeit eines SOC ist vielen bewusst, doch oft fehlen intern die finanziellen und personellen Ressourcen. Ein externes SOC bietet hier eine effiziente und nachhaltige Lösung. Es bringt hochqualifizierte Fachkräfte, modernste Technologien und bewährte Prozesse zusammen, ohne dass intern umfangreiche Ressourcen aufgebaut werden müssen.

**Was macht InfoGuard im Vergleich zu anderen Anbietern besonders?**
Bei InfoGuard liegt der volle Fokus auf Cyber Security und Cyber Defence. Die durchgängige Überwachung der Kundeninfrastruktur durch unsere beiden SOCs in Deutschland und der Schweiz hat höchste Priorität. Drei zentrale Erfolgsfaktoren zeichnen unsere SOC-Services besonders aus: Unser SOC basiert erstens auf einer offenen XDR-Architektur, unterstützt verschiedenste Hersteller und ist somit flexibel und nahtlos in die Kundeninfrastruktur integrierbar. Zweitens profitieren Unternehmen von unserem eigenen und erfahrenen CSIRT – einer der führenden Incident-Response-Einheiten im gesamten DACH-Raum. Auch Kunden ohne SOC-Dienstleistungen können über einen IR-Retainer oder diverse Versicherungen auf diesen Service zugreifen. Drittens erbringen wir sämtliche Dienstleistungen vollständig eigenständig durch hochqualifizierte, deutschsprachige Experten an unseren Standorten in Deutschland, der Schweiz und Österreich. Über 90 SOC- und CSIRT-Spezialisten sorgen dank operativem 24/7-Live-Betrieb und durchgehend personeller Bedrohungsüberwachung Tag und Nacht für bestmöglichen Schutz.

*Thomas Meier, CEO von InfoGuard*

InfoGuard SWISS CYBER SECURITY

## Genius Tip

»Cybersicherheit ist zur **strategischen Managementverantwortung** geworden. Wer Sicherheit strategisch denkt, schützt nicht nur Daten und Systeme, sondern auch **Reputation, Innovationskraft** und **Wettbewerbsfähigkeit** der Organisation. Stärken Sie Ihre Cyberresilienz deshalb mit einem erfahrenen Partner, der nicht nur Technik versteht, sondern Cybersicherheit **ganzheitlich beherrscht** und Ihre Sprache spricht.«

# »Cyber Defense Center im 24/7-Betrieb erfordern Knowhow und Personal«

**Seit 1999 steht ConSecur für umfassende, maßgeschneiderte IT Security Consulting-Dienstleistungen. CEO und Sales Manager Jens Wübker und Management Consultant und Manager ConSecur Academy Matthias Rammes sprechen im Interview über IT-Sicherheit, Managed Services und die richtigen Mitarbeiter.**

**Herr Wübker, Herr Rammes, wie verändert sich der Handlungsdruck für KMU durch gesetzliche Vorgaben?**
*Matthias Rammes:* Aus vielen Gesprächen mit Geschäftsführerenden und leitenden Angestellten weiß ich, dass der Handlungsdruck enorm steigt. Gesetze und Vorgaben, wie z.B. NIS2, die DSGVO oder aber auch branchenspezifische Vorgaben, stellen jeden Tag Herausforderungen dar, mit den Gesetzen und Regelungen konform zu bleiben.

*Jens Wübker:* Darüber hinaus zwingen zunehmend reale Bedrohungsszenarien und Bedrohungslagen die Unternehmen dazu, Cyber-Gefahren ernst zu nehmen und Gegenmaßnahmen zu implementieren. Insbesondere ist festzustellen, dass nicht nur die »großen« Konzernstrukturen hier im Fokus stehen, sondern dass immer mehr auch mittelständische Unternehmen verstärkte Aufmerksamkeit »genießen«. Und um hier einen »reaktiven Ansatz« entgegenstellen zu können, bedarf es nicht unerheblicher personeller Ressourcen, die zu den regulatorischen Herausforderungen zusätzlichen Handlungsdruck erzeugen.

**Warum sind viele Unternehmen beim Spagat zwischen Sicherheitsanforderungen und begrenzten Budgets überfordert?**
*MR:* Meiner Meinung nach ist hier die Vielzahl der unterschiedlichen Regularien die besondere Herausforderung. Gerade kleinere Unternehmen stehen vor einem riesigen Berg an Gesetzen und wissen oft nicht, wo sie anfangen sollen. Auch die oft sehr wage formulierten Anforderungen in den Gesetzen nehmen sie als besondere Herausforderung wahr. Wie viel ist genug und wieviel ist ggf. zu viel?

*JW:* Vor allem sollte man berücksichtigen, dass es nicht reicht, mit dem zur Verfügung stehenden Budget technische Maßnahmen umzusetzen. Trotz aller Technologie und KI müssen personelle Kapazitäten aufgebaut werden, die mit der Technik zielgerichtet den Bedrohungen begegnen können.

**Sind sich die Unternehmen der verschiedenen Bereiche, die Sicherheitslücken aufweisen oder gegen Regularien verstoßen, immer voll bewusst?**
*MR:* In den meisten der mir bekannten Fällen nicht. Und voll bewusst schon gar nicht. In einer kleinen und übersichtlichen IT-Infrastruktur mag ein volles Bewusstsein über die aktuelle Konfiguration und über die aktuellen Systeme noch möglich sein, aber je größer eine IT-Infrastruktur wird, desto schwieriger wird es auch, eine Übersicht über mögliche Schwachstellen, Sicherheitslücken oder gar etwaige Verstößen gegen Regularien zu behalten.

*JW:* Ich würde behaupten, dass es schlicht nicht möglich ist, sich zu jedem Zeitpunkt jeder Sicherheitslücke bewusst zu sein. Gemäß BSI-Lagebericht wurden 2023 täglich über 70 neue Schwachstellen in Softwareprodukten gemeldet. Im Rahmen einer im Auftrag des Bitkom durchgeführten Studie in 2024 waren in den letzten 12 Monaten 81 % der deutschen Unternehmen Opfer eines Angriffs und 10 % haben es vermutet. Hierbei wurden 66 % der Angriffe durch die Analyse von Log-Daten und 33 % durch interne Untersuchungen aufgedeckt. Das zeigt klar, dass Unternehmen sowohl auf technologischer Ebene wie auch auf organisatorischer und personeller Ebene ausreichend Kapazitäten benötigen, um sich diesen Gefahren stellen zu können. Unsere Erfahrungen zeigen jedoch, dass bei den organisatorischen und personellen Ressourcen häufig noch Luft nach oben ist.

**Welche Rolle spielen Managed Security Services, um IT-Sicherheit effizient, skalierbar und Compliance-konform umzusetzen?**
*MR:* Managed Security Services bieten, ähnlich wie andere Dienstleistungen, die Möglichkeit, sich die Profis für einen bestimmten Bedarf ins Unternehmen zu holen.

*JW:* In den meisten Fällen ist das Problem für fehlende personelle Kapazitäten nicht die mangelnde Bereitschaft, überhaupt Personal einzustellen, sondern das richtig qualifizierte Personal zu finden und entsprechend ans Unternehmen zu binden. Und genau hier setzen Security Service Provider wie wir an. Insbesondere wenn man an Bereiche wie Cyber Defense Center im 24/7-Schichtdienst denkt, die viel Knowhow und Ressourcen erfordern.

**Wie wichtig ist es, dass Unternehmen die einzelnen IT-Prozesse zum Schutz ihrer Arbeit verstehen und aktiv unterschützen?**
*MR:* Essenziell. Die Digitalisierung schreitet voran und die meisten Unternehmen können ohne ihre digitale Infrastruktur kaum noch den Betrieb aufrechterhalten. Sollten dann Regeln und Prozesse zum Schutz dieser Infrastruktur fehlen, gefährde ich die Existenz meines Unternehmens.

*JW:* Welches genau der zweite Ansatzpunkt für uns ist, unsere Kunden bei der Bewältigung von Cyber-Risiken zu unterstützen. Alle Managed Services helfen nicht, wenn sich Auftraggeber anschließend voll und alleinig auf den Service Provider verlassen. Wir können dabei helfen, mit unseren Services die personellen Herausforderungen zu minimieren oder zu verringern. Nichtsdestotrotz ist auch auf Auftraggeberseite das notwendige Knowhow zur Abwehr von Cyber-Risiken notwendig, da dieses eine Gemeinschaftsaufgabe von Auftraggeber und Provider ist. Über unsere Akademie bieten wir hierzu Crash-Kurse oder aber auch umfangreiche Recruiting- und Ausbildungsprogramme an, um unsere Kunden zu unterstützen, Personal und Knowhow im notwendigen Umfang aufzubauen. Sei es, um eine eigenes Cyber Defense Center zu betreiben oder sich gemeinsam mit einem Service Provider den Herausforderungen von Compliance-Anforderungen oder Cyber-Bedrohungen zu stellen. Unser Recruiting- und Ausbildungskonzept setzt zudem darauf, bei der Suche nach neuen Mitarbeitern nicht nur auf IT- und IT-Security-Kompetenzen zu schauen, sondern eher andere Qualitäten wie Problemlösungskompetenzen oder den Willen, auch mal neue Wege zu gehen, zu berücksichtigen und qualifizierte Quereinsteiger zu finden.

MR: Eine gewisse Technik- bzw. Informatikaffinität sollte schon vorhanden sein, aber viel wichtiger ist die persönliche Einstellung, Hintergründe verstehen zu wollen, sich eigenständig Informationen beschaffen zu können und hartnäckig Probleme lösen zu wollen. Sobald diese Grundeinstellung vorhanden ist, schließen sich etwaige Wissenslücken von ganz allein.

**Ihre Cyber Threat Intelligence beschäftigt sich mit den Cyber-Angriffen von morgen. Wie funktioniert sie?**
*JW:* Um eine Früherkennung von spezifischen Bedrohungen zu ermöglichen, welche entweder zu neu sind, um in den gängigen Sicherheitstools bereits erkannt zu werden, oder aber spezifisch gegen ein bestimmtes Unternehmen oder eine Branche gerichtet sind, haben wir im Rahmen unseres Managed Cyber Threat Intelligence Services folgende Funktionen etabliert:

**CTI–IoC Feed:** Anbindung unserer CIT–IoC-Plattform an eine bestehende Analyseplattform (z. B. SIEM, EDR, IDS, etc.). Die IoC können dann durch die jeweilige Analyse-Plattformen in den Regelwerken genutzt werden. Die IoC werden von uns über verschiedenen Quellen gesammelt, analysiert und bewertet und dann, auf den jeweiligen Kunden optimiert, ausgespielt.

**CTI–Newsletter:** Tagesaktuelle, auf den Auftraggeber bezogene Security News, basierend auf den IoC und weiteren Quellen per E-Mail.

**External Attack Surface Management:** Monitoring im Clear-, Deep- und Dark-Web auf mögliche Hinweise zu bevorstehenden (bspw. Erwähnungen in Chats von Angreifergruppen) oder eingetretenen Kompromittierungen (bspw. Ransom-Note, leaked credentials) sowie weitere mögliche Bedrohungen wie Typo-Squatting-Domains (Detektion ähnlich lautender Domains wie bspw. »consecur.de <> comsecur.de«) inkl. Alarmierung und optionalem Schwachstellen-Scanning.

*MR:* Im Prinzip nutzen wir die Angriffe oder Angriffsversuche auf unsere eigenen Systeme oder die unserer Kunden, um die Techniken und Taktiken der Angreifer zu verstehen. Dieses Wissen teilen wir dann über ein standardisiertes Vorgehen mit unseren Kunden.Diese Informationen, z.B. sogenannte »Indicators of Compromise«, können dann zur Erkennung weiterer Angriffe aber auch zum Blockieren von Angriffsversuchen genutzt werden.

***Matthias Rammes***
***Management Consultant***
***& Manager***
***ConSecur Academy***

***Jens Wübker***
***CEO & Sales Manager***

**ConSecur**
[security and consulting]

## Genius Tip

**»You better know your enemy.**
Sei deinen Angreifern
immer einen Schritt voraus!«

# »Resilienz und Betriebsfähigkeit sind grundlegende Säulen zum Erhalt einer Unternehmung«

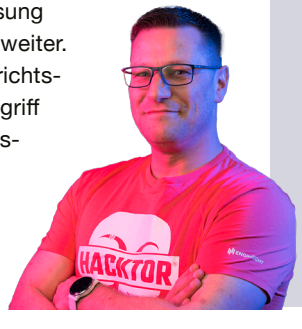
**Nicht warten, starten! Michael Rainer, Business Development Manager Public bei der Enginsight GmbH, erklärt, warum sich deutsche Unternehmen und Verwaltungen schnellstmöglich nicht nur präventiv, sondern auch resilient und souverän gegen Cyberangriffe wappnen sollten.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Rainer, Sie rufen deutsche Unternehmen dazu auf, mehr auf europäische Sicherheitslösungen zu setzen. Warum?**
Das sehe ich pragmatisch! Wir haben Leistungen und Lösungen in Europa und Deutschland. Damit haben wir das Thema der DSGVO schon einmal erledigt. Weiter sind hiesige Lösungen näher an den Anforderungen, Rahmenbedingungen und Bedürfnissen - nicht nur für Unternehmen, sondern auch für öffentliche Einrichtungen. Nicht zuletzt wird auch der Wirtschaftskreislauf geschlossen und die Finanzkraft fließt nicht ab. Der aktuell vielleicht wichtigste Punkt: Wer auf EU-Lösungen setzt, macht seine Sicherheit nicht von der Willkür unberechenbarer Politgrößen abhängig.

**Welche Rolle spielen Security Operations Center (SOC) – und wie lassen sich diese durch KI automatisieren oder verbessern?**
Das Thema SOC sehe ich in erster Instanz eher kritisch. Die wenigsten Unternehmen sind in der Lage, ein eigenes SOC zu betreiben; 24/7 schon gar nicht. Schauen wir also auf SOC als externe Dienstleistung. Leider sehen viele es als Allheilmittel, mit welchem man selbst keinerlei Arbeit mehr hat. Weit gefehlt! Für den Einsatz eines SOC sollten schon gewisse Grundlagen geschaffen sein, da ein Betrieb sonst kaum möglich ist und wenn, sehr teuer werden kann. Zudem stellt sich auch immer die Frage, ob das SOC nur Monitoringdienste übernimmt oder auch Incident Response. Letzteres setzt entsprechende Zugriffsrechte in die Infrastruktur voraus. Andernfalls muss der Kunde eigene Mitarbeiter im Bereitschaftsdienst vorhalten, die im Ernstfall umgehend reagieren können. Unter den richtigen Voraussetzungen und mit den passenden Ressourcen ist ein (proaktives) SOC eine super Sache. KI kann darin gute Dienste leisten und tut es in vielen Fällen auch schon. Ich distanziere mich jedoch von der gehypten »Zauberstab-KI«. Sie muss zweckmäßig, backdoorfrei, transparent und nachjustierbar sein. Wenn diese dann auch noch On-Premises und offline lauffähig ist, haben wir beste Voraussetzungen zu sicheren Automatismen, welche den menschlichen Aufwand reduzieren und Freiräume entstehen lassen, die anderweitig gut genutzt werden können.

**Welche konkreten Vorteile bieten On-Premises-Lösungen in Bezug auf eine durchgehende Kontrolle und Datensicherheit?**
Kampfmodus! Damit kann man sich im Falle eines Angriffs oder des Verdacht darauf forensisch korrekt verhalten: Gehe nicht zum Hauptschalter und sorge für Dunkelheit, sondern kappe einfach die Internetverbindung und die gesamte Lösung läuft ohne Funktionseinbuße offline weiter. Schließlich wollen wir durchweg gerichtsverwertbare Daten erheben, den Angriff abwehren und vor allem die Betriebsfähigkeit erhalten. Weiter hat man On-Premises mit einer entsprechend backdoorfreien Lösung die absolute Datenhoheit, was ich bei derart relevanten und sicherheitstechnischen Daten als essenziell ansehe. Nicht zuletzt bedürfen sämtliche Onlinedienste und gerade ein SIEM sehr schnell sehr viel Bandbreite, welche nicht in jedem Fall gegeben ist.




*Michael Rainer, Business Development Manager Public, Enginsight GmbH*

**Sie sagen: Resilienz, Betriebsfähigkeit und Informationssicherheit sind keine netten Empfehlungen.**
Resilienz und Betriebsfähigkeit sind aus meiner Sicht grundlegende Säulen zum Erhalt einer Unternehmung oder Einrichtung. Allzu oft rennt man Sicherheitsrisiken, Schwachstellen und Konfigurationen hinterher. Demnach ist eine nachgelagerte Sicherheitsinstanz, welche Angriffe erkennt und abwehrt, viel wert. Gerade die Anti-KI oder Schwachstelle Mensch, wie ich sie liebevoll nenne, ist unberechenbar. Arbeitsalltag, zu wenig Zeit für permanentes, awarenessgerechtes Verhalten und fehlendes technisches Wissen und Verständnis sorgen täglich für erhöhte Erfolgschancen der Angreifer.

ENGINSIGHT

**sec.enginsight.com/welt**

## Genius Tip

»**Einfach mal machen**; mit praxisnahen, bedarfsgerechten und automatisierten **Methoden zur Absicherung** aus **holistischer Perspektive**. Und sich dann auch **entspannt** in den **Feierabend** verabschieden!«



# Neue Einfallstore durch KI: Wie Unternehmen ihre IT-Sicherheit anpassen müssen

**Künstliche Intelligenz verändert das Kräfteverhältnis in der Cyberabwehr. Dino Huber leitet die Cyber-Security-Einheit von DATAGROUP und analysiert im Gespräch, wie sich die Bedrohungslage verschärft hat und warum neue Sicherheitskonzepte gefragt sind.**

**Warum greifen klassische Sicherheitskonzepte nicht mehr?**
*Dino Huber:* Klassische Schutzmaßnahmen wie Firewalls, Antivirensysteme oder VPNs arbeiten regelbasiert und reaktiv. Sie erkennen nur bekannte Muster oder Angriffe, die bereits dokumentiert wurden. Moderne Angreifer nutzen jedoch KI, um gezielt neue Schwachstellen zu identifizieren, sich dynamisch anzupassen und bestehende Regeln zu umgehen. Firewalls filtern, was explizit blockiert wird, Antivirensysteme erkennen bekannte Schadsoftware und VPNs öffnen oft weitreichende Zugriffsmöglichkeiten ohne ausreichende Kontrolle. Genau hier setzen heutige Angriffe an. Um dieser Bedrohung zu begegnen, müssen Unternehmen auf eine Sicherheitsstrategie umstellen, die auf kontinuierlicher Prüfung, kontextbasierter Analyse und KI-gestützter Erkennung ungewöhnlicher Aktivitäten basiert.

### Neue Angriffsvektoren durch KI

**Was macht Cloud- und IoT-Umgebungen besonders angreifbar?**
In Cloud-Infrastrukturen fehlt es oft an klarer Segmentierung. Daten und Anwendungen liegen zu nah beieinander, was die Ausbreitung von Angriffen erleichtert. Bei IoT-Systemen ist veraltete Software ein zentrales Problem. Sicherheitsupdates werden selten priorisiert, weil der Fokus auf dem laufenden Betrieb statt der Sicherheit liegt. Diese strukturellen Schwächen nutzt KI gezielt aus, indem sie Muster im Datenverkehr erkennt und automatisiert angreift. Unternehmen benötigen deshalb Systeme, die auffällige Aktivitäten im gesamten Netzwerk erkennen.

**Wie wird die Lieferkette zur Schwachstelle?**
*V*iele Angriffe erfolgen über Drittanbieter, zum Beispiel durch manipulierte Updates oder Phishing. Die eigene IT ist oft eng mit externen Systemen vernetzt, ohne dass deren Sicherheitsniveau klar ist. KI nutzt öffentlich verfügbare Informationen, um potenzielle Schwächen zu identifizieren. Ein systematisches Monitoring der digitalen Angriffsflächen hilft dabei, Risiken in der Lieferkette sichtbar zu machen und gemeinsam mit Partnern geeignete Maßnahmen zu vereinbaren.

**Was macht Ransomware so gefährlich?**
Die einfache Verfügbarkeit von Ransomware-Diensten senkt die Einstiegshürden für Kriminelle. Künstliche Intelligenz erhöht zusätzlich die Wirksamkeit dieser Angriffe, beispielsweise durch gefälschte Stimmen oder täuschend echte Videos. Die Angriffe erfolgen automatisiert und treffen Unternehmen jeder Größe. Auch kleine Betriebe sind betroffen, oft als unbeabsichtigte Nebenziele. Das Risiko ist längst nicht mehr auf Großunternehmen beschränkt.

### Was Unternehmen tun müssen

**Wie sieht eine resiliente Sicherheitsstrategie aus?**
Eine Zero-Trust-Architektur ist die Basis. Kein Zugriff wird automatisch als sicher eingestuft. Jede Verbindung muss unabhängig von Identität oder Gerät überprüft werden. Ergänzend helfen KI-gestützte Systeme, verdächtige Aktivitäten in Echtzeit zu erkennen. Unternehmen sollten ihre Sicherheitsvorkehrungen regelmäßig testen und ihre Schutzkonzepte kontinuierlich verbessern. IT-Sicherheit gehört auf die Agenda der Geschäftsleitung und muss im ganzen Unternehmen verankert sein. Auch die Lieferkette braucht klare Anforderungen und regelmäßige technische Überprüfungen. Wer sich zusätzlich auf spezialisierte Dienstleister stützt, kann Sicherheit flexibel und zielgerichtet aufbauen.

**Was ist entscheidend für die Zukunft?**
IT-Sicherheit ist kein fixer Zustand, sondern ein laufender Prozess. Bedrohungslagen ändern sich ständig, deshalb müssen auch Sicherheitsstrategien regelmäßig angepasst werden. Ein gutes Notfallmanagement gehört ebenso dazu. Nur wer vorbereitet ist, kann im Ernstfall strukturiert und wirksam reagieren.

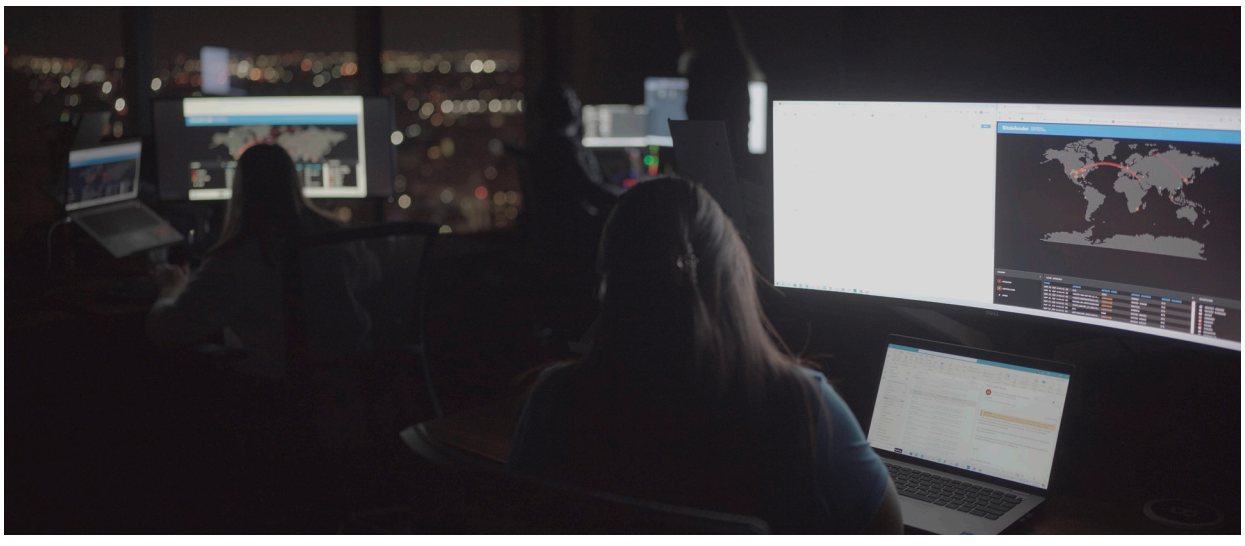
DATAGROUP

## Genius Tip

**Cyberhelden** werden durch den **Partner** gemacht, den sie wählen:

Dino Huber, Geschäftsführer der DATAGROUP Cyber Security
E-Mail: cybersecurity@datagroup.de
Sprechen Sie uns gerne zu unseren Managed Security Services an.

# Von Insellösungen zur Plattformstrategie: Wie Sicherheit, Risiko und Compliance zusammenwachsen



**Als führender Anbieter von Cybersecurity-Lösungen bietet Bitdefender strategische, ganzheitliche Lösungen bei der Prävention, Erkennung und Bereinigung von Bedrohungen. Jörg von der Heydt, Regional Director DACH, über die Wirkung von Bitdefender GravityZone, einer umfassenden Security-, Risiko-Management und Compliance-Plattform sowie der neuen PHASR-Technologie, die KI-basiert, dynamische und automatisierte Sicherheit ermöglicht.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr von der Heydt, Cybersecurity wird zur strategischen Aufgabe. Was folgt daraus für Unternehmen mit ihren komplexen Infrastrukturen und Compliance-Anforderungen?**
Über Cybersecurity reden wir seit vielen Jahren. Sie sollte längst Chefsache sein, denn es geht nicht mehr nur darum, gefährliche Entwicklungen oder Angriffe zu beobachten und abzuwehren. Es geht darum, dass Unternehmen Cybersecurity als strategisches Mittel verstehen, um den operativen Betrieb aufrecht zu erhalten, auszubauen, sich einen Wettbewerbsvorteil zu schaffen und aktiv neue Dinge zu ermöglichen. Es geht um mehr als nur um Firewalls und einzelne Security-Tools. Die Angreifer sind oft längst bereits im Unternehmen unterwegs, sie arbeiten mit der neuesten Technologie – und sie können nur mit ganzheitlichen Strategien abseits des bisherigen Silodenkens erfolgreich bekämpft werden.

**Was kann KI für die Cybersicherheit und damit auch den störungsfreien Erfolg eines Unternehmens leisten?**
Am besten könnte sie in den Köpfen der Unternehmer aufräumen (lacht). KI kann keine Wunder bewirken. Wenn ich aber über große Datenmengen und wirksame Algorithmen verfüge, kann ich mit KI einen entsprechenden Mehrwert ziehen. Ich kann sehen, was überall in der Welt passiert und welche Branchen gerade angegriffen werden. Ich kann dem Angreifer gezielt das Leben schwer machen und meine Angriffsfläche drastisch verkleinern. Mit weit über 600 Millionen Sensoren und den daraus generierten Telemetriedaten verfügt Bitdefender über diesen Datenlake. Eine Erkenntnis daraus: Wenn es Angreifern zu schwer gemacht wird, wenden sie sich anderen Zielen zu. Mit KI können die Hürden für erfolgreiche Angriffe immer größer werden.

**Statt vieler einzelner Lösungen schaffen Sie mit der Plattform GravityZone und der PHASR-Technologie nun Übersicht und Ordnung. Wie?**
Wir sind seit 2008 als Pionier in Sachen KI unterwegs. Uns war von Anfang an klar, dass wir bezüglich Cybersecurity auch die individuellen Angriffsflächen analysieren und schützen müssen. Wir betrachten also nicht nur jede Abteilung, beispielsweise den Vertrieb oder das Marketing – sondern definieren die individuellen Angriffsflächen pro User und Endgerät. KI hilft uns dabei, das Nutzerverhalten jedes einzelnen Users genau zu analysieren. Viele Angriffe erfolgen über standardmäßig installierte legitime Tools, die aber nur von sehr wenigen Usern genutzt werden. KI analysiert das individuelle Nutzerverhalten und gibt die entsprechenden Tools dann frei oder sperrt sie. Diese individuelle Anpassung schließt etliche Sicherheitslücken.

**Wie verändert PHASR das Verständnis von Endpunktsicherheit – weg von Alarmflut hin zu risikobasierter Steuerung?**
Die PHASR-Technologie untersucht das Verhalten, das es über die letzten 30 Tage an einem Endpoint wahrgenommen hat – und übersetzt es entsprechend in Policies. Die KI berücksichtigt also das, was die Mitarbeitenden konkret tun und zum Arbeiten brauchen. Diese Analyse nimmt den Mitarbeitenden die Angst vor einem Automatismus, den sie nicht verstehen oder der sie einfach übergeht. Die KI funktioniert als Absicherungsmechanismus, der Risiken viel gezielter und trotzdem automatisch eindämmt.

**Das heißt, die Plattform wird durch immer mehr Daten und die unterstützende Threat Intelligence-Datenbank immer besser?**
Auch das. Dieses dauernde Dazulernen ist generell das, was die Bitdefender-DNA ausmacht. Wir wollen wissen, was Angreifer als nächstes vorhaben. Daher betreiben wir ein breites Darkweb-Monitoring und geben uns dazu als Hacker aus. So sehen wir, welche Schwachstellen gerade adressiert werden, welche neuen Angriffstools oder auch -taktiken gerade ausprobiert werden. Dieses Wissen hilft uns, Kunden proaktiv bei der Abwehr neuartiger Angriffe zu unterstützen.

***Jörg von der Heydt,***
***Regional Director DACH***

**Wie funktioniert das Zusammenspiel aus KI, Risikoanalyse und dynamischer Reaktion?**
Das Zusammenspiel kann nur funktionieren, wenn ich als Unternehmen einen ganzheitlichen Blick wage. Besonders KMU haben Angst vor Compliance-Regeln oder einem umfassenden Risikomanagement. Sie kämpfen mit den verschiedenen Regelwerken und Tools – und glauben oft, im Grunde keine Kontrolle zu haben. Dabei betreiben alle Unternehmen ja bereits ein Security- und damit auch Risiko-Management. Die Frage ist also: Welches Gap habe ich bei zentralen Sicherheitsfragen? Wie kann ich die einzelnen Lücken schließen? Wie kann ich die Compliance-Richtlinien umsetzen?

**Was bedeutet das für Compliance-Umgebungen mit komplexen IT-Strukturen?**
Ich muss als Unternehmen wissen: Wer beschäftigt sich mit Risikomanagement, wer mit dem Sicherheitsmanagement? Compliance gibt hier lediglich Strukturen vor, an denen ich gemeinsam mit den Mitarbeitenden arbeite, um alles so abzusichern, dass mein Geschäft heute und in Zukunft funktioniert und nicht gestört werden kann. Es ist wichtig zu verstehen, dass diese Bereiche eng verzahnt sind und sich in weiten Teilen überschneiden. Zunächst benötigt es eine qualifizierte Risikoeinschätzung zu Kosten und Nutzen. Welche Endpoints sind wichtig für das Business? Wie verhalten sich dort die Nutzer? Mit den Daten, die ich bereits am Endpoint zur Verfügung habe, kann ich Compliance-Regeln abgleichen – und dies in Echtzeit und kontinuierlich, nicht nur einmal im Jahr zum nächsten Audit. Wenn Sie auf diese Weise automatisiert Sicherheit abklopfen können, merken Sie als Unternehmen plötzlich, dass viele komplexe Dinge händelbar werden.

**Wo liegen die größten Praxispotenziale – z. B. im Mittelstand, bei kritischer Infrastruktur oder in hybriden IT-Setups?**
Komplexe Strukturen brauchen keine kleinteiligen Antworten. Das ist ein beliebtes Missverständnis. Im Gegenteil. Komplexe Strukturen brauchen eine Lösung, die alle Clients erfassen kann. Unternehmen haben beispielsweise 1.000 Mitarbeitende, dann haben sie in der Regel auch 1.000 Clients, Laptops, dazu Server, dazwischen einige Switches, Firewalls und Router. Der größte Teil dieser Infrastruktur – also die Client-Server-Welt - kann mit unserer Plattform adressiert werden. Jeder Endpoint kann gezielt auf Compliance überprüft und sogar mit einem Fix-Button über die Plattform adaptiert oder repariert werden. Leider unterschätzen speziell kleinere und mittlere Unternehmen, wie sehr ihre Compliance von Bedeutung ist. Denn immer mehr Unternehmen wollen nur noch Partner, die beispielsweise nach den NIS-2-Richtlinien arbeiten oder zertifiziert sind. Die tatsächlichen Maßnahmen, um NIS 2 umzusetzen, sind gar nicht das Problem. Viele Unternehmen wissen nicht, wo sie stehen. Dabei helfen wir. Wir schätzen die vorhandene Infrastruktur ein und beschreiben die Probleme, um sie dann möglichst schnell und effizient lösen zu können. Compliance, also strukturiertes Risiko-Management, ist besonders für KMU wichtig, die zunehmend von digitalen Prozessen abhängig sind. Ich rate deshalb: Machen Sie die Gap-Analyse und regeln Sie Ihre Compliance jetzt! Viele KMU haben Angst vor Aufwand und Kosten, die mit der Erfüllung von Compliance-Vorgaben verbunden ist. Aber nochmal: Die eigentliche Angst entsteht durch das Unwissen, weil ich nicht weiß, wie hoch mein Risiko ist. Und Sie müssen als Unternehmen, das im Geschäft bleiben will, immer bedenken: Die eigene Compliance schützt auch andere Unternehmen und Partner.

**bitdefender.com/de-de/phasr**

Bitdefender® Global Leader In Cybersecurity

# »Künstliche Intelligenz: Schlüssel zur digitalen Transformation und Wettbewerbsfähigkeit«

**Wie treibt Künstliche Intelligenz (KI) die Digitalisierung voran und welche konkreten Schritte müssen Unternehmen einleiten, um KI bei sich erfolgreich zu integrieren? Antworten von Prof. Dr. Axel Müller-Groeling, Vorstand für Forschungsinfrastrukturen und Digitalisierung der Fraunhofer-Gesellschaft, und Prof. Dr. Ingo Weber, Direktor für Digitalisierung und IuK-Infrastruktur der Fraunhofer-Gesellschaft.**

**Herr Prof. Müller-Groeling, Herr Prof. Weber, was hat digitale Transformation mit KI zu tun?**
*IW*: In Deutschland sprechen wir oft von Digitalisierung, im Englischen hingegen unterscheidet man drei Begriffe: Digitization (Umwandlung analoger in digitale Informationen), Digitalization (Nutzung digitaler Technologien zur Veränderung von Geschäftsprozessen) und Digital Transformation (umfassende Veränderung von Geschäftsmodellen und -kulturen durch digitale Technologien). KI spielt in allen drei Bereichen eine Schlüsselrolle, aber ihr transformatives Potenzial entfaltet sich vor allem in der Digital Transformation.

**Wie können wir unsere Wettbewerbsfähigkeit durch KI steigern?**
*AMG*: KI ist transformativ, weil sie teilweise menschliche Fähigkeiten übertrifft, insbesondere in der Datenanalyse, Mustererkennung und bei manchen Entscheidungen. Zudem verbreitern sich die Fähigkeiten von KI zunehmend, was ihre Integration in unsere Prozesse erleichtert. Selbst kleine KI-Assistenzen, wie automatisierte Textproduktion oder Unterstützung bei Recherchen, können die Produktivität erheblich steigern. Und es gibt Anwendungen, in denen KI den Menschen bereits heute oder in naher Zukunft ersetzen kann – auch in Form autonomer KI-Agenten. Deutschland und Europa sind aktuell in Sorge, technologisch im internationalen Wettbewerb zurückzufallen. KI bietet uns jetzt eine Chance, dem durch gezielte Investitionen und strategische Implementierung entgegenzuwirken.

**Welche Chancen haben Deutschland und Europa, ganz oben mitzuspielen?**
*IW*: Die Leistung von Large Language Models (LLMs) wie ChatGPTs KI hängt neben dem Modell selbst sehr von der Qualität der Datengrundlage ab. Viele der hochwertigsten Daten sind allerdings vertraulich. In Deutschland und Europa entstehen gerade besondere Datenräume, die sicheren und kontrollierten Datenzugang ermöglichen, ohne dass sensible Daten das geschützte Umfeld verlassen müssen. Das ermöglicht prinzipiell KI-Modelle neuer Qualität – gerade in hochsensiblen Bereichen wie dem Gesundheitswesen und der Finanzbranche. Diese Datenräume definieren eindeutige Datennutzungsrechte und stellen sicher, dass sowohl das Training als auch die Anwendung der KI-Modelle im Einklang mit geltendem Recht und den Restriktionen der Datengeber erfolgen. Das kann ein großer Wettbewerbsvorteil sein.

**Wie kommen Unternehmen nun ins Handeln? Wo sollen sie anfangen?**
*IW*: KI-Implementierungen werden schnell unternehmensspezifisch. Ihre volle Wirkmacht entfalten sie erst in der Kombination aus hochwertigem Modell und spezialisierten Datensätzen für Training und Inferenz. Ich glaube, Unternehmen, die KI adaptieren möchten, sollten viel Energie auf einen Bottom-up-Ansatz verwenden. Anstatt nur top-down eine KI-Strategie zu entwerfen, sollte KI als Entdeckungsverfahren betrachtet werden. Dazu gehört, KI-Tools frühzeitig im Unternehmen verfügbar zu machen, um Mitarbeitende zu ermutigen, mit der Technologie zu experimentieren und innovative Anwendungsmöglichkeiten zu finden. So kann es gelingen, Schlüsselanwendungen zu finden, deren Automatisierung signifikanten Mehrwert bieten, sei es als KI-Assistenz, KI-Agent oder Gruppe von KI-Agenten.

*AMG*: Maßgeschneiderte KI-Lösungen bieten höhere Effizienz und bessere Ergebnisse in unternehmensspezifischen Problemstellungen als generische Lösungen. Die Einführung von KI-Methoden stellt eine umfassendere Transformation von Unternehmen dar als lediglich die Anwendung der beeindruckenden State-of-the-Art KI-Modelle. Hier können geeignete Institutionen, darunter auch Fraunhofer, mit tiefer Domänen- und KI-Expertise Unternehmen maßgeblich unterstützen.

**Was bedeuten die US-Wahlergebnisse für unseren Umgang mit KI?**
*AMG*: Die USA-Wahl lässt die Souveränität Europas wieder in den Vordergrund rücken. Der Bereich KI profitiert aktuell besonders von dem Austausch mit den USA. Sollte dieser Austausch spürbar eingeschränkt werden, wären die Auswirkungen auf die Fähigkeiten Europas gravierend. Daher sollten wir eine Diskussion darüber führen, inwieweit die europäischen und nationalen Initiativen ausreichende strategische KI-Souveränität erzeugen.

**Prof. Dr. Ingo Weber (links) und Prof. Dr. Axel Müller-Groeling betonen die strategische Bedeutung maßgeschneiderter KI-Lösungen für Unternehmen.**

---

## Genius Partner • Spike Reply DE

*think about: Cyber Security*

# NIS2 als Weckruf: Warum Unternehmen Cybersicherheit jetzt ganzheitlich denken müssen

**Ein Experteninterview mit Daniel E. Schormann, Geschäftsführer von Spike Reply DE, über die neue EU-Richtlinie, die Bedeutung einer gelebten Sicherheitskultur und den Ansatz »Security by Design«.**

**Herr Schormann, die EU-Richtlinie NIS2 verschärft die Anforderungen an die Cybersicherheit für viele Unternehmen erheblich. Ist das der längst überfällige Weckruf?**
Absolut. NIS2 ist mehr als nur eine weitere Regulierung – es ist ein klares Signal, dass der bisherige, oft reaktive Ansatz in der Cybersicherheit nicht mehr ausreicht. Viele Unternehmen haben Sicherheit bisher primär als technisches Problem betrachtet und auf Einzelmaßnahmen gesetzt. NIS2 zwingt sie nun, Cybersicherheit als strategisches und ganzheitliches Thema zu begreifen, das die gesamte Organisation durchdringen muss. Der regulatorische Druck sorgt dafür, dass echte Veränderungen angestoßen werden, die über die reine Implementierung technischer Lösungen hinausgehen. Wir beobachten, dass viele Organisationen erst durch diesen externen Anstoß die notwendigen internen Diskussionen führen und Budgets bereitstellen.

***Daniel E. Schormann, Geschäftsführer, Spike Reply DE***

**Sie sprechen die Notwendigkeit eines ganzheitlichen Ansatzes an. Welche Rolle spielt dabei die Sicherheitskultur in Unternehmen?**
Eine entscheidende. Technische Maßnahmen allein können keinen hundertprozentigen Schutz bieten, wenn die Mitarbeiter nicht für Sicherheitsrisiken sensibilisiert sind und sich ihrer Verantwortung bewusst sind. Eine starke Sicherheitskultur bedeutet, dass jeder Mitarbeiter, vom Vorstand bis zum Praktikanten, ein Grundverständnis für Cybersicherheit hat und entsprechende Verhaltensweisen im Arbeitsalltag etabliert. Es geht darum, Awareness zu schaffen, aber auch klare Prozesse und Verantwortlichkeiten zu definieren. Nur so kann Sicherheit wirklich gelebt und nicht nur als lästige Pflicht empfunden werden. Letztendlich ist der Mensch oft das schwächste Glied in der Sicherheitskette, aber er kann durch die richtige Schulung und Einbindung zur stärksten Verteidigungslinie werden.

**Wie lässt sich eine solche Sicherheitskultur wirksam aufbauen?**
Das erfordert ein klares Bekenntnis der Unternehmensführung und eine kontinuierliche Auseinandersetzung mit dem Thema. Einmalige Schulungen reichen nicht aus. Es braucht regelmäßige Trainings, praxisnahe Beispiele und eine offene Kommunikationskultur, in der auch über Fehler und Beinahe-Vorfälle gesprochen werden kann, ohne dass gleich Sanktionen drohen. Wichtig ist auch, die Mitarbeiter aktiv einzubeziehen und sie zu »Security Champions« zu machen, die das Thema in ihren Teams vorantreiben. Gamification-Ansätze können ebenfalls helfen, das Bewusstsein spielerisch zu schärfen und die Motivation hochzuhalten.

REPLY SPIKE

# »Technologie neu denken: Wie Circular-Tech-Modelle Unternehmen zukunftsfähig machen«

**Ein Interview mit Dr. Mathias Wagner, CEO von CHG-MERIDIAN**

**Herr Wagner, angesichts wirtschaftlicher Unsicherheiten und wachsender Innovationsanforderungen stehen viele Unternehmen unter Druck. Die häufig vorgeschlagene Lösung: Transformation. Was bedeutet das für Unternehmen und welche Rolle spielen Circular-Tech-Modelle dabei?**
Transformation ist mehr als nur ein Schlagwort. Für mich bedeutet sie: aktiv gestalten, nicht nur reagieren. Und genau das ist jetzt nötig, denn viele Unternehmen stehen aktuell im Spannungsfeld zwischen steigendem Innovationsdruck – Stichwort KI, Automatisierung, Digitalisierung – und knappen Budgets. Circular-Tech-Modelle, also Nutzungsmodelle wie Leasing, Miete oder Device-as-a-Service, beispielsweise für IT, auf Basis eines zirkulären Wirtschaftssystems, bieten hier eine echte strategische Chance. Sie schaffen finanzielle Freiräume und erlauben es den Unternehmen, gezielt dort zu investieren, wo Innovation strategischen Mehrwert kreiert.

**Was genau verstehen Sie unter einem Circular-Tech-Modell?**
Circular-Tech steht für einen ganzheitlichen Ansatz im Umgang mit Technologie: Statt IT-Hardware klassisch zu kaufen, setzen Unternehmen auf Nutzung. Die Geräte werden dabei von uns über ihren ganzen Lebenszyklus begleitet, von der Bereitstellung über die Nutzung, Rücknahme, die Wiederaufbereitung und Wiedervermarktung. Im Vergleich zum klassischen Kauf, können Unternehmen damit zum einen ihre operativen Kosten senken und sind gleichzeitig in der Lage sich agiler an neue wirtschaftliche Herausforderungen anzupassen, bspw. für die Implementierung KI-gestützter Prozesse für die es neueste Hardware braucht.

**Und wo liegt der strategische Vorteil?**
Ganz klar in der Kombination aus Flexibilität, Liquidität und Innovationskraft. Wer flexibel auf immer neue Anforderungen reagieren kann, etwa durch temporäre Erweiterung der IT-Infrastruktur, verschafft sich einen klaren Wettbewerbsvorteil. Zudem können die laufenden Kosten für IT-Nutzung als Betriebsausgaben verbucht werden, das entlastet die Bilanz und schafft Raum für andere Investitionen.

**Und wie sieht es mit der Nachhaltigkeit aus?**
Jedes Gerät wird am Ende der Nutzung entweder wiederaufbereitet oder recycelt. Das ist nicht nur ökologisch sinnvoll, sondern erfüllt auch regulatorische Anforderungen; Stichwort ESG und EU-Berichtspflichten. Unternehmen können durch zirkuläre IT ihre Nachhaltigkeitsziele messbar unterstützen und nach außen glaubwürdig kommunizieren.

**Was empfehlen Sie Unternehmen, die vor der Entscheidung stehen: Kaufen oder Nutzen?**
Stellen Sie sich die Frage: Wollen Sie Technologie besitzen? Oder wollen Sie sie strategisch nutzen? Wer Innovation leben will, braucht ein Modell, das Veränderung erlaubt. Die Entscheidung für Circular-Tech-Lösungen ist deshalb eine Entscheidung für Zukunftsfähigkeit. Unsere Erfahrungen zeigen, dass sich durch Circular-Tech-Modelle, wie Leasing, Miete oder Device-as-a-service im Vergleich zu Neuanschaffungen Einsparungen im zweistelligen Prozentbereich erzielen lassen. Gleichzeitig steigt die Innovationsgeschwindigkeit spürbar. Für viele Unternehmen ist das der Schlüssel, um trotz begrenzter Budgets ganz vorne mitzuspielen.

*Dr. Mathias Wagner, CEO von CHG-MERIDIAN*

CHG technology2use®

## Über die CHG-MERIDIAN-Gruppe

Die CHG-MERIDIAN-Gruppe zählt zu den führenden globalen technology2use-Unternehmen für die Bereiche IT, Industrie und Healthcare. Mit rund 1.600 Mitarbeiter:innen weltweit entwickelt, finanziert und managt sie maßgeschneiderte Technologielösungen, basierend auf dem »Nutzen statt Besitzen«-Prinzip. Aktuell verwaltet CHG-MERIDIAN ein Technologieportfolio im Wert von 11,73 Milliarden Euro (Stand 2024).

**www.chg-meridian.com**



# Die richtigen Informationen zum richtigen Zeitpunkt!

## Wie Data Analytics hilft, schneller bessere Entscheidungen zu treffen.

**In einer zunehmend datengetriebenen Welt ist Data Analytics zum zentralen Instrument für Unternehmen und Organisationen geworden. Data Analytics bezeichnet die Auswertung großer Datenmengen, um Muster, Zusammenhänge und Trends zu erkennen. Dabei kommen verschiedene Analysearten zum Einsatz – von der deskriptiven Analyse (Was ist passiert?) bis hin zur präskriptiven Analyse (Was sollten wir tun?).**

**Das Grundproblem in den meisten Organisationen.**
Organisationen treffen im Wesentlichen zwei Arten von Entscheidungen: Große strategische Entscheidungen durch das Topmanagement und täglich unzählige kleinere, taktische Entscheidungen durch Mitarbeitende. Während für die Sammlung, Analyse und anschliessende Aufbereitung der Datenbasis für strategische Entscheidung nahezu unbegrenzte Mittel zur Verfügung stehen, werden die meisten Entscheidung von Abteilungen oder der dort Mitarbeitenden häufig weniger auf Basis einer abgestimmten, qualitätsgesicherten und aufgabenbezogenen Datenbasis, sondern auf Basis von eigenen Erfahrungen, daraus resultierenden Einschätzungen und mit Hilfe einer aufwändigen eigenen Datenzusammenführung und Auswertung gefällt. Nur ein Bruchteil der Zeit verbleibt dann noch für das Abwägen von konkreten Handlungsoptionen und das Treffen einer »guten« Entscheidung.

**Was ist eine gute Entscheidung?**
Eine gute Entscheidung hilft Organisation, die strategischen und daraus abgeleiteten operativen Ziele zu erreichen. Dieses gilt insbesondere für Entscheidungen der vorab erwähnten Mitarbeitenden. Sie haben meist eine unmittelbare Auswirkung auf das Betriebsergebnis oder die Kostenlage eines Unternehmens. Mag hier jede einzelne Entscheidung für sich gesehen als nicht relevant anerkannt werden, stellt die

Summe aller Entscheidungen nichts anderes als die Umsetzung der strategischen Entscheidungen des Topmanagements dar. Umso wichtiger ist es also, allen Entscheider:innen in einer Organisation die jeweils richtigen Informationen für das Treffen von guten Entscheidungen zeitnah bereitzustellen.

**Was ist der Wert einer Information?**
Der Wert einer Information liegt nicht allein darin, sie zu besitzen, sondern diese im täglichen Geschäftsbetrieb gewinnbringend zu nutzen. Je häufiger eine Information als Basis einer Entscheidung dient, desto wertvoller ist sie. Hierbei kommt es insbesondere darauf an, dass der Wert mit jeder einzelnen Entscheidung zunimmt und noch einmal gesteigert wird, wenn diese Information über der eigenen Verantwortungsbereich hinaus als Grundlage für Abstimmungen dient.

**Wie die CAS AG mit Data Analytics Unternehmen hilft, den Wert von Information durch bessere Entscheidungen zu heben.**
In den Kundenprojekten der CAS AG werden zunächst die Informationsbedarfe im Unternehmen und Systemarchitekturen identifiziert/analysiert. Entscheidungsprozesse werden aufgenommen und bewertet. Erkannte Handlungsbedarfe werden gemeinsam priorisiert und münden in einer Anforderungsmatrix für eine passende Data Analytics Plattform. Hierbei spielt das sogenannte Data Fabric Architekturkonzept eine zunehmende Rolle, das darauf abzielt, Daten aus verschiedenen Quellen, Systemen und Formaten nahtlos miteinander zu verbinden, bereitzustellen und zu steuern – unabhängig davon, wo sie sich befinden (On-Premise, Cloud, Hybrid). Statt Daten zu zentralisieren, wie es klassische Data-Warehouse-Modelle oft tun, verbindet Data Fabric verteilte Datenquellen intelligent miteinander – durch Metadaten, Automatisierung und semantische Integration. Die jahrzehntelange Erfahrung der CAS AG in System- und Datenintegrationsprojekten ist hierbei der entscheidende Faktor.

**Ralf Verlage | Bereichsleiter Data Analytics**
**www.c-a-s.de/data-analytics**

CAS AG

## Genius Tip

»**Daten** sind überall massenweise vorhanden, aber praktisch **schwer nutzbar**. Organisationen, die hier **strategisch investieren**, verschaffen sich einen **echten Vorsprung**.«

# #LetsSpeedUpEurope

## Ist Europa bei der Digitalen Souveränität am Draht und Drücker?

Bild: Soliman Cifuentes/Unsplash

**In seinem Buch »Digitale Souveränität für Europa« (Haufe Freiburg 2023), das viele Beiträge prominenter Politiker und Wissenschaftler vereint, setzt Herausgeber Markus Ferber auf eine dringend notwendige digitale Neuorientierung, sprich »Grundlage dafür, dass wir in Europa in Politik, Wirtschaft und Gesellschaft auch im digitalen Raum selbstbestimmt handeln und entscheiden können«.**

**Text** Rüdiger Schmidt-Sodingen

Wo viele »etablierte Plattformen mittlerweile als De-facto-Regulierer fungieren«, so analysiert es der ehemalige Bundesregierungssprecher und Intendant des Bayerischen Rundfunks Ulrich Wilhelm, müsse Europa endlich »in die technologische Tiefe gehen und eine eigene digitale Infrastruktur entwickeln«. Das sei zwar »risikoreich und komplex, aber auch mit der enormen Chance für Europa verbunden, Abhängigkeiten zu vermeiden und auch im digitalen Raum eine positive gestaltende Rolle einnehmen zu können«.

Die eigentliche Herausforderung, so Wilhelm, liege dabei im Ausgleich ökonomischer Interessen und gesellschaftlicher Zielvorstellungen. »Eine solche technische Infrastruktur sollte daher als Teil der öffentlichen Daseinsvorsorge begriffen werden, um der Quasi-Monopolstellung der großen Anbieter eine effektive Alternative entgegenzusetzen.« Randolf Carr und Wolfgang Ischinger, beide bis 2022 bei der Münchner Sicherheitskonferenz tätig, betonen, dass eine echte europäische Lösung nur mithilfe der USA möglich sei: »Europa muss zunächst sein digitales Haus in Ordnung bringen. Und zweitens müssen Europa und die USA das transatlantische Vertrauen im digitalen Bereich stärken.«

**Digitale Souveränität meint Kooperation, nicht Isolation**

Prof. Dr. Utz Schliesky, Direktor des Schleswig-Holsteinischen Landtages und Vorstand des Lorenz-von-Stein-Instituts an der Kieler Christian-Albrechts-Universität gibt zu bedenken, dass digitale Räume bislang von privaten Konzernen errichtet und gesteuert werden, die auch als »Kontrolleure des Zugangs und zulässiger Aktivitäten« auftreten. Dementsprechend bestehe »zunächst einmal keine für die Souveränität erforderliche Beherrschungsmöglichkeit dieser Räume für den Staat«. Dies werfe »die Frage nach der Inhaberschaft digitaler Souveränität auf«. »In dem Begriff der digitalen Souveränität“, so Schliesky weiter, »spiegelt sich nichts Geringeres als der Kampf des demokratischen Verfassungsstaates und der in ihm zusammengeschlossenen Bürger um die eigene politische Selbstbestimmung in digitalen Räumen und die Beherrschung dieser Räume zur Gewährleistung von Sicherheit.« Wer Volkssouveränität ernst nehme, müsse den »Ableitungs-, Zurechnungs- und Verantwortungszusammenhang zwischen Volk und Staatsgewalt in digitalen Räumen« neu konzipieren und herstellen.

Neben Plädoyers für mehr Zusammenarbeit und eine aktive Plattformregulierung kommt in dem Buch auch eine Neu- oder Reorganisation der Arbeit zur Sprache. »Die Mitarbeiter selbst sind gefordert, auf die Dynamik zu reagieren, schnell Entscheidungen zu treffen und diese selbstorganisiert umzusetzen«, so Clemens Drilling und Prof. Dr. Helmut Klausing, bevor Claudia Plattner, seit 2023 Präsidentin des Bundesamts für Sicherheit in der Informationstechnik, die unlängst eine unabhängige Cloud-Lösung mit Google einfädelte, zu mehr Optimismus aufruft. »Ja, wir liegen zurück. Aber ein Kampf geht über zwölf Runden und wir sind erst in Runde vier. Hier ist noch gar nichts entschieden. (…) Digitale Souveränität in Europa ist erreichbar. Wachsen wir über uns hinaus und schaffen wir Resultate – und das schnell. Nicht übermorgen, nicht morgen und nicht einmal heute Nachmittag. Jetzt. #LetsSpeedUpEurope!«

---

**Genius Partner • CSE – Center of Safety Excellence GmbH** *think about: Cyber Security*

# Strategien für Mittelständler: Schützen Sie Ihre Anlagen vor Cybergefahren!

**Cybergefahren werden vom Mittelstand oft unterschätzt. Cyberangriffe auf mittelständische Anlagen nehmen zu. In einem Experteninterview spricht Professor Dr. Jürgen Schmidt, Executive Director des CSE Center of Safety Excellence gGmbH in Pfinztal, über den Schutz vor Cyberangriffen auf mittelständische Unternehmen.**

**Herr Schmidt, Sie leiten das CSE Center of Safety Excellence, haben über 25 Jahre bei BASF gearbeitet und lehren an den Universitäten in Karlsruhe und Kaiserslautern. Seit Jahren setzen Sie sich für den Schutz von Anlagen vor Cyberangriffen ein, nun auch für kleine und mittlere Unternehmen (KMU). Sind KMU in Deutschland tatsächlich von Hackern bedroht?**
Ja, insbesondere bei KMUs mit Produktionsanlagen sind die Angriffe intensiver geworden. Im Mai haben Hacker zwei Biogasanlagen in Norddeutschland angegriffen und erhebliche Schäden verursacht. Viele Betreiber können sich kaum vorstellen, dass sie Ziel solcher Angriffe sind.

*Professor Dr. Jürgen Schmidt, Executive Director, CSE Center of Safety Excellence gGmbH*

**Wie unterstützt das CSE Center of Safety Excellence diese Unternehmen?**
Das CSE entwickelt die Software EvaSecur, die ab 2026 kostenfrei angeboten und vom Bundesministerium für Wirtschaft und Energie gefördert wird. EvaSecur deckt die regulatorischen Vorgaben bedarfsgerecht ab und erhöht das Sicherheitsniveau, die Produktivität der Anlagen sowie das Wissen im Bereich Cybersecurity. Dies gilt für Anlagen wie Biogas, Kraftwerke, Windenergie, Verpackung und Produktion, die von Zehntausenden Unternehmen in Deutschland betrieben werden. Details siehe *www.evasecur.de*.

**Kann EvaSecur ohne IT-Fachkenntnisse angewendet werden?**
Ja! EvaSecur bietet eine unkomplizierte 80%-Lösung – den Basis-Schutz. Die Anwender sollen die Hemmschwelle überwinden, im fachfremden Bereich Cybersecurity aktiv zu werden.

**Berücksichtigt EvaSecur auch die gesetzlichen Anforderungen?**
Ja, EvaSecur wird aus fünf Modulen bestehen, die sich an den gesetzlichen Vorgaben und den Empfehlungen des Basis-Grundschutzes orientieren: (1) Gefahrenbeurteilung einer Anlage, (2) Asset-Liste mit den relevanten Assets des Produktionsnetzwerks, (3) Schwachstellenanalyse, (4) Liste mit Gegenmaßnahmen und (5) Awareness-Training zum Thema Cybersecurity. Mit EvaSecur wird die Beurteilung von Maßnahmen abhängig von den Risiken in einer Anlage durchgeführt. CSE entwickelt EvaSecur in enger Zusammenarbeit mit Betreibern.

CSE CENTER OF SAFETY EXCELLENCE

CYBERsicher EvaSecur IT-/OT-Sicherheit für den Mittelstand

# Innovationsmotor Souveräne Cloud

**Im Interview mit Nikolaus Hagl, Head of Sovereign Cloud Germany bei SAP und Geschäftsführer der Delos Cloud GmbH, sprechen wir über digitale Souveränität, die Rolle der Cloud, und warum beides entscheidend für Europas digitale Zukunft ist.**

**Herr Hagl, warum ist digitale Souveränität mehr als ein Buzzword?**
Digitale Souveränität bedeutet, dass Institutionen ihre Daten sicher verwahren und nutzen können, ohne unerwünschten Zugriff von außen. Damit ist sie einer der wichtigsten Bausteine internationaler Sicherheit und die Grundlage für Handlungsfähigkeit und Resilienz.

Derzeit nehmen geopolitische Spannungen zu und technologische Entwicklungen beschleunigen sich. Während Länder wie die USA oder China gezielt in eigene Technologien investieren, ist Europa oft zurückhaltender – und riskiert dadurch wachsende Abhängigkeit von externen Anbietern. Digitale Souveränität ist weit mehr als nur ein Buzzword: Sie ermöglicht es uns, selbstbestimmt über Daten, Prozesse und unsere digitale Infrastruktur entscheiden zu können.

**Welche Rolle spielt die Cloud dabei?**
Cloud-Lösungen sind das Fundament nahezu aller digitaler Prozesse, egal ob alltägliche Aufgaben oder komplexe Innovationsprojekte. Gerade deshalb sind sie so zentral für die Frage der digitalen Souveränität: Wer Kontrolle über die Cloud-Infrastruktur hat, bestimmt auch, wie Daten verarbeitet, gespeichert und vor allem geschützt werden.

Für uns in Deutschland und Europa bedeutet das konkret: Wenn wir unsere sensiblen Daten und kritischen Anwendungen in einer souveränen Cloud-Umgebungen betreiben, die unseren Vorgaben und Gesetzen unterliegen, stärken wir Unabhängigkeit, Vertrauen und Innovation. Ohne eine sichere und leistungsfähige Cloud-Infrastruktur bleibt digitale Souveränität ein leeres Versprechen.

**Was macht eine souveräne Cloud aus?**
Eine souveräne Cloud ermöglicht es Organisationen, Daten, Anwendungen und Prozesse vollständig unter eigener Kontrolle und nach den jeweiligen nationalen Standards betreiben zu können. Für uns ist eine Cloud dann souverän, wenn sie technisch, betrieblich, juristisch souverän ist und volle Datensouveränität gewährleistet. Diese Souveränitätsstandards erfüllen nur wenige Angebote am Markt. Gerade für die Verwaltung und regulierte Branchen ist das aber essenziell. Sie müssen nicht nur höchste Anforderungen an IT-Sicherheit und Datenschutz erfüllen, sondern auch flexibel und innovationsfähig bleiben. Mit einer souveränen Cloud stärken wir unsere digitale Unabhängigkeit, schützen kritische Infrastrukturen und schaffen das nötige Vertrauen für die Digitalisierung von Staat und Wirtschaft.

**Innovationsfähigkeit ist ein interessantes Stichwort. Wie passen denn Innovation und digitale Souveränität zusammen?**
Neue Technologien wie Künstliche Intelligenz oder Big Data benötigen große Mengen sensibler Daten und leistungsfähige Infrastrukturen. Ohne eine souveräne Cloud, die höchste Sicherheits- und Datenschutzstandards erfüllt wie unser Angebot, könnten viele dieser Innovationen gar nicht realisiert werden – oder würden von vornherein auf Misstrauen stoßen. Souveräne Cloud-Umgebungen spielen hier eine Schlüsselrolle als einer der wichtigsten Enabler für digitale Innovationen.

**Souveräne Clouds unterliegen strikten Anforderungen. Steht das Innovationen nicht im Weg?**
In Deutschland ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) federführend für die Vorgaben, die an souveräne Clouds gestellt werden. Die Vorgaben für IT-Sicherheit, Datenschutz und Geheimschutz sind enorm hoch, aber wichtig und richtig, denn genau diese Standards sorgen dafür, dass sensible Daten wirklich geschützt sind. Gleichzeitig dürfen wir auch nicht die Wirtschaftlichkeit aus den Augen verlieren. Deshalb ist ein gegenseitiges Verständnis von Regulatorik und Anbietern wichtig. Als SAP haben wir seit Februar 2024 einen Kooperationsvertrag mit dem BSI, um diesen wichtigen Austausch voranzutreiben.

***Nikolaus Hagl ist Head of Sovereign Cloud Germany bei SAP und Geschäftsführer und CEO der Delos Cloud GmbH.***

Souveräne Clouds bieten einen sicheren Rahmen, in dem innovative Technologien entwickelt, getestet und eingesetzt werden können, ohne dass Angst vor Kontrollverlust oder unklaren Rechtslagen bestehen muss. In Kombination mit Hyperscaler-Technologie und der damit verbundenen Flexibilität und Skalierbarkeit ermöglichen sie Organisationen, Innovationen schnell und effizient umzusetzen und bei Erfolg unkompliziert auszurollen. Das stärkt die Handlungs- und Wettbewerbsfähigkeit.

**Die Delos Cloud ist eine von vielen souveränen Clouds. In Europa und auch in Deutschland sind Sie also nicht der einzige Anbieter – wie unterscheidet sich die Delos Cloud von anderen?**
Die Delos Cloud wurde speziell für die Anforderungen der deutschen Verwaltung entwickelt. Sie ermöglicht es den öffentlichen Auftraggebern in Deutschland, sicher und reguliert Cloud-Dienstleistungen zu nutzen und erfüllt höchste Standards für Datenschutz, Geheimschutz und IT-Sicherheit.

Das entscheidende Unterscheidungsmerkmal ist die souveräne Nutzung von Hyperscaler-Technologie. Wir kombinieren die technologische Stärke des globalen Hyperscalers Microsoft mit vollständiger Kontrolle über Technik, Daten und Betrieb. Das bedeutet konkret: Die Speicherung und Verarbeitung der Daten erfolgt ausschließlich in unseren eigenen Rechenzentren in Deutschland durch sicherheitsüberprüftes deutsches Personal. Alle Daten verbleiben zu 100% in Deutschland. Wir sind eine deutsche Firma mit einem deutschen Geschäftsführer, die der deutschen Gerichtsbarkeit unterliegt. Es bestehen keine Herausgabepflichten gegenüber Drittstaaten. Microsoft als Technologie-Lieferant hat keinen Zugriff auf die Plattform. Im Vergleich zum Wettbewerb geht die Delos Cloud damit weit über reine Datenresidenz hinaus.

Zudem ist unsere Cloud-Plattform Anbieterneutral und Technologieoffen. Damit ist die Cloud-Plattform offen zur Nutzung von Fachanwendungen jeglicher Art, sowohl Open Source als auch kommerzielle Lösungen oder Eigenentwicklungen unserer Kunden. So bieten wir unseren Kunden die Wahlfreiheit und Flexibilität, die für sie passende Lösung zu nutzen.

**Mit der Delos Cloud möchten Sie eine sichere Nutzung von Microsoft-Anwendungen ermöglichen. Wie kontrollieren Sie denn, dass Microsoft keinen Zugriff hat?**
Als deutsche Eigentümerin, Betreiberin und Lizenzgeberin der Cloud-Plattform stellt die Delos Cloud GmbH sicher, dass Microsoft als Technologielieferant keinen Zugriff erhält. Das bedeutet, Microsoft hat weder Zugriff auf die Infrastruktur noch auf Kundendaten. Die Updates stellt Microsoft zwar zur Verfügung, allerdings erfolgt die Prüfung durch Delos Cloud und zusätzlich durch das Bundesamt für Informationstechnik. Das BSI hat jederzeit die Möglichkeit, die Updates im Detail zu kontrollieren. Im unwahrscheinlichen Fall, dass Unterstützung durch Microsoft benötigt wird, gibt es einen vom BSI geprüften und festgelegten Prozess, in dem Microsoft lediglich beratend hinzugezogen wird. Das bedeutet also, dass Delos Cloud kein »Feigenblatt« für Microsoft ist, wie hin und wieder fälschlicherweise behauptet wird.

**Herr Hagl, Open-Source-Software wird oft als Schlüssel zur digitalen Souveränität genannt. Wie bewerten Sie ihre Rolle in einer souveränen Cloud-Architektur?**
Open-Source-Lösungen spielen eine wichtige Rolle für digitale Souveränität. Gleichzeitig ist es wichtig, sie in einen sicheren und verlässlichen Rahmen einzubetten. Souveränität bedeutet nicht nur Offenheit, sondern auch Kontrolle, und die Fähigkeit, technische und regulatorische Anforderungen dauerhaft zu erfüllen. Gerade bei kritischen Infrastrukturen braucht es verlässliche Governance und hohe Sicherheitsstandards.

Wir verstehen Open Source nicht als alleinige Lösung, sondern als strategische Komponente innerhalb einer souveränen Cloud-Architektur. Auch die Delos Cloud ist offen für Open-Source-Anwendungen. Entscheidend ist die Fähigkeit, offene Technologien mit robusten Betriebsmodellen und klaren Zuständigkeiten zu kombinieren. So entsteht ein System, das Vertrauen schafft, innovationsfähig bleibt und die Handlungsfähigkeit deutscher und europäischer Institutionen dauerhaft absichert.

**In drei Worten: Was braucht Europa, um digital souverän und innovativ zu bleiben?**
Meine drei Ms: Motivation, Mut und Machen!

DELOS CLOUD

# Warum Datensouveränität allein nicht ausreicht

**Die schwierige geopolitische Lage macht einen souveränen Umgang mit Daten unerlässlich. Ingo Kraupa, Mitbegründer und CEO der noris network AG, über neue und alte Clouds, mehr Datensouveränität und Sicherheit im Rahmen neuer Krisen und gesetzlicher Anforderungen.**

**Herr Kraupa, wie tangiert die geopolitische Lage die Datenverarbeitung und Datensicherheit hiesiger Unternehmen?**
In den letzten Jahren haben fast alle größeren Unternehmen einen Teil ihrer Anwendungen in die Cloud verlagert, sei es strategisch motiviert oder auf Druck der Anbieter, die sich dadurch Vereinfachungen in der Serviceerbringung und Wettbewerbsvorteile versprechen. Der Erfolg gibt den Unternehmen recht. Die Qualität der Services ist in der Regel gut und für den internen IT-Betrieb ist es eine starke Vereinfachung.

Insbesondere im öffentlichen sowie im regulierten Umfeld ist die Euphorie in letzter Zeit aber deutlich gesunken. Teils sind die avisierten Kosteneinsparungen nicht wie erwartet eingetreten, teils gab es bei der Migration große Herausforderungen. Teilweise waren Services von Sicherheitsvorfällen betroffen. Die Frage, wie geschützt die eigenen Daten in der Cloud wirklich sind und ob im Zweifel eine Rückführung der Anwendungen in die eigene IT bzw. zu einem dritten Provider einfach möglich ist, hat viele Unternehmen schon länger beschäftigt. Mit Donald Trumps zweiter Amtszeit hat sich die gefühlte Unsicherheit verstärkt, was zu einer gestiegenen Nachfrage von souveränen Clouds geführt hat.

**Das heißt: Für eine umfassende Kontrolle und ein sicheres Arbeiten sollten Unternehmer auf Cloud-Dienste von deutschen Anbietern setzen?**
Der Unternehmer sollte sich grundsätzlich Gedanken darüber machen, wem er seine Daten und Prozesse anvertraut. Ich glaube, dass die meisten deutschen Unternehmen das auch durchaus tun und die Risiken für sich einschätzen. Es hat aber den Anschein, dass die Risikobewertung sich in letzter Zeit etwas verschiebt zugunsten von souveränen Angeboten europäischer Provider. Sie unterliegen dem EU-Rechtsrahmen, insbesondere der GDPR, und betreiben ihre Infrastrukturen oft ausschließlich in Europa oder innerhalb Deutschlands.

Leider ist es für die Unternehmen gar nicht so einfach, ihre Cloud-Anwendungen zurück in das eigene Rechenzentrum oder zu einem deutschen Anbieter zu transferieren. Denn die Anbieter machen es einem dabei nicht unbedingt leicht.

**Welche Auswirkungen hat der Data Act auf die Cloud-Strategien von Unternehmen?**
Der europäische Data Act ist, vereinfacht gesprochen, die GDPR für alle nicht-personenbezogenen Daten. Er regelt eine Reihe von auf den ersten Blick sehr sinnvollen Dingen. Beispielsweise werden Nutzer von vernetzten Geräten in die Lage versetzt, Zugang zu von ihnen erzeugten Daten zu erhalten.

Er regelt aber auch den sogenannten Cloud Switch – also den Wechsel von einem Cloud-Anbieter zu einem anderen – sehr konkret, um die Abhängigkeit von einzelnen Anbietern zu reduzieren. Europäische Cloud-Nutzer haben ein Recht auf einen Anbieterwechsel, wobei Wechselgebühren schrittweise bis auf 0 Euro abgeschafft werden. Insbesondere wird auch die Möglichkeit der Rückführung in die eigene »On-Premise« Infrastruktur unterstützt. Wenn das Gesetz hier hält, was es verspricht, ist das ein extremer Fortschritt hin zu einer echten Souveränität. Was viele noch nicht wissen: Der Cloud Switch gemäß dem Data Act wird ab dem 12. September 2025 verbindlich wirksam.

**Wie unterstützen Sie mit noris network die neuen gesetzlichen Anforderungen?**
Wir beraten unsere Kunden dabei, die beste Entscheidung für den Ort ihrer Anwendungen und Daten zu treffen. Viele unserer Kunden kennen die Risiken, die Gesetzeslage und technischen Notwendigkeiten sehr genau und haben daraus eine klare Strategie abgeleitet. Als zertifizierter deutscher IT-Dienstleister mit mehreren eigenen hochsicheren Rechenzentren reicht unser Angebot von Colocation (»Wir liefern Fläche, Strom und Kühlung«) über die Private Cloud bis zum Full-IT-Outsourcing (»Wir betreiben Kundenanwendungen«). Bei besonders hohen Sicherheitsanforderungen liefert noris auch ganze Rechenzentrumsmodule, meistens KI-Module, weil die bestehenden Rechenzentren die Last nicht abkönnen. Um den sich ändernden gesetzlichen und regulatorischen sowie den Sicherheitsanforderungen Rechnung zu tragen, leisten wir uns einen eigenen Bereich, der sich nur mit diesen Themen beschäftigt.

**Wie können Unternehmen denn ohne Bedenken zwischen Cloud-Anbietern wechseln, um eine kontinuierliche Kontrolle über ihre Daten und deren Sicherheit zu bekommen?**
Theoretisch ist das ab dem 12. September ganz einfach. Die Anbieter sind verpflichtet, beim Wechsel kostenfrei zu unterstützen. Wie es in der Praxis ausschaut, wird sich zeigen. Denn natürlich sind die Angebote in der Cloud alles andere als einheitlich, transparent und durchstandardisiert. Hier bildet der Sovereign Cloud Stack der noris (nSC) eine rühmliche Ausnahme, da er mit anderen Herstellern voll kompatibel ist – allerdings nur im Standardumfang. Verlässt man diesen, steht man sofort wieder vor ähnlichen Herausforderungen. Gleichwohl ist der Cloud Switch ein Schritt in die richtige Richtung für mehr Wettbewerbsfähigkeit und weniger Vendor Lock-In. Denn nicht nur die Souveränität der Daten ist entscheidend, sondern auch die Souveränität, die Funktionalität bei einem Anbieterwechsel ausfallfrei wiederherzustellen. Ganz einfach ist das nicht.

**Es geht also bei der »Cloud 2.0« nicht mehr nur um Speicherplatz, sondern um Sicherheit und Compliance?**
So ist zumindest der Gedanke. Es geht um noch mehr Kontrolle für den Cloud-Anwender, um die Nutzung von Standards und offenen Schnittstellen, um die Hybridfähigkeit und Vernetzungsfähigkeit der Clouds, um eine sichere nutzergesteuerte Verschlüsselung von Daten in der Cloud, die Unterstützung der kostenlosen und vollständigen Rückführung von Daten und Applikationen aus der Cloud und das alles unter Verwendung KI-gestützter Dienste. Hier kann eine moderne Cloud aber auch massiv unterstützen, beispielsweise durch automatische Compliance- und Security-Checks.

**Wie sieht die Zukunft für deutsche Cloud-Anbieter aus, die auf Datensouveränität und höchste Sicherheitsstandards setzen?**
Gut. Wir verzeichnen in diesem Bereich gerade eine verstärkte Nachfrage – aber wir bewegen uns nun auch eher im Bankenumfeld und im öffentlichen Sektor. Die jüngsten Urteile bei Datenschutzverstößen haben gezeigt, dass Sicherheitsvorfälle, neben dem finanziellen und dem Imageschaden, auch empfindlich sanktioniert werden können. »Sicherheit ist Dividende« war ein Werbeslogan meiner Kindheit. Ich würde ihn ergänzen mit »Souveränität tut Not«.

**Welche Themen oder auch zusätzlichen Compliance-Regeln werden Sie mit noris network in den nächsten Jahren noch beschäftigen?**
Ich beschäftige mich tatsächlich lieber damit, wie wir unsere eigene Cloud so gut machen, dass wir mit den etablierten Clouds immer besser mithalten können. Aber um die Frage zu beantworten: KRITIS und DORA sind für uns aktuelle Themen sowie dank des EnEfG der Anschluss unserer Abwärme an das Fernwärmenetz. Wir gehen davon aus, dass die KI-Nutzung uns in den nächsten Jahren eine Reihe weiterer Regularien bringen wird – und leisten hier bereits die Vorarbeit mit hochsicheren, mandantenfähigen KI-Infrastrukturen.

noris network

» Nicht nur die **Souveränität der Daten** ist entscheidend, sondern auch die Souveränität, die **Funktionalität** bei einem **Anbieterwechsel** ausfallfrei **wiederherzustellen.** «

*Ingo Kraupa, Mitbegründer & CEO noris network AG*

## Genius Tip

**Cloud Switch gilt ab 12. September**

Ab dem **12. September** dürfen Cloud-Anbieter schrittweise bei einem Wechsel **keine zusätzlichen Kosten** mehr in Rechnung stellen. **Haben Sie eine Rechnung erhalten? Fordern Sie ihr Geld zurück!**

# »Unser Ziel ist nicht nur Schutz, sondern auch Selbstbestimmung«

**Wie können Unternehmen mehr Transparenz erreichen und gleichzeitig die Anforderungen der DSGVO erfüllen? Holger Suhl, Country Manager DACH der ESET Deutschland GmbH, über europäische Sicherheitslösungen, digitale Souveränität und eine unverhoffte Win-win-Situation.**

**Herr Suhl, was bedeutet »Made in Europe« im Kontext von IT-Sicherheit und digitaler Souveränität von Unternehmen?**
Für mich heißt »Made in Europe« ganz klar: Exzellente Technik nutzen, Kontrolle behalten und Vertrauen in den Datenschutz haben. Wir erleben immer wieder, dass Unternehmen mit Produkten arbeiten, bei denen sie gar nicht genau wissen, wo ihre Daten am Ende landen oder wer darauf zugreifen darf. Das kann schnell problematisch werden, vor allem wenn Anbieter aus Drittstaaten ins Spiel kommen. Wenn ein Produkt komplett in Europa entwickelt, betrieben und gewartet wird – und ausschließlich europäischen Gesetzen unterliegt – dann schafft das Vertrauen. Und genau dieses Vertrauen ist heute ein echter Standortvorteil.

*Holger Suhl, Country Manager DACH, ESET Deutschland GmbH*

**Wie können europäische Lösungen helfen, die Anforderungen der DSGVO besser zu erfüllen?**
Indem sie Datenschutz nicht nur als Hürde sehen, sondern als Teil der Lösung. In Europa ist der Schutz persönlicher Daten gesetzlich verankert. Das spiegelt sich auch in der Art wider, wie wir Software entwickeln. Wir bei ESET achten zum Beispiel darauf, dass unsere Systeme möglichst wenig personenbezogene Daten verarbeiten. Beispielsweise analysiert unsere KI-gestützte Lösung »AI Advisor« Sicherheitsvorfälle lokal und nachvollziehbar. Es gibt keine unnötige Datenübertragung oder intransparente Blackbox-Entscheidungen. Das ist kein Zufall, sondern Teil unserer europäischen Haltung.

**Welche Herausforderungen ergeben sich für die Sicherheit und das tägliche Arbeiten im globalen Gefüge?**
Die größte Herausforderung ist aus meiner Sicht die fehlende Transparenz. Viele Unternehmen nutzen Sicherheitslösungen aus den USA oder Asien und wissen nicht, ob es etwa gesetzliche Verpflichtungen zur Datenweitergabe an Behörden gibt. Hinzu kommt die zunehmende Komplexität von Cyberangriffen. Angriffe sind heute oft staatlich gelenkt oder strategisch motiviert. Wer hier geschützt sein will, braucht nicht nur gute Technik, sondern auch rechtliche Klarheit. Und die bekommen Unternehmen nur, wenn sie auf Lösungen setzen, die mit den europäischen Rahmenbedingungen kompatibel sind.

**Welche Rolle spielt ESET bei der Förderung von Datenschutz und digitaler Souveränität in Europa?**
Wir verstehen uns als Teil eines europäischen Sicherheitsökosystems. Seit über 30 Jahren entwickeln wir unsere Produkte in der EU, mit eigenen Forschungszentren und ohne Abhängigkeit von globalen Cloudanbietern. Unsere Infrastruktur steht in Europa: Unter anderem betreiben wir ein eigenes Rechenzentrum in Deutschland. Wir arbeiten eng mit Behörden, CERTs und der Wissenschaft zusammen, analysieren gezielte Angriffe auf europäische Institutionen und versorgen unsere Kunden mit relevanter Threat Intelligence. Unser Ziel ist nicht nur Schutz, sondern auch Selbstbestimmung: Wer weiß, was in seinem Netzwerk passiert, kann selbst entscheiden kann, wie er reagiert. Er agiert also nicht fremdbestimmt. Und genau das ist für uns digitale Souveränität.

ESET
Digital Security
Progress. Protected.

**www.eset.de**

## Genius Tip

»**Sicherheitslösungen** schützen nur dann wirklich, wenn auch ihr **Ursprung vertrauenswürdig** ist. Wer auf **europäische Anbieter** setzt, bekommt nicht nur **modernste Technik** – sondern auch **Transparenz, Datenschutz** und **Kontrolle** zurück.«

# »KI verändert alles – und das ist gut so«

**Uwe Bergmann, CEO des Digitalisierungsspezialisten COSMO CONSULT, erklärt, wie Cloud- und KI-Technologien Unternehmen auf den Kopf stellen – und warum man davor keine Angst haben muss.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Bergmann, Cloud und KI entwickeln sich rasant. Viele Unternehmen fragen sich: Werden wir gerade von allen Seiten überholt?**
In manchen Bereichen – ja. Die Geschwindigkeit, mit der KI sich weiterentwickelt, ist tatsächlich atemberaubend. Und es wird noch schneller. Andererseits war der Zugang zu leistungsfähiger Technologie noch nie so einfach und breit verfügbar. Entscheidend ist jetzt, sich zu fragen: Wo stehen wir – und wie kommen wir ins Handeln?

**Aber reicht Handeln? KI verändert ganze Geschäftsmodelle – stehen wir nicht längst mitten in einer Revolution?**
Das tun wir auch. KI ist nicht einfach eine neue Software-Schicht – sie verändert die Art, wie wir arbeiten, entscheiden und planen. Sie automatisiert nicht nur Teilaufgaben, sondern ganze Wertschöpfungsketten. Aber das ist kein Kontrollverlust, sondern ein Sprungbrett für Neues. Die Frage ist nicht: »Was nimmt mir KI weg?« Sondern: »Was kann sie mir abnehmen, damit ich mich auf das Wesentliche konzentrieren kann?« KI verändert alles – und das ist gut so.

*Uwe Bergmann*
*CEO*
*COSMO CONSULT*

**Was heißt das konkret? Können Sie ein Beispiel nennen?**
Ein Beispiel aus dem Vertrieb: Beim Kundentermin ist eine KI live dabei. Sie erkennt Neugier, Einwände oder neue Chancen – und gleicht die Kundenwünsche in Echtzeit mit dem eigenen Lösungsportfolio ab. Gleichzeitig greift sie auf Lastenhefte, Notizen oder Kundendaten zu. Mit einem Klick gibt sie dem Vertriebsteam die perfekten Verkaufsargumente an die Hand. Wer das einmal in Aktion erlebt hat, weiß: In dieser Technologie steckt enormes Potenzial.

**Klingt nach High-End – ist das auch für mittelständische Unternehmen realistisch?**
Auf jeden Fall. Genau das ist die Stärke der Cloud: Sie macht diese leistungsstarken KI-Anwendungen überhaupt erst nutzbar – unabhängig von Unternehmensgröße oder Standort. Viele unserer Kunden sind mittelständische Unternehmen in anspruchsvollen Märkten. Für sie zählt, dass Prozesse durchgängig funktionieren – vom Vertrieb bis zum Service, vom Einkauf bis zur Produktion. Denn entscheidend ist: Alles greift ineinander – vom ERP-System über CRM und Business Analytics bis zur KI.

**Aber Technologie allein reicht nicht, oder? Viele Transformationen scheitern nicht am Tool, sondern am Menschen.**
Genau. Digitalisierung ist immer auch ein Kulturprojekt. Man kann nicht einfach Software einführen und hoffen, dass sich der Rest von selbst ergibt. Es braucht Kommunikation, Schulung – und Führungskräfte mit echtem Verständnis für Veränderung. In erfolgreichen Projekten sehen wir immer: Der Wandel wird nicht gemacht, er wird gelebt – von der Werkbank bis zum Vorstand.

**Und was raten Sie Unternehmen, die noch ganz am Anfang stehen?**
Zuerst: Sich ehrlich machen. Viele wissen gar nicht, wo ihre Daten liegen oder wie ihre Prozesse wirklich laufen. Eine klare Analyse ist der erste Schritt. Dann folgt der Fahrplan – pragmatisch, aber ambitioniert. Und: Man sollte sich Partner ins Boot holen. Niemand muss das allein stemmen.

**Sind Unternehmen in Deutschland bereit für diesen Wandel?**
Viele ja – aber viele stochern noch im Nebel. Wir beobachten: Skandinavien oder die Niederlande sind oft strategischer unterwegs. In Deutschland hält man sich gerne an bewährten Lösungen fest. Dabei ist klar: Ohne moderne Infrastruktur kann keine KI ihre Stärke ausspielen. Und ohne klare Strategie helfen auch die besten Tools nichts. Künstliche Intelligenz ist gekommen, um zu bleiben. Jetzt liegt es an uns, sie intelligent zu nutzen.

## Genius Tip

»KI bietet große Chancen – doch **wo anfangen?** Der **COSMO AI Pathfinder** zeigt, wie Sie KI im Unternehmen **sinnvoll nutzen** können – **kostenlos** und mit nur **wenigen Klicks**. Einfach die eigene URL eingeben, praxisnahe Anwendungsideen erhalten – und den **ersten Schritt zur KI-Strategie** machen.«

**QR-Code scannen und den COSMO AI Pathfinder kostenlos ausprobieren:**

COSMOCONSULT



# »Compliance als Chance – und Wettbewerbsvorteil«

**Seit 2018 stellt sich das Team der Plattform Athereon GRC den Herausforderungen bei Governance, Risk und Compliance. Marius Kleber, Gründungsmitglied und Manager Sales & Marketing, über die zunehmende Regulierungsdichte in ohnehin stürmischen Zeiten.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Kleber, wie können und sollten sich Unternehmen in diesen Tagen den vielen Regulierungen stellen?**
Die zunehmende Regulatorik führt aktuell zu viel Frust und Unsicherheit mangels passender Strategien. Wo früher vor allem kritische Infrastrukturen betroffen waren, treffen NIS2 oder CSRD jetzt auch Mittelständler und KMU. Ein strukturiertes Vorgehen ist nötig, aber das lässt sich angesichts der Komplexität der Anforderungen und internen Prozesse kaum mit Excel-Listen lösen. Und egal, ob Sie als großes Unternehmen bereits ein Team für Compliance-Lösungen installiert haben oder sich als Mittelständler Unterstützung von außen holen – das Ziel muss sein, alle Anforderungen übersichtlich und automatisiert erfüllen zu können.

**Welche regulatorischen Neuerungen erfordern aktuell den größten Handlungsdruck – und woran scheitert die Umsetzung in der Praxis?**
Akut den größten Handlungsdruck bei Informationssicherheitsmanagementsystemen (ISMS) erfordern die Richtlinien NIS2 und DORA. Das liegt sicher auch an der langsamen Gesetzfindung, die Unternehmen dazu ermuntert hat, die Themen auf die lange Bank zu schieben. Gleichzeitig nehmen aufgrund der unsicheren geopolitischen Lage Cyberangriffe zu. Sie müssen sich als Unternehmen also sehr umfangreich mit der Informationssicherheit beschäftigen – in IT- und Non-IT-Bereichen. Es fehlen aber das Know-how und die passenden Ansätze

**Sie sehen GRC als Steuerungsrahmen, der auch mittelfristig zu mehr Resilienz verhilft?**
Absolut. Unser Motto lautet deshalb: »Compliance als Chance«. Denn durch die Umsetzung der Anforderungen und die Operationalisierung eines echten ISMS beschäftigen sich Unternehmen gleichzeitig mit Cyberrisiken, ihrer IT-Landschaft und den Abhängigkeiten von ihren Prozessen sowie Zuliefererketten. Dadurch können sie Schwachstellen früher erkennen und Mechanismen für eine höhere Resilienz automatisch implementieren.

**Wie kann GRC gerade im Mittelstand vom Reputationsrisiko zum Wettbewerbsvorteil werden?**
Man macht GRC, weil man es machen muss. Aber der Wettbewerbsvorteil liegt klar auf der Hand. In immer mehr Branchen werden Aufträge oder Ausschreibungen nur an Unternehmen vergeben, die GRC-Zertifizierungen haben oder Nachweise erbringen können. Denken Sie nur an ISMS im Automotive-Sektor, ESG im Energie-Sektor etc. Das sind klare Wettbewerbsvorteile.

*Marius Kleber,*
*Gründungsmitglied,*
*Manager*
*Sales & Marketing,*
*Athereon GRC*

**Welche Lehren lassen sich aus Kundenprojekten ziehen – was funktioniert, was nicht?**
Was sicher funktioniert, ist, wenn unsere Software Athereon GRC nahtlos und ressourcenschonend in die bereits bestehende IT-Landschaft eines Unternehmens integriert werden kann und die Compliance-Werkzeuge effizient mit den jeweiligen Unternehmensdaten genutzt werden können. Auch die parallele Umsetzung regulatorischer Rahmenwerke innerhalb der Software funktioniert gut. Jedoch: Die Software leitet zwar durch die Anforderungen und Umsetzungen, nichtsdestotrotz ist ein Grundwissen sowie ein Auseinandersetzen mit GRC und den eigenen Strukturen unerlässlich, um die Compliance-Anforderungen erfüllen zu können.

Athereon GRC

**www.athereon.de**

## Genius Tip

»Von **NIS2** sind in Deutschland ca. **30.000** (EU-weit 160.000) **Unternehmen** betroffen. Haben Sie keine Angst vor komplexen GRC-Anforderungen. Die **hochspezialisierten Werkzeuge**, bspw. von Athereon GRC, helfen dabei, die **Anforderungen effizient umzusetzen**. Sehen Sie **Compliance als Chance** und profitieren Sie als Unternehmung von einer **gesamt-gesteigerten Resilienz** in unsicheren Zeiten!«

# Zukunft mit KI: Einfach machen!

**In der aktuell schwierigen wirtschaftlichen Lage sollten Unternehmen die massiven Vorteile durch den Einsatz von KI unbedingt nutzen, anstatt ängstlich und zurückhaltend zu reagieren. Im Interview erklärt Rainer Holler, CEO des deutschen Technologieanbieters VIER, wie der Einstieg gelingt und warum KI längst so zugänglich ist wie ein Stromanschluss.**

Rainer Holler ist CEO der VIER GmbH.

**Rainer Holler, viele Unternehmen in Deutschland, insbesondere im Mittelstand, tun sich sehr schwer mit dem Einsatz von KI…**
Ja, das ist leider richtig. Aktuelle Zahlen des Digitalverbands Bitkom zeigen, dass gerade ein Drittel der deutschen Unternehmen KI einsetzt. Demnach gelingt es nach eigener Einschätzung bislang nur 25 Prozent der deutschen Unternehmen, die Potenziale von KI gut zu nutzen. Der Rest lässt die Chancen einfach liegen. Das ist ziemlich dramatisch, denn es schadet nicht nur den Unternehmen selbst, sondern auch der deutschen Gesamtwirtschaft.

**Aber warum ist Künstliche Intelligenz so ein Problem oder wird als Problem empfunden?**
Meiner Meinung nach denken viele – zu viele – dass KI ein reines IT-Thema ist oder nur für Großkonzerne geeignet sei. Sie fürchten hohe Kosten, Kontrollverlust und finden KI insgesamt viel zu komplex. Und dann ist da noch der »EU AI Act«, auch das noch…. Viele beschäftigen sich also lieber erst gar nicht damit. Infolgedessen fehlt das Knowhow, was KI eigentlich macht, warum es funktioniert und was das kostet. Dabei lohnt sich der Einsatz von KI schon für sehr kleine Unternehmen und ist mit Sicherheit keine Raketentechnik, die man als normaler Mensch nicht verstehen kann.

**KI einzusetzen ist also auch für sehr kleine Unternehmen von Vorteil?**
Ja, denn der Hebel von KI liegt in der Skalierung. Egal, wie groß oder klein ein Unternehmen ist, alles kann viel effizienter werden. KI kann im Handumdrehen 30 Prozent der Routineaufgaben übernehmen. Der Einsatz von KI funktioniert dabei am besten nach der »Low Hanging Fruits-Strategie«. Das bedeutet: Ich delegiere die drei Dinge, die mich tagtäglich am meisten beschäftigen, an eine KI-Lösung. Das lohnt sich für die Fahrschul-Lehrerin, die ihre Terminvereinbarung mit KI automatisiert. Und auch für einen Dax-Konzern mit 20.000 Mitarbeitern, der einen Bot betreibt, um sämtliche Standard-Anfragen an die Personalabteilung zu beantworten und auf Wunsch auch passende Weiterbildungsangebote für einen Mitarbeiter zusammenstellt.

**KI bringt Unternehmen also erhebliche Entlastung, oder?**
Mehr als das. Der Nutzen ist insgesamt enorm: Es geht um Effizienzsteigerung durch Automatisierung, um Personalisierung und sogar um bessere Kundenerlebnisse. Ein Beispiel: Ein Kunde ruft wegen eines verloren gegangenen Pakets mit einer Jeans für 35 Euro an. Noch während des Telefonats sammelt die KI alle relevanten Informationen aus verschiedenen Systemen und zeigt sie dem Servicemitarbeiter in Echtzeit an. Die Bestell- und Bezahlhistorie zeigt, dass der Kunde bereits 1.700 Euro für das Unternehmen ausgegeben hat. Daher kann der Mitarbeiter sofort entscheiden, dass die nicht gelieferte Jeans für 35 Euro einfach erneut zugeschickt wird. Ergebnis: Der Kunde ist glücklich, fühlt die Wertschätzung und hat ein tolles Service-Erlebnis, obwohl er zunächst eine Beschwerde hatte.

**Auf solche Ergebnisse zu verzichten, kann sich eigentlich kein Unternehmen leisten.**
Richtig. Und es schadet, wie schon gesagt, auch der Gesamtwirtschaft. Bekanntlich befindet sich Deutschland in einer Wirtschaftskrise. Und wer sie nicht nur überstehen, sondern beenden will, für den ist das Thema Effizienzgewinn zentral. KI-basierte Lösungen und AI-Technologie können hier maßgebliche Vorteile bringen, auf die kein Unternehmen verzichten sollte. Doch viele Entscheider unterschätzen, wie gut KI heute schon funktioniert – ohne große, eigene IT. Dabei ist KI längst so leicht zugänglich wie ein Stromanschluss.

**Beim Thema KI spielen Datenschutz und Datensicherheit eine wichtige Rolle. Ist das ein Vorteil für Deutschland?**
Absolut! In Zeichen geopolitischer Spannungen wird der Fokus auf deutsche Datenhaltung zum Wettbewerbsvorteil. Die jetzige US-Regierung und ihre Tech-Politik führen dazu, dass europäische Unternehmen verstärkt nach Alternativen zu amerikanischen Cloud-Anbietern suchen. Wir betreiben unsere eigene Cloud-Infrastruktur in deutschen Rechenzentren. Wir erfüllen damit höchste Sicherheitsstandards und das zahlt sich aus. Aber es geht um mehr als das: Aktuell geht es auch um die Zukunft des Innovationsstandorts Deutschland. Ein Blick auf die weltpolitische Lage zeigt, wie megawichtig das ist. Wie entwickelt sich das Verhältnis von USA und Europa? Was geschieht zwischen Russland und China? Krisen und Kriege bestimmen unsere Nachrichten. Ich denke daher, es ist dringend Zeit, dass wir uns auf uns selbst besinnen und unser eigenes Rennen rennen.

**Aber da hört man doch ständig, dass Deutschland im internationalen Vergleich nicht genug investiert und zurückbleibt….**
Das Argument, dass der Staat nicht genug Geld gibt, kenne ich natürlich. Aber: Was ist mit so »Nebensächlichkeiten« wie Innovationsgeist, Mut, Entschlossenheit, Willenskraft, Ideenreichtum, die man mit allem Geld der Welt gar nicht kaufen könnte? Soll ich tatsächlich glauben, dass wir all das in Deutschland nicht besitzen? Blödsinn. Also muss das Motto doch lauten: Weniger lamentieren, sondern machen!

**Und während viele Unternehmen weiter zögern, geht die KI-Entwicklung weiter. Die nächste Stufe heißt Agentic AI. Was unterscheidet solche AI Agents von bisherigen Bots?**
Ganz allgemein kann man vielleicht sagen, dass AI Agents autonom arbeiten und eigenständig handeln können. AI Agents treffen ohne menschliche Unterstützung Entscheidungen und erledigen komplexe Aufgaben. Klassische Chatbots basieren vor allem auf definierten Skripten und reagieren nur auf Eingaben. Autonome AI-Systeme können dagegen mit Kunden in Echtzeit kommunizieren, Sprachbarrieren durch Echtzeitübersetzungen überwinden und untereinander Informationen austauschen.

**Das klingt, als bräuchten wir den Menschen gar nicht mehr …**
Beim KI-Einsatz geht es nicht um ein »Entweder-Oder« zwischen Mensch und Maschine. Vielmehr sind Mensch und KI eine symbiotische Einheit. KI kann riesige Datenmengen in Sekundenbruchteilen analysieren, Standardprozesse automatisieren. Der Mensch punktet bei Empathie und Kreativität und ist bezüglich der strategischen Verantwortung und der Entscheidungsfindung unverzichtbar. Es geht um die optimale Arbeitsteilung. Der Mensch erhält quasi Überwachungsfähigkeiten für KI-Anwendungen. Als Supervisor schaut er zum Beispiel in ein Gespräch zwischen Kunde und KI und unterstützt, wenn das nicht gut läuft. Wir nennen das »Human in the Loop«. So entsteht echte Teamarbeit zwischen Mensch und KI. In Zukunft wird es deshalb den CAIO geben, den Chief AI Officer, der die KI-Thematik technisch und kulturell denkt.

**Was raten Sie Unternehmen, die mit KI starten wollen, aber vorsichtig sind?**
Mein Tipp: Einfach anfangen! Starten Sie in einem geschützten Raum mit einer ersten Anwendung dann schauen Sie, wie es läuft. Meistens beginnt man dabei mit Prozessen, die auf menschlicher Sprache beruhen, denn generative KI wie ChatGPT beruht auf gesprochener oder geschriebener Sprache. Diese finden sich im Vertrieb, im Marketing und im Kundendialog. Auch die Softwareentwicklung – Stichwort Maschinensprache – ist geeignet. Holen Sie sich Unterstützung oder Begleitung von KI-Experten und Partnern, analysieren Sie die bisherigen Prozesse und definieren Sie, was mit KI optimiert werden kann und welche Lösung dazu passt. KI ist nicht so komplex, wie man anfänglich denkt, versprochen!

VIER

# Die Last vom Menschen auf die Technik verlagern

## Wie die Smart Factory funktioniert

Bild: Hyundai Motor Group/Unsplash

**Luka Kozamernik, Projektmanager von Hisense Europe, plädiert in seinem Buch »Digital Factory. A Digital Compass for Smart Manufacturing« (Springer Switzerland 2024) für mehr Weit- und Umsicht bei der Digitalisierung.**

**Text** Rüdiger Schmidt-Sodingen

Technologie könne »einen großen Beitrag zur Steigerung von Effizienz, Produktivität und Beschäftigungsmöglichkeiten am Arbeitsplatz leisten«. Es sei jedoch wichtig, »das Potenzial der Technologie zu berücksichtigen«, bestimmte Arbeitsplätze zu ersetzen und gleichzeitig neue zu schaffen. Tatsächlich komme es zusätzlich darauf an, »sich des potenziellen Missbrauchs von Technologie bewusst zu sein und die Auswirkungen von Robotern auf Arbeiter und Menschen in der Umgebung einer Fabrik zu berücksichtigen«.

Die zunehmende Komplexität der Herstellungsprozesse mache es notwendig, Lasten neu zu verteilen, sprich »einen Teil der Komplexität in eine technologische Lösung zu übertragen«. Allein die vorausschauende Wartung, die dank Computeralgorithmen vorhersagen kann, wann ein bestimmtes Maschinenteil ausgetauscht werden muss, sei ein Grund, digital umzubauen. »Das erleichtert die Planung der Maschinenwartung und vermeidet unnötige Ausfallzeiten.« Dass Fertigungsunternehmen immer noch mehr Geld in physische Anlagen statt in digitale Strukturen stecken, sei nur bedingt nachvollziehbar. »Fertigungsunternehmen werden keine Mitarbeiter entlassen, müssen sie aber weiterbilden, da sich die Fertigung drastisch verändern wird – digitale Bildung und Kompetenz werden für alle in der Branche entscheidend sein.«

**Austausch von Wissen – in Echtzeit**

Wer Digitalisierung also nur als weiteren IT-Posten begreift, greift bald ins Leere. Längst geht es darum, mithilfe von Datenströmen auch an kontinuierlichen Verbesserungen zu arbeiten, die erst die Mitarbeitenden, dann die Maschinen und schließlich die Kunden mitnehmen. Führungskräfte und Mitarbeitende, die sich nur auf ihre Fachgebiete konzentrieren, seien folglich der Hauptgrund für den Digitalisierungs-Flop in Unternehmen. Die Königsdisziplin sei »die Integration aller vorhandenen Softwaresysteme, Maschinen, Geräte und Mitarbeiter in einen digitalen Gesamtorganismus. Dieser digitale Organismus ermöglicht effizientere Produktionsprozesse und vor allem die Implementierung intelligenter Automatisierung und autonomer Roboter, um bei gleichbleibender Mitarbeiterzahl und gleichem Platzangebot eine höhere Rentabilität zu erzielen«.

Kozamerniks prägnante Abhandlung wird besonders da interessant, wo sie die Robustheit eines Unternehmens mit der Höhe des Mitarbeiterengagements kurzschließt. Wer die Digitalisierung dazu nutzt, auch Arbeitspläne, Maßnahmen zur Work-Life-Balance, Urlaubsplanungen und Feedback-Systeme zu installieren oder zu pushen, könne das Engagement und die Akzeptanz der Mitarbeitenden entscheidend verbessern. Zugleich warnt der Autor vor einer halbherzigen Implementierung von Systemen, die beispielsweise Echtzeitdaten oder IIoT-Technologie ausschließen. »Eine digitale Fabrik ist viel mehr als nur die Erfassung von Echtzeitdaten. Ohne sie kann man jedoch nicht von einer digitalen Fabrik sprechen.« Wer seine Fabrik in die Zukunft führen wolle, müsse nicht nur Produkte, sondern ab sofort auch (wieder) »Flexibilität, Vielfalt und Innovation« herstellen. Automatisierter Datenaustausch werde weiterhin eine wichtige Rolle spielen, ebenso wie die Zugänglichkeit und Wiederverwendung von Daten. Der Schlüsselbegriff sei und bleibe »Zusammenarbeit«: »Schließlich ist auch der Austausch von Wissen, Erfahrungen und Best Practices für den Erfolg einer intelligenten Fabrik entscheidend.«

---

**Genius Partner • Hima Group**

*think about: OT-Security*

# Digitalisierte Zukunft: Erstrebenswertes Ziel oder unheimliche Bedrohung?

**Wir befinden uns inmitten einer Fortsetzung der industriellen Revolution, die große Chancen aber auch erhebliche Risiken in sich birgt. Dies gilt speziell für Einrichtungen, deren Motivation es ist, betriebliche Risiken zu minimieren. Diese werden landläufig als Sicherheitseinrichtungen bezeichnet.**

So wie Anfang des vorletzten Jahrhunderts die Weber durch Zerschlagen der Webstühle die industrielle Revolution nicht aufhalten konnten, ist auch heute der technologische Trend hin zur Integration in die Informationstechnologie und der Nutzung künstlicher Intelligenz auch bei Sicherheitssystemen nicht aufzuhalten, indem wir auf vollständige Abkapselung und Trennung sicherer Systeme setzen. Es gilt vielmehr erkannte Risiken und Nutzen zu bewerten und die richtigen Schlüsse zu ziehen.

Goethes Zauberlehrling zeigt uns, wie neue Möglichkeiten nicht genutzt werden sollten. Er zeigt uns aber auch, dass der Mensch es ist, dessen Fähigkeiten wir unterstützen müssen. Verfügbare Statistiken zeigen, dass etwa 2/3 der dokumentierten Unfälle auf menschliche Fehler zurückzuführen sind. Hier ist der Ansatzpunkt, an dem die Digitalisierung und gerade auch KI helfen können, echten Mehrwert zu schaffen. Die dabei nutzbaren Möglichkeiten umfassen das gesamte Spektrum an Interaktionen, die zwischen der Sicherheitstechnik einerseits und den Nutzern andererseits notwendig sind.

Damit liegt ein Feld vor uns, welches ein großes Potential zur Verbesserung der funktionalen Sicherheit bietet, indem Fehler bei Planung und Betrieb vermieden werden.

Bekanntlich ist wo viel Licht ist auch viel Schatten. Der Schatten begegnet uns in der Gestalt stark zunehmender Bedrohungen von Anlagen durch gezielte Cyber-Angriffe. Die OT-Security beschreibt entsprechende Schutzmaßnahmen.

»Ohne OT-Security gibt es keine Funktionale Sicherheit«. So gesehen haben wir ein Ehepaar vor uns, dessen Ehepartner allerdings unterschiedlicher kaum sein könnten. Einer der beiden setzt auf die ausschließliche Nutzung betriebsbewährter Elemente, um bekannte Risiken zu beherrschen, der andere ist auf den Schutz des ersten Partners konzentriert und muss dazu flexibel agieren können, da sich die Bedrohungslage täglich ändert. Intensivieren wir die Digitalisierung über ein arriviertes Maß hinaus, so schaffen wir auch zusätzliche Angriffsvektoren, welche unserer Aufmerksamkeit bedürfen. Besonders der Aspekt der lateralen Angriffe, bei denen ein Angreifer zunächst die schwächste Stelle eines Systems auswählt, um angegriffene Systeme dann von »innen« heraus zu korrumpieren, bedarf der besonderen Aufmerksamkeit.

Bei HIMA beschäftigen wir uns seit mehr als 2 Jahrzehnten mit dieser Thematik und bieten unseren Kunden unter #safetygoesdigital eine umfassende Lösung, welche hilft, die Vorteile der Digitalisierung zu nutzen, ohne gleichzeitig erweiterte Risiken zu schaffen.

***Peter Sieber, Vice President Strategic Marketing, HIMA Group***

# »Automatisierung neu denken: mit integriertem Datenmanagement, Cybersicherheit und KI«

**Emerson liefert Steuerungs- und Softwarelösungen, um Fertigungsprozesse transparenter, sicherer und umweltfreundlicher zu machen. Philipp Strauch, Vice President DACH, über mehr Cybersicherheit, besseren Datenschutz und eine sichere IT-OT-Integration in der Automatisierung.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Strauch, wie muss heute, im Zeitalter der Digitalisierung, eine moderne Automatisierung aussehen oder funktionieren?**
Eine moderne Automatisierung muss Offenheit und Datentransparenz fördern, indem sie eine Architektur bereitstellt, die Datensilos beseitigt und die Nutzung transformativer Technologien ermöglicht. Der rasche technologische und industrielle Fortschritt im Bereich der Künstlichen Intelligenz, verbunden mit einem gesteigerten Bedarf an Rechenleistung und der enormen Menge sowie Komplexität isolierter Daten aus industriellen Anlagen, macht es notwendig, dass Unternehmen einen neuen, kosteneffizienten Ansatz finden. Dieser Ansatz sollte es ermöglichen, die Automatisierung auf Unternehmensebene umfassend zu nutzen und gleichzeitig bestehende Investitionen zu sichern.

Emersons Vision der Boundless Automation℠ integriert intelligente Feldgeräte, Edge-Computing und Cloud-Technologien, um Daten schnell in Erkenntnisse umzuwandeln und überall zugänglich zu machen. Diese Architektur erfordert eine einheitliche Datenstruktur, die erlaubt, dass Informationen nahtlos zwischen verschiedenen Aufgabenbereichen fließen und Software ihr volles Potenzial entfaltet. Bei der Emerson Exchange im Mai haben wir außerdem unser »Project Beyond« vorgestellt, eine softwaredefinierte, OT-fähige Plattform, die Datenmanagement, Cybersicherheit und KI integriert und so die industrielle Automatisierung ganz neu denken wird.

**Wie sichern Unternehmen den Zugriff auf sensible Daten in der Automatisierung?**
Unternehmen sichern den Zugriff auf sensible Daten in der Automatisierung durch die Implementierung von robusten Cybersicherheitsstrategien, die sich auf Offenheit und inhärente Sicherheit konzentrieren. Die Nutzung moderner Edge-Technologien und ein breiteres Cloud-Management ermöglichen es Unternehmen, sensible Daten in offenen Softwareumgebungen zu verwalten, die dennoch sicher sind. Tools zur Cyber-Resilienz maximieren die Sicherheit und ermöglichen ein vertrauenswürdiges Umfeld für den Austausch und die Verwaltung von Daten.

**Sie haben den Emerson Cybersecurity Assessment Service geschaffen, der Schwachstellen in Netzwerken und Anlagen identifiziert und beurteilt. Wie funktioniert dieser Service?**
Aufgrund der zunehmenden Cyberbedrohungen in verschiedenen Branchen und den kontinuierlich steigenden Anforderungen an Compliance hat Emerson Servicedienstleistungen für die Beurteilung der Cybersicherheit ins Leben gerufen. Dieser Service unterstützt unsere Kunden dabei, Schwachstellen in Anlagenkomponenten zu identifizieren und analysieren und praktische Empfehlungen zu geben, um Sicherheitsrisiken durch geeignete Schutzmaßnahmen zu minimieren. Im Rahmen der Bewertung werden zunächst die Anlagenkomponenten identifiziert und dokumentiert. Anschließend erfolgt eine eingehende Schwachstellenanalyse für jedes Gerät, gefolgt von Maßnahmenvorschlägen zur Verbesserung der gesamten Cybersicherheit.

So erleichtert unser Cybersecurity Assessment Service die Erkennung von Bedrohungen und Schwachstellen, die die Zuverlässigkeit und Verfügbarkeit von Steuerungssystemen, Netzwerken und weiteren kritischen Anlagen beeinträchtigen könnten.

**Welche Herausforderungen ergeben sich bei der Verknüpfung von IT und OT, insbesondere im Hinblick auf Sicherheitsrisiken?**
Ein wesentlicher Treiber moderner Edge-Technologien ist die zunehmende Softwareverbreitung, die auch Aufgaben traditioneller Hardware übernimmt. Unternehmen nutzen diese offenen und sicheren Softwareumgebungen, um Daten über verschiedene Aufgabenbereiche hinweg zugänglicher und die Bereitstellung sowie Verwaltung von Software einfacher zu gestalten, was Komplexitäten verringert und Datensilos auflöst. Die Verknüpfung von IT und OT bringt Herausforderungen in den Bereichen Sicherheit und Datenmanagement mit sich, da traditionelle Sicherheitsmethoden oft nicht ausreichen, um den Anforderungen der modernen OT-Bereiche gerecht zu werden. Sicherheitsrisiken ergeben sich durch unterschiedliche Protokolle, Systeme und Technologien, die integriert werden müssen, ohne die Sicherheit zu gefährden. Unternehmen müssen sicherstellen, dass ihre Netzwerke gut strukturiert und durchdringend überwacht sind, um Cyber-Bedrohungen abzuwehren.

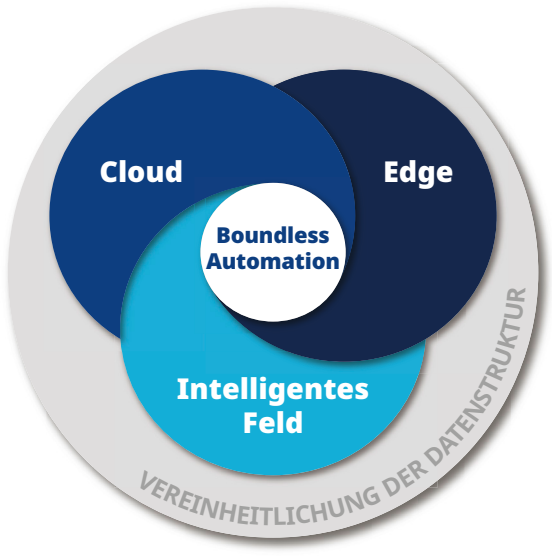
Die drei wesentlichen Strategien sind: Erstens Entkoppeln von Software und Hardware, sodass Funktionen über verschiedene Bereiche hinweg portabel sind. Zweitens eine einheitliche Datenstruktur, die die Integration und Zugänglichkeit von Daten aus unterschiedlichen Systemen fördert. Drittens der Einsatz administrativer Tools, die die Verwaltung komplexer Technologiearchitekturen ermöglichen. Das moderne Edge erleichtert die Implementierung und Verwaltung von OT-Systemen, die größere Flexibilität vor Ort sowie tief integrierte Rechenleistung und verbesserte Konnektivität zwischen Feld und Cloud bieten.

**NAMUR Open Architecture (NOA) garantiert im Grunde eine lückenlose Anlagenüberwachung. Wie verändert NOA den Automatisierungssektor?**
NAMUR Open Architecture verändert den Automatisierungssektor durch die Einführung eines offenen und strukturierten Systems, das eine lückenlose Überwachung und bessere Interoperabilität zwischen verschiedenen Aufgabenbereichen ermöglicht. NOA fördert die Integration und den transparenten Austausch von Daten zwischen Anlagen, was es Unternehmen ermöglicht, effizienter zu arbeiten und fundierte Entscheidungen auf der Grundlage umfassend verfügbarer Informationen zu treffen.

**Welche Sicherheitsstrategien sind im Zusammenhang mit NOA essenziell?**
Sicherheitsstrategien im Zusammenhang mit NOA müssen sich auf die Sicherstellung der Integrität und Vertraulichkeit von Daten konzentrieren, während Offenheit und Zugänglichkeit gefördert werden. Unternehmen sollten eine mehrschichtige Sicherheitsarchitektur implementieren, die Monitoring, Zugriffsverwaltung und Verschlüsselung umfasst, sowie regelmäßige Sicherheitsbewertungen und Audits durchführen, um potenzielle Bedrohungen frühzeitig zu erkennen und zu adressieren.

**Warum wird das Zero-Trust-Modell immer relevanter, und wie kann es in der Industrie effektiv umgesetzt werden?**
Das Zero-Trust-Modell wird zunehmend relevant, da es eine strikte Sicherheitsphilosophie verfolgt, bei der keinem Benutzer oder Gerät automatisch vertraut

***Philipp Strauch***
***Vice President DACH***
***Emerson***




wird. Dieses Modell minimiert das Risiko von Sicherheitsverletzungen durch kontinuierliche Überprüfung und Validierung von Zugriffsanforderungen. In der Industrie kann es durch strikte Zugangskontrollen, Netzwerksegmentierung und Echtzeit-Überwachung effektiv umgesetzt werden, um eine maximale Sicherheit der Infrastrukturen zu gewährleisten.

**Auf welche Themen sollten sich Unternehmen in den nächsten Jahren konzentrieren, um Anlagen und besonders auch kritische Infrastrukturen störungsfrei und effizienter zu betreiben?**
Unternehmen sollten sich auf die Verbesserung ihrer Cybersicherheit, die Integration moderner Automatisierungsarchitekturen wie Boundless Automation℠, und die Nutzung von KI und maschinellem Lernen für Echtzeit-Analysen konzentrieren. Zusätzlich sollten sie ihre Infrastruktur regelmäßig auf Schwachstellen prüfen und modulare Designs für Flexibilität und Anpassungsfähigkeit implementieren. Die Sicherung von Datenzugriffen und die ständige Optimierung von Betriebsstrategien wird entscheidend sein, um störungsfrei und effizient zu arbeiten. Projekte wie Emersons »Project Beyond« unterstützen dabei, diese Ziele zu erreichen, indem sie eine nahtlose Integration moderner Technologien ermöglichen und so eine kontinuierliche Optimierung fördern.

**Emerson.de/ProjectBeyond**

EMERSON

## Genius Tip

»Verwandeln Sie **Daten** in **Erkenntnisse** – indem Sie eine einheitliche **Datenstruktur** nutzen, die erlaubt, dass **Informationen** nahtlos zwischen **verschiedenen Aufgabenbereichen** fließen und **Software** ihr **volles Potenzial** entfaltet.«

# Digitalisierung in der Automatisierung – Grundstein für strategische Partnerschaften

**Die industrielle Automatisierung erlebt durch die Digitalisierung einen tiefgreifenden Wandel. Was früher als reine Effizienzsteigerung durch Maschinen galt, wird heute durch datengetriebene Prozesse, Künstliche Intelligenz (KI) und vernetzte Systeme zu einem strategischen Wettbewerbsvorteil.**

**Transparenz und Effizienz durch Datenintegration**
Ein zentrales Element der Digitalisierung ist die intelligente Nutzung von Daten. Unsere modernen Automatisierungslösungen erfassen, analysieren und visualisieren Prozessdaten. Kunden profitieren dadurch von einer nie dagewesenen Transparenz: Produktionskennzahlen, Qualitätsdaten und Wartungszustände sind jederzeit abrufbar.

» Die **Digitalisierung** in der Automatisierung ist **kein Selbstzweck**, sondern ein **klarer Nutzenbringer** für **Kunden.** «

*Andreas Höcherl*
*Head of Innovation & Strategic Projects, TU Innovation & Strategic Projects*

Dies ermöglicht nicht nur eine schnellere Entscheidungsfindung, sondern auch eine vorausschauende Produktionsplanung mit z.B. Predictive Maintenance oder Predictive Quality. Die Ausfallzeiten werden auf ein Minimum reduziert und die Anlagenverfügbarkeit maximiert.

**Individualisierte Lösungen durch modulare Systeme**
Digitalisierung erlaubt es, Automatisierungslösungen modular und skalierbar zu gestalten. Kunden erhalten dadurch exakt auf ihre Bedürfnisse zugeschnittene Systeme – sei es in der Medizintechnik, in der E-Mobilität oder anderen Branchen. Die Digitalisierungslösungen der **STRAMA-**GROUP zeigen, wie durch digitale Plattformen, diverse Softwarelösungen und standardisierte Schnittstellen die Automatisierung individuell und modular ergänzt wird.

**Schneller zur Marktreife durch digitale Zwillinge**
Digitale Zwillinge – also virtuelle Abbilder realer Anlagen – ermöglichen es, Abläufe bereits vor der physischen Umsetzung zu simulieren und zu optimieren. Kunden können so frühzeitig Einfluss auf das Design nehmen, Varianten testen und Time-to-Market deutlich verkürzen. Aber auch in der strategischen Produktionsplanung können verschiedene Szenarien in der Simulation digital getestet werden. In der Realität wird somit gewährleistet, dass die optimale Lösung umgesetzt wird.

**Nachhaltigkeit und Ressourceneffizienz**
Durch datenbasierte Prozessoptimierung lassen sich Ressourcen gezielter einsetzen. Energieverbräuche, Materialeinsatz und Ausschussquoten können kontinuierlich überwacht und reduziert werden. Die Digitalisierung leistet damit einen aktiven Beitrag zur Nachhaltigkeit – ein Aspekt, der für viele Kunden zunehmend an Bedeutung gewinnt.

**Zukunftssicherheit durch offene Systeme**
Ein weiterer Vorteil digitalisierter Automatisierung ist die Zukunftssicherheit. Offene, standardisierte Schnittstellen ermöglichen die einfache Integration neuer Technologien – sei es KI, Augmented Reality oder neue Sensorik. Kunden können ihre Anlagen flexibel erweitern und bleiben technologisch auf dem neuesten Stand.

**Kundenbindung durch digitale Services**
Neben der Hardware gewinnen digitale Services an Bedeutung. Kundenportale, Remote-Support, digitale Schulungen und automatisierte Ersatzteilbestellungen schaffen Mehrwert über den gesamten Lebenszyklus einer Anlage hinweg. Die Digitalisierung wird so zum Bindeglied zwischen Hersteller und Kunde – und zur Grundlage für langfristige Partnerschaften.

**Fazit**
Die Digitalisierung in der Automatisierung ist kein Selbstzweck, sondern ein klarer Nutzenbringer für Kunden. Sie schafft Transparenz, Effizienz, Individualität und Zukunftssicherheit. Unternehmen, die diese Potenziale konsequent nutzen, positionieren sich nicht nur als Technologieführer – sie werden zum strategischen Partner ihrer Kunden.

STRAMAGROUP



# »Roboter werden in immer mehr Bereichen als vielseitige und dynamische Unterstützer wahrgenommen«

**Bereits 1969 baute Kawasaki Robotics die ersten Robotersysteme. Mittlerweile stellt Kawasaki Robotics EMEA Roboter für viele unterschiedliche Bereiche her. Timo Ehlers, Head of Product Management & Marketing, erläutert, wie Robotik den Fachkräftemangel lösen kann.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Ehlers, Roboter sind aus vielen Produktionsprozessen nicht mehr wegzudenken. Wie können sie konkret dabei helfen, den Fachkräftemangel zu beheben?**
Roboter übernehmen zunehmend viele körperlich belastende und auch gefährliche Aufgaben – vom Palettieren über Metallverarbeitung bis hin zum Lackieren. Dabei geht es aber nie darum, Menschen durch Roboter zu ersetzen. Das Know-how von Fachkräften wird immer wertvoll und notwendig bleiben. Die gezielte Einbindung von Robotern ermöglicht es Unternehmen, ihre Mitarbeiter effizienter einzusetzen und von ihren Fähigkeiten besser zu profitieren.

**Mit welchen Herausforderungen haben Sie zu tun, um Roboter in Fertigungsprozesse zu integrieren?**
Insbesondere in kleinen und mittelständischen Unternehmen nehmen wir nach wie vor Zurückhaltung beim Thema Automatisierung wahr. Oft stehen Sorgen vor aufwändigen Investitionen im Vordergrund. Wir unterstützen Betriebe dabei, Automatisierung passgenau zu gestalten. Tatsächlich hören wir von unseren Kunden häufig, dass sich die Automatisierung von Produktionsprozessen nicht nur deutlich einfacher gestaltet, sondern sich die Investition viel schneller rechnet als angenommen. Eine oft unterschätzte Herausforderung ist der verfügbare Platz: Viele Produktionen in Deutschland haben die bestehenden, oft älteren Räumlichkeiten über Jahre hinweg maximal ausgereizt. Neben präziser, gemeinsamer Planung helfen hier jedoch auch das kompakte Design und der hohe Arbeitsbereich unserer Roboter. Bei allen Herausforderungen gilt: Branchen- und Prozess-Know-how sind entscheidend, um unsere Kunden gemeinsam mit unseren Integratoren richtig zu beraten.

*Timo Ehlers, Head of Product Management & Marketing, Kawasaki Robotics*

**Roboter werden zunehmend auch in Dienstleistungsberufen wichtig, etwa im Pflege- oder Bildungsbereich. Wie entwickelt sich dort die Zusammenarbeit zwischen Mensch und Roboter?**
Wir sehen schon heute deutlich weniger Berührungsängste – Roboter werden in immer mehr Bereichen als vielseitige und dynamische Unterstützer wahrgenommen. Im industriellen Kontext wird dies besonders anhand von Cobots wie unserer CL-Serie deutlich: Kollaborative Roboter müssen nicht mehr zwingend mit Sicherheitszäunen versehen werden, sind besonders intuitiv zu bedienen und ermöglichen völlig neue Anwendungsszenarien sowie Zielgruppen. Aber auch in den Bereichen Pflege und Service steht uns eine spannende Zeit bevor: Mit dem mobilen Serviceroboter Nyokkey oder dem in diesem Jahr mit überwältigender Resonanz vorgestellten Reitroboter Corleo geht Kawasaki ganz neue Wege. Das Joint Venture Medicaroid zwischen Kawasaki und Sysmex bietet zudem Chirurgieroboter und weitere Lösungen für die Medizin vor. Während Service- und Pflegeroboter in Japan schon länger eine wichtige Rolle spielen, sehen wir auch in Europa ein stark wachsendes Interesse.

**Welche Robotik-Innovationen werden in den nächsten Jahren Unternehmen entlasten und wieder wettbewerbsfähiger machen können?**
Cobots werden sich auch in den kommenden Jahren deutlich weiterentwickeln und vielen Anwendern den Zugang zur Automatisierung verschaffen. Intuitive und vielfältige Bedienoptionen jenseits des klassischen Programmierens – darunter manuelles Teaching und Simulationen – werden zunehmend gefragter. Darüber hinaus sehen wir den Faktor Flexibilität als entscheidend: Roboterlösungen müssen anpassbar sein und etwa auch bei kleinen Losgrößen schnell reagieren können. Moderne und KI-gestützte Kamerasysteme machen dies schon heute möglich, etwa beim Greifen aus Kisten oder sogar beim Palettieren und Depalettieren. Durch die Einbindung von KI können auch Mitarbeiter, die nicht programmieren können, neue Prozesse gestalten und anpassen – und somit ihre Erfahrung und Expertise gezielt einsetzen.

Kawasaki Robotics

## Genius Tip

»Durch die Innovationen unserer Zeit werden die **Möglichkeiten von Roboterlösungen** signifikant **erweitert** und **erleichtert**. Unternehmen, die diese Chance **nicht erkennen** laufen in Gefahr, **Wettbewerbsfähigkeit einzubüßen**.«

# »Wir holen die Software von Robotern ins 21. Jahrhundert«

**Zu wenig Personal, zu hohe Kosten, zu volatile Lieferketten. Um ihre Probleme in den Griff zu bekommen, kann die deutsche Fertigungsindustrie nur auf eine kluge, sprich softwaregetriebene und KI-gestützte Robotik und Automatisierung setzen. Christian Piechnick, CEO des Dresdner Scaleups Wandelbots, über Roboter als bahnbrechendes Hilfsmittel der kommenden Jahre.**

**Interview** Rüdiger Schmidt-Sodingen


**Herr Piechnick, wie kann Automatisierung die Kosten- und Personalprobleme in der Fertigung lösen?**
Wir haben in Deutschland nicht nur ein Kostenproblem, sondern es fehlen generell Fachkräfte. Sicher sind die Personalkosten in Deutschland hoch, aber das ist nicht das eigentliche Problem. Im vergangenen Jahr lag das Defizit bei 700.000 Stellen, die nicht besetzt werden konnten. In den nächsten 18 Jahren könnte die Lücke auf fünf Millionen Stellen anwachsen. Das heißt, die deutsche Industrie hat dann kein Personal-, sondern ein Existenzproblem. Wenn niemand mehr da ist, der in der Fabrik schleift, dann gibt es auch keine Aufträge mehr und Sie können den Betrieb schließen. Ganz davon abgesehen, dass die stetig steigende Nachfrage nicht bedient wird. Gleichzeitig ist die Verlagerung von Produktionsstätten angesichts der unsicheren globalen Lage auch keine Lösung mehr. Reshoring ist angesagt – und Automatisierung ist die einzige Lösung, um den Produktionsstandort Deutschland nicht nur zu erhalten, sondern kräftig auszubauen. Dazu muss Automatisierung aber weniger komplex, günstiger und zugänglicher werden.

**Sie sagen: Roboter müssen vielseitiger werden, die Automatisierung einfacher.**
Es braucht in der Fertigung eine hohe Präzision und Zuverlässigkeit. Bislang war es so, dass Automatisierung sehr teuer und auch sehr komplex war. Sie brauchen nur in die Automobilfabriken zu schauen. Während der Automatisierungsgrad bei Lackierung und Karosserie hoch ist, liegt er bei der Montage weiterhin unter zehn Prozent. Global laufen lediglich ein Prozent der Fertigungsprozesse automatisiert. Das hängt auch damit zusammen, dass Sie zur Roboterprogrammierung enormes Expertenwissen brauchen. Das ist einerseits teuer, andererseits aber eben auch sehr speziell und langwierig. Dort sind über die Jahre Silos entstanden, die den Einsatz von Robotern im Grunde unflexibel gemacht haben. Für Unternehmen mit höherem Individualisierungsgrad, also geringeren Losgrößen, ist die regelmäßige Anpassung der Roboterprogramme schlichtweg nicht erschwinglich.

**Hier kommt Ihr Plan zur »Demokratisierung der Robotik« ins Spiel?**
Richtig. Wir bieten mit Wandelbots NOVA eine Softwareplattform für die Robotik, deren einheitliches Betriebssystem für Roboter die Einsatzmöglichkeiten revolutioniert. Die meisten Roboter arbeiten mit Programmiersprachen aus den 80er Jahren. Sie sind eigentlich in der Zeit steckengeblieben. Wir holen die Software von Robotern nun ins 21. Jahrhundert. Mit unserem Produkt kann jeder Mensch einem Roboter eine Aufgabe beibringen, ganz ohne Programmierkenntnisse. Am Anfang haben wir gedacht, das Auslesen der Daten bestehender Anlagen wäre schon der Durchbruch, aber es war nur eine Bereicherung. Dann haben wir mit Simulationen gearbeitet, um Daten für Roboter zu gewinnen. Das war der Durchbruch. Wir bekommen durch Simulationen das Milliardenfache an Daten – und können nun bei konkreten Problemen KI einsetzen, um in der virtuellen Welt Lösungen für die reale Welt zu finden.

**Welche Rolle spielt KI?**
Roboter wurden bislang manuell programmiert. Dazu waren spezielle Programmierer notwendig, die zwei bis drei Wochen brauchten, um die Roboter für ihre Aufgaben zu programmieren. KI hat zwei entscheidende Einflüsse. Einmal können Roboter flexibler werden. Sie können beispielsweise scannen und »sehen«, was sie tun müssen. So scannt ein Roboter ein Bauteil und macht aufwändige CAD-Zeichnungen überflüssig. Der zweite entscheidende Punkt ist der Digitale Zwilling. Unsere Software berechnet in wenigen Minuten am Digitalen Zwilling des eingescannten Bauteils den idealen Roboterpfad. Per Button lässt sich dieser Pfad 1:1 auf die physische Anlage übertragen, der Prozess wird vom Roboter exakt so ausgeführt, wie von der Software erzeugt. Sie müssen sich vorstellen, dass selbst große Autohersteller bislang kaum digitale Abbilder von den Maschinen haben, die in ihren Werkshallen stehen. Witzigerweise hat die Halbleiterfirma NVIDIA entscheidend zur Entwicklung beigetragen, indem sie ihre Erkenntnisse aus computergenerierten Filmen in die Industrie eingebracht hat. Die Grundlage, um KI-Modelle zu trainieren, sind eben Daten.

**Dadurch werden Roboter in immer mehr Bereichen einsetzbar?**
Wir sind selbst immer wieder erstaunt, was für Lösungen mithilfe unserer Systeme nun möglich sind. Das Unternehmen Boskalis hat beispielsweise Roboter entwickelt, die gezielt Sprengstoff entsorgen können. Die Roboter entschärfen Bomben, indem sie sich die gefundene Granate ansehen und berechnen, wie der Sprengstoff herausgelöst werden muss. Bislang war dieser Prozess nur von Menschen durchführbar und sehr aufwändig und noch dazu gefährlich. Mit Robotern wird noch sehr viel möglich sein. Sie dürfen nicht vergessen, dass der steile Anstieg der Wachstumskurve für Computer in den 1990er Jahren gelang. Plötzlich hatten alle einen Computer. Das gleiche wird nun mit Robotern passieren, getrieben durch KI. Ich rechne damit, dass wir nicht sofort, aber mittelfristig einen ähnlichen Durchbruch wie bei ChatGPT im Consumer-Bereich sehen werden. Humanoide Roboter werden noch mehr Aufgaben erledigen. Zwar werden sie zunächst noch so viel kosten wie ein Oberklassewagen, aber sie werden auch im Heimbereich eingesetzt werden können – und in der Industrie immer mehr Spezialarbeiten übernehmen.

**Was bedeutet das für ein Industrieland wie Deutschland?**
Ganz klar: Mit KI können Sie Investitionen schützen und Prozesszeiten nachhaltig optimieren. Roboter können dank KI im gleichen Zeitraum 40 Prozent mehr produzieren. Microsoft ist nicht nur einer unserer Investoren, wir arbeiten auch technologisch eng mit ihnen zusammen. Gleichzeit sorgen wir für einen souveränen Weg Deutschlands. Microsoft stellt die Infrastruktur, wir stellen die Daten. Und ich sehe eine große Chance, dass Deutschland und Europa dank KI-gestützter Robotik viele neue Geschäftsfelder finden. Der Bereich Robotic & Manufacturing kann zum Leuchtturmprojekt für Europa werden. Das Potenzial ist da. Wir können jetzt aufholen, was wir in den letzten zehn Jahren verschlafen haben. Wenn Sie beispielsweise vor zehn Jahren in den USA eine Fabrik besichtigt haben, fühlten Sie sich wie im Museum. Heute ist das anders. Die Fabriken sind absolut modern. Man sollte jedoch nicht vergessen, dass die Haupt-Knowhow-Träger hier bei uns sitzen. Das Prozesswissen ist bei uns. Und wenn Roboter die Computer der nächsten zwei Jahrzehnte sind, werden die Karten völlig neu gemischt, auch dank vieler europäischer Ideen und Projekte, die in die Robotik einfließen werden: grüne Energie, Nachhaltigkeit, Kreislaufwirtschaft. Ein schönes Beispiel ist Miele, die Cradle-to-Cradle nun als Teil ihres Geschäftsmodells sehen. Konkret bedeutet das, dass Miele ab einem gewissen Zeitpunkt nie wieder Rohstoffe einkaufen muss. Firmen, die so etwas aufbauen, gehen vorneweg – und sichern die Zukunft unserer Kinder.

**Hat sich die deutsche Industrie zu lange ausgeruht?**
Die Digitalisierung wurde hierzulande größtenteils verpennt, die Produktion nicht modernisiert und angepasst. Wir brauchen einfach bessere Infrastrukturen, mehr mutige Entscheidungen – auch von den richtigen Leuten, die dann neue Dinge durchsetzen. Im Automobilbereich haben es Schaeffler und BMW geschafft, aus ihrem Knowhow etwas zu machen, es in Daten und entsprechende Anwendungen und Automatisierungen zu überführen. Wie gesagt: Das Potenzial und auch die Vorbilder sind da.

Wandelbots

## Genius Tip

»Wir sprechen nicht über Optimierungen, sondern über **Revolution – do or die**. KI wird in der Produktion zu so starken **Veränderungen** führen, die heute **keiner absehen kann**. Die **Unternehmen**, die in der Lage sind, **KI** für sich einzusetzen, werden **gewinnen**, alle anderen werden verschwinden.«

# »Adaptive und integrierte (Teil-)Automatisierung, die den Menschen effizienter und produktiver macht!«

**Die digitale Transformation und die rasante Entwicklung der KI-Möglichkeiten definieren die Zusammenarbeit von Mensch und Maschine neu. Björn Riechers, Geschäftsführer der 1972 gegründeten RK Rose + Krieger GmbH, über zunehmend gefragte Komponenten und Funktionsmodule für Automatisierungs- und Produktionsanwendungen, die alle Arbeitenden entlasten und den Ressourceneinsatz effizient gestalten.**

**Herr Riechers, wie beeinflusst die Digitalisierung die Produktion und damit die verschiedenen Arbeitsplätze, an denen Menschen oder Roboter arbeiten?**
Die Digitalisierung ermöglicht in Herstellungs- und Produktionsprozessen eine höhere Produktvarianz sowie individuellere Produkte durch Automation und Assistenzsysteme. Sie entlastet Mitarbeiter von schweren, monotonen manuellen Tätigkeiten und verbessert die Mensch-Maschine-Interaktion. Kollaborierende Roboter, Maschinentechnikelemente und digitalisierte Assistenzsystems unterstützen die Mitarbeiter bei körperlich belastenden oder monotonen Tätigkeiten und sichern eine hohe Prozessqualität.

**Wie lassen sich denn sowohl bei der manuellen Montage als auch bei vollautomatisierten Anlagen die Montagesysteme individuell verbessern?**
RK Rose+Krieger bietet modulare Lösungen, die sich an spezifische Anforderungen in den jeweiligen Kundenanwendungen anpassen lassen. Ergonomische Arbeitsplatzgestaltung und kognitive Assistenzsysteme optimieren die Produktivität und Fehlerfreiheit. Hubsäulen und Linearachsen aus dem Komponentenportfolio von RK Rose+Krieger erweitern den Aktionsradius von Cobots, um mehrere Arbeitsplätze zu verknüpfen. Der RK Rose+Krieger-Modulbaukasten für (teil-) automatisierte Montagelinien ermöglicht dann auch, sukzessive den Automatisierungsgrad zu erhöhen.

**Ein Stichwort heißt Entlastung. Was ändert sich an den menschenzentrierten Arbeitsplätzen?**
Ergonomische Arbeitsplätze und Assistenzsysteme minimieren körperliche und kognitive Belastungen, steigern die Zuverlässigkeit und Produktivität der Mitarbeiter und ermöglichen eine höhere Abwechslung am Montagearbeitsplatz. Cobots übernehmen präzise und repetitive Aufgaben, die für Menschen belastend sind, und wirken der Ermüdung am Arbeitsplatz entgegen.

**Welche Rolle spielt Nachhaltigkeit bei der Optimierung der Montagearbeitsplätze?**
Nachhaltigkeit wird in der Fertigung durch schlanke Prozesse und abgestimmte Logistik erreicht. Die effiziente Nutzung der Möglichkeiten von KI und Digitalisierung ermöglicht die Optimierung des Ressourceneinsatzes und bedeutet eine Minimierung von Fehlern und Ausschuss. Digitale und intelligente Werker-Assistenzsysteme wie das Phoenix Mecano SETAGO-System unterstützen dies zusätzlich.

**Kann das Arbeiten von Menschen, also auch ohne Roboter, noch weiter optimiert und erleichtert werden?**
Ja, denn eine ergonomische und in der Höhe flexible, anpassbare Arbeitsplatzgestaltung, kognitive Assistenzsysteme sowie eine auf den Prozess abgestimmte Anordnung von Werkzeugen und Maschinentechnik optimieren und erleichtern die manuelle Fertigung und Montage und reduzieren Fehler, z.B. auch durch Poka-Yoke-Systeme, die eine falsche Materialverwendung verhindern. Zusätzlich können durch das Verwenden von maschinentechnischen Elementen, etwa mit Kamerasystemen, die Arbeitsergebnisse geprüft und im Prozess und Kundenauftrag dokumentiert werden.

**Sie weisen gleichzeitig auf die enormen Möglichkeiten der Robotertechnik hin. Werden bestimmte Produktionsprozesse in Unternehmen noch zu wenig hinterfragt oder neu gedacht?**
Oft zögern gerade mittelständische Unternehmen mit der Integration von Robotik und AMR-Lösungen und ähnlichem, da dies oft mit einer hohen Investitionsleistung verbunden wird.

RK Rose+Krieger hat mobile Cobot-Lösungen, etwa den RK Easy Cuve, im Portfolio, die es ermöglichen, mit einem Cobot an mehreren Arbeitsstationen zu arbeiten und so das Investitionsvorhaben klein zu halten und schneller einen »Return-on-Investment« zu bekommen. In vielen klassischen Montagelinien zeigt sich, dass es Potenzial gibt, Prozesse durch integrierte Verkettung und (Teil-)Automatisierung zu optimieren.

**Ein großes Feld ist die intelligente Mensch-Maschine-Interaktion. Was für Herausforderungen und Lösungen gibt es dort?**
Herausforderungen liegen in der fehlerfreien Umsetzung komplexer und sich oft ändernder Prozesse. Die Lösung für diese Herausforderung sind kognitive Assistenzsysteme, wie unser SETAGO-System oder auch andere marktübliche Poka-Yoke-Anwendungen, die den Mitarbeiter durch den Prozess führen und Fehler korrigieren. In diesem Zusammenhang können durch die Integration von Maschinentechnikelementen, wie VISION-Systeme und Handhabungstechnik (wie z.B. Greifer), die in ihren neuesten Versionen auch für die kollaborative Interaktion in manuell ausgeführten Arbeitsvorgängen ausgelegt sind, weitere Prozesssicherheit und Effizienzgewinne erzielt werden.

**Wie sehr können Sie mit Virtual Reality und Simulation diese Mensch-Maschine-Interaktion neu oder besser planen?**
RK Rose+Krieger nutzt Simulationen in LEAN Solutions-Workshops, um Systemansätze zu testen und die Mensch-Maschine-Interaktion zu optimieren. Cardboard-Workshops ermöglichen realitätsnahe Tests der zukünftigen Lösungen. VR und Simulation ermöglicht unseren Kunden, die zukünftige Lösung schon vor der Installation zu erleben und zu optimieren, so dass Iterationsschleifen minimiert werden können. Das spart Zeit, Geld und Ressourcen.

**Wie werden sich in den nächsten Jahren die Möglichkeiten von Cobots und digitalen Assistenzsystemen noch weiterentwickeln?**
In diesem Kontext werden sich der Einsatz von KI-Lösungen mit Zugang zu breitem Expertenwissen, die heutigen Möglichkeiten der Arbeitsplatz- sowie der schlanken Prozessgestaltung und der Einsatz von intelligenten und sich auf den Menschen anpassenden und lernenden Assistenzsysteme weiterentwickeln.  Das alles wird die Einsatzmöglichkeiten für digitale und automatisierte Produktionsabläufe auf eine heute noch unvorstellbare Ebene hieven.

RK ROSE+KRIEGER
A Phoenix Mecano Company

Björn Riechers, Geschäftsführer
RK Rose + Krieger GmbH

## Genius Tip

»Für mittelständische Unternehmen in Familienhand ist eine **Investition** in mobile, flexible und skalierbare Automatisierungslösung oft eine sehr **große Entscheidung**. Weiterhin wird in diesen Unternehmen sehr viel Wert daraufgelegt, dass die **Stammbelegschaft** in Beschäftigung bleibt. Mit dem **modularen** und flexiblen **Systemlösungsansatz** von RK Rose+Krieger lassen sich **vielfältige Werkstatt- und Industrieanwendungen** in der Produktion und/oder Montage (teil-) **automatisieren** und **digitalisieren**, wobei oft ein **Produktivitätsgewinn** von bis zu 30 % oder mehr erzielt wird.«

# »Produkt-Cybersicherheit wird Pflicht – Hersteller müssen jetzt handeln, um Millionen-Strafen zu vermeiden«

**Die zunehmende Cyberkriminalität zwingt die EU-Kommission zum Handeln. 2026 tritt die erste Stufe des ab 2027 vollständig geltenden EU Cyber Resilience Act (CRA) in Kraft, um eine höhere Produktsicherheit zu gewährleisten. Jan C. Wendenburg, CEO der führenden europäischen Security- und Compliance-Geräte-Analyse-Plattform ONEKEY, erklärt, auf was sich Unternehmen, die vernetzte Produkte herstellen oder handeln, einstellen müssen.**

**Interview** Rüdiger Schmidt-Sodingen

**Herr Wendenburg, welche Auswirkungen hat der CRA konkret auf die Hersteller und Händler von vernetzten Geräten?**
Der CRA ist die weltweit umfassendste Regelung zur Cyber-Produktsicherheit. Sie erzwingt für alle Hersteller von smarten Produkten die Einführung, Implementierung und Überwachung von produktbezogener Cybersicherheit. Es geht praktisch um alle Produkte, in denen Software steckt. Die EU spricht von »Produkten mit digitalen Elementen« – dies reicht von »Industrial Automation«, also industriellen Steuerungen, Robotik, Fertigung, industrieller oder allgemeiner Infrastruktur (Versorgung, Wasser, Strom, Klima, Gas-Regelungen), bis zu Transport und Logistik (Bahn, Verkehrsleittechnik, etc.) und Consumer-Elektronik (Babyfon, Kühlschrank, Home-Automation, Spielzeuge, etc.). Die Cyber-Sicherheit beginnt bei der Planung, mit der Berücksichtigung sogenannter »Secure by Design«-Konzepte, betrifft die (Software-)Entwicklung, mit einer kontinuierlichen Prüfung und Kontrolle während des Entwicklungsprozesses, und die Produktion, mit Verteilung der Software, bis zur Wartung samt Software-Updates und Software-Stücklisten. Konkret dürfen zukünftig keine Produkte mit ausnutzbaren Schwachstellen mehr in Verkehr gebracht werden. Die Besonderheit ist, dass alle Hersteller weltweit, egal, wo sie auf der Welt ihren Sitz haben, davon betroffen sind, sofern sie Produkte in der EU verkaufen wollen. Sie müssen jetzt aktiv handeln, um die Konformität ihrer Produkte sicherzustellen und zu beweisen. Bei Nichtbeachtung dürfen die Produkte in der EU nicht mehr verkauft werden.

**Jan C. Wendenburg, CEO ONEKEY**

**Betroffen von der Regelung sind Hersteller, Importeure und Händler. Was bedeutet das für die Produktlieferketten?**
Der CRA schreibt vor, dass der »Inverkehrbringer« des Produktes für die Einhaltung haftet, also Hersteller, Importeur oder Distributor. Das heißt, ein deutscher oder europäischer Maschinen- oder Produkthersteller, der Software oder Komponenten von seinen Sub-Lieferanten, in seinem Produkt verwendet, haftet auch für die Komponenten seiner Sub-Lieferanten. Für jede Software in Produkten ist eine Software-Stückliste, die sogenannte SBOM (Software Bill of Materials) zu erstellen und aktuell zu halten – diese muss alle Komponenten der Software, auch die Komponenten Dritter, im Detail enthalten. Die Haftung ist nicht delegierbar, d.h. der Hersteller, Importeur oder Distributor haftet selbst. Er kann sich also nicht darauf berufen, dass er nur Komponenten oder Software Dritter verwendet. Die Strafen sind empfindlich. Sie können bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes betragen. Wir haben bei der EU-Datenschutzregelung (GDPR) aus 2018 gesehen, dass die Behörden diese Strafen in Millionenhöhe bei Nichtbeachtung auch durchsetzen.

» Der **CRA** erzwingt für **alle Hersteller** von smarten Produkten die Einführung, Implementierung und Überwachung von **produktbezogener Cybersicherheit.** «

**Welche technischen und organisatorischen Massnahmen sind erforderlich, um die neuen Compliance-Vorgaben zu erfüllen?**
Der »Inverkehrbringer« muss die Prüfung, Analyse, Bewertung und Dokumentation auf Software-Schwachstellen bei jedem Produkt vor dem Verkauf und über die vorhersehbare Produkt-Lebensdauer gewährleisten. Grundsätzlich sind diese Maßnahmen kontinuierlich zu dokumentieren.

**Wie unterstützt ONEKEY durch automatisierte Firmware-Analyse und Software-Stücklisten (SBOMs) die Umsetzung der regulatorischen Anforderungen?**
ONEKEY ist Spezialist für die automatisierte Prüfung von Cybersicherheit und Compliance für Software in Produkten, sogenannter »Embedded Software«. Vereinfacht gesagt, automatisiert ONEKEY die wesentlichen Aufgaben und Auflagen des CRA für den Hersteller bzw. Inverkehrbringer. Das erfolgt durch eine automatisierte Erstellung einer Software-Stückliste (SBOM), die Analyse der Software auf mögliche Schwachstellen, die automatisierte Bewertung, ob diese Schwachstellen auch wirklich relevant sind, und die erforderliche Dokumentation. Alles erfolgt im Kontext der gesetzlichen Auflagen und Anforderungen, d.h. mögliche Verstöße oder fehlende Sicherheitsmaßnahmen werden angezeigt. Auch mögliche und empfohlene Maßnahmen zu Behebung werden vollautomatisch ermittelt und aufgezeigt. Diese Prüfung auf Schwachstellen und Compliance dauert nicht – wie üblicherweise bei einer manuellen Durchführung – Wochen, sondern vollautomatisch lediglich 15 bis 30 Minuten. Durch den einzigartigen, zum Patent angemeldeten »Compliance Wizard« werden zusätzlich Compliance-Problemfelder in der Software identifiziert und können anschließend in einem geführten Dialog, wie ein Online-Assistent, bearbeitet, bewertet und dokumentiert werden. So können die wesentlichen Anforderungen weitestgehend automatisiert und mit Hilfe des eingebauten Expertenwissens behoben werden. Dies spart erheblich Zeit, Ressourcen und Geld. Insbesondere bei der Wartung von Software, also Updates, fallen normalerweise erhebliche Kosten zur Überwachung von Schwachstellen an, hier lässt sich die Bewertung von neuen Schwachstellen, die oft mehrere Stunden am Tag dauert, fast vollständig automatisieren.

**Hersteller müssen Informationen über ausgenutzte Schwachstellen eines Produkts praktisch sofort mit den Marktüberwachungsbehörden und der ENISA teilen. Auch hier hilft Ihre Plattform?**
Die ONEKEY-Plattform automatisiert die Meldungen an die ENISA oder deren nationale Behörden, wie das deutsche Bundesamt für Sicherheit in der IT (BSI), vollständig. Diese Funktion wird bereitgestellt, sobald das BSI den Zugang für diese Meldungen freigeschaltet hat.

**Welche Fallstricke erleben Unternehmen aktuell bei der Vorbereitung auf den CRA – und was sollten sie unbedingt beachten?**
Für viele Unternehmen ist der CRA nicht transparent und die Regelungen zur Produktklassifizierung, d.h. welches Produkt ist wie betroffen und muss welche Regelungen wie beachten, sind oft unklar. Wichtig ist, dass erst einmal alle Produkte, in denen Software steckt, »betroffen« sind. Es gibt ein paar Ausnahmen wie z.B. Bereiche, in denen bereits vergleichbare oder höhere Anforderungen bestehen, etwa der automobile Fahrzeugbereich, medizinische Geräte wie Insulinpumpen oder Herzschrittmacher, die Bereiche Flugzeugbau und Verteidigung. Es ist wichtig, zu Beginn festzustellen, welche Produkte betroffen sind, und für sie einen klaren Fahrplan zu erstellen. ONEKEY kann dafür eine schnelle, erste Einschätzung geben und so kostengünstig über die automatisierte Analyse ein sofortiges Ergebnis liefern. Zudem hat ONEKEY ein Team von weltweit anerkannten Spezialisten, das sehr individuell auf die Bedürfnisse von Unternehmen eingehen und helfen kann. Von individuellen Analysen und Hilfestellungen bis zur konkreten Implementierung der Prozesse und notwendigen Werkzeuge und schließlich der Übernahme der kontinuierlichen Überwachung von Produkten und deren Schwachstellen.

ONEKEY

## Genius Tip

»Der **CRA** ist ab 2026/2027 **verpflichtend** und ein ›**Game Changer**‹ für alle Hersteller und Importeure. Rechtzeitige Vorbereitung vermeidet später **teure Nachholarbeiten**. Durch **Automatisierung** lässt sich viel Zeit, Ressourcen und Geld sparen. **ONEKEY** bietet eine schnelle, unverbindliche ›**Standortbestimmung**‹, um den **aktuellen Handlungsbedarf** zu ermitteln.«

# »Sicherheit ist kein IT-Thema – sondern Führungsaufgabe«

**Mit über 5.000 Experten an 12 Standorten verwirklicht act digital, vormals Alter Solutions, maßgeschneiderte Cybersecurity-Lösungen. Johannes Krause, Head of Business Development, und Dr. Jochen Rill, Head of Cybersecurity, über das wachsende Bedürfnis nach ganzheitlichen Lösungen und die Sicherheitslage der Unternehmen.**

**Herr Krause, Herr Dr. Rill, alle reden von Sicherheit. Was bedeutet das für Unternehmen?**
*Johannes Krause:* Cybersicherheit beginnt nicht mit Firewalls – sondern mit Haltung. Mit Verantwortung auf Entscheiderebene. Viele Unternehmen unterschätzen das Risiko, weil sie sich in falscher Sicherheit wiegen: »Wir sind zu klein«, »Uns wird schon nichts passieren«, »Das macht die IT«. Doch genau diese Naivität ist brandgefährlich. Wer so denkt, hat bereits ein Einfallstor geschaffen – durch eigenes Verhalten, durch fehlende Prozesse oder durch das bewusste Wegschauen im Management.

*Dr. Jochen Rill:* Häufig sehen wir, dass gerade das Top Management davon ausgeht, dass IT-Sicherheit »von der IT gemacht werden muss« und man den Rest des Unternehmens damit am besten in Ruhe lassen soll.

**Wo beginnt denn echte Sicherheit im Unternehmen?**
*JK:* Echte Sicherheit beginnt ganz oben. Sie ist keine Fußnote im IT-Budget, sondern ein aktives Führungsinstrument. Wer heute Geschäftsmodelle, Partnerschaften oder Technologien entscheidet, entscheidet damit automatisch auch über Risiken. Und wer das ignoriert, gefährdet nicht nur die IT – sondern die gesamte Organisation. Sicherheit braucht strategische Verankerung, kontinuierliche Kommunikation und Management-Entscheidungen, die Sicherheit aktiv mitdenken.

*JR:* Damit ein Unternehmen ein hohes Maß an IT-Sicherheit erreichen kann, müssen technische Maßnahmen, Prozesse passgenau ausgewählt werden und Mitarbeitende mit allen Maßnahmen und Prozessen, die sie selbst anwenden müssen, vertraut sein. Wichtig ist auch, dass dem Unternehmen überhaupt klar ist, vor welchen Bedrohungen es sich schützen muss. In der Regel sind das nicht die »russischen Hacker«, »APT« oder »Zero Day Exploits«, sondern gewöhnliche Kriminelle, die sich menschliche Fehler oder mangelnde Softwareupdates zunutze machen – hier muss die Sensibilisierung beim Management anfangen.

**Was sind aus Ihrer Sicht die größten Fehler, die Unternehmen aktuell machen?**
*JK:* Der größte Fehler ist das Missverständnis, dass man Sicherheit einfach einkaufen kann. Ein neues Tool ersetzt keine Sicherheitskultur. Wir erleben es immer wieder: Unternehmen investieren in Lösungen – aber Prozesse fehlen, Mitarbeitende sind nicht eingebunden, die Anwendung wird nicht erklärt. Das Ergebnis? Ein Passwort-Manager ist da, aber niemand nutzt ihn. Es gibt Security-Policies, aber keiner kennt sie. Technik ohne gelebte Praxis – ist wirkungslos. Sicherheit kann man nicht einkaufen – man muss sie leben.

**Welche Rolle spielen das Security Management und das Security Engineering?**
*JR:* Bei Security Management geht es darum, die IT-Sicherheit im Unternehmen risikobasiert zu managen – und zwar im Sinne eines »Managementsystems« mit fest definierten Zielen, Prozessen, Handlungsanweisungen und kontinuierlicher Verbesserung. Ein gut umgesetztes und aktiv gelebtes Security Management hilft dabei, für den eigenen Schutzbedarf geeignete Maßnahmen auszuwählen und diese Auswahl kontinuierlich zu hinterfragen, um bei Änderungen der Risikolage schnell nachzusteuern zu können. Beim Security Engineering geht es darum, System- und Softwarearchitekturen so zu gestalten, dass sie schon in der Konzeption möglichst sicher sind. Und es geht darum, Sicherheitsmaßnahmen an den richtigen Stellen möglichst wirksam einzusetzen – also eigentlich um die konkrete Anwendung von Sicherheitsmaßnahmen.

**Welche Rolle spielt dabei die Unternehmenskultur?**
*JK:* Eine zentrale. Sicherheitskultur heißt nicht Kontrolle, sondern Vertrauen. Mitarbeitende müssen wissen: Ich darf fragen, ich darf melden, ich darf Fehler offen ansprechen – bevor sie zur Katastrophe werden. Nur in einer offenen und klaren Kultur kann man auf Angriffe reagieren, bevor sie eskalieren. Die beste Technik bringt nichts, wenn sie im Schatten einer Kultur der Unsicherheit eingesetzt wird.

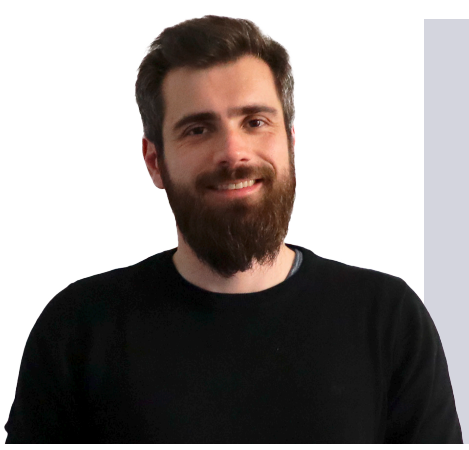
**Was empfehlen Sie konkret? Was funktioniert?**
*JK:* Fangen Sie nicht bei der Technik an – sondern bei der Haltung. Schulen Sie Ihre Mitarbeitenden praxisnah und wiederholt: Phishing, Passwortschutz, Umgang mit verdächtigen Anhängen. Erklären Sie Ihre Maßnahmen verständlich. Kommunizieren Sie Sicherheitsprozesse so, wie Sie auch Vertriebsprozesse erklären würden. Und holen Sie sich bei Bedarf unabhängige Beratung – nicht von denen, die Ihnen gleichzeitig ein Produkt verkaufen wollen. Denn Vertrauen entsteht nicht durch Marketing, sondern durch Aufrichtigkeit. Wer Prozesse nicht erklärt, darf sich über Sicherheitslücken nicht wundern.

**Wie finden Unternehmen in Zeiten des Fachkräftemangels denn die richtigen Lösungen, die dann auch von möglichst vielen Mitarbeitenden verstanden werden?**
*JR:* Das ist tatsächlich alles andere als einfach. Grundsätzlich gilt: Je komplexer die Systeme und die IT-Infrastruktur, desto schwieriger wird es mit dem Verständnis und eventuell sinkt dann auch wieder die Gesamtsicherheit. Gerade bei XDR und NDR-Lösungen gibt es regelmäßig kritische Sicherheitslücken. Anstatt sich einen bunten Zoo an Lösungsanbietern einzukaufen, ist es in der Regel sinnvoller sich auf einige wenige zu beschränken, von deren Sicherheit und Mehrwert man überzeugt ist. Vorsicht vor unseriösen Marketingversprechen: Kein Produkt, das Sie einkaufen können, kann ihnen Schutz vor allen Angriffen bieten, ohne, dass Sie dabei ihre Prozesse verändern müssen (auch nicht mit KI). Ein hohes Maß an IT-Sicherheit entsteht nur durch richtiges Zusammenwirken von technischen und organisatorischen Maßnahmen. Im Zweifel sollte man sich an ein unabhängiges Beratungsunternehmen wenden, das selbst keine Sicherheitsprodukte vertreibt.


**Wie ist allgemein die Lage in Unternehmen bezüglich Cybersecurity? Was für Strategien oder Infrastrukturen finden Sie dort bereits vor?**
*JR:* Die Lage ist überwiegend schlecht. Gerade bei Unternehmen, die eine eigene Windows-basierte Infrastruktur betreiben, gelingt es uns im Rahmen von Penetrationstests häufig schon nach wenigen Tagen, die Kontrolle über die komplette Infrastruktur zu bekommen. Die Gründe dafür sind vielfältig, aber häufig haben die Unternehmen Schwierigkeiten mit der Komplexität der Systeme, um damit notwendige Sicherheitsupdates zeitnah (oder überhaupt) zu installieren. Geld und Personalressourcen für IT-Sicherheit sind häufig auch nicht vorhanden. Wir haben nur selten einen Penetrationstest von IT-Infrastruktur, bei dem wir überhaupt nichts finden. Bei IT-Produkten sieht die Lage etwas besser aus. Hersteller von IT-Produkten haben häufig ein besseres Risikobewusstsein für die Sicherheit der Produkte, die sie entwickeln, als für ihre eigene IT-Infrastruktur.

**Wie können Business-Entscheider in Zukunft besser Verantwortung übernehmen?**
*JK:* Indem sie sich nicht länger hinter der IT verstecken. Wer Unternehmen führt, muss wissen, was ein erfolgreicher Angriff für Kundendaten, Reputation und Geschäftsfähigkeit bedeutet. Und wer das verstanden hat, trifft andere Entscheidungen – bewusster, vorausschauender, sicherer. Unser Ziel bei act digital ist es, genau da anzusetzen: Wir wollen nicht nur Technik zu liefern, sondern Menschen befähigen und Organisationen resilienter zu machen – ganzheitlich, glaubwürdig und mit Augenmaß.

***Johannes Krause, Head of Business Development, act digital***



***Dr. Jochen Rill, Head of Cybersecurity, act digital***

## Genius Tip

»**Sicherheit** ist kein IT-Thema – sondern **Führungsaufgabe**. Wer **Risiken** versteht und **Verantwortung** übernimmt, baut **echte Resilienz** auf. Alles andere ist **Selbsttäuschung** – und ein **Risiko**, das Sie sich **nicht leisten** können.«