EINE PUBLIKATION VON SMART MEDIA

SMART.

Öffentliche Sicherheit

März '26

Dr. Ferri Abolhassan

Der CEO von T-Systems nimmt die deutsche IT-Sicherheit unter die Lupe und spricht über die Wichtigkeit der digitalen Resilienz.

Lesen Sie mehr auf fokus.swiss

Holger Berens

Resilienz und Augenmaß

Sicherheit ist ein grundlegendes Ziel jedes Menschen, aber auch der Politik und der Wirtschaft. Sie bedeutet mehr als das Nichtvorhandensein von Bedrohungen. Sicherheit bedeutet auch die Möglichkeit von Planungen, die sowohl das persönliche Leben als auch die Gesellschaft betreffen. Die Frage der öffentlichen Sicherheit ist in Europa in den vergangenen Jahren wieder stärker in das Zentrum politischer und gesellschaftlicher Aufmerksamkeit gerückt. Lange Zeit galt Stabilität in vielen Bereichen unseres Alltags als selbstverständlich. Energie floss aus der Steckdose, Kommunikationsnetze funktionierten zuverlässig, Versorgungsketten arbeiteten nahezu unsichtbar im Hintergrund. Die geopolitischen Entwicklungen der letzten Jahre haben deutlich gemacht, dass diese Stabilität kein Naturzustand ist – sie ist das Ergebnis kontinuierlicher Anstrengung.

Der russische Angriffskrieg gegen die Ukraine hat Europa in einer Weise erschüttert, die viele Menschen zuvor kaum für möglich gehalten hätten. Energieversorgung, Lieferketten und digitale Infrastrukturen sind seitdem stärker in den Fokus sicherheitspolitischer Überlegungen gerückt. Gleichzeitig zeigen andere internationale Spannungen – etwa im Nahen Osten und im Verhältnis zwischen Israel, den USA und dem Iran –, wie schnell regionale Konflikte globale Auswirkungen entfalten können. In einer vernetzten Welt betreffen politische und militärische Entwicklungen häufig auch jene Systeme, auf die unser Alltag angewiesen ist.

Vor diesem Hintergrund wird deutlich, welche zentrale Rolle der Schutz kritischer Infrastrukturen innehat – also Versorgungssicherheit, Lebensmittelversorgung, Gas, Wasser, Energie, Daten- und Gesundheitsversorgung und vielem mehr. Diese Systeme bilden das Rückgrat moderner Gesellschaften. Wenn sie ausfallen oder beeinträchtigt werden, hat das unmittelbare Folgen für Wirtschaft, Staat und Bevölkerung.

Die Europäische Union hat auf diese veränderte Sicherheitslage mit Initiativen reagiert. Ein wichtiger Baustein sind die NIS2-Richtlinie und das KRITIS-Dachgesetz, die europaweit ein höheres Niveau der Cybersicherheit und der physischen Sicherheit in zentralen

Wirtschafts- und Infrastruktursektoren schaffen sollen. Ziel ist es, Mindeststandards zu etablieren, Verantwortlichkeiten klarer zu definieren und die Zusammenarbeit zwischen Unternehmen, Behörden und europäischen Institutionen zu stärken.

Deutschland arbeitet parallel an einem eigenen gesetzlichen Rahmen, dem KRITIS-Dachgesetz. Es soll bestehende Regelungen bündeln und den Schutz kritischer Infrastrukturen sektorübergreifend weiterentwickeln. Dabei geht es nicht nur um technische Fragen der IT-Sicherheit, sondern auch um organisatorische Resilienz, Krisenvorsorge und die Fähigkeit, auf Störungen schnell und koordiniert zu reagieren.

Ein weiterer Baustein der aktuellen Sicherheitsarchitektur ist der sogenannte OPlan DEU Deutschland. Dieses Konzept beschreibt die zivil-militärische Zusammenarbeit (ZMZ) von Staat, Wirtschaft und Gesellschaft in Krisen- und Verteidigungssituationen. Ziel ist es, Abläufe und Verantwortlichkeiten frühzeitig zu klären und insbesondere die Funktionsfähigkeit kritischer Infrastrukturen auch unter außergewöhnlichen Belastungen sicherzustellen.

Aus Sicht des Bundesverbands für den Schutz Kritischer Infrastrukturen ist diese Entwicklung grundsätzlich zu begrüßen. Die Herausforderungen lassen sich nur in enger Zusammenarbeit zwischen Staat, Wirtschaft und Gesellschaft bewältigen. Kritische Infrastrukturen werden in Deutschland zu einem großen Teil von privaten Unternehmen betrieben. Deshalb ist es entscheidend, dass regulatorische Maßnahmen nicht nur Pflichten definieren, sondern auch Kooperation und Austausch fördern.

Gleichzeitig müssen wir darauf achten, die aktuelle Sicherheitsdebatte mit Augenmaß zu führen. Internationale Krisen dürfen nicht zu überstürzten Entscheidungen oder reflexartigen Reaktionen führen. Sicherheit entsteht nicht durch kurzfristige Maßnahmen allein, sondern durch langfristige Strategien, sorgfältige Planung und kontinuierliche Investitionen in Resilienz.

Gerade in Zeiten erhöhter Aufmerksamkeit ist es wichtig, zwischen notwendiger Vorsorge und unbegründeter Besorgnis zu unterscheiden. Eine resiliente Gesellschaft zeichnet sich dadurch aus, dass sie Risiken erkennt, vorbereitet handelt und zugleich ihre Handlungsfähigkeit bewahrt. Panik oder politischer Kurzschluss helfen in solchen Situationen nicht weiter.

Öffentliche Sicherheit ist zudem nicht allein Aufgabe von Behörden oder Unternehmen. Sie ist ein Gemeinschaftsprojekt. Politik muss verlässliche Rahmenbedingungen schaffen, Unternehmen ihre Systeme widerstandsfähig gestalten und auch die Gesellschaft spielt eine Rolle – etwa durch ein wachsendes Bewusstsein für digitale Sicherheit und verantwortungsbewusstes Verhalten in Krisensituationen.

Der Schutz kritischer Infrastrukturen ist keine kurzfristige Aufgabe, sondern ein dauerhafter Prozess. Er erfordert Innovation, organisatorische Lernfähigkeit und vor allem eine enge Zusammenarbeit zwischen allen relevanten Akteuren.

Öffentliche Sicherheit in einer vernetzten Welt bedeutet daher vor allem eines: aufmerksam bleiben. Risiken frühzeitig erkennen, Strukturen widerstandsfähig gestalten und zugleich die Offenheit unserer Gesellschaft bewahren. Wenn Politik, Wirtschaft und Gesellschaft diese Verantwortung gemeinsam wahrnehmen, können wir den Herausforderungen unserer Zeit mit Besonnenheit begegnen – und mit der Zuversicht, dass Sicherheit und Stabilität auch künftig gewährleistet bleiben.

Text **Holger Berens, Vorstandsvorsitzender des Bundesverbands für den Schutz Kritischer Infrastrukturen e. V. (BSKI)**

Lesen Sie mehr.

Smart Öffentliche Sicherheit.

Verlag und Herausgeber

Smart Media Agency AG, Gerbergasse 5, 8001 Zürich, Schweiz

Redaktion (verantwortlich)
Kevin Meier
Smart Media Agency AG,
Gerbergasse 5, CH – 8001 Zürich
Tel +41 44 258 86 10

Layout (verantwortlich)
Mathias Manner
Smart Media Agency AG,
Gerbergasse 5, CH – 8001 Zürich
Tel +41 44 258 86 10

Anzeigen (verantwortlich)
Jonas Koch
Smart Media Agency AG,
Gerbergasse 5, CH – 8001 Zürich
Tel +41 44 258 86 10

Druckerei
Axel Springer SE

Viel Spaß beim Lesen!
Jonas Koch
Project Manager

Bild iStockphoto/BrianAJackson

Resilienz made in Europe – wie man geopolitische Turbulenzen übersteht

Markus Epner
Leiter der Akademie der F24 AG

Mitarbeitende, deren Einreise an den Grenzen verweigert wird; Zugriffe auf Cloud-Accounts, die ohne Vorwarnung gesperrt werden; internationale Verpflichtungen, die zurückgestellt werden. Solche Szenarien, die einst wie weit hergeholte Krisensimulationen klangen, sind zu plausiblen Stresstests geworden. 2026 sehen sich Risikomanager:innen einer Landschaft mit hoher Dynamik und vernetzten Risiken ausgesetzt. Traditionelles Krisenmanagement bleibt essenziell, reicht aber nicht mehr völlig aus. Eine neue Kernkompetenz wird entscheidend: Resilienz – die Möglichkeit, unter Störungen erfolgreich zu bleiben.

Wenn die Lieferantenbeziehung zum systematischen Risiko wird

Im Jahre 2026 sind Lieferantenökosysteme nicht mehr rein operationelle Abhängigkeiten – sie sind Risikonetzwerke. Geopolitische Fragmentierung, sich schnell ändernde Regulationen und strategische Cyberaktivität können Kettenreaktionen bei Dienstleistern, Regulierungsbehörden und Kunden auslösen. Die Herausforderung ist nicht fehlende Informationen, sondern die organisatorische Fähigkeit, Warnsignale schnell zu interpretieren und selbst mit unvollständigen Informationen sicher zu handeln. Deshalb wird Risikointelligenz zum Erfolgsfaktor: Organisationen brauchen ein gemeinsames Bewusstsein, vom Rechtsteam über die IT bis zur Einkaufsabteilung. Wenn Risiken systematisch sind, werden die Silos selbst zum Risiko.

Technologie als geopolitisches Instrument und KI als Beschleuniger

Eine stabile digitale Infrastruktur ist heute eine unternehmerische Voraussetzung. Die Cyberkriminalität bleibt die größte Bedrohung für Unternehmen und wird zunehmend professioneller. Angreifer:innen nutzen automatisierte Informationsbeschaffung, während durch KI Desinformation und »Social Engineering« verstärkt werden. Gleichzeitig wird Governance schwieriger: Innovationszyklen verkürzen sich und Technologie ist kein neutrales Werkzeug mehr – sie ist Effizienztreiber, Risikoquelle und Machtinstrument zugleich. Die Schlussfolgerung ist klar: Resilienz erfordert kontinuierliche Überwachung und Früherkennung von »unsichtbaren« Risiken – von Kompromittierungen bei Lieferanten über schleichende Zugangsbeschränkungen bis hin zu politischen Kurswechseln oder langfristiger Infiltration kritischer Infrastrukturen.

Vertrauen wird zum Kontrollziel

2026 können politische Ankündigungen störende Effekte haben, noch bevor sie in Kraft treten. Sie wirken sich auf Planungssicherheit, Compliance und Datenschutz aus. Deshalb wird Vertrauen zum Kontrollziel – nicht nur Vertrauen in die technischen Fähigkeiten der Dienstleister, sondern auch in deren operationelle und regulatorische Umgebung.

Für Führungskräfte stellt sich die Frage: Wo sind wir Instabilitäten ausgesetzt, auf die wir keinen Einfluss haben, und wo können wir Stabilität in unser Ökosystem einbauen?

Stabilität als Fundament für Resilienz

Es gibt zwar kein einheitliches Konzept, das für alle Fälle passt, aber die zukünftige Risikologik basiert auf einem einheitlichen Grundsatz: Man muss Stabilität wo immer möglich sicherstellen – aber auch die Fähigkeit haben, schnell zu reagieren, wenn dies eben nicht möglich ist.

Pragmatische Lösungsschritte:

- **Analyse der digitalen und analogen Infrastruktur:** Unternehmenskritische Schnittstellen, Problempunkte und neu auftretende Schwachstellen müssen identifiziert werden. Dies nicht nur in der Technologie – Verträge, Lieferketten, Zugriffsrechte und Sensibilisierung der Belegschaft sind ebenso wichtig.

- **Geschwindigkeit in der Entscheidungstreffung:** Es braucht Prozesse, die Signale schnell verifizieren und schnelle Reaktionen ermöglichen können, auch wenn noch nicht alle Informationen vorhanden sind. 2026 ist Geschwindigkeit wichtiger als Vollständigkeit.

- **Reduktion systemischer Lücken:** Hier helfen Partner:innen mit bewiesener Verlässlichkeit, Rechenschaft, transparenten Operationen und stabilen Sicherheitsstandards.

- **Plan für Kaskadeneffekte:** Testszenarien, in denen rechtliche Änderungen, Sanktionen, Marktverzerrungen oder Lieferausfälle einen messbaren Effekt auf Compliance, Verfügbarkeit und die Kundschaft haben, müssen erarbeitet werden.

In Europa kaufen – Beschaffung als Resilienzhebel

Der Beschaffungsprozess kann die Verwundbarkeit eines Unternehmens wesentlich beeinflussen. Die Priorisierung europäischer Lieferanten kann geopolitische und regulatorische Gefahren reduzieren – besonders für unternehmenskritische Systeme. Wenn die Fähigkeit, Gefahren vorherzusehen, abnimmt, wird Optimierung durch Resilienz ersetzt. Die Beschaffung ist eine der schnellsten Möglichkeiten, das eigene Fundament zu verlagern.

Vorteile der europäischen Beschaffung:

- **Dateneigentum und -sicherheit:** Europäische Dienstleister arbeiten unter den gesetzlichen Richtlinien und Erwartungen der EU, was eine bessere Kontrolle über sensible Daten ermöglicht und Haftungsrisiken minimiert.

- **Regulatorische und rechtliche Stabilität:** Die rechtlichen Rahmen und Prozesse der EU bieten eine höhere Vorhersehbarkeit für Resolutionen, Pflichten und die Sicherstellung der Compliance.

- **Reduziertes Risiko von Regulationskonflikten:** Für Organisationen, die von DORA, NIS2, KRITIS und GDPR betroffen sind, helfen Lieferanten mit etablierten Compliance-Strukturen Friktionen, Lücken und vertragliche Unsicherheiten zu minimieren.

- **Verlässlichkeit und Nähe:** Kürzere Eskalationswege, konsistente Teams und dieselben Zeitzonen unterstützen schnellere Reaktionen bei Krisen und die tägliche Resilienz.

- **Transparenz und Kooperation:** 2026 wird Kooperation selbst zu einem Resilienzfaktor. Europäische Ökosysteme, einheitliche Standards und grenzübergreifende Kollaborationen stärken die gemeinsame Intelligenz und koordinierte Handlungsfähigkeit.

Resilienz von der Absicht zur Ausführung

Im Jahre 2026 ist Resilienz kein Notfallrucksack für den Krisenfall, sondern ein kontinuierliches Operationsmodell: Frühwarnsysteme, Risikoerkennung und koordinierte Antworten – regelmäßig geprobt. Probleme eskalieren schneller und bestrafen langsame Koordination. Governance wird persönlicher, da Führungsverantwortung und Haftung zusammenwachsen. Deshalb sind Dokumentation und wiederholbare Entscheidungsprozesse nicht mehr wegzudenken.

Eine neue Perspektive: Unsicherheit zur Möglichkeit machen

Der ständige geopolitische und technologische Wandel ändert den Krisenmodus zur Grundeinstellung. Der Vorteil ist, dass Unternehmen, die in Resilienz investieren, sich abheben können – weil sie Gefahren früher erkennen und verfügbar bleiben, während andere ins Stocken geraten.

Nun ist es Zeit für einen Resilienzcheck: Verantwortlichkeiten klären, die Lieferkette testen und die Beschaffung strategisch verändern, um jene Verwundbarkeiten zu reduzieren, auf die man keinen direkten Einfluss hat.

Mit Krisen leben – Was ist Resilienz?

Resilienz ist die Fähigkeit, trotz Rückschlägen erfolgreich zu bleiben, sich anzupassen und den Betrieb fortzusetzen. In den letzten 20 Jahren hat sich der Fokus vom Incident-Management auf das Krisenmanagement und die Sicherstellung der Geschäftskontinuität verlegt. Im Jahr 2026 setzt sich diese Entwicklung fort: Die entscheidende Herausforderung ist nicht ein einzelnes »Top-Risiko«, sondern die Grenzen traditioneller Modelle, die von stabilen Wahrscheinlichkeiten und isolierten Szenarien ausgehen. Resiliente Organisationen stellen kontinuierliche Überwachung und geübte Reaktionsprozesse sicher. Sie akzeptieren, dass die Vorhersehbarkeit abnimmt, sind gegen Kettenreaktionen gewappnet und optimieren ihre Anpassungsfähigkeit. Wahre Resilienz kombiniert Flexibilität, technische Robustheit und ein lernbereites Mindset.

Weitere Informationen unter:
f24.com

25 YEARS F24

Markus Ebner verfügt über umfangreiche Erfahrung in den Bereichen Sicherheit und Krisenmanagement. Er diente während der Bosnien- und Kosovokriege als Offizier bei den Spezialeinheiten und war über zwei Jahrzehnte lang in Führungspositionen in der Wirtschaft tätig, vor allem bei der Lufthansa und bei Boehringer Ingelheim. Markus hat Abschlüsse in Sicherheits- und Krisenmanagement von der Universität Kiel sowie in Sicherheits- und Krisenstudien von der Polizeihochschule Schleswig-Holstein.

KRITIS neu denken

Kritische Infrastruktur wurde lange vor allem als IT-Thema verhandelt. Im Zentrum standen Firewalls, Netzwerke und die Abwehr digitaler Angriffe. Mit dem KRITIS-Dachgesetz verschiebt sich dieser Blick. Entscheidend ist nicht mehr nur, ob Systeme digital abgesichert sind, sondern ob Anlagen, Standorte und Abläufe auch dann funktionieren, wenn die Lage unübersichtlich wird. Der Bundesrat hat dem Gesetz am 6. März 2026 zugestimmt. Damit gelten erstmals bundeseinheitliche und sektorübergreifende Mindeststandards für den Schutz kritischer Infrastrukturen in Deutschland.

Mehr als Cybersicherheit

Gemeint ist keine Abkehr vom bisherigen IT-Sicherheitsrecht, sondern seine Erweiterung. Die NIS2-Richtlinie schärft die Cybersicherheitsanforderungen, die CER-Richtlinie richtet den Fokus auf die Resilienz kritischer Einrichtungen. Gemeint ist damit die Fähigkeit, wesentliche Dienstleistungen nicht nur vor Angriffen zu schützen, sondern sie auch bei Störungen aufrechtzuerhalten und nach Vorfällen wiederherzustellen. Genau an dieser Schnittstelle setzt das KRITIS-Dachgesetz an: Es ergänzt die bestehenden Regeln zur IT-Sicherheit um Vorgaben für den physischen Schutz und die Belastbarkeit des Betriebs.

Wer unter das Gesetz fällt

Greifbar wird das dort, wo der Staat den Kreis der betroffenen Einrichtungen neu bestimmt. Erfasst werden kritische Anlagen aus elf Sektoren: Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheit, Trinkwasser, Abwasser, Siedlungsabfallentsorgung, Informationstechnik und Telekommunikation, Ernährung, Weltraum sowie die öffentliche Verwaltung. Eine Einrichtung gilt dabei nur dann als kritisch, wenn sie für die Gesamtversorgung essenziell ist und mehr als 500 000 Personen versorgt. Das zeigt: Es geht nicht um wenige Hochsicherheitsbereiche, sondern um die Versorgung des Alltags – vom Stromnetz bis zur Verwaltung.

Vom Schutz einzelner Systeme zum Schutz des Betriebs

Die eigentliche Neuerung liegt weniger in der Liste der Sektoren als in der Logik des Gesetzes. Geschützt werden soll nicht mehr nur die digitale Infrastruktur eines Betriebs, sondern seine Handlungsfähigkeit insgesamt. Die Bundesregierung nennt dafür konkrete Beispiele: Notfallteams, stärkerer Objektschutz und Maßnahmen zur Ausfallsicherheit. Hinzu kommen Risikoanalysen und Risikobewertungen, die staatliche Stellen erarbeiten und den Betreibern zur Verfügung stellen, sowie eine Meldepflicht für Vorfälle. Sicherheit wird damit nicht nur daran gemessen, ob ein Angriff abgewehrt wird, sondern auch daran, ob ein Betrieb Ausfälle abfangen, Störungen einordnen und zentrale Leistungen weiterführen kann.

Bild **iStockphoto/Kobus Louw**

» Das BSI beschreibt die IT-Sicherheitslage in Deutschland 2025 weiterhin als angespannt.

Diese Verschiebung trägt einer Realität Rechnung, die in vernetzten Infrastrukturen längst Alltag ist. Fällt Energie aus, geraten Kommunikation und Verkehr unter Druck. Werden Kommunikationswege unterbrochen, wird Krisenkoordination schwieriger. Stockt Verwaltung, verlangsamt sich oft auch die Reaktion auf Störungen in anderen Bereichen. Die CER-Richtlinie stellt deshalb bewusst nicht nur auf Verhinderung ab, sondern auf Vorsorge, Reaktion und Wiederherstellung. Resilienz meint in diesem Sinne die Fähigkeit, Belastungen zu absorbieren, sich anzupassen und den Betrieb zurück in einen stabilen Zustand zu führen.

Neue Pflichten, neue Verantwortung

Für Betreiber kritischer Infrastruktur bleibt das nicht folgenlos. Im parlamentarischen Verfahren wurde das Gesetz noch ergänzt: Die Bundesländer können zusätzliche kritische Anlagen identifizieren, wenn die betreffenden Dienstleistungen allein in ihre Zuständigkeit fallen. Zudem soll das Gesetz bereits nach zwei Jahren evaluiert werden. Das spricht dafür, dass der Rechtsrahmen nicht als starres Endprodukt gedacht ist, sondern als Instrument, das auf neue Risiken und neue Abhängigkeiten reagieren muss.

Parallel dazu verschärft NIS2 die organisatorische Verantwortung. Das BSI beschreibt die Umsetzung als Projekt für das gesamte Unternehmen und betont, dass die Geschäftsleitung die rechtlichen Anforderungen umsetzen und überwachen muss. Sicherheit wird damit zur Führungsaufgabe – nicht nur in der IT, sondern auch im Betrieb, in der Krisenkommunikation und in der Organisation von Zuständigkeiten. Gerade darin liegt der tiefere Wandel: Resilienz entsteht nicht durch eine einzelne Schutzmaßnahme, sondern durch das Zusammenspiel aus Technik, Prozessen, Vorbereitung und klarer Verantwortung.

Ein Gesetz für eine verletzliche Gegenwart

Dass dieser breitere Ansatz gerade jetzt kommt, ist kein Zufall. Das BSI beschreibt die IT-Sicherheitslage in Deutschland 2025 weiterhin als angespannt. Zugleich wächst die Einsicht, dass sich kritische Dienstleistungen nicht allein durch digitale Schutzschichten absichern lassen. Wer Strom, Wasser, Gesundheit, Kommunikation oder Verwaltung schützen will, muss das Ganze in den Blick nehmen: Systeme, Standorte, Personal, Meldewege und die Fähigkeit, auch unter Druck handlungsfähig zu bleiben. Genau darin liegt die eigentliche Aussage des KRITIS-Dachgesetzes. Es verschiebt den Fokus vom reinen IT-Schutz hin zu einer umfassenderen Resilienzlogik – und macht Widerstandsfähigkeit damit zur neuen Leitidee kritischer Infrastruktur.

Text **Walter Nogueira**

»Wie moderne Energietechnik das Rückgrat unserer Sicherheit stärkt«

Kritische Infrastruktur muss immer verfügbar sein – im Falle von Rechenzentren bedeutet das unter anderem die unterbrechungsfreie Versorgung mit elektrischer Energie. Was früher als Nischenthema der IT galt, entscheidet heute über die Stabilität moderner Staaten. Welche technischen und strategischen Weichen nun gestellt werden müssen, erläutert Adrian Guggisberg, Präsident Distribution Solutions bei ABB.

Adrian Guggisberg
Präsident Distribution Solutions, ABB

Herr Guggisberg, Datenzentren galten lange als technische Spezialthemen. Warum sprechen wir heute im Kontext öffentlicher Sicherheit über sie und mit welchen Fragestellungen sehen Sie sich als Technologiekonzern mit Schwerpunkt Energie- und Automatisierungstechnik konfrontiert?
Rechenzentren bilden längst das funktionale Rückgrat moderner Gesellschaften. Ein Ausfall von Rechenzentren kann in kürzester Zeit Folgen für zentrale gesellschaftliche Abläufe haben, weshalb für sie die grundlegende Anforderung für kritische Infrastruktur gilt: maximale Verfügbarkeit. Mit wachsender Größe und Leistung steigt jedoch nicht nur ihre Bedeutung, sondern auch die Komplexität – etwa bei der schnellen Umsetzung, der Sicherstellung optimaler Verfügbarkeit und einer zugleich praktikablen Skalierbarkeit. Für genau diese Aufgabenstellungen erarbeiten wir gemeinsam mit Marktteilnehmern aus den Bereichen Rechenzentren, Energieversorgung und Netzbetrieb Lösungen.

Welche Anforderungen ergeben sich aus den zuvor genannten Themen für die unterschiedlichen Interessensgruppen?
Die Anforderungen gehen schon lange über die reine Produktlieferung hinaus. Die konzeptionelle Phase beginnt deutlich früher und ist entscheidender als eine nachgelagerte Produktoptimierung. In dieser Phase wird die Energieversorgungsarchitektur für die geforderte Performance erarbeitet. Dabei sind unter anderem der stetig steigende Energieverbrauch pro Quadratmeter Serverfläche zu berücksichtigen, ebenso wie Ausfallsicherheit, Energieeffizienz und der Energiebezug am Netzanschlusspunkt. Hier erfolgt der Schulterschluss mit den zuständigen Netzbetreibern: Wir unterstützen Rechenzentren dabei, auch für die Zukunft skalierbar zu sein, ohne das Netz und nachgelagerte Anlagen über ihre Grenzen hinaus zu belasten. Idealerweise werden sie sogar zu netzdienlichen Teilnehmern.

Können Sie das etwas mehr im Detail erläutern?
Zukünftige Chip-Technologien benötigen immer mehr Energie auf immer engerem Raum. Diese Energieversorgung ist zwangsläufig mit Verlusten verbunden, die aus wirtschaftlichen wie technischen Gründen minimiert werden müssen. Abwärme bedeutet dabei nicht nur unnötige Energieverluste, sondern belastet auch die Komponenten und mindert die Zuverlässigkeit der Systeme.

Vor diesem Hintergrund arbeiten wir an der Entwicklung künftiger Gleichstromtechnologien, die insbesondere für die Energieversorgung dynamischer KI-Workloads als Ergänzung zu bestehenden Wechselstromsystemen benötigt werden. Innerhalb des Rechenzentrums lässt sich die Verfügbarkeit durch verschiedene Maßnahmen maximieren: durch redundante Auslegung der Systeme, vorausschauende Diagnose und den Einsatz hochverfügbarer Betriebsmittel. Es geht vor allem darum, eventuelle Ausfälle örtlich einzugrenzen, sodass die gesamte Anlage weiterlaufen kann.

Ein spezielles Dilemma entsteht beim Netzanschluss: Rechenzentren wachsen schrittweise über Jahre. Damit dies möglich ist, muss die Leistung am Anschlusspunkt ebenso wachsen. Damit wächst aber auch die sogenannte Kurzschlussleistung, die für den Schutz der angeschlossenen Verbraucher problematisch werden kann. Hierfür bieten wir marktführende Technologien, die sowohl eine hohe Flexibilität beim Netzausbau als auch modulare Konzepte für die Rechenzentrumsbetreiber ermöglichen.

Was Ihren letzten Punkt – die Bedeutung eines Rechenzentrums beim Netzanschluss – anbetrifft: Wie sehen Sie Rechenzentren im größeren Kontext der Infrastruktur?
Rechenzentren werden zu Großverbrauchern: Laut der Internationalen Energieagentur (IEA) wird sich ihr weltweiter Strombedarf in den nächsten fünf Jahren mehr als verdoppeln. Einzelne Anlagen für KI-Anwendungen benötigen künftig so viel Energie wie eine größere Stadt. Das erfordert eine intelligente Integration ins Energiesystem, insbesondere im Zusammenspiel mit erneuerbaren Energien und Batteriespeichern. Intelligente Systeme sind erforderlich, um bestehende Infrastrukturen besser und effizienter auszunutzen, ohne dabei die Verfügbarkeit der elektrischen Energie zu beeinträchtigen. Hier zeigt sich noch erheblicher Innovationsbedarf, wie etwa der großflächige Stromausfall in Spanien im Jahr 2025 gezeigt hat.

Bei ABB arbeiten wir daher sowohl an digitalen Lösungen zur frühzeitigen Erkennung von Problemen als auch an innovativen Lösungen, die gezielte Eingriffe ermöglichen und die Stabilität des Gesamtsystems systematisch verbessern.

In diesem Kontext können Rechenzentren künftig auch eine netzstabilisierende Rolle übernehmen, indem die ursprünglich nur für den Inselbetrieb vorgesehene unterbrechungsfreie Notstromreserve auch im angrenzenden Mittelspannungsverteilnetz genutzt werden kann. Diese Funktionalität könnte in Zukunft ähnlich wie netzdienliche Gaskraftwerke einen Beitrag zur sicheren Energieversorgung leisten.

Wie wichtig ist es für die Ausfallsicherheit kritischer Infrastruktur, dass Schlüsseltechnologien in Deutschland entwickelt und getestet werden?
Für die Resilienz kritischer Infrastruktur ist es wichtig, kritisches Wissen gezielt aufzubauen und dauerhaft zu erhalten. Systeme für Rechenzentren müssen auch unter Extrembedingungen zuverlässig funktionieren – dafür braucht es spezifische Entwicklungs- und Testkompetenz. In Ratingen betreiben wir eines der weltweit größten Kompetenzzentren für Mittelspannungstechnik. Dort simulieren wir verschiedenste Extremsituationen – auch solche, die den enormen Leistungsbedarf eines Rechenzentrums in kritischen Momenten nachbilden. Unsere Schaltanlagen müssen solche Situationen innerhalb von Sekundenbruchteilen sicher beherrschen. Diese Expertise – Made in Germany – ist unser Beitrag zum sicheren und nachhaltigen Betrieb kritischer Infrastruktur.

> **Für die Resilienz kritischer Infrastruktur ist es wichtig, kritisches Wissen gezielt aufzubauen und dauerhaft zu erhalten. Systeme für Rechenzentren müssen auch unter Extrembedingungen zuverlässig funktionieren.**
>
> – Adrian Guggisberg, Präsident Distribution Solutions, ABB

Über ABB
ABB ist ein führendes globales Technologieunternehmen in den Bereichen Elektrifizierung und Automation, das eine nachhaltigere und ressourceneffizientere Zukunft ermöglicht. Durch die Verbindung von technischer Expertise und Digitalisierung sorgt ABB dafür, dass Industrien hohe Leistungen erbringen und gleichzeitig effizienter, produktiver und nachhaltiger werden, um ihre Ziele zu übertreffen. Bei ABB nennen wir das »Engineered to Outrun«.

ABB-Technologie sichert Planung und Betrieb von Rechenzentren
Eine Vielzahl von Rechenzentren weltweit setzt auf Technologie von ABB. Ob Cloud-Anwendungen oder KI-Infrastrukturen im Gigawatt-Maßstab – gemeinsam mit unseren Kunden und Partnern realisieren wir die elektrotechnische Infrastruktur für hochmoderne, zuverlässige Rechenzentren. Unsere global erprobten und lokal entwickelten Lösungen sorgen dafür, dass diese effizient und stabil betrieben werden können. Von der Energie- bis zur Leittechnik investiert ABB in Menschen, Technologien und lokale Präsenz, damit Rechenzentren der nächsten Generation jederzeit genau das haben, was sie brauchen.

Besuchen Sie uns auf der Data Centre World in Frankfurt, Stand K130 (6.–7. Mai, 2026)

Weitere Informationen unter:

Sicherheit als Lösung – nicht als Produkt

Kritische Infrastrukturen, komplexe Gebäudestrukturen und neue Anforderungen an den Zutritt verändern den Sicherheitssektor spürbar. Roberto Creutziger, Leiter Vertrieb Gemos bei BKS GmbH, und Dirk Wellsow, Produktmanager für elektronische Schließsysteme, sprechen über die wachsende Verzahnung von physischer Sicherheit und IT-Lösungen über die Rolle integrierter Systeme – und darüber, weshalb Sicherheit heute weit über einzelne Komponenten hinausgeht.

Roberto Creutziger
Leiter Vertrieb Gemos

Dirk Wellsow
Produktmanager für elektronische Schließsysteme

Wo liegen für Unternehmen und Einrichtungen aktuell die größten Herausforderungen beim Schutz kritischer Infrastrukturen?
Creutziger: Die größte Herausforderung ist aus meiner Sicht, dass physische Sicherheit und IT-Sicherheit nicht mehr getrennt betrachtet werden können. Genau diese stärkere Verzahnung erhöht den Handlungsdruck. Hinzu kommen hohe Investitionen, weil es im KRITIS-Umfeld oft nicht nur um einzelne Gebäude, sondern um weitläufige Anlagen geht, die umfassend abgesichert werden müssen. Gleichzeitig steigen die administrativen Anforderungen, etwa bei Meldeketten, Dokumentationspflichten und Haftungsfragen. Viele Unternehmen stellen erst jetzt fest, dass sie von diesen Vorgaben überhaupt betroffen sind, obwohl ihnen dafür oft noch die nötigen Strukturen und Ressourcen fehlen.

Wie hilft Gemos dabei, komplexe, heterogene Systemlandschaften zusammenzuführen?
Creutziger: Die Stärke von Gemos liegt vor allem darin, dass wir unterschiedliche Gewerke und Fabrikate herstellerneutral auf einer Oberfläche zusammenführen können. Statt zwischen verschiedenen Systemen zu wechseln, arbeiten die Nutzenden mit einer einheitlichen, intuitiven Benutzeroberfläche und klar definierten Abläufen. Das ist besonders dann entscheidend, wenn schnell gehandelt werden muss. Lagepläne, automatisierte Workflows und dokumentierte Maßnahmenketten helfen dabei, Übersicht zu schaffen und Prozesse verlässlich umzusetzen. Gerade für KRITIS-Betreiber ist das ein großer Vorteil, weil aus vielen Einzelsystemen ein integrierter Handlungsrahmen wird. Gleichzeitig reduziert das die Komplexität im Alltag und hilft dabei,

auch in Stresssituationen strukturierter und fehlerfrei zu handeln. Wichtig – BKS begleitet die Unternehmen bei der Planung und Implementierung des Systems durchgängig.

Viele Lösungen von BKS sind auch klassisch mechanisch. Wo gewinnt Elektronik heute an Bedeutung?
Wellsow: Elektronik spielt auch bei klassischen Schließlösungen eine immer größere Rolle. Besonders relevant sind hybride Lösungen, also die Verbindung mechanischer und elektronischer Komponenten. Damit lassen sich Zutrittsrechte deutlich flexibler steuern, etwa bei zeitlich begrenzten Berechtigungen, wechselnden Nutzergruppen oder in Bereichen mit erhöhten Sicherheitsanforderungen oder auch ganz einfach über elektronische Kontakte im Türschloss, ob eine Tür verriegelt ist oder nicht. Solche Lösungen spielen ihre Vorteile auch im Rahmen von Modernisierungen in Bestandsgebäuden aus. Hinzu kommen smarte mobile Anwendungen, bei denen das Smartphone selbst zum Schlüssel wird – wie beispielsweise unsere ixalo | key App sowie Cloud-basierte Lösungen, die Verwaltung und Updates vereinfachen. Das ist vor allem dort sinnvoll, wo hohe Sicherheitsanforderungen bestehen oder bestehende Infrastrukturen nicht von heute auf morgen komplett ersetzt werden können. Aus meiner Sicht geht es dabei nicht nur um Komfort, sondern auch um mehr Flexibilität, bessere Steuerbarkeit und langfristig oft um wirtschaftliche Vorteile.

Interview **Walter Nogueira**

Das ganze Interview unter:
bks.de

Die systemkritische Rolle von Erdgasspeichern in Deutschland

Im Interview beleuchtet Daniel Mercer, Geschäftsführer der Storengy Deutschland GmbH, die zentrale Rolle der Erdgasspeicher und zeigt auf, warum jetzt die Weichen für eine erfolgreiche Wasserstoffzukunft gestellt werden müssen.

Daniel Mercer
Geschäftsführer

Herr Mercer, Erdgas ist nach wie vor ein zentrales Fundament der deutschen Wärmeversorgung und spielt gerade in den Wintermonaten eine essenzielle Rolle. Ist die Versorgungssicherheit in Deutschland zum jetzigen Zeitpunkt gewährleistet?
Für den Moment lässt sich diese Frage bejahen, doch die Antwort verlangt nach einer differenzierten Einordnung. Der britische Wirtschaftswissenschaftler Dieter Helm definiert Versorgungssicherheit als die »ununterbrochene Verfügbarkeit von Energie zu einem Preis, den die Kunden sowohl fähig als auch bereit sind zu zahlen«. Obwohl die gesetzlich vorgeschriebenen Mindestfüllstände, wie etwa die 30-Prozent-Marke zum 1. Februar, formal eingehalten werden konnten, muss man die Versorgungslage im Winter 2025/26 dennoch als äußerst angespannt bezeichnen. Und die Rahmenbedingungen werden zusehends schwieriger.

Dank LNG-Importen (Liquefied Natural Gas) über den Wasserweg konnte eine Mangellage verhindert werden. Ist dieses System zukunftsfähig?
Nein. Erdgasspeicher sind systemisch schlicht nicht durch Importe ersetzbar. 2022 kam es zu einem massiven Preissprung, da die Kosten für die Umleitung von LNG-Ladungen deutlich über denen von Pipelinegas lagen. Es war eine brutale Situation, die wir nur mit der »großen Preiskeule« meistern konnten. Mittelfristig ist dies ein Modell, das wir uns ökonomisch nicht leisten können. Zwar wird es kaum dazu kommen, dass die Menschen im Winter in ihren Wohnungen frieren müssen, doch der eigentliche Impact manifestiert sich anderswo: Steigen die Gaspreise dauerhaft, verlieren wir industrielle Kapazitäten. Dieser Substanzverlust im Industriesektor ist in Deutschland bereits spürbar und gefährdet somit direkt unsere wirtschaftliche Sicherheit.

Storengy ist mit fünf Speicherstandorten und einem Arbeitsgasvolumen von 1,6 Milliarden Kubikmetern ein Schwergewicht in der deutschen Speicherung. Welche Auswirkungen hat Ihre Arbeit auf diese prekäre Lage?
Die Regierung muss jetzt die passenden Weichen stellen und stärkere Anreize

für den Bau zusätzlicher Wasserstoffspeicher setzen, damit die Energiewende gelingt. Untergrundspeicher können erneuerbare Energieüberschüsse aus dem Sommer in den Winter übertragen.

Könnte der viel zitierte »Wasserstoffhochlauf« hier eine Linderung bringen? Schließlich soll der Aufbau einer Wasserstoffwirtschaft die Dekarbonisierung der Industrie beschleunigen.
Durchaus, doch man darf nicht vergessen: Auch der Wasserstoffhochlauf wird ohne massive Speicherlösungen nicht gelingen. Wir benötigen große saisonale Speicher, um Angebot und Nachfrage effizient zu synchronisieren. Aktuelle Studien prognostizieren für Deutschland bis zum Jahr 2045 einen Bedarf von bis zu 80 TWh an Wasserstoffspeicherkapazität. Storengy geht hier bereits voran: Mit dem Projekt »SaltHy« in Harsefeld entwickeln wir eine der ersten Wasserstoffkavernen Deutschlands. Wir haben bereits mit der Genehmigungsarbeit begonnen, da hier ein klarer Anreiz zur Umsetzung besteht. Norddeutschland hat das Potenzial, zur »Batterie Europas« zu werden – vorausgesetzt, die regulatorischen und finanziellen Rahmenbedingungen werden jetzt zügig geschaffen. Daher ergeht erneut der dringende Appell an die Politik, die notwendigen Anreize zu setzen. Die Marktteilnehmer, und somit auch wir von Storengy, stehen bereit.

Weitere Informationen unter:
storengy.de

Warum dynamische Schutzkonzepte und neue Managementkonzepte jetzt über Resilienz entscheiden

Europas Kritische Infrastrukturen verändern sich in einer zunehmend unsicheren Welt – und zwingen Führungskräfte zum Umdenken. Sicherheit wird damit zur Managementaufgabe.

Stromausfälle, Cyberangriffe, geopolitische Spannungen: Europas Kritische Infrastrukturen (KRITIS) wie Energieversorgung, Kommunikationsnetze, Verkehrswege und Rechenzentren stehen zunehmend unter Druck. Unsicherheit ist keine Ausnahme mehr, sondern Teil der neuen Realität. Umso wichtiger ist es, diese lebenswichtigen Systeme so aufzustellen, dass sie auch unter veränderten Rahmenbedingungen zuverlässig funktionieren. Resilienz bedeutet genau das: handlungsfähig zu bleiben, selbst wenn Stabilität nicht mehr selbstverständlich ist.

Wirtschaftliche Stärke, politische Handlungsfähigkeit und gesellschaftliche Stabilität hängen maßgeblich von der Verfügbarkeit Kritischer Infrastruktur ab. Doch diese entsteht nicht zufällig. Sie ist das Ergebnis strategischer Planung, klar definierter Betriebsmodelle und der Fähigkeit, Schutzkonzepte laufend an neue Bedrohungslagen anzupassen.

Sicherheit wird in dieser volatilen Umwelt zur Aufgabe der Unternehmensführung. Investitionsentscheidungen, Organisationsstrukturen und der Einsatz neuer Technologien bestimmen maßgeblich, wie resilient Unternehmen und Infrastrukturen tatsächlich sind.

Neue Risiken verlangen neue Schutzkonzepte

Das Sicherheitsmanagement von Unternehmen befindet sich daher in einem tiefgreifenden Wandel. Starre Konzepte stoßen zunehmend an ihre Grenzen und werden durch dynamische Ansätze ergänzt. Cyber- und physische Sicherheit wachsen zusammen – während der Kostendruck steigt. Für Betreiber bedeutet das konkret: Sicherheitsmaßnahmen müssen wirksamer und zugleich wirtschaftlicher werden. Innovative Technologien und neue Bewertungsmodelle für Investitionen gewinnen deshalb an Bedeutung. Besonders deutlich zeigt sich dieser Bedarf bei weit verteilten kritischen Anlagen wie Umspannwerken.

»Gerade bei abgelegenen Standorten sind schnelle Interventionen im Ereignisfall schwierig. Zudem sind klassische Ansätze der individuellen Planung und Umsetzung sicherheitstechnischer Anlagen oft zeit- und kostenintensiv«, erklärt Tristan Haage, Co-Geschäftsführer von e-shelter security.

Technologie reduziert Komplexität

Neue technologische Ansätze ermöglichen es, Sicherheit effizienter und skalierbarer zu organisieren. »Wir entwickeln standardisierte Komplettlösungen für den Schutz Kritischer Infrastrukturen. Auf Basis erprobter ›Good Practices‹ lassen sich Konzepte schneller umsetzen und effizienter betreiben. KI-gestützte Systeme helfen zudem, Risiken frühzeitig zu erkennen, ohne dass Betreiber komplexe Einzellösungen aufwendig integrieren müssen«, ergänzt Christian Meine, Co-Geschäftsführer von e-shelter security.

Allerdings erhöhen technologische Innovationen nicht nur die Effizienz, sondern eröffnen auch neue Angriffsflächen. Damit steigen die Anforderungen an die Technologie- und Regulierungskompetenz auf Führungsebene. Neue Lösungen müssen nicht nur hinsichtlich ihrer Leistungsfähigkeit bewertet werden, sondern unterliegen zunehmend selbst regulatorischen Vorgaben – etwa im Bereich künstlicher Intelligenz und Datenschutz. Gleichzeitig wächst der regulatorische Druck auf die Betreiber Kritischer Infrastruktur. Sicherheit wird so endgültig zu einer Führungsaufgabe, die strategisches Denken, technologische Expertise und regulatorisches Verständnis gleichermaßen erfordert. Neue gesetzliche Vorgaben beschleunigen diese Entwicklung zusätzlich.

Regulierung erhöht den Handlungsdruck

Die verschärfte Bedrohungslage führt zu einem deutlich strengeren regulatorischen Rahmen. Mit der europäischen Cybersicherheitsrichtlinie NIS-2 werden nicht nur Verantwortung, sondern auch Haftungsrisiken für Geschäftsleitungen ausgeweitet. Auch nationale KRITIS-Regelungen sowie bekannte Standards wie der BSI-IT-Grundschutz erhöhen die Anforderungen an Dokumentation, Auditierbarkeit und kontinuierliches Risikomanagement.

Zudem rücken regulatorische Initiativen jetzt verstärkt physische Schutzaspekte in den Fokus. Mit dem KRITIS-Dachgesetz wird die EU-CER-Richtlinie in nationales Recht umgesetzt. Betreiber müssen Risiken künftig beispielsweise systematisch analysieren, geeignete Maßnahmen nachweisen und Störungen strukturiert melden. So werden regelmäßige Überprüfungen zu zentralen Anforderungen moderner Sicherheitsorganisationen – und damit zu einem Thema auf Managementebene.

Fragmentierte Sicherheitsstrukturen werden zum Risiko

In vielen Organisationen sind Sicherheitsstrukturen historisch gewachsen. Zutrittskontrolle, Videoüberwachung, Perimeterschutz oder Brandmeldetechnik wurden über Jahre hinweg getrennt beschafft und betrieben. Entsprechend fragmentiert sind häufig auch Verantwortlichkeiten und Prozesse.

In der neuen Sicherheitsrealität entscheidet jedoch weniger die Leistungsfähigkeit einzelner Technologien über den Schutz kritischer Anlagen als deren Integration in Prozesse, Managementstrukturen und klare Zuständigkeiten.

»Wir beobachten einen klaren Trend zu integrierten digitalen Gefahrenmanagementsystemen. Sie verbinden unterschiedliche Einzellösungen und ermöglichen einen effizienteren Umgang mit Vorfällen. Gleichzeitig lassen sich regulatorische Anforderungen an Auditierbarkeit und Reporting besser erfüllen«, sagt Tristan Haage. »Risiken entstehen heute vor allem dort, wo Systeme nicht in eine übergeordnete Sicherheitsarchitektur eingebettet sind.«

Sicherheit wirtschaftlich organisieren

Der Aufbau robuster Schutzstrukturen ist kein einmaliges Projekt, sondern ein fortlaufender Prozess. Für die Betreiber Kritischer Infrastruktur bedeutet das steigende Anforderungen / doppelte Herausforderungen – organisatorisch wie wirtschaftlich. Die Modernisierung von Sicherheitskonzepten erfordert Investitionen, gleichzeitig wächst der Druck, diese effizient einzusetzen.

Neue Betriebsmodelle wie Managed Security-Services können Unternehmen spürbar entlasten. Sicherheitsleistungen werden dabei kontinuierlich und vertraglich geregelt bereitgestellt – ähnlich wie bei etablierten Software-as-a-Service-Modellen. Dadurch lassen sich etwa Lifecycle-Management, Zutrittskontrolle oder Besuchermanagement zentral organisieren und präzise steuern.

»Wir empfehlen Unternehmen, mit einem strukturierten Health-Check zu beginnen. Innerhalb weniger Wochen lassen sich so in der Regel kritische Assets und Schutzziele identifizieren und konkrete Handlungsbedarfe ableiten«, rät Christian Meine.

Resilienz strategisch steuern

Denn die Fähigkeit, auch unter unsicheren Bedingungen handlungsfähig zu bleiben, wird zu einem entscheidenden Faktor für Stabilität und Wettbewerbsfähigkeit. Für die Betreiber Kritischer Infrastruktur bedeutet das: Sicherheit muss strategisch geplant, organisatorisch verankert und technologisch neu gedacht werden. Die Verantwortung dafür liegt im Top-Management. Wer entsprechende Strukturen systematisch aufbaut und konsequent weiterentwickelt, stärkt die Widerstandsfähigkeit der eigenen Organisation nachhaltig.

Text **Dr. Tristan Haage** und **Dr. Christian Meine, Geschäftsführer e-shelter security**

Weitere Informationen unter:
e-shelter.io

e–shelter security

> »Die Fähigkeit, auch unter unsicheren Bedingungen handlungsfähig zu bleiben, wird zu einem entscheidenden Faktor für Stabilität und Wettbewerbsfähigkeit.

Dr. Ferri Abolhassan

»Sicherheit ist kein Kostenblock, sondern eine Wachstumsversicherung«

Die zunehmende Bedrohungslage im Cyberraum zwingt Unternehmen und Behörden zu einem radikalen Umdenken beim Schutz kritischer Infrastrukturen. Dr. Ferri Abolhassan, CEO von T-Systems und Mitglied des Telekom-Vorstands, treibt den Aufbau souveräner digitaler Infrastrukturen voran und sieht Sicherheit als essenziellen Wachstumsmotor für den deutschen Mittelstand und Großunternehmen. Im Interview spricht er über digitale Resilienz und erläutert, wie Europa eigene technologische Standards setzen kann.

Interview **Ayman Duran** Bild **zVg**

Dr. Abolhassan, wie hat sich Ihre Rolle vom »Security-Macher« bei der Telekom hin zum Gestalter von digitaler Souveränität und Resilienz für Wirtschaft und Staat entwickelt?
Beide Themen begleiten mich schon meine ganze Karriere. Als ich vor zehn Jahren die IT-Division von T-Systems geleitet habe, habe ich die heutige »T-Sec« mit aufgebaut. Jetzt, als CEO von T-Systems und Mitglied des Telekom-Vorstands, verstehe ich mich mehr als Architekt von souveränen digitalen Infrastrukturen. Unsere Aufgabe als gesamtes Team Magenta ist es, eine digitale Grundversorgung zu schaffen, vergleichbar mit Strom oder Wasser – eben nur für Daten, KI oder Cloud-Lösungen. Damit stärken wir konkret die Resilienz und Wettbewerbsfähigkeit von Unternehmen, Behörden und damit auch die des Landes.

Warum ist digitale Resilienz heute genauso systemrelevant wie klassische physische Sicherheit?
Digitale Resilienz bedeutet, Systeme so zu bauen, dass sie gegen Cyberangriffe, Sabotage und Ausfälle gerüstet sind. Wie in der physischen Sicherheit muss man dafür sorgen, dass man bei Attacken handlungsfähig bleibt. Wenn wir kritische Störungen in Fabriken, Krankenhäusern oder bei Energieversorgern haben – man denke an den Stromausfall in Berlin im Winter durch einen Brandanschlag –, dann kann das Millionen und viel an Vertrauen kosten und im schlimmsten Fall Menschenleben gefährden. Wir erleben eine digitale Zeitenwende, in der Sicherheit und Verfügbarkeit genauso mitgedacht werden müssen wie Funktionalität und Kosten.

Sie gelten als Mann für Vertrieb und Wachstum. Wie verkaufen Sie das oft als Kostenfaktor betrachtete Thema »Cybersecurity« an Vorstände?
Es ist ein Denkfehler, den Unternehmen heute nicht mehr machen sollten. Sicherheit ist kein Kostenblock, sondern eine Wachstumsversicherung. Vorstände unterschreiben heute nicht mehr nur für Umsatz und Marge, sondern auch für Resilienz, Lieferfähigkeit und Compliance – auch gegenüber den Kunden und der Legislation. Ich argumentiere nicht in Firewalls, sondern in Geschäftsrisiken: Können sie jederzeit produzieren? Können sie jederzeit für ihre Kundschaft oder Patient:innen da sein? In meinen Gesprächen mit CEOs und CIOs sehe ich vermehrt, dass die wachsende Bedrohungslage erkannt und ernst genommen wird.

Ist absolute Sicherheit heute eine Illusion und müssen wir uns stattdessen primär auf schnelle Wiederherstellung und Resilienz konzentrieren?
Absolute Sicherheit ist im digitalen Raum leider eine Illusion. Wer anderes behauptet, verspricht zu viel. Man kann sich bestmöglich schützen, aber nie zu 100 Prozent. Es geht eher darum, Sicherheitsvorfälle schnell zu erkennen, einzudämmen und IT-Systeme wieder sicher hochzufahren. Dies erfordert umfassende Resilienz – vom Design der Architektur über Notfallpläne bis hin zu Zero-Outage-Standards.

> Wir erleben eine digitale Zeitenwende, in der Sicherheit und Verfügbarkeit genauso mitgedacht werden müssen wie Funktionalität und Kosten.
>
> – Dr. Ferri Abolhassan

Sie haben vor über zehn Jahren »Zero Outage« bei T-Systems angestoßen. Welche Lehren daraus sind für Behörden, Krankenhäuser, Energieversorger und andere Betreiber kritischer Infrastrukturen heute am wichtigsten – auch mit Blick auf NIS-2?
»Zero Outage« ist seit Jahren unsere DNA. Qualität und Sicherheit sind keine Projekte, sondern eine Denkweise. »Zero Outage« hat gezeigt, dass man Standards, Prozesse und Training konsequent durchhalten muss, um Störungen und Ausfälle niedrig zu halten. Das ist kein Sprint, sondern ein Marathon. Für Energieversorger oder Banken bedeutet das, nicht nur Checklisten abzuarbeiten, sondern Ende-zu-Ende zu denken: Von der Lieferkette über Betriebsprozesse bis hin zu klaren Verantwortlichkeiten im Krisenfall.

Wie verändern der AI Act und NIS-2 die Spielregeln für Unternehmen und Behörden – und was müssen Entscheider:innen jetzt tun, um nicht nur compliant, sondern wirklich widerstandsfähig zu werden?
Beide werden oft als Bürokratiemonster bezeichnet. Das sehe ich anders. Sie sind ein guter Sicherheitsgurt für die digitale Transformation, weil sie uns zwingen, Risiken ernst zu nehmen, Verantwortlichkeiten zu klären und Resilienz messbar zu machen. Wer das proaktiv nutzt und vertrauenswürdige digitale Dienste aufbaut, hat im Markt einen echten Vorteil. Unsere Rolle ist es, diese Regeln in praxistaugliche Lösungen zu übersetzen, damit es für Kunden machbar, einfach und greifbar ist.

Viele sprechen von »digitaler Souveränität«. Was macht eine KI- oder Cloud-Lösung aus Ihrer Sicht wirklich souverän – technisch, rechtlich und politisch?
Es gibt drei Dimensionen: Datensouveränität heißt, dass die Daten in einem europäischen Rechenzentrum liegen, verschlüsselt sind und die Kundschaft die Kontrolle hat. Rechtliche Souveränität stellt sicher, dass kein Zugriff durch ausländische Behörden möglich ist. Technologisch fragen wir: Haben wir offene Standards, Interoperabilität und die Fähigkeit, Workloads zu verlagern, statt in einem proprietären Lock-in zu landen? Erst wenn Unternehmen genau die souveräne Cloud-Lösung erhalten, die zu ihren Anforderungen passt, entsteht echte digitale Freiheit.

Haben wir in Europa den Kampf um Hardware und Plattformen verloren und können wir unsere Souveränität nur noch auf der Software- und Sicherheitsebene verteidigen?
Im Wettlauf um die großen Hyperscaler-Plattformen und Teile der Hardwareproduktion sind andere vorne. Aber Souveränität heißt nicht, alles selbst zu bauen, sondern strategische Stellhebel zu kontrollieren: Daten, Prozesse, Standards und Sicherheit. In München beispielsweise haben wir am 4. Februar gemeinsam mit Nvidia, SAP, Siemens und anderen die weltweit erste industrielle KI-Cloud eröffnet. Das ist ein Beispiel dafür, wie wir mitspielen können: durch Partnerschaften und Allianzen. Es ist noch viel zu tun. Aber natürlich müssen wir auch damit klarkommen, dass wir in gewissen Feldern abhängig sind.

Die Telekom engagiert sich jetzt stärker im Defense-Bereich, unter anderem über ein Millioneninvestment in Quantum Systems, ein Drohnen-Start-up aus München. Was war der Hintergrund und inwiefern profitiert die Gesellschaft von dieser Kooperation?
Ohne Sicherheit gibt es keine Freiheit. Das gilt in der digitalen wie in der physischen Welt. Mit unserem Engagement im Defense-Bereich antworten wir auf die Bedrohungslagen aus dem Aus- und Inland. Das lässt sich auch auf den Verteidigungssektor, Spionageabwehr, Schutz von Stadien beispielsweise bei Großereignissen wie EM oder WM und insgesamt auf den Bevölkerungsschutz übertragen. Es geht dabei um aktiven Schutz unserer Netze, demokratischen Institutionen und letztlich der Menschen. Und das halten wir für eine notwendige Sache.

Öffentliche Sicherheit ist mehr als Technik: Was müssen Staat, Wirtschaft und Wissenschaft jetzt konkret unternehmen, damit Europa bei KI, Cloud und Defense nicht nur aufholt, sondern eigene Standards setzt?
Wir dürfen nicht naiv sein. Man könnte sagen: Der Zug ist abgefahren. Ich sage: Der Zug ist nur so lange abgefahren, wie es keinen neuen Zug gibt. Und wir setzen gerade in München einen neuen aufs Gleis. Das ist unser Beitrag für die Unternehmensinitiative »Made for Germany«. Wir wollen hier vorangehen, Deutschland und Europa besser und stärker machen.

Weitere Informationen zur KI-Fabrik:

Gemeinsam handlungsfähig: Sicherheit neu denken

Marode Infrastrukturen, geopolitische Risiken und steigende Anforderungen an eine verlässliche Versorgung zwingen Politik und Wirtschaft dazu, das Thema Schutz und Resilienz neu zu denken. Im Interview erklären die Expertinnen des internationalen Beratungsunternehmens für Bau, Immobilien und Infrastruktur Drees & Sommer SE – Anke Stadelmeyer (Head of Security & Defense) und Kristina Volland (Key Account Managerin Bundesministerium der Verteidigung) – warum eine höhere Widerstandsfähigkeit nur im Zusammenspiel aller Akteure gelingt.

Anke Stadelmeyer
Head of Security & Defense

Kristina Volland
Key Account Managerin
Bundesministerium der Verteidigung

Frau Stadelmeyer, wie hat sich das Verständnis von Sicherheit in den vergangenen Jahren verändert?
Anke Stadelmeyer: Stromausfälle, Terroranschläge und der Nahost-Konflikt zeigen, wie vernetzt und verletzlich Sicherheit heute ist. Sie reicht weit über militärische Stärke im Ernstfall hinaus. Sie beginnt präventiv, kennt keine Landesgrenzen und umfasst ebenso eine verlässliche Energie- und Wasserversorgung, robuste Infrastrukturen und Unternehmen, resiliente Gebäude sowie stabile Verkehrs- und Datennetze. Im Kern geht es um drei untrennbare Bereiche: den Schutz von Menschen, von Daten und von der gebauten Umwelt.

Wenn Sie von sicherer gebauter Umwelt sprechen, was meint das konkret?
Anke Stadelmeyer: Einerseits brauchen wir solide Straßen und Brücken, klimaresiliente Gebäude sowie eine widerstandsfähige kritische Infrastruktur. Aktuell ist jede dritte Brücke in Deutschland sanierungsbedürftig. Über ein Drittel der Fahrstreifen-Kilometer auf Bundesstraßen und fast ein Fünftel auf Autobahnen weisen einen erhöhten Sanierungsbedarf auf. Das blockiert im Ernstfall militärische und zivile Transporte, Einsatzfahrzeuge erreichen zum Beispiel Kliniken nicht. Andererseits müssen kritische Infrastrukturen zur medizinischen sowie zur Energie- und Wasserversorgung auch unter Extrembedingungen zuverlässig arbeiten. Eine gebaute Umwelt, die selbst nicht stabil ist, kann im Ernstfall nur eingeschränkt schützen.

Frau Volland, bei Drees & Sommer betreuen Sie Projekte für den zivilen und militärischen Schutz. Welche Faktoren sind entscheidend, damit beides reibungslos funktioniert?
Kristina Volland: Die Bundeswehr steht vor einem historisch beispiellos hohen Infrastrukturbedarf. Sicherheitspolitische Entwicklungen und der enorme Sanierungsrückstand erhöhen den Druck zusätzlich. Im vergangenen Jahr waren mehr als eine Milliarde Euro für Neu- und Ersatzbauten vorgesehen – und fast jedes dritte Bestandsgebäude gilt als stark sanierungsbedürftig. Solche Volumina und ambitionierten Zeitvorgaben verlangen ein konsequent koordiniertes Vorgehen von der Planung bis zur Umsetzung. Beschleunigte Verfahren, Direktvergaben und gebündelte Ausschreibungen schaffen dabei Tempo. Entscheidend bleibt jedoch die Personaldecke: Fehlen Fachkräfte – in der öffentlichen Hand wie auch in Vergabestellen – geraten selbst gute Verfahren ins Stocken. Wo interne Kapazitäten knapp sind, sichert externe Expertise Qualität und Geschwindigkeit.

Im Kern geht es um drei untrennbare Bereiche: den Schutz von Menschen, von Daten und von der gebauten Umwelt.

– Anke Stadelmeyer, Head of Security & Defense

Wo sehen Sie den größten Handlungsbedarf im Zivilschutz auf lokaler und kommunaler Ebene?
Kristina Volland: Noch sind Vernetzung und Informationsfluss zwischen den wesentlichen Akteuren des Zivil- und Militärschutzes zu dezentral und uneinheitlich organisiert. Austausch findet statt, jedoch zu wenig flächendeckend und nur in Teilen vertieft. Bisher wurden im Wesentlichen nur die Städte und Kommunen ausführlicher informiert, die im militärischen Kontext des Operationsplans Deutschland konkret benannt wurden.

Wie können solche Lücken geschlossen werden?
Kristina Volland: Dafür braucht es erstens eine belastbare bundesweite Datenbasis, zweitens klare Informationswege und drittens eine abgestimmte Vernetzung aller relevanten Stellen – von Feuerwehren und Rettungsdiensten über Hilfsorganisationen bis hin zur Bundeswehr. Wie das gelingen kann, zeigen wir aktuell gemeinsam mit einem unserer Auftraggeber in einem bayerischen Pilotprojekt, das kommunale Prozesse, Datenflüsse und Akteursstrukturen gezielt miteinander verzahnt. So entsteht ein Modell, das beispielhaft für eine koordinierte Zusammenarbeit stehen kann.

Wie können Unternehmen zur gesamtgesellschaftlichen Resilienz beitragen?
Kristina Volland: Viele Unternehmen könnten mehr Verantwortung übernehmen und sich deutlich widerstandsfähiger aufstellen. Mit dem Schutz von Lieferketten und Werksgeländen entlasten sie im Krisenfall auch die Organe des Zivilschutzes. Doch selbst Organisationen, die nach dem KRITIS-Dachgesetz als kritisch gelten, setzen ihre Vorgaben noch nicht vollumfänglich um. Würden gerade diese Einrichtungen hier proaktiv agieren, wären wir bereits einen großen Schritt weiter. Denn die Sicherheit eines Landes ist keine rein militärische Aufgabe, sondern eine gesamtgesellschaftliche. Wirtschaft, Länder und Kommunen tragen hier gleichermaßen Verantwortung. Widerstandskraft entsteht nur gemeinsam.

Frau Stadelmeyer, sehen Sie bereits eine stärkere Nachfrage nach krisensicheren Lösungen?
Anke Stadelmeyer: Ja, eindeutig. Die Bedeutung widerstandsfähiger Strukturen nimmt in allen Bereichen zu. Wir unterstützen unsere Kunden bei der Planung und Auslegung kritischer Infrastrukturen – von resilienten Gebäuden über sichere Bauwerke für die Verkehrsinfrastruktur bis hin zu robusten digitalen Systemen wie etwa Datacenter. In der Industrie sorgen wir zudem für robuste Lieferketten und stärken Produktions- und Logistiksysteme. Unser Anspruch ist, Organisationen und Unternehmen so aufzustellen, dass sie stabil, handlungsfähig und geschützt bleiben – gerade in herausfordernden Zeiten.

Viele Unternehmen könnten mehr Verantwortung übernehmen und sich deutlich widerstandsfähiger aufstellen.

– Kristina Volland, Key Account Managerin Bundesministerium der Verteidigung

Dr. Jonathan Davis
Partner und Managing Director
Drees & Sommer Digital Services

Cybersicherheit als entscheidender Schutzfaktor
Cybersicherheit ist heute ein zentraler Faktor für die Stabilität und Handlungsfähigkeit eines Landes. Kritische Infrastrukturen wie Energieversorgung, Verkehr oder Gesundheitswesen sind stark digitalisiert und eng miteinander vernetzt. Auch Industrieunternehmen setzen zunehmend auf vernetzte Produktionssysteme – und werden dadurch anfälliger für Angriffe. Ein erfolgreicher Cyberangriff kann daher unmittelbare Folgen für Wirtschaft, Versorgungssicherheit und das Vertrauen der Bevölkerung haben.

Umso wichtiger ist ein ganzheitlicher Sicherheitsansatz. Moderne Technologie allein genügt nicht. Ebenso entscheidend sind klare Prozesse, definierte Verantwortlichkeiten und ein ausgeprägtes Sicherheitsbewusstsein in den Organisationen. Nur so lassen sich Angriffe frühzeitig erkennen und Schäden begrenzen. Dazu zählen unter anderem regelmäßige Cyberresilienzübungen für Betreiber kritischer Infrastrukturen sowie die konsequente Umsetzung bewährter Sicherheitsprinzipien wie Security by Design oder Zero Trust in staatlichen und unternehmensweiten digitalen Systemen.

Für viele Unternehmen stellt eine hohe Informationssicherheit zudem einen strategischen Erfolgsfaktor dar und sichert künftige Kundenbeziehungen und Aufträge. Gleichzeitig steigen die regulatorischen Anforderungen sowie die Erwartungen von Kunden und Partnern, die Einhaltung anerkannter Sicherheitsstandards und Zertifizierungen nachzuweisen. Eine ganzheitliche Cybersecuritystrategie stärkt somit die Zukunftsfähigkeit von Unternehmen – intern wie extern.

Weitere Informationen unter:
dreso.com/de/security-and-defense

und **dreso.com**

DREES & SOMMER

KRITIS ist Chefsache: Das müssen C-Level jetzt im Blick haben.

Deutschlands kritische Infrastrukturen (KRITIS) stehen massiv unter Druck. Ob veraltete Abwassernetze, reibungslose Lieferketten oder moderne Datenströme: Fällt ein Teil dieses komplexen Systems aus, gerät das Ganze ins Wanken. Ein gefährlicher Dominoeffekt, den viele Entscheider noch immer unterschätzen.

Aktuelle Vorfälle belegen in beunruhigender Regelmäßigkeit: Isolierte Einzelmaßnahmen reichen für den KRITIS-Schutz nicht mehr aus. Echte Sicherheit entsteht nur, wenn alle Ebenen integriert gedacht und gesteuert werden. Das erfordert auf C-Level den Mut zur klaren Priorisierung und zu interdisziplinärem Handeln.

Die Gefahr lauert an den Schnittstellen

KRITIS lässt sich nicht mehr klassisch verwalten. Sie ist heute ein komplexes Geflecht aus physischen Anlagen, Cloud-Architekturen und vernetzten Steuerungstechnologien. Oft wird im Management fälschlicherweise angenommen, Risiken lägen primär innerhalb isolierter Systeme. Tatsächlich befinden sich die größten Schwachstellen – aber auch die größten Potenziale – an den Schnittstellen. Genau dort, wo Gewerke und Zuständigkeiten aufeinandertreffen. Wer diese durch klare Ownership auf C-Level meistert, profitiert von effizienteren Betriebsmodellen und resilienten Lieferketten.

Resilienz als strategische Kernaufgabe

Resilienz entscheidet heute maßgeblich über Wettbewerbsfähigkeit, Investitionsklima und langfristige Wertschöpfung. Wer sie lediglich als IT- oder Sicherheitsthema abtut, riskiert operative Störungen und massive Wertverluste. Organisationen, die Resilienz ganzheitlich in ihre strategische Steuerung integrieren, schaffen die Basis für stabile Betriebsmodelle und Marktvertrauen.

Eraneos unterstützt Sie dabei, KRITIS ganzheitlich zu denken und Potenziale systematisch auszuschöpfen – von der strategischen Governance über digitale Plattformen bis zur technologischen Umsetzung in der gesamten Organisation.

eraneos

Maßgeschneiderte Expertise kombiniert mit der Kraft, Transformation in großem Maßstab voranzutreiben.

19 Standorte in 12 Ländern

1.300+ spezialisierte Fachkräfte

brandeins /thema 2026 Beste Unternehmensberater · BEST OF CONSULTING 2024 Wirtschafts Woche · Top Company 2025 kununu

Fortune-500-Unternehmen, mittelständische Unternehmen (KMU) und staatliche Organisationen vertrauen uns. Ausgezeichnet als führendes Beratungsunternehmen und Top-Arbeitgeber.

Christian Wetter
Partner Strategy & Growth

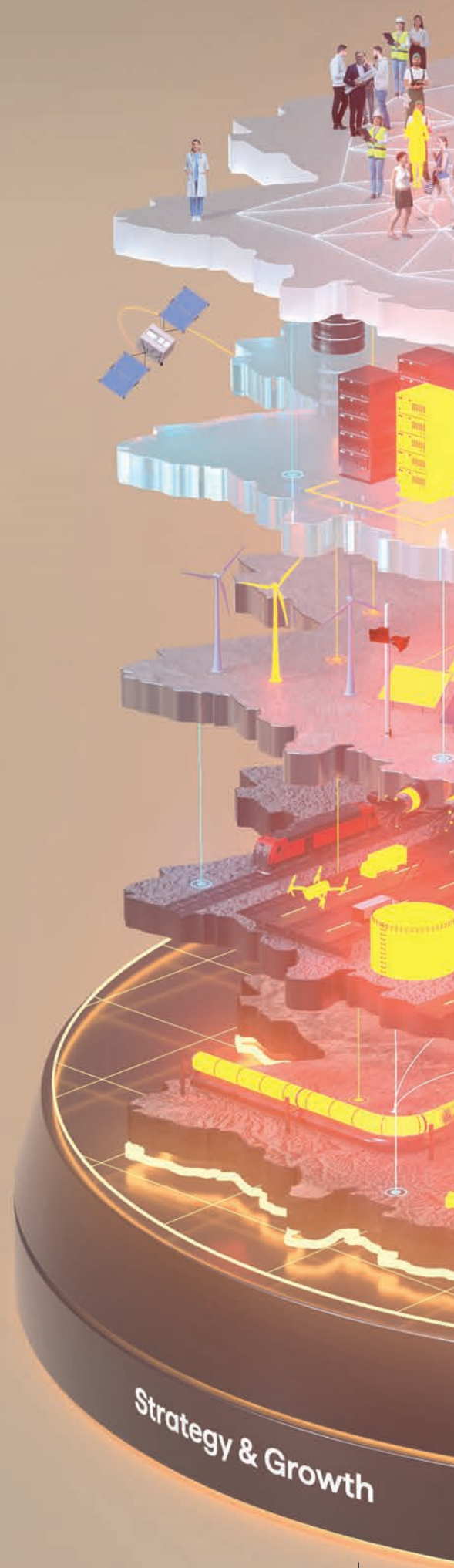
„Für KRITIS-Unternehmen ist die Resilienz des Kerngeschäfts der zentrale Maßstab. Telekommunikation und Energie funktionieren beispielsweise nur im Verbund und bilden das Rückgrat moderner Volkswirtschaften. Im Hinblick auf Resilienz sind künftig geografisch redundante Glasfasernetze, Multi-Orbit-Satelliten, energiegesicherte Netzknoten und ein hoch automatisierter Betrieb entscheidend. Wer diese Systeme nicht integriert denkt, wird mit großen Herausforderungen konfrontiert. Die Verfügbarkeit von Daten in Echtzeit wird dabei zum Schlüssel für neue Geschäftsmodelle."

Sergej Lietzenberger
Partner Management & Technology

„Die Realität ist: Die Infrastruktur in Deutschland ist über Jahre hinweg zu wenig ausgebaut worden. Netze, Systeme und Steuerungsstrukturen stoßen vielerorts an ihre Grenzen. KRITIS wird künftig dort funktionieren, wo Betreiber zwei Dinge beherrschen: funktionalen Ausbau und netzübergreifende Steuerung mit Echtzeitdaten. Wer diese Kompetenzen aufbaut, schützt seine Systeme und schafft die Grundlage für effizientere Infrastruktur und neue Wertschöpfung. Sicherheit ist damit längst ein wirtschaftlicher Faktor."

Michael Martin
Partner Resilienz und Cybersecurity

„Operative Resilienz und Cybersicherheit schützen kritische Infrastruktur wie ein unsichtbares Nervensystem: wachsam, vernetzt und widerstandsfähig. Digitale, organisatorische und physische Maßnahmen müssen ineinandergreifen, damit digitale und physische Angriffe früh erkannt und gestoppt werden. Klare Zuständigkeiten, Notfallpläne und Schulungen sichern den Betrieb, ohne Innovation auszubremsen."



Strategie bestimmt die Widerstandsfähigkeit der KRITIS. Politik und C-Level definieren unverzichtbare Prozesse, tragbare Risiken und gezielte Investitionen. Echtzeitdaten sind dabei der Schlüssel: Sie machen Abhängigkeiten sichtbar, beschleunigen Entscheidungen und maximieren den Schutz. So wird Resilienz zum strategischen Treiber für verlässliche Versorgung, neue Geschäftsmodelle und langfristigen wirtschaftlichen Erfolg.

200 Mrd. €

Gesamtschaden durch Cyberangriffe pro Jahr

Quelle: BKA, Bitkom

48 %

der KRITIS-Betreiber verfügen über kein System zur Angriffserkennung.

Quelle: BSI-Lagebericht

149.000

neue Malware-Varianten pro Tag

Quelle: BSI-Lagebericht

#4

Deutschland gehört nach den USA, Indien und Japan zu den vier am stärksten von Ransomware-Angriffen betroffenen Ländern.

Quelle: BSI-Lagebericht

80 %

der angezeigten Cyberangriffe treffen kleinere und mittlere Unternehmen.

Quelle: BSI-Lagebericht

Kritische Infrastruktur hat viele verschiedene Ebenen. Die fünf wichtigsten sehen Sie hier. Erst wenn alle Ebenen zusammenspielen, entstehen Resilienz und wirtschaftlicher Mehrwert.

Der Schutz und auch die **wirtschaftliche Weiterentwicklung** kritischer Infrastruktur hängen heute vom Zusammenspiel moderner Technologien und strategisch agierender **Führung** ab, wobei der Gestaltungswille in der Unternehmensführung der entscheidende Part ist. Wenn auf dieser Basis Strategie, Cybersicherheit, Netztechnologie und Betrieb eng miteinander verzahnt sind, steuern KRITIS-Betreiber ihre Systeme datenbasiert in Echtzeit und im Rahmen einer funktionierenden Governance, erkennen Risiken frühzeitig und entwickeln ihre Infrastruktur nachhaltig weiter.

Resilienz zeigt sich im Betrieb. Sie entsteht aus dem Zusammenspiel von operativer Sicherheit und Cybersicherheit entlang der gesamten Infrastruktur. Dazu gehören abgesicherte OT-Systeme, kontrollierte Fernzugriffe, geschützte Schnittstellen und belastbare Cloud-Architekturen ebenso wie eine verlässliche Steuerung externer Dienstleister. Erst gemeinsam mit klarer Governance, funktionierenden Notfall- und Krisenstrukturen sowie gut vorbereiteten Teams wird daraus ein belastbares Gesamtsystem. So bleibt kritische Infrastruktur auch unter Störungen oder Angriffen handlungsfähig. Zudem wird Sicherheit zur Voraussetzung für stabile Versorgung, Innovation und wirtschaftliche Leistungsfähigkeit.

Öffentliche Sicherheit beginnt digital

Wenn ein Krankenhaus auf Papier zurückfällt, wenn in einer Kommune plötzlich keine Termine mehr gebucht werden können oder wenn ein Versorger seine Systeme isolieren muss, wirkt das zunächst wie ein IT-Problem. In der Praxis ist es aber oft eine Frage der öffentlichen Sicherheit. Moderne Gesellschaften funktionieren über digitale Ketten: Identitäten, Zahlungsflüsse, Einsatzplanung, Logistik, Kommunikation. Wer diese Ketten stört, greift nicht nur Daten an, sondern auch die Handlungsfähigkeit.

Wenn digitale Angriffe Betrieb werden

Cyberangriffe sind längst nicht mehr nur spektakuläre Einzelfälle. Sie sind ein kontinuierliches Risiko, das öffentliche Einrichtungen genauso betrifft wie Unternehmen – oft sogar stärker, weil Abläufe und IT-Landschaften über Jahre hinweg schrittweise erweitert wurden, Budgets begrenzt sind und die Abhängigkeit von externen Dienstleistern zunimmt. Gleichzeitig ist der Schaden in der Öffentlichkeit sichtbarer: Ausfälle treffen Bürger:innen direkt, Datenpannen erschüttern Vertrauen, und jede Stunde Stillstand kostet nicht nur Geld, sondern auch Legitimation.

Dabei ist die Bedrohung häufig unspektakulär: ein kompromittiertes Konto, eine ungepatchte Schwachstelle, ein falsch konfigurierter Cloud-Dienst. Aus kleinen Einstiegen entstehen große Folgen – weil Systeme miteinander sprechen, weil Zugriffsrechte zu weit reichen und weil Notfallabläufe im Alltag selten geübt werden.

Das neue Dreieck: Erpressung, Identität, Tempo

Ransomware bleibt das disruptive Kernmuster: nicht nur Verschlüsselung, sondern Erpressung über Datenabfluss, Drohkulissen und Druck auf Dienstleister. Gleichzeitig haben sich Einfallstore verschoben. Identitäten sind zum primären Angriffspunkt geworden. Wer Zugriff hat, braucht oft keine komplizierte Exploit-Kette mehr – dann reicht es, sich im System zu orientieren und die vorhandenen Zugriffsrechte auszunutzen.

Gleichzeitig werden Zeitfenster kürzer. Schwachstellen werden schneller ausgenutzt, weil Scans, Exploit-Tests und automatisierte Angriffsabläufe effizienter geworden sind. Patchen ist ein Wettlauf, nicht nur eine technische Pflicht.

KI macht Täuschung skalierbar

Der sichtbarste KI-Effekt liegt nicht in neuen Wunderwaffen, sondern in der Professionalisierung von Täuschung. Phishingmails wirken sprachlich sauber, passen sich an Rollen und Situationen an und werden in Serie produziert – mehrsprachig, konsistent, plausibel. Auch am Telefon und in Videocalls steigt der Druck: Wenn Stimmen und Bilder überzeugender imitierbar werden, verliert der Kanal als Beweis an Wert. Das trifft besonders Organisationen, deren Abläufe auf Routine und Vertrauen beruhen.

Viele Analysen beschreiben diese Verschiebung als wachsende Relevanz von »cyber-enabled fraud«: Betrug, der digitale Prozesse ausnutzt, ohne Systeme zwingend zu zerstören. Für die öffentliche Sicherheit ist das heikel, weil Schäden oft erst spät auffallen und Gegenmaßnahmen weniger in neuer Technik liegen als in sauberer Organisation: klare Freigabewege, ein konsequentes Vier-Augen-Prinzip, dokumentierte Ausnahmen und Identitäten, die wirklich abgesichert sind.

Neue Angriffsflächen: Wenn KI selbst zum System wird

Parallel entsteht eine zweite Ebene: KI wird in immer mehr Prozesse eingebaut. Damit entstehen neue Angriffsflächen, die nicht wie klassische Softwarefehler aussehen, aber ebenso wirksam sind. »Prompt Injection« etwa zielt darauf, ein System über Eingaben umzulenken: Es soll Regeln ignorieren, Daten preisgeben oder Handlungen auslösen, die nicht vorgesehen sind. Hinzu kommen Risiken rund um Schnittstellen zu internen Systemen und die Lieferkette von Modellen und Plug-ins.

Das führt zu einem nüchternen Grundsatz: KI ist keine Abkürzung aus Sicherheitsarbeit heraus. Sie ist eine zusätzliche Schicht, die dieselben Fragen verlangt wie jede kritische Software – wer hat Zugriff, welche Daten fließen, welche Outputs werden weiterverarbeitet und welche Ausfälle sind tolerierbar.

Resilienz statt Perfektion

Die wirksamste Antwort auf diese Lage ist weniger ein einzelnes Produkt als eine Sicherheitsarchitektur, die mit Realität rechnet. Im Kern geht es um vier Disziplinen.

Erstens: Identität und Zugriff als Kontrollzentrum – mit starker Authentifizierung, minimalen Rechten, konsequenter Trennung von Administratorrollen und laufender Prüfung von Ausnahmen.

Zweitens: Segmentierung und Begrenzung des Schadensradius. Wer Systeme logisch und organisatorisch trennt, verhindert, dass ein einzelner Zugang gleich eine ganze Organisation öffnet.

Drittens: Wiederherstellbarkeit. Backups, Offline-Kopien, klare Wiederanlaufpläne und Übungen zeigen, ob der Betrieb auch unter Stress funktioniert.

Viertens: Governance, die Entscheidungen beschleunigt, statt sie zu blockieren. Gemeint ist eine klare Steuerung der Cybersicherheit bei Zuständigkeiten, Entscheidungswegen und Prioritäten. Orientierung bietet dabei das »NIST Cybersecurity Framework 2.0«, ein international verbreiteter Leitfaden für Cyberrisikomanagement. In Europa steigt zudem der Erwartungsdruck durch konkrete Rechtsakte: die »NIS2-Richtlinie«, die Sicherheits- und Meldepflichten für wichtige Einrichtungen verschärft, sowie »DORA«, das im Finanzsektor digitale Betriebsresilienz und Vorfallmanagement verbindlicher regelt.

Denn am Ende beginnt öffentliche Sicherheit nicht erst bei Blaulicht und Notruf, sondern bei der digitalen Grundversorgung. KI verschärft das Spiel nicht, weil sie alles neu erfindet, sondern weil sie das Bekannte schneller, billiger und überzeugender macht. Wer darauf nur mit Alarmismus reagiert, verliert. Wer mit Resilienz, klaren Prozessen und geübter Handlungsfähigkeit antwortet, macht Cybersicherheit zu dem, was sie sein muss: Infrastruktur.

Text **Walter Nogueira**

AI ist längst Teil der Angriffslandschaft

2026 wird für die Cybersicherheit ein Jahr, in dem künstliche Intelligenz die Bedrohungslage maßgeblich prägt. AI ist längst fixer Bestandteil der Angriffslandschaft: Ein großer Teil der Phishingkampagnen wird automatisiert erstellt und auch weniger versierte Angreifende erhalten Fähigkeiten, die früher professionellen Gruppen vorbehalten waren. Fehlerfreier Code, überzeugende Phishingmails oder automatisierte Angriffsschritte senken die Einstiegshürden und erhöhen das Schadenspotenzial – besonders bei InsiderRisiken.

Dr. Elisabetta Castiglioni
CEO

Zugleich entsteht eine neue Qualität von Angriffen: hochgradig personalisiertes Spear-Phishing, lernende Web-Exploits und AI-Agenten, die sich in Echtzeit anpassen. Klassische, rein reaktive Schutzmechanismen reichen dafür nicht mehr aus. Unternehmen müssen ihre Sicherheitsarchitekturen automatisieren, adaptiv gestalten und Threat-Intelligence in Echtzeit integrieren.

»Intelligente Systeme erkennen Muster, die Menschen verborgen bleiben, und reagieren nahezu in Echtzeit. A1 Digital entwickelt Lösungen, die menschliche Expertise mit maschineller Intelligenz verbinden.

AI ist für mich jedoch nicht nur Teil des Problems, sondern ein zentraler Baustein der Defensive. Intelligente Systeme erkennen Muster, die Menschen verborgen bleiben, und reagieren nahezu in Echtzeit. A1 Digital entwickelt Lösungen, die menschliche Expertise mit maschineller Intelligenz verbinden – von AI-gestützter Anomalieerkennung über automatisierte Incident-Response bis zu sicherem Edge-Computing und dem Schutz industrieller Systeme und kritischer Infrastrukturen. Nur durch diesen integrierten Ansatz können Unternehmen den Anforderungen des Jahres 2026 gerecht werden.

Weitere Informationen unter:
a1.digital

A1 Digital

»Digitale Souveränität ist im öffentlichen Sektor ein strategischer Imperativ«

Rolf Schumann
Co-CEO Schwarz Digits

Behörden stehen unter enormem Modernisierungsdruck. Während Fachkräftemangel und demografischer Wandel Abteilungen belasten, erwarten Bürgerinnen und Bürger schnelle digitale Services und Prozesse. Effizienzsteigerung und Digitalisierung sind daher unverzichtbar – doch gerade im öffentlichen Sektor, der zu den zentralen Säulen der kritischen Infrastruktur eines Staates zählt, muss dies mit klarem Fokus auf Souveränität und Sicherheit erfolgen. Denn nicht nur stehen hier hochsensible Daten und das Vertrauen der Bürgerinnen und Bürger auf dem Spiel, auch die Unabhängigkeit der staatlichen Organe vor externer Einflussnahme muss unbedingt gewahrt bleiben.

Herr Schumann, warum hat digitale Souveränität für die öffentliche Verwaltung an Dringlichkeit gewonnen?
Die geopolitischen Rahmenbedingungen und das transatlantische Verhältnis haben sich verändert. Gleichzeitig steigen mit der Technologieabhängigkeit auch die Bedeutung digitaler Infrastrukturen und die Bedrohung durch hybride Angriffe. Die Kontrolle über die eigenen Daten und IT-Systeme zu behalten ist heute entscheidend für die Resilienz. Daher ist es wichtig, bei der Wahl der Technologiepartner genau hinzusehen. Wer sich von außereuropäischen Anbietern abhängig macht, die anderen politischen Interessen und Gesetzen unterliegen, geht hohe Risiken ein. Für den öffentlichen Sektor, der das Rückgrat des Staates bildet, ist das keine Option.

Was braucht der öffentliche Sektor, um digitale Souveränität zu etablieren?
Digitale Souveränität ist ein Konzept, das die gesamte IT-Architektur betrifft – von der Cloud-Infrastruktur über den digitalen Arbeitsplatz und die Cybersicherheit bis hin zur künstlichen Intelligenz. All diese Schichten müssen zusammengedacht werden, denn Souveränität in einer Ebene verliert ihren Wert, wenn eine andere kompromittierbar bleibt. Um Komplexität zu reduzieren, empfiehlt es sich, mit einem europäischen Anbieter zusammenzuarbeiten, der alle Bereiche aus einer Hand abdecken kann. Schwarz Digits hat ein komplettes Ökosystem an leistungsstarken, souveränen Lösungen aufgebaut, mit der Stackit Cloud als Fundament. Alle Daten werden ausschließlich in Europa gespeichert und verarbeitet. Dabei ist die kompromisslose Einhaltung der DSGVO gewährleistet, ebenso wie die Umsetzung der Sicherheitsvorgaben laut C5-Testat des Bundesamts für Sicherheit in der Informationstechnik.

Welche Rolle spielen Cybersicherheit und künstliche Intelligenz in einer Souveränitätsstrategie?
Cybersicherheit ist eine entscheidende Voraussetzung für Souveränität, denn wer erfolgreich angegriffen wird, verliert die Kontrolle über seine Systeme. Cyberkriminelle agieren heute voll automatisiert, zunehmend KI-gestützt und greifen über alle Ebenen der IT-Umgebung hinweg an. Um kritische Assets zu schützen und die Resilienz sicherzustellen, müssen Verteidiger in der Lage sein, Bedrohungen in der gesamten IT-Umgebung in Echtzeit zu erkennen und Risiken zu priorisieren. Dafür ist eine digital souveräne, ganzheitliche Cybersecurity-Plattform erforderlich. Künstliche Intelligenz wiederum vergrößert die Angriffsfläche und muss unbedingt in einer Souveränitätsstrategie berücksichtigt werden. Denn der Treibstoff jeder KI sind Daten. Wer vertrauliche Informationen in KI-Modelle außereuropäischer Anbieter einspeist, riskiert Kontrollverlust und Datenabfluss. Je stärker KI außerdem in kritische Geschäftsprozesse integriert wird, desto weitreichender und gefährlicher werden die Auswirkungen einer potenziellen Kompromittierung von Trainingsdaten oder Modellen. Daher ist es wichtig, KI von Grund auf sicher und souverän auf Basis von europäischen Modellen zu implementieren.

Welche Maßnahmen sollte der öffentliche Sektor jetzt angehen?
Um die Digitalisierung voranzubringen und die Effizienz zu steigern, sind KI und Cloud-Technologie unverzichtbar – aber im Einklang mit europäischem Datenschutz, dem EU AI Act und unter Wahrung voller Kontrolle über Daten und Systeme. Im ersten Schritt empfiehlt sich die Einführung einer souveränen Cloud-Plattform als Fundament für eine skalierbare, leistungsfähige Infrastruktur. Auf dieser können dann alle weiteren Lösungen aufsetzen, von souveräner Kollaboration und Kommunikation über KI bis zu einer ganzheitlichen Sicherheitsarchitektur. Eine Multi-Cloud- und Open-Source-Strategie sowie offene Schnittstellen verhindern dabei einseitige Abhängigkeiten und sorgen für Transparenz.

Wer souveräne Cloud, ganzheitliche Cybersicherheit und verantwortungsvolle KI konsequent zusammenführt, schafft die Grundlage für eine zukunftsfähige digitale Verwaltung. Effizienz und Resilienz gehen dabei Hand in Hand. Wer diese Weichenstellung versäumt, nimmt dagegen wachsende Abhängigkeiten, strukturelle Sicherheitsdefizite und letztlich eine Einschränkung der staatlichen Handlungsfähigkeit in Kauf. Digitale Souveränität ist für den öffentlichen Sektor daher keine Option, sondern ein strategischer Imperativ.

Weitere Informationen unter:
schwarz-digits.de

schwarz digits

Smart Industry in Deutschland – worauf es jetzt ankommt

Olaf Niemeitz
Managing Director Networks & Security, Axians Deutschland

Die deutsche Industrie befindet sich 2026 in einem Spannungsfeld aus wirtschaftlicher Unsicherheit, Innovationsdruck und zugleich wachsenden Möglichkeiten durch digitale Technologien. Während laut DIHK-Digitalisierungsumfrage 2026 viele Unternehmen ihren Digitalisierungsgrad als solide einschätzen, bremsen Bürokratie, schleppende Entscheidungsprozesse und hohe Cybersicherheitsrisiken die Transformation weiterhin aus.

Gleichzeitig ist technologischer Fortschritt – insbesondere KI, Cloud-Ökosysteme und vernetzte Produktion – der zentrale Motor für die zukünftige Wettbewerbsfähigkeit unserer Industrie. Chancen entstehen vor allem durch Effizienzgewinne, Automatisierung und datengetriebene Geschäftsmodelle. Die Risiken liegen dagegen im Fachkräftemangel, geopolitischer Volatilität sowie einer abnehmenden Innovationskraft.

Vernetzte Infrastrukturen für positive Dynamik
Geht man in die konkrete unternehmerische Praxis, so erleben wir derzeit allerdings auch viel positive Dynamik und »Machertum«. Vernetzte Infrastrukturen, digital gesteuerte Maschinen und Anlagen sind heute Alltag bei den Kunden von Axians. Noch bis vor wenigen Jahren arbeiteten die Produktionsnetzwerke dabei häufig lokal und im isolierten Netzwerk. Nun kommunizieren Anlagen vernetzt über Internet oder private Ende-zu-Ende-Netze mit den Möglichkeiten von Cloud und KI. Dies ermöglicht smarte Fabriken und Prozesse, welche die neuen KI-Möglichkeiten hier in Deutschland wertschöpfend nutzen.

Auf solchen High-Performance-Industrie-Netzwerken baut die weitere Automatisierung unserer Industrie und jedes datengetriebenen Geschäftsmodells auf. Im Lauf der Zeit haben sich die Fähigkeiten der Wireless-Technologien gegenüber kabelgebundenen Netzen erheblich verbessert. Wichtig ist die Erhöhung der Datenübertragungsrate von wenigen Megabit pro Sekunde auf mehrere Gigabit pro Sekunde. Viele Maschinen bieten heute robuste Wireless-Schnittstellen an. Zudem können auch private 5G- & zukünftig auch 6G-Campus-Netze die industriellen Services agiler machen – z. B. durch die Positionsbestimmung etwa von autonomen Transportfahrzeugen oder mobilen Robotern in der Fertigungslinie.

Integrierte KI-Lösungen mit IT- und OT-Security für die Praxis
So automatisieren Unternehmen ihre Produktion oder entwickeln ganz neue integrierte KI-Lösungen aus Maschinen, Leittechnik, Industriesoftware und Daten. Mit KI-Plattformen und Software-gestützter Automatisierung werden physische Fabriken als digitale Zwillinge KI-gestützt simuliert und optimiert. Die Frage der nötigen Datensouveränität wird dabei häufig diskutiert, die Antworten sind allerdings kundenspezifisch und benötigen eine Analyse entlang der geltenden Regulierung. Ganzheitliche IT- und OT-Security-Lösungen sorgen dabei für durchgängigen Schutz der Fabriken, ihrer Maschinen und Anlagen sowie der Produktionsgüter.

Ein Cybersecurity-Kunde von Axians stammt aus der Nahrungsmittelindustrie. Als einer der größten Käsehersteller Deutschlands mit Fokus auf Qualität und Nachhaltigkeit verfügt er über 6000 vernetzte Assets in seinen Werken und in der Verwaltung. Über ein durch Axians betriebenes Security-Operations-Center wird ein Security-Information- und Event-Managment-System mit Analyse-, Bewertungs- und Abwehrmechanismen eingesetzt. Die Umsetzung von KRITIS-Anforderungen und umfassende Cybersicherheit werden so rund um die Uhr nachhaltig sichergestellt.

Essenziell bleibt insgesamt für industrielle Digitalisierungsprojekte, alle relevanten Abteilungen einzubeziehen – also Management, Produktion, Planung, Einkauf, Logistik, Vertrieb, IT & Cybersicherheit sowie Compliance & Datenschutz. Nur in enger Zusammenarbeit wird die digitale Transformation unserer Industrie gelingen.

Text **Olaf Niemeitz, Managing Director Networks & Security, Axians Deutschland**

Weitere Informationen unter:
axians-secure.de

Treffen Sie uns auf der Hannover Messe:

axians

Kritische Infrastruktur ist das eigentliche Schlachtfeld des Cyberkriegs

Ein Klick im Netz und in einem Krankenhaus in Berlin gehen die Bildschirme aus. Ein unbemerkter Login und die Bänder eines Logistikers stehen still.

Björn Trappe
Managing Director,
ehem. militärischer Cyberoperateur

Regulierung ist kein Selbstzweck. Richtig umgesetzt wird sie zu einem strategischen Vorteil.

Die Illusion, Cyberkrieg spiele sich vor allem in Rechenzentren ab, ist bequem. Tatsächlich entscheidet er sich an Umspannwerken, in Wasserwerken, Logistikzentren, Krankenhäusern und Telekommunikationsnetzen. Aus Sicht einer professionellen Angreiferin oder eines Angreifers ist kritische Infrastruktur kein Ziel unter vielen. Sie ist der Hebel, der mit begrenztem Einsatz maximale Wirkung entfaltet. Wer Daten stiehlt, verursacht Kosten. Wer Versorgung stört, erzeugt Unsicherheit, politischen Druck und wirtschaftliche Reibung zugleich. Genau deshalb beschreibt die europäische Richtlinie zur Resilienz kritischer Einrichtungen solche Dienste als unverzichtbar für wesentliche gesellschaftliche Funktionen und wirtschaftliche Aktivitäten. Ihr Ausfall zieht Folgen nach sich, weit über den betroffenen Sektor hinaus.

Zäsur im Netz: vom Zugriff zur Wirkung

Westliche Sicherheitsbehörden warnen seit einiger Zeit vor einer Verschiebung der Bedrohung. Staatliche Akteure sitzen schon lange nicht mehr nur in Netzen, um mitzulesen. Sie positionieren sich, um im Krisenfall stören zu können. Die amerikanische Cyberbehörde CISA formuliert das ungewöhnlich klar: Es geht um Vorpositionierung in informationstechnischen Netzen, um von dort in industrielle Steuerungsumgebungen vorzudringen und im Fall geopolitischer Spannungen oder militärischer Konflikte störende Effekte auszulösen. Das ist die eigentliche Zäsur. Was lange als nachrichtendienstliche Theorie galt, ist heute operative Realität: Der Zugang selbst ist nicht mehr der Erfolg, sondern lediglich die Vorbereitung auf den Moment, in dem Wirkung verlangt wird.

Wer so denkt, interessiert sich nicht vorrangig für Kundendaten. Relevant sind Netzpläne, Fernwartungszugänge, technische Dokumentation, Alarmbilder, Konfigurationsstände, Bedienerinformationen und vor allem die Frage, welche Abhängigkeit welche andere mitreißt. Jüngste Industrieberichte zeigen, dass mehrere Gruppen genau dieses Wissen sammeln. Sie identifizieren Ingenieursarbeitsplätze, ziehen Alarm- und Konfigurationsdaten ab und kartieren die Netze, um physische Prozesse so präzise zu verstehen, dass sie später gezielt gestört werden können. Ebenso bemerkenswert ist die Arbeitsteilung. Ein Akteur beschafft den Zugang, ein anderer bereitet die operative Wirkung vor. Das verkürzt die Strecke vom Eindringen bis zum Ausfall erheblich. Zugleich verfügen weltweit weniger als zehn Prozent der industriellen Netze über ausreichende Sichtbarkeit und Überwachung. Wer angegriffen wird, merkt es häufig erst, wenn der Betrieb bereits sichtbar leidet.

Einfache Mittel, große Wirkung – und die Frage der Souveränität

Für diese Art von Wirkung braucht es oft keine exotische Schadsoftware. Häufig reichen schlecht geschützte Fernzugänge, zu weitreichende Partnerzugriffe, fehlende Trennung zwischen Unternehmens-IT und Produktion sowie schwache Überwachung an den Übergängen. Genau deshalb ist es ein Irrtum, Ransomware in der Industrie als reines Büroproblem abzulegen. Laut dem aktuellen Dragos OT/ICS Cybersecurity Report 2026 zeichnet sich ein düsteres Bild der industriellen Cybersicherheit ab, da das spezialisierte Sicherheitsunternehmen für das Jahr 2025 eine Rekordaktivität von 119 Ransomware-Gruppen mit Angriffen auf über 3300 Organisationen verzeichnete. Der operative Schaden entstand oft nicht durch den direkten Eingriff in Maschinen, sondern durch Angriffe auf Virtualisierung, Leitstandunterstützung und Überwachungssysteme. Wenn Bedienende nichts mehr sehen und nichts mehr steuern können, steht die Produktion trotzdem still. Der Gegner braucht dann keine spektakuläre Sabotage. Es genügt, die betrieblichen Abhängigkeiten besser zu verstehen als der Betreiber selbst.

An dieser Stelle beginnt die Frage der Souveränität. Sie ist kein politisches Schlagwort, sondern eine nüchterne Betriebsgröße. Souverän ist nicht, wer alles allein baut. Souverän ist, wer die eigenen kritischen Abhängigkeiten kennt, Fernzugriffe beherrscht, Produktlebenszyklen überblickt, Sicherheitsupdates verlässlich erhält und im Krisenfall nicht erst im Ausland um Handlungsfähigkeit bitten muss. Wer bei Netzkomponenten, Steuerungssoftware, Cloud-Diensten, Identitäten oder Fernwartung den Überblick verliert, verliert im Ernstfall Entscheidungsspielraum. Genau hier gewinnt der Cyber Resilience Act an Bedeutung. Er führt verbindliche Cybersicherheitsanforderungen für Hardware und Software über den gesamten Lebenszyklus ein. Die Verordnung ist seit Dezember 2024 in Kraft. Meldepflichten für aktiv ausgenutzte Schwachstellen greifen ab September 2026. Die zentralen Pflichten gelten ab Dezember 2027. Das ist mehr als Regulierung. Es ist ein Schritt hin zu belastbarer digitaler Souveränität in der Lieferkette.

Bilanzästhetik mit Resilienz verwechseln

Für Entscheiderinnen und Entscheider ist der eigentliche Punkt ein anderer: Kritische Infrastruktur ist längst kein Thema mehr, das man der Technikabteilung überlässt. Die europäische NIS2-Richtlinie gilt seit dem 18. Oktober 2024. In Deutschland ist das Umsetzungsgesetz seit dem 6. Dezember 2025 in Kraft. Betroffene Unternehmen müssen sich registrieren, erhebliche Sicherheitsvorfälle melden und Risikomanagementmaßnahmen implementieren und dokumentieren. Das Bundesamt für Sicherheit in der Informationstechnik weist ausdrücklich darauf hin, dass die Verantwortung für Umsetzung und Überwachung bei der Geschäftsleitung liegt. Das ist richtig. Denn im Cyberkrieg scheitert selten nur Technik. Es scheitern Entscheidungen, Verantwortlichkeiten und Prioritäten. Wer als Vorstand Sicherheit noch immer als Kostenstelle betrachtet, verwechselt Bilanzästhetik mit Resilienz.

Ebenso wichtig ist, dass Europa die digitale und physische Resilienz nicht länger getrennt behandelt. Die Richtlinie zur Resilienz kritischer Einrichtungen und das deutsche KRITIS-Dachgesetz zielen genau darauf ab. Das Gesetz ist seit dem 17. März 2026 in Kraft und schafft bundeseinheitliche Mindeststandards für den Schutz kritischer Infrastrukturen, gestützt auf Risikoanalysen und Meldepflichten. Diese Verbindung ist strategisch entscheidend. Ein Cybereffekt entfaltet seine volle Wirkung selten isoliert. Seine größte Schlagkraft erreicht er, wenn digitale Störung, Desinformation und physischer Angriff oder deren glaubhafte Androhung zusammenfallen. Dann wird aus einem technischen Vorfall eine Lage. Dann verzögert sich Wiederherstellung, dann steigt der psychologische Druck, dann wird aus Betriebsstörung politische Wirkung. Genau deshalb gehört zum Schutz kritischer Infrastruktur immer auch physische Robustheit.

Regulierung ist kein Selbstzweck – sie ist ein strategischer Vorteil

Die gute Nachricht lautet deshalb nicht, dass Europa bereits sicher wäre. Sie lautet, dass die Regulatorik inzwischen in die richtige Richtung weist. NIS2, das KRITIS-Dachgesetz und der CRA bilden zusammen erstmals einen Rahmen, der Governance, Meldedisziplin, Produktverantwortung, physische Sicherheit und operative Widerstandskraft miteinander verbindet. Das ist genau der Weg, den professionelle Angreiferinnen und Angreifer fürchten. Nicht, weil Gesetze beeindrucken. Sondern weil konsequent umgesetzte Regeln Transparenz schaffen, Zugänge verengen, Lieferketten härten, Krisenabläufe schärfen und die Kosten eines Angriffs deutlich erhöhen.

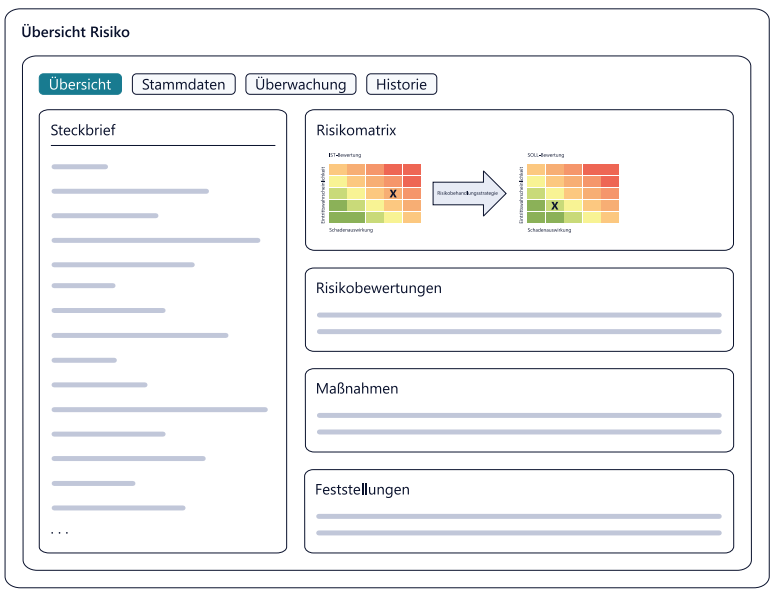
Regulierung ist kein Selbstzweck. Richtig umgesetzt wird sie zu einem strategischen Vorteil. Ob diese Wirkung in der Praxis tatsächlich erreicht wird, wird sich jedoch erst im Ernstfall zeigen. Und genau daran entscheidet sich die Souveränität des Standorts.

Weitere Informationen unter:
laokoon-security.com

Laokoon SecurITy

Warum Informationssicherheit ein System braucht

Informationssicherheit ist längst keine isolierte IT-Aufgabe mehr. Sie ist zu einer Managementfrage geworden, die Organisation, Prozesse, Verantwortlichkeiten und regulatorische Anforderungen zugleich betrifft. Genau an dieser Schnittstelle setzt die ibi systems GmbH mit ihrer Lösung iris an: Je stärker Unternehmen digital arbeiten, desto mehr steigt der Druck, Risiken nicht nur zu erkennen, sondern sie strukturiert zu bewerten, Maßnahmen nachzuhalten und die eigene Sicherheitslage nachvollziehbar zu steuern. Warum ein ISMS- und GRC-Tool für viele Organisationen heute nicht mehr Kür, sondern Voraussetzung ist, zeigt sich genau in diesem Spannungsfeld.



Zwischen Regulierung, Risiken und Nachweisen

Die Herausforderung beginnt selten bei einer einzelnen Vorschrift. Sie entsteht dort, wo verschiedene Anforderungen gleichzeitig erfüllt, dokumentiert und in den Alltag übersetzt werden müssen. Externe Regelwerke wie ISO 27001, NIS-2 oder DORA treffen auf interne Richtlinien, gewachsene Prozesslandschaften, unterschiedliche Zuständigkeiten und steigende Erwartungen an Transparenz. Wer diese Gemengelage mit Insellösungen, Tabellen und Einzelbestimmungen steuert, verliert schnell den Überblick. Ein wirksames Informationssicherheitsmanagement braucht deshalb eine gemeinsame Daten- und Prozessbasis. Zugleich braucht es Entscheidungsgrundlagen, die nicht nur Fachabteilungen, sondern auch Führungskräften einen klaren Blick auf Risiken, Prioritäten und Handlungsbedarf ermöglichen.

Hier setzt ibi systems iris an. Die modulare Plattform für ISMS und GRC bündelt relevante Daten und Abläufe in einem zentralen System und schafft damit die Voraussetzung für mehr Transparenz, schnelleres Reporting und effizientere Arbeitsabläufe. Statt einzelne Aufgaben nebeneinander zu verwalten, lässt sich mit iris ein Rahmen schaffen, in dem Informationssicherheit als durchgängiger Managementprozess sichtbar und handhabbar wird.

ISMS ganzheitlich statt punktuell denken

Der eigentliche Mehrwert eines ISMS zeigt sich dort, wo Zusammenhänge sichtbar werden und Informationssicherheit über die reine Dokumentation hinaus als steuerbarer Prozess greifbar wird. ibi systems iris folgt dabei einem ganzheitlichen Ansatz: In der Software lassen sich Organisationsstruktur, Assets, Prozesse sowie interne und externe Regelwerke abbilden und miteinander verknüpfen. Dadurch wird Informationssicherheit nicht nur formal dokumentiert, sondern in ihren konkreten Bezügen zur Organisation steuerbar. Standards wie ISO/IEC 27001 oder der IT-Grundschutz können genutzt, interne Anforderungen referenziert und Verantwortlichkeiten nachvollziehbar hinterlegt werden.

Besonders relevant ist das dort, wo Sicherheitsarbeit oft fragmentiert verläuft: bei Gap-Analysen, Audits, Feststellungen, Schwachstellen, Vorfällen, Risiken und offenen Maßnahmen. In iris lassen sich diese Elemente nicht nur erfassen, sondern in Beziehung setzen und fortlaufend nachverfolgen. So entsteht ein ISMS, das nicht bloß auf ein Audit hinarbeitet, sondern die Sicherheitslage im laufenden Betrieb abbildet. Kritische Risiken, offene Punkte und Informationssicherheitsvorfälle werden Teil einer gemeinsamen Steuerungslogik.

ibi systems iris zeigt, wie sich Informationssicherheit auf dieser Grundlage als durchgängiger Managementprozess steuern lässt – nachvollziehbar, ganzheitlich und nah an den Anforderungen moderner Organisationen.

Von der Prüfung zur Verbesserung

Ein starkes ISMS endet nicht bei der Bestandsaufnahme. Entscheidend ist, ob aus Prüfungen konkrete Folgeschritte entstehen. Dafür stellt ibi systems iris Funktionen bereit, mit denen Prüfungen geplant, durchgeführt und ausgewertet werden können. Prüfvorlagen sorgen für eine einheitliche Basis, wiederkehrende Prüfungen lassen sich automatisiert anlegen und geführte Prüfungsabläufe erhöhen die Vergleichbarkeit der Ergebnisse. Werden Abweichungen festgestellt, können daraus direkt Feststellungen, Risiken und Maßnahmen abgeleitet werden. Aus isolierten Prüfpunkten wird so ein kontinuierlicher Verbesserungsprozess.

Hinzu kommt ein Reporting, das Informationssicherheit für verschiedene Rollen überhaupt erst greifbar macht. Standardisierte und individuell anpassbare Berichte, Dashboards und Drilldown-Funktionen helfen dabei, Fortschritt, Handlungsbedarf und Prioritäten sichtbar zu machen. Relevante Informationen können so zielgruppenspezifisch aufbereitet werden, statt in verschiedenen Listen, Systemen oder E-Mail-Verläufen verteilt zu bleiben. Auch für Management-Reviews entsteht damit eine fundiertere Grundlage, um Entwicklungen einzuordnen und Maßnahmen gezielter zu priorisieren.

Warum GRC mitgedacht werden muss

Informationssicherheit funktioniert in der Praxis selten losgelöst von Governance, Risk und Compliance. Der GRC-Blick erweitert das ISMS um jene Bereiche, in denen Sicherheitsanforderungen in Prozesse, Kontrollen und Nachweise übersetzt werden müssen. ibi systems iris unterstützt etwa beim Management interner und externer Vorgaben, bei der Planung und Nachverfolgung von Audits, beim Risikomanagement nach gängigen Standards oder beim Aufbau eines zentralen Anforderungskatalogs für verschiedene Compliance-Vorgaben. Daraus entsteht mehr Übersicht und die Möglichkeit, Synergien zwischen verschiedenen Prüf- und Steuerungslogiken zu nutzen.

Wie relevant dieser integrierte Blick ist, zeigt sich besonders dort, wo Risiken außerhalb der eigenen Systemgrenzen entstehen. Lieferantenprüfungen gewinnen an Gewicht, weil die Sicherheit von Anwendungen, Infrastruktur und Prozessen zunehmend auch von Dritten abhängt. iris unterstützt hier nicht nur die initiale Prüfung, sondern auch die fortlaufende Überwachung von Schwachstellen, Risiken und Gegenmaßnahmen über alle Lieferanten hinweg. Das stärkt das ISMS gerade an Schnittstellen zur Lieferkette und zu externen Partnern.

Steuerbarkeit wird zum Sicherheitsfaktor

Mit zunehmender Komplexität der Anforderungen an die Informationssicherheit stoßen isolierte Einzelmaßnahmen an ihre Grenzen. Gefragt ist eine Lösung, die Anforderungen zusammenführt, Verantwortlichkeiten klar abbildet, Prüfprozesse strukturiert, Risiken sichtbar macht und Verbesserungen systematisch nachverfolgt. ibi systems iris zeigt, wie sich Informationssicherheit auf dieser Grundlage als durchgängiger Managementprozess steuern lässt – nachvollziehbar, ganzheitlich und nah an den Anforderungen moderner Organisationen. Genau darin liegt die Stärke eines ISMS- und GRC-Tools.

Text **Walter Nogueira**

Weitere Informationen unter:
ibi-systems.de

Wenn Drohnen dauerhaft beobachten

Ob kritische Infrastruktur, Grenzabschnitte oder Großveranstaltungen: Sicherheitskräfte müssen immer häufiger große Räume dauerhaft überwachen. Neue Technologien setzen dabei zunehmend auf Drohnen und intelligente Sensorik aus der Luft.

Häfen, Industrieanlagen oder Energieparks gehören zu den Orten, die heute besonders geschützt werden müssen: Sie erstrecken sich über enorme Flächen. Wer solche Gebiete sichern muss, steht schnell vor einem praktischen Problem. Ein vollständiger Überblick ist nötig, doch Personal ist begrenzt. Patrouillen können immer nur einen Teil eines Geländes abdecken, Kameras sehen nur, was in ihrem Blickfeld liegt. Gerade dort, wo viele Menschen arbeiten oder sich große Besuchermengen bewegen, ist es jedoch wichtig, Veränderungen früh zu erkennen.


Bild **iStockphoto/MindStorm-inc**

Neue Risiken verändern die Anforderungen

Der Schutz kritischer Infrastruktur ist in den vergangenen Jahren stärker in den Fokus gerückt. Energieanlagen, Verkehrsnetze oder Industriekomplexe gelten heute als besonders sensible Bereiche. Gleichzeitig haben geopolitische Spannungen und Sabotagefälle gezeigt, wie verwundbar große Anlagen sein können. Sicherheitskonzepte müssen deshalb häufiger auch weitläufige Areale einbeziehen, in denen sich nicht ständig Personal aufhalten kann. Viele bekannte Überwachungssysteme sind für solche Aufgaben nur begrenzt geeignet. Feste Kameras liefern zwar kontinuierliche Bilder, doch ihr Blickfeld bleibt eingeschränkt. Gebäude, Vegetation oder Geländeformen können Bereiche verdecken. Auch Kontrollgänge oder Fahrzeugpatrouillen bieten nur eine Momentaufnahme. In großen Anlagen oder offenen Geländeabschnitten entsteht dadurch leicht ein unvollständiges Lagebild.

Drohnen eröffnen neue Möglichkeiten

Seit einigen Jahren nutzen Sicherheitskräfte deshalb zunehmend Drohnen. Ein kurzer Flug genügt oft, um ein Gelände aus der Luft zu überblicken. Polizei, Rettungsdienste und Betreiber großer Anlagen greifen bereits darauf zurück. Der Vorteil liegt auf der Hand: Aus der Höhe lässt sich ein Gebiet ganz anders beobachten als vom Boden aus. Allerdings hat diese Technik auch eine klare Grenze. Klassische Drohnen bleiben meist nur vergleichsweise kurz in der Luft, bevor sie wieder landen müssen. Für eine dauerhafte Beobachtung wären mehrere Geräte im Wechsel nötig. Das erhöht den Aufwand und bindet zusätzliches Personal.

Wenn eine Drohne dauerhaft oben bleibt

Deshalb gibt es inzwischen Systeme, die einen anderen Weg gehen. Bei ihnen ist die Drohne über ein Kabel mit einer Bodenstation verbunden. Über diese Leitung wird Energie zugeführt, gleichzeitig können Daten übertragen werden. Die Drohne bleibt damit dauerhaft in der Luft und kann über längere Zeit an derselben Position eingesetzt werden. Der Effekt ist einfach, aber wirkungsvoll.

Eine Drohne, die dauerhaft über einem Gebiet schwebt, liefert kontinuierlich Bilder und Sensordaten. Veränderungen lassen sich schneller erkennen, weil der Blickwinkel konstant bleibt. Gleichzeitig erweitert die Höhe den Überblick. Bereiche, die vom Boden aus kaum sichtbar wären, geraten plötzlich ins Blickfeld.

Sensoren liefern zusätzliche Informationen

Solche Systeme bestehen meist nicht nur aus einer Kamera. Häufig werden mehrere Sensoren kombiniert. Optische Kameras liefern detaillierte Bilder, während Wärmebildsensoren auch bei Dunkelheit oder schlechter Sicht Aktivitäten sichtbar machen können. Andere Sensoren können zusätzliche Hinweise auf Bewegungen oder Veränderungen geben.

Mit der wachsenden Datenmenge wird auch die Auswertung wichtiger. Moderne Systeme nutzen Software, die Bewegungsmuster analysieren kann. Auffällige Situationen lassen sich so schneller erkennen: Sicherheitskräfte müssen nicht jede Kamera permanent beobachten, sondern erhalten Hinweise, wenn etwas Ungewöhnliches geschieht.

Vom Sensor zum Lagebild

Die Informationen werden häufig in bestehende Lage und Informationssysteme integriert. Dort lassen sie sich mit anderen Datenquellen sicher verbinden. Für Einsatzleitungen entsteht so ein aktuelles Bild der Situation, das ständig ergänzt wird. Wird eine ungewöhnliche Bewegung registriert, können Einsatzkräfte sofort informiert werden.

Die Einsatzmöglichkeiten sind vielfältig. Im militärischen Bereich können solche Systeme zur Sicherung von Feldlagern oder militärischen Einrichtungen genutzt werden. Auch Grenzabschnitte lassen sich aus der Luft besser beobachten. Betreiber kritischer Infrastruktur interessieren sich ebenfalls zunehmend für diese Form der Überwachung.

Auch bei Katastrophen und Großveranstaltungen hilfreich

Im Katastrophenschutz kann der Blick von oben ebenfalls wertvolle Informationen liefern. Bei Waldbränden oder Überschwemmungen lassen sich Entwicklungen aus der Luft oft schneller erkennen. Einsatzleitungen erhalten dadurch zusätzliche Hinweise über die Lage vor Ort. Auch bei Großveranstaltungen kann eine Drohne helfen, Menschenströme besser zu beobachten. Sicherheitskräfte erkennen schneller, wenn sich ungewöhnliche Situationen entwickeln. Gerade bei sehr großen Besucherzahlen kann diese zusätzliche Perspektive hilfreich sein.

Technologie als Unterstützung

Technik ersetzt zwar keine Einsatzkräfte. Sie kann jedoch dabei helfen, Informationen schneller zu sammeln und Entscheidungen auf eine breitere Grundlage zu stellen. Systeme, die große Räume dauerhaft aus der Luft beobachten und Daten automatisch auswerten, könnten deshalb künftig eine wichtige Ergänzung für Sicherheitsorganisationen sein.

Text **Thomas Soltau**

Autarke Infrastruktur für eine neue Sicherheitslage

Geopolitische Spannungen, hybride Bedrohungen und wachsende Anforderungen rücken resiliente Versorgungsstrukturen stärker in den Fokus. Militärische Liegenschaften, medizinische Einrichtungen oder systemrelevante Industrien müssen auch bei Netzausfällen oder Sabotage handlungsfähig bleiben. Veolia hat dafür integrierte Lösungen für Wasser-, Energie- und Abfallmanagement und ist seit Jahren Partner kritischer Infrastrukturen. Wie solche Systeme funktionieren und warum Autarkie strategisch wichtiger wird, erklärt Olaf Kipp, Gesamtkoordinator Military & Defence bei Veolia Deutschland.

Olaf Kipp
Gesamtkoordinator
Military & Defence

Herr Kipp, welche neuen Anforderungen entstehen dadurch für sicherheitsrelevante Standorte?
Viele Versorgungsstrukturen sind über Jahrzehnte unter stabilen Rahmenbedingungen entstanden und vor allem auf Effizienz und Wirtschaftlichkeit ausgelegt, weniger auf Szenarien mit längerfristigen Störungen oder sicherheitsrelevanten Ausfällen. Heute verschiebt sich der Fokus deutlich stärker auf Resilienz.

Betreiber müssen sicherstellen, dass zentrale Funktionen auch dann aufrechterhalten werden können, wenn externe Netze nur eingeschränkt verfügbar sind. Für sicherheitsrelevante Standorte bedeutet das vor allem Versorgungssicherheit und eine größere Unabhängigkeit von externen Infrastrukturen und Systemen, die auch unter außergewöhnlichen Bedingungen funktionsfähig bleiben. Entscheidend ist, dass die kritische Betriebsfähigkeit eines Standorts auch bei Störungen der öffentlichen Infrastruktur gewährleistet werden kann.

Wie funktioniert ein Standort, der sich im Krisenfall selbst versorgen kann, also autark ist?
Autarkie bedeutet nicht vollständige Isolation vom öffentlichen Netz. Dennoch geht es darum, kritische Infrastrukturen auch dauerhaft eigenständig zu betreiben. Im Wasserbereich kann dies über eigene Brunnenanlagen, Aufbereitungssysteme und ausreichende Speicherkapazitäten erfolgen. In der Energieversorgung entsteht Autarkie meist durch die Kombination mehrerer dezentraler Technologien wie beispielsweise Photovoltaik, Geothermie sowie Strom- und Wärmespeicher. Entscheidend ist dabei das Zusammenspiel dieser Komponenten. Erst die intelligente Kopplung von Erzeugung, Speicherung und Steuerung ermöglicht es, einen Standort auch im Inselbetrieb zu betreiben. Dadurch entsteht eine deutlich höhere Versorgungssouveränität gegenüber externen Infrastrukturen.

> **Resiliente Infrastruktur basiert auf Robustheit und klaren Betriebsstrukturen. Anlagen müssen auch unter eingeschränkten Bedingungen zuverlässig funktionieren und stabil betrieben werden können.**
>
> – Olaf Kipp, Gesamtkoordinator Military & Defence

Viele Standorte sind weiterhin stark von externen Netzen abhängig. Wo sehen Sie die größten Risiken?
Zentrale Netze sind leistungsfähig und effizient, gleichzeitig erhöhen sie die Abhängigkeit von komplexen Versorgungsketten. Störungen können durch technische Defekte, Extremwetterereignisse oder Cyberangriffe entstehen und sich schnell auf einzelne Standorte auswirken.

Unsere Lösung dazu ist eine Versorgungsanlage direkt am Standort, das heißt innerhalb des Zaunes. Öffentliche Netze sind damit eine Ergänzungsfunktion oder dienen zur Einspeisung aus diesen Anlagen in das Netz.

Veolia verbindet Energie-, Wasser- und Stoffkreisläufe in integrierten Lösungen. Warum ist diese sektorübergreifende Betrachtung so wichtig?
Weil sich daraus erhebliche Synergieeffekte ergeben. Energie- und Wassersysteme sind technisch eng miteinander verbunden und lassen sich effizient miteinander koppeln.

Abwärme aus Energieprozessen kann beispielsweise für thermische Verfahren in der Wasseraufbereitung genutzt werden. Gleichzeitig lassen sich bestimmte industrielle Wärmeprozesse wiederum zur Energieerzeugung einsetzen. Wenn Planung, Bau und Betrieb solcher Systeme integriert erfolgen, reduziert das Schnittstellen und erhöht die Effizienz der gesamten Infrastruktur. Gerade bei komplexen Standorten mit hohem Energie- und Wasserbedarf führt diese sektorübergreifende Planung zu stabilen und resilienten Versorgungsstrukturen.

Solche Standorte müssen auch unter extremen Bedingungen funktionieren. Welche Anforderungen stellt das an die Infrastruktur?
Resiliente Infrastruktur basiert auf Robustheit, Redundanz und klaren Betriebsstrukturen. Anlagen müssen auch unter eingeschränkten Bedingungen zuverlässig funktionieren und stabil betrieben werden können. Ziel ist eine Infrastruktur mit hoher technischer und organisatorischer Durchhaltefähigkeit, die auch unter erschwerten Bedingungen zuverlässig funktioniert, etwa bei reduzierter Personalverfügbarkeit oder eingeschränkten logistischen Möglichkeiten.

Welche Rolle spielen digitale Technologien und künstliche Intelligenz in solchen Systemen?
Digitale Systeme ermöglichen eine kontinuierliche Überwachung von Anlagen, eine präzise Analyse von Betriebszuständen und eine frühzeitige Erkennung möglicher Störungen. Künstliche Intelligenz kann beispielsweise helfen, Energieflüsse zu optimieren, Lastprofile vorherzusagen oder Wartungsbedarfe frühzeitig zu erkennen.

Gerade bei kritischen Infrastrukturen bleibt jedoch entscheidend, dass alle Systeme transparent und jederzeit kontrollierbar bleiben.

Welche Rolle kann Veolia für Betreiber solcher Standorte spielen?
Die strategische Bedeutung resilienter Versorgungsstrukturen wird heute kaum noch unterschätzt. Die eigentliche Herausforderung liegt weniger in der Erkenntnis als vielmehr in der praktischen Umsetzung. Komplexe Infrastrukturprojekte erfordern langfristige Planung, technisches Know-how und stabile Betriebsmodelle. Wir bündeln unsere Erfahrungen aus kommunaler Infrastruktur, industriellen Versorgungssystemen und anderen kritischen Einrichtungen in unserem Geschäftsbereich Veolia Industrial Solutions. Ziel ist es, weitere integrierte und skalierbare Versorgungssysteme zu planen, zu bauen und zu betreiben, welche die kritische Betriebsfähigkeit sicherheitsrelevanter Standorte dauerhaft gewährleisten und damit auch unter außergewöhnlichen Bedingungen stabil funktionieren.

Weitere Informationen unter:
veolia.de/branche-defense

VEOLIA

SAP-Security: Die unterschätzte Blackbox in der IT-Sicherheitsarchitektur

In den meisten Unternehmen gelten SAP-Systeme noch immer als Blackbox, besonders aus Sicht der zentralen IT-Security. Diese betrachtet sie häufig isoliert und bindet sie nicht in übergreifende Sicherheitsprozesse wie Patch- und Vulnerability-Management, Threat-Detection oder Incident-Response ein. Grund dafür ist der hohe Spezialisierungsgrad einer SAP-Umgebung bei gleichzeitiger Kritikalität für die Organisation. Durch diese Berührungsängste entstehen gefährliche Lücken. Besonders unterschätzt werden Schwachstellen im Berechtigungsmanagement, unzureichende Nutzersensibilisierung sowie eine fehlende durchgängige Sicherheitsarchitektur, die vom Security-Design über sichere Konfiguration bis hin zu Code-Security und -Monitoring reicht. Um SAP-Systeme effektiv abzusichern, braucht es einen ganzheitlichen, proaktiven Ansatz und ein Umdenken in der Sicherheitsstrategie aller Unternehmen. Denn die Hersteller und Betreiber von Systemen und Applikationen sind *nicht* für die IT-Sicherheit der Unternehmen verantwortlich.

Oliver Villwock
Consulting Director mit Schwerpunkt SAP-Security
cbs Corporate Business Solutions

Robert Stricker
Abteilungsleiter Security Consulting
Materna

Oliver Villwock, Consulting Director mit Schwerpunkt auf SAP-Security bei cbs Corporate Business Solutions, und Robert Stricker, Abteilungsleiter Security Consulting der Materna, sprechen im Interview über die Dringlichkeit, die unternehmenseigenen Kronjuwelen besser abzusichern – und sich um die SAP-Sicherheit zu kümmern.

Herr Villwock, Herr Stricker, SAP-Systeme gelten vielen als Blackbox. Wie könnte man Licht in diese Blackbox bringen?
Villwock: Für effektive SAP-Sicherheit braucht es drei Dinge: Transparenz durch spezialisierte Tools, fundiertes SAP-Know-how zur Einordnung von Risiken und daraus abgeleitete wirksame Schutzmaßnahmen.

Stricker: Zusätzlich muss geklärt sein, wer für SAP-Security eigentlich verantwortlich ist. Dann muss das Management SAP als sicherheitskritisch anerkennen, denn kritische Geschäftsprozesse hängen oft direkt von SAP ab, werden sicherheitstechnisch aber unzureichend berücksichtigt.

Wie lässt sich die SAP-Security in bestehende Strukturen integrieren?
Villwock: SAP-Security muss auf Governance-Ebene starten, verankert in der IT-Security-Policy mit klaren Zuständigkeiten und Kommunikationswegen. Operativ braucht es Transparenz, um Altlasten in Konfiguration und Design schrittweise zu beheben. Eine realistische, extern begleitete Roadmap sorgt für nachhaltige Sicherheit ohne Überforderung von Budget und Organisation.

Stricker: Unternehmen sollten SAP konsequent in bestehende Security-Prozesse integrieren, mit klaren Verantwortlichkeiten, fundierter Risikoanalyse und Einbindung unter anderem in Patch-, Change- und Incident-Management. SAP-Security ist Teil der Gesamtstrategie, kein Sonderfall.

Was sind aus Ihrer Sicht die wichtigsten ersten Schritte für Unternehmen, die SAP-Security ernst nehmen wollen?
Villwock: Ein klares Assessment ist der erste Schritt: Wo stehen wir? Was haben wir? Wer ist wofür verantwortlich? Ohne Bestandsaufnahme fehlt die Grundlage für jede sinnvolle Planung.

Durch S/4-Transformation, Cloud-Migration und neue Architekturen entsteht die Chance, Security von Anfang an neuzudenken. Wer jetzt richtig handelt, verhindert den nächsten Security-Stau.

Wie sehen Sie denn die Entwicklung in den nächsten Jahren? Wird SAP-Security jetzt endlich zur Priorität werden?
Stricker: Es muss! Laut NIS2-Richtlinie müssen kritische Geschäftsprozesse geschützt werden, und da führt (fast) kein Weg an SAP vorbei. SAP steuert zentrale Abläufe, teils nicht nur in der IT, sondern auch in OT-Bereichen.

Villwock: SAP beinhaltet die Kronjuwelen von Unternehmen. Wer SAP-Security nicht ernst nimmt, gefährdet die Resilienz seines Unternehmens. Jetzt zu handeln ist unerlässlich, sonst wird es in Zukunft teuer und riskant.

Was ist Ihre Mission in diesem Bereich?
Stricker: Berührungsängste abbauen. SAP wird in Sachen Informationssicherheit oft wie eine Blackbox behandelt, die keiner versteht. Das führt zu Unsicherheit und Stillstand. Unsere Mission ist es, genau hier anzusetzen: SAP darf kein blinder Fleck bleiben, denn die Risiken sind aufgrund der Kritikalität der verarbeiteten Daten hoch. SAP abzusichern und zu überwachen ist jedoch keine Raketenwissenschaft.

Villwock: Unsere Mission ist klar: Kunden zu helfen, Transparenz zu schaffen und SAP-Security nachhaltig, effizient, vorausschauend und zukunftssicher umzusetzen. Der Markt ist überladen mit Tools, aber es fehlt fundierte Beratung, die Tools, Prozesse und Menschen sinnvoll verbindet. Genau da setzen wir an.

SAP beinhaltet die Kronjuwelen von Unternehmen. Wer SAP-Security nicht ernst nimmt, gefährdet die Resilienz seines Unternehmens.

– Oliver Villwock,
Consulting Director mit Schwerpunkt SAP-Security
cbs Corporate Business Solutions

Unternehmen sollten SAP konsequent in bestehende Security-Prozesse integrieren, mit klaren Verantwortlichkeiten, fundierter Risikoanalyse und Einbindung in Patch-, Change- und Incident-Management.

– Robert Stricker,
Abteilungsleiter Security Consulting Materna

Von der automatisierten zur adaptiven Intralogistik

Mit Riesenschritten entwickelt sich die Intralogistik in Richtung hochgradig vernetzter, adaptiver Systeme, die häufig unter dem Begriff »Logistics 5.0« zusammengefasst werden: Autonome, mobile Roboter (AMR), eine enge Mensch-Roboter-Kollaboration, KI-gestützte Entscheidungsunterstützung sowie resiliente und flexible Strukturen verändern Produktion, Lager und Versand – und sorgen dabei für mehr Sicherheit und Geschwindigkeit.

Fernab der Öffentlichkeit finden in großen Produktionsstätten, Lagerhallen und beim Versand gerade tiefgreifende Veränderungen statt. Damit Produkte schneller produziert und ausgeliefert werden können, müssen alle damit zusammenhängenden Prozesse wie Wareneingang, Herstellung, Verpackung, Lagerung, Kommissionierung und Versand in extrem hoher Geschwindigkeit sicher ineinandergreifen. Dieses Tempo basiert auf vernetzten, datengetriebenen und zunehmend autonomen Systemen mit KI-gestützter Robotik.

Autonome mobile Roboter (AMR) spielen dabei eine Schlüsselrolle. Sie übernehmen innerbetriebliche Transporte und navigieren selbstständig mittels Sensorik, 3D-Vision und künstlicher Intelligenz. Die wendigen Helfer lassen sich flexibel skalieren und gut in bestehende Umgebungen integrieren, denn sie benötigen keine festen Leitlinien oder Förderbänder. Der Erfolg gibt den AMR recht: Weltweit werden jährlich mehr als 100 000 solcher Systeme neu eingesetzt. Die an den individuellen Bedarf angepassten Roboter rollen außerhalb von Verteilerzentren auch beispielsweise in Krankenhäusern zum schnellen Transport von großen Medikamentenmengen – auch über verschiedene Stockwerke – durch die Flure. AMR haben ebenso Einzug in Möbelunternehmen gehalten, wo sie den tonnenschweren Materialfluss steuern – und dabei Verletzungsgefahr und Fehlerquote gegen Null bringen.

Vorbei ist die Zeit, in der Lagermitarbeitende täglich kilometerweit laufen mussten, um ein bestimmtes Produkt zu finden und von A nach B zu bringen. Roboter können das Wunschprodukt inzwischen selbstständig heraussuchen und transportieren. Dieses »Goods-to-Person«-Prinzip reduziert Laufwege und steigert Effizienz und Genauigkeit. Zunehmend werden auch bislang schwer automatisierbare Prozesse erschlossen, etwa das Depalettieren, die Wareneingangsprüfung mittels Computer Vision oder sogar das Be- und Entladen von Lkw. Wurde bis vor ein paar Jahren viel dafür getan, »an der Rampe« ein paar Minuten Zeit einzusparen, hat jetzt die entsprechende Software das Zepter in der Hand

Bild **iStockphoto/zorazhuang**

Während die Maschinen repetitive Tätigkeiten übernehmen, können die menschlichen Mitarbeitenden entlastet werden und Tätigkeiten mit mehr Wertschöpfung ausführen.

– ein Zepter, das »Warehouse Execution Systems« (WES), KI-gestützte Optimierung und Echtzeit-Datenintegration zu einem Gesamtsystem mit intelligenter Steuerung verknüpft.

Ein zentraler Vorteil dieser Verknüpfung ist die Produktivitätssteigerung: Robotisierte Systeme können rund um die Uhr arbeiten, werden nicht müde, nicht unaufmerksam und verletzen sich nicht. In vielen Fällen lässt sich die Leistung von Lagerprozessen deshalb um ein Vielfaches erhöhen.

Gleichzeitig werden körperlich sehr belastende oder monotone Tätigkeiten durch Roboter übernommen, was Unternehmen unabhängiger von schwer zu besetzenden Positionen macht.

Auch die Flexibilität steigt deutlich: Moderne Robotersysteme können schnell an veränderte Anforderungen angepasst werden, etwa bei saisonalen Schwankungen oder kurzfristigen Änderungen in der Nachfrage. Skalierbare Roboterschwärme ersetzen dabei zunehmend starre Fördertechnik. Ein weiterer Vorteil liegt in der Datentransparenz, denn robotisierte Systeme erzeugen kontinuierlich Daten über Durchsatz, Auslastung und Fehlerquoten. Diese bilden die Grundlage für eine systematische Optimierung von Prozessen.

Nicht jedes Unternehmen muss jetzt allerdings zwangsweise ganze Armeen von Robotern kaufen – die automatisierten Helfer lassen sich auch mieten. Neue Geschäftsmodelle wie Robotics-as-a-Service (RaaS), bei denen Unternehmen Robotik-Lösungen mieten statt kaufen, senken Einstiegshürden und erleichtern insbesondere mittelständischen Betrieben den Zugang zur Automatisierung.

Die Einführung von Robotik verändert Arbeitsabläufe und Rollenprofile, und viele Mitarbeitende stehen den neuen »Kollegen« erst einmal skeptisch gegenüber. Geschäftsführerinnen und Geschäftsführer, die AMRs bereits einsetzen, betonen deshalb, wie wichtig es ist, Mitarbeitende frühzeitig mit einzubeziehen, ihnen Fragen zu stellen, ihre Arbeitsweise zu verstehen. Positiv wirkt sich hierbei die Zusammenarbeit mit einem erfahrenen Integrator aus, denn dieser weiß um technische Hürden und findet optimale Lösungen. Während die Maschinen repetitive Tätigkeiten übernehmen, können die menschlichen Mitarbeitenden entlastet werden und Tätigkeiten mit mehr Wertschöpfung ausführen. Der zentrale Wandel liegt also weniger im Wegfall von Arbeit als in der Verschiebung von Qualifikationsanforderungen. Die Roboter zerstören also nicht zwangsläufig Jobs, sondern erhöhen die Nachfrage nach qualifizierten Fachkräften in den Bereichen Technik, Datenanalyse und Systemsteuerung.

Bis in zehn Jahren wird sich der Arbeitsmarkt in der Logistik spürbar verändern: Tätigkeiten wie Laufkommissionierung, klassische Staplerfahrten und manuelle Sortierung und Verpackung werden stark zurückgehen, während Bereiche wie Robotikbetrieb, Datenanalyse, Leitstandssteuerung und Qualitätskontrolle wachsen. Gleichzeitig entstehen neue Rollen wie Robotik- und Automationsspezialistinnen zur Wartung und Integration der Systeme sowie Daten- und KI-Experten, um Prozesse zu analysieren und Materialflüsse zu optimieren.

Trotz Automatisierung kann die Beschäftigung in der Intralogistik insgesamt steigen, da E-Commerce, Liefergeschwindigkeit und Systemkomplexität zunehmen und mehr technisches Personal erforderlich sein wird.

Text **SMA**

Warum Kontrolle im Störfall entscheidend wird

Tobias Löhr & Bernd Schäfer
Associate Partners

Moderne IT-Systeme bestehen aus vielen vernetzten Softwarebausteinen in komplexen Entwicklungs- und Betriebsumgebungen. Risiken entstehen oft unsichtbar im technischen Unterbau. Technische Souveränität bedeutet daher, Abläufe auch bei Ausfällen oder Kompromittierungen stabil zu halten. Wer die eigene Systemlandschaft versteht, kann robuster agieren.

Herr Löhr, wo entstehen heute die kritischsten Schwachstellen?
Viele Risiken liegen in der Software-Lieferkette. Anwendungen bestehen aus zahlreichen Komponenten aus unterschiedlichen Quellen, die automatisiert verarbeitet werden. Fehlerhafte oder ungeprüfte Bestandteile können sich unbemerkt verbreiten. Da diese Schwachstellen tief in komplexen Strukturen verborgen sind, werden sie oft erst spät sichtbar. Organisationen analysieren daher zunehmend systematisch ihre Softwarezusammensetzung.

Wie gelangen solche Schwachstellen in Systeme?
Häufig entstehen sie in automatisierten Build-Prozessen. Diese bestehen aus vielen abgestimmten Schritten und Werkzeugen. Wird hier etwas manipuliert, übernimmt die Software die Veränderung automatisch. Aufgrund der Komplexität fällt dies oft erst im Betrieb auf. Transparenz in dieser »Herstellungsschicht« ist daher entscheidend.

Welche Risiken entstehen durch Abhängigkeiten von Dienstleistern?
Viele Systeme sind auf externe Funktionen wie Cloud-Dienste oder Validierungen angewiesen. Fallen diese aus, geraten interne Prozesse ins Stocken – auch ohne eigenen Fehler. Daher wird es wichtiger zu verstehen, welche externen Abhängigkeiten kritisch sind und wie sich Ausfälle abfedern lassen.

Wie lassen sich diese Risiken beherrschen?
Entscheidend ist ein realistischer Umgang mit Komplexität. Ziel ist nicht die vollständige Fehlervermeidung, sondern Stabilität unter realen Bedingungen. Dafür braucht es Transparenz, ein klares Verständnis der eigenen Prozesse und Tests, die Ausfälle simulieren. So erkennen Organisationen frühzeitig ihre Schwachstellen.

Welche Rolle spielt NIS2?
Die NIS2-Richtlinie fordert, Risiken in Lieferkette, Software-Herstellung und Betrieb getrennt zu betrachten. Sie verlangt Transparenz und betont die Verantwortung des Managements. Entscheidend ist der Nachweis, dass Systeme auch bei Ausfällen funktionsfähig bleiben. Damit rückt die Belastbarkeit in den Fokus und macht technische Souveränität zur strategischen Aufgabe.

Was bedeutet das für die Öffentlichkeit?
Digitale Sicherheit heißt nicht Fehlerfreiheit, sondern Verlässlichkeit trotz Fehlern. In komplexen Systemen wird die Fähigkeit entscheidend, auch bei Störungen die Kontrolle zu behalten. Technische Souveränität basiert daher auf belastbaren Strukturen und klaren Verantwortlichkeiten.

Weitere Informationen unter:
p3-group.com

Vernetzte Roboter für sichere Lieferketten

Moderne Roboter können eigenmächtig Entscheidungen treffen und dadurch Störungen und Ausfallzeiten verhindern. Gregor Spieker, Sales Leader Western Europe bei Teradyne Robotics, erklärt, was Unternehmen dabei beachten sollten.

Gregor Spieker
Sales Leader Western Europe,
Teradyne Robotics

Herr Spieker, in der industriellen Produktion sehen wir gerade, wie sich der »Roboter als eigenständige Maschine« hin zum »Roboter als vernetztes digitales Asset« wandelt. Was bedeutet diese Entwicklung?
Früher arbeiteten Roboter weitgehend isoliert: Programmierung, Steuerung und Wartung fanden direkt vor Ort statt – so wie bei allen anderen Maschinen auch. Daten beschränkten sich meist auf den einzelnen Roboter und nur selten waren Systeme in eine übergeordnete SCADA-Struktur eingebunden.

Heute sind Roboter fester Bestandteil eines vernetzten Produktionsumfelds. Sie kommunizieren mit anderen Maschinen, IT-Systemen, Cloud-Diensten und Analytics-Plattformen und liefern Echtzeitdaten über Leistung, Zustand und Prozessabläufe. Gesteuert werden sie zunehmend über digitale Zwillinge und KI-basierte Assistenten. Damit werden Roboter zu digitalen Assets, die aktiv Daten erzeugen, analysieren und diese in Entscheidungsprozesse einfließen lassen.

Die Vorteile liegen auf der Hand: Vernetzte Roboter steigern die Produktivität, reduzieren Stillstände, unterstützen vorausschauende Wartung und ermöglichen flexible Anpassungen an wechselnde Produktionsbedingungen. Zudem können sie zentral überwacht und gesteuert werden – inklusive Remote-Updates, Konfigurationen und Fehlerdiagnosen.

Wenn eine stärkere Vernetzung eine stärkere Angriffsfläche bietet, wird dann die vernetzte Produktion zum Sicherheitsrisiko?
Cybersicherheit in der Industrie folgt anderen Anforderungen als in klassischen IT-Umgebungen. Produktionsanlagen müssen rund um die Uhr verfügbar, echtzeitfähig und über viele Jahre hinweg zuverlässig betreibbar sein. Eingriffe wie Software-Updates oder Netzwerkänderungen sind nur eingeschränkt möglich, um den laufenden Betrieb nicht zu gefährden.

Zudem sind industrielle Systeme geprägt von langen Lebenszyklen, proprietären Schnittstellen und engen Wechselwirkungen zwischen Steuerungen, Sensorik und Robotik. Deshalb müssen Unternehmen ihre IT-Sicherheitskonzepte anpassen: Ein wirksamer Ansatz verbindet technische Schutzmaßnahmen mit klaren organisatorischen Regeln und berücksichtigt auch den Faktor Mensch. Vorgaben wie der Cyber Resilience Act, NIS2 oder die neue Maschinenverordnung verlangen eine ganzheitliche Cybersicherheitsstrategie über den gesamten Lebenszyklus von Anlagen.

Können Cobot-Zellen, AMR-Flotten und klassische Robotersysteme im Verbund die Sicherheit der industriellen Lieferkette erhöhen?
Klassische Industrieroboter und industrielle Cobots unterscheiden sich in ihrem Einsatzgebiet: Klassische Industrieroboter arbeiten meist eingehaust und bewegen schwere Komponenten in hoch automatisierten Umgebungen. Industrielle Cobots sind flexible, leicht umrüstbare Roboter, die direkt mit Menschen zusammenarbeiten können und sich für vielseitige Aufgaben eignen.

> **Heute sind Roboter fester Bestandteil eines vernetzten Produktionsumfelds. Sie kommunizieren mit anderen Maschinen, IT-Systemen, Cloud-Diensten und Analytics-Plattformen und liefern Echtzeitdaten über Leistung, Zustand und Prozessabläufe.**
>
> – Gregor Spieker, Sales Leader Western Europe, Teradyne Robotics

Autonomous Mobile Robots (AMRs) navigieren selbstständig in ihrer Umgebung und führen Aufgaben aus. In der Intralogistik können sie den Transport und die Verteilung von Materialien innerhalb eines Unternehmens übernehmen. Sie lassen sich zudem mit Cobots kombinieren, um mobile und flexible Automationslösungen zu schaffen.

Im Verbund liefern diese Systeme wertvolle Daten aus Fertigung, Logistik und Materialfluss. Sie ermöglichen eine frühzeitige Erkennung von Engpässen und reduzieren das Ausfallrisiko durch menschliche Fehler – gerade bei körperlich belastenden oder monotonen Tätigkeiten. Zugleich unterstützen sie Unternehmen dabei, den Arbeitskräftemangel abzufedern.

Welche Rolle spielen digitale Zwillinge, sichere Datenpipelines und verschlüsselte Kommunikation für schnelle Reaktionsfähigkeit?
Alle drei Komponenten sind zentrale Bausteine moderner Industrie-5.0-Architekturen:

Digitale Zwillinge ermöglichen Simulationen von Ausfällen, Materialengpässen oder Prozessänderungen, bevor reale Störungen auftreten.

Sichere Datenpipelines übertragen Informationen zuverlässig von Maschinen zu Analyse- und Steuerungssystemen – als Grundlage für schnelle, konsistente Entscheidungen.

> **PolyScope X stärkt die Sicherheit industrieller Lieferketten, weil die Plattform von Grund auf flexibel und cyberresilient gestaltet ist.**
>
> – Gregor Spieker, Sales Leader Western Europe, Teradyne Robotics

Verschlüsselte Kommunikation schützt Betriebsdaten vor unbefugtem Zugriff und reduziert das Risiko von Cyberangriffen und Produktionsunterbrechungen.

Können autonome Systeme sich künftig selbst reorganisieren, wenn Lieferketten unterbrochen werden?
Die Vision autonomer Produktion klingt erst einmal vielversprechend, erfordert jedoch umfassende Voraussetzungen: vollständig vernetzte Systeme, Echtzeitdaten, digitale Zwillinge für Szenarienplanung sowie KI-Algorithmen für die Bewertung von Engpässen und die Priorisierung von Aufträgen. Cobots und AMRs müssen flexibel Aufgaben übernehmen können, während stabile Netzwerke und sichere Kommunikation gewährleistet sein müssen.

Einige dieser Elemente sind bereits Realität – etwa dynamische AMR-Routenplanung, flexible Cobot-Programmierung oder simulationsgestützte Produktionsplanung.

Warum erhöht PolyScope X als moderne, modulare und cloudfähige Softwareplattform die Sicherheit industrieller Lieferketten?
PolyScope X stärkt die Sicherheit industrieller Lieferketten, weil die Plattform von Grund auf flexibel und cyberresilient gestaltet ist. Ihr modularer Aufbau erleichtert es, Prozesse schnell anzupassen oder einzelne Funktionen auszutauschen, ohne gleich ganze Programme neu schreiben zu müssen. So lassen sich Änderungen in der Produktion deutlich schneller umsetzen und Störungen gezielt eingrenzen.

Gleichzeitig unterstützt PolyScope X sichere Remote-Zugriffe, die für Service und Support unverzichtbar sind. Störungen können also auch dann behoben werden, wenn niemand vor Ort ist – ein wesentlicher Vorteil in Situationen, in denen Lieferketten unter Druck stehen oder der Zugang zu Fachpersonal eingeschränkt ist.

Hinzu kommt eine robuste Cybersecurity-Architektur mit rollenbasierten Berechtigungen, Systemhärtung und sicherheitsoptimierten Updates. Diese Mechanismen stellen sicher, dass nur autorisierte Personen Änderungen vornehmen können und sensible Daten geschützt bleiben – eine wichtige Grundlage für stabile, verlässliche Abläufe.

Auch die neu gestaltete Benutzeroberfläche macht viele Aufgaben einfacher und transparenter. Bedienerinnen und Bediener können Anpassungen selbst durchführen, Fehler schneller erkennen und Stillstandzeiten reduzieren. Insgesamt hilft PolyScope X Unternehmen damit, flexibler zu reagieren, Risiken früher zu erkennen und ihre Lieferketten widerstandsfähiger aufzustellen.

Weitere Informationen unter:
universal-robots.com

UR | MiR
TERADYNE Robotics