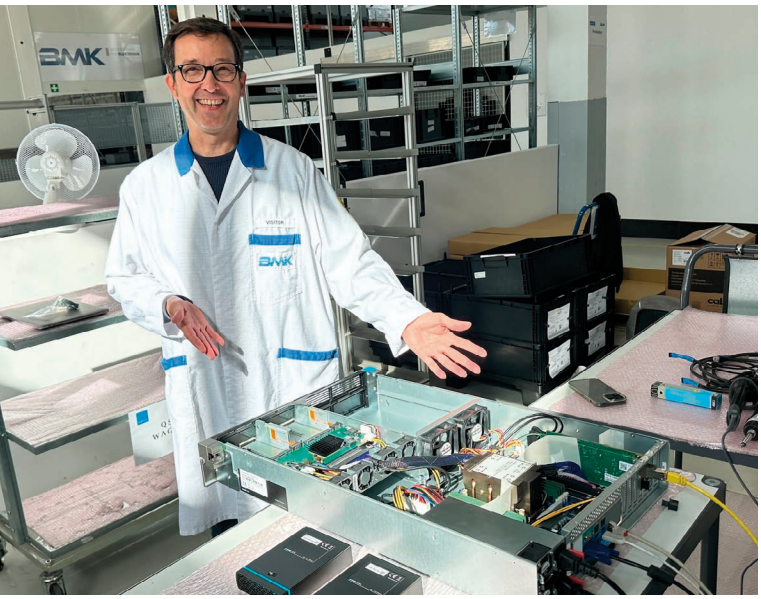
Sicher vernetzt: Wie Cyberresilienz smarte Industrieautomation schützt

In der digital vernetzten Industrie zählt nicht nur die Effizienz intelligenter Systeme, sondern auch ihre Widerstandsfähigkeit. Klare Strategien zur Absicherung und Wiederherstellung zeigen, worauf es jetzt ankommt.



Wenn der Stillstand eintritt, geschieht das selten mit Vorwarnung. Eine E-Mail, ein Klick – und plötzlich kommt die Produktion zum Erliegen, Maschinen stoppen, Daten verschwinden. Die moderne Industrie ist hochgradig digitalisiert, doch damit auch verwundbar. Ransomware, Datendiebstahl, Angriffe auf Lieferketten: Cyberrisiken sind kein Randthema mehr. Sie sind Realität und sie fordern neue Antworten.

Heute reicht die klassische IT-Sicherheit nicht mehr aus. Es geht nicht nur allein um das Abwehren von Angriffen, sondern um die Fähigkeit, auch im Krisenfall weiterarbeiten zu können. Cyberresilienz entwickelt sich zur Schlüsselkompetenz intelligenter Automationssysteme. Wer vernetzt produziert, muss vorausschauend absichern.

Industrie 4.0: Neue Chancen, neue Risiken

Sensorik, Aktorik, Edge-Computing und Cloud-Plattformen haben Produktion und Logistik flexibler gemacht. Doch sie erzeugen auch Angriffsflächen. In der Praxis zeigt sich, dass nicht mehr nur kritische Infrastrukturen, sondern auch mittelständische Industrieunternehmen zunehmend ins Visier professioneller Angreifer geraten. Die Einstiegspunkte sind vielfältig: ungepatchte Systeme, falsch konfigurierte Schnittstellen, mobile Geräte, Mitarbeitende im Homeoffice.

Ransomware

Insbesondere Ransomware hat sich zu einem Dauerproblem entwickelt. Immer mehr Angriffe zielen nicht nur auf die Verschlüsselung von Daten, sondern auf deren Diebstahl und Veröffentlichung. Laut dem „HarfangLab State of Cybersecurity Report 2025“ fürchten 53 Prozent der europäischen Unternehmen heute Datenlecks mehr als Systemausfälle. Für Industrieunternehmen bedeutet das: Produktionsgeheimnisse, Rezepturen oder Maschinenparameter könnten öffentlich werden oder als Druckmittel dienen.

Von der Vorbereitung zur Verteidigung

Was bedeutet Cyberresilienz heute? Resilienz beginnt nicht mit Firewalls oder KI-gesteuerter Bedrohungserkennung. Sie beginnt mit Fragen wie: Welche Systeme sind kritisch? Welche Daten dürfen keinesfalls verloren gehen? Welche Abläufe müssen auch im Krisenfall funktionieren? Die Kartierung und Bewertung der eigenen Informationssysteme ist die Grundlage jeder Resilienz-Strategie.

Ein Beispiel

Wie entscheidend dieser strukturierte Ansatz sein kann, zeigte sich bei einem mittelständischen Automobilzulieferer. Nach einem gezielten Ransomware-Angriff waren zentrale Systeme verschlüsselt, der Betrieb stand still. Nur weil das Unternehmen im Vorfeld auf eine physisch getrennte und regelmäßig getestete Backup-Umgebung gesetzt hatte, gelang der Wiederanlauf innerhalb eines Werktags. Die Lösegeldforderung blieb ohne Wirkung.

Vorausschauende Wiederanlaufstrategien

Solche Angriffe machen deutlich: Es sind nicht nur technische Schutzmaßnahmen gefragt, sondern vor allem vorausschauende Wiederanlaufstrategien. Denn wie schnell ein Unternehmen nach einem Angriff wieder arbeitsfähig ist, entscheidet über wirtschaftliche Folgen, rechtliche Konsequenzen und Vertrauensverluste. Die DSGVO verlangt in Artikel 32 unter anderem die rasche Wiederherstellung der Datenverfügbarkeit nach sicherheitsrelevanten Vorfällen. Mit der EU-Richtlinie NIS-2 wird Cybersicherheit außerdem zur festen Managementaufgabe.

Fehlende Kontrolle untergräbt Sicherheit

Ein zentrales Problem vieler Unternehmen ist der Kontrollverlust über ihre eigenen Systeme. Im HarfangLab-Report geben nur 19 Prozent der Firmen an, vollständige Kontrolle über Infrastruktur und Sicherheitslösungen zu haben. IT-Landschaften sind oft unübersichtlich,

Autor:
Roland Stritt
CRO
FAST LTA
https://www.fast-lta.de/de

Das neue Slilent Brick System

Der Silent Brick Pro kann in eine Schutzhülle gesteckt werden. Dadurch ist er gut geschützt.

über verschiedene Anbieter verteilt und schwer aktuell zu halten.

Gerade in der vernetzten Automation kann das fatal sein. Wenn Maschinen über Clouds gesteuert, Sensordaten extern gespeichert oder Services von Drittanbietern betrieben werden, ist die Transparenz oft gering. Sicherheitslücken können sich unbemerkt ausbreiten. Bei einem Vorfall ist unklar, wer wofür verantwortlich ist. Das ist ein kritischer Punkt, denn rechtlich haftbar bleibt in der Regel das Unternehmen selbst.

Spezifische Herausforderungen der Industrie

Die Industrie steht vor besonderen Herausforderungen, wenn es um Datensicherheit und -verfügbarkeit geht. Produktionsumgebungen sind oft auf Echtzeitprozesse angewiesen, in denen kurze Unterbrechungen schwerwiegende Folgen haben. Gleichzeitig sind viele Anlagen auf jahrzehntealte Systeme angewiesen, die nur eingeschränkt aktualisierbar sind. Hinzu kommen rechtliche Verpflichtungen zur langfristigen, fälschungssicheren Archivierung technischer Nachweise.

Zudem fehlt es häufig an physischen Sicherheitskonzepten in verteilten Werksstrukturen oder bei Maschinen, die über das Internet erreichbar sind. Technische Maßnahmen greifen zu kurz, wenn organisatorische und physische Konzepte fehlen. Entscheidend ist die Kombination aus widerstandsfähiger Speichertechnik, klaren organisatorischen Regeln und regelmäßiger technischer Prüfung. Nur so lässt sich echte Cyberresilienz erreichen.

Backup allein reicht nicht

In der Theorie sind Backups eine Selbstverständlichkeit. Viele Unternehmen scheitern nicht an der Datensicherung, sondern an der Wiederherstellung. Laut dem Veeam Report Ransomware Trends and Proactive Strategies 2025 waren im vergangenen Jahr rund 89 Prozent der Backup-Repositories Ziel von Angriffen, 34 Prozent wurden zumindest teilweise gelöscht.

Besonders riskant ist, dass nur ein kleiner Teil der Unternehmen die Integrität der Backups vor dem Einspielen prüft. Schadsoftware kann so unbemerkt in die Sicherung gelangen und beim Restore erneut zuschlagen. Moderne Recovery-Konzepte beruhen deshalb auf regelmäßigen Tests, isolierten Backup-Repositories, Unveränderbarkeit und Wiederherstellungen in abgeschotteten Umgebungen.

Langzeitspeicher mit WORM-Funktionalität

Industrieunternehmen setzen zunehmend auf Langzeitspeicher mit WORM-Funktionalität, um revisionssichere Backups zu erstellen. Diese werden häufig für technische Dokumentationen, Qualitätssicherungsnachweise oder Maschinendaten mit langen Aufbewahrungsfristen genutzt. Besonders in regulierten Bereichen wie Medizintechnik oder Engineering spielen solche Systeme eine wichtige Rolle. Hier zählen neben der Datensicherheit auch Energieeffizienz und eine lückenlose Nachvollziehbarkeit, etwa für Audits und gesetzliche Prüfungen.

On-Premises erlebt ein Comeback

Ein wachsender Anteil europäischer Unternehmen prüft die Rückkehr zu lokaler Infrastruktur. Nicht, weil Cloudlösungen per se unsicher wären, sondern weil sie Kontrollverlust bedeuten können. Das gilt insbesondere bei Zugriffen aus dem Ausland oder bei unklarer Transparenz über Speicherung und Datenbewegung. Besonders sensible Informationen aus Industrie, Medizin oder Verwaltung benötigen Infrastruktur, die vollständig in europäischer Hand liegt. Das betrifft nicht nur physische Speicherorte, sondern auch Softwarearchitekturen und die Verwaltung kryptografischer Schlüssel.

Mehr Unabhängigkeit

Laut HarfangLab wünschen sich 70 Prozent der befragten Unternehmen mehr Unabhängigkeit von außereuropäischen Technologieanbietern. Die Motive sind Souveränität, Vertrauen und Compliance. On-Premises-Modelle bieten klare Vorteile bei Rückverfolgbarkeit, Audits und schneller Reaktion im Ernstfall. Sie ermöglichen es, langfristige Archivierungspflichten zuverlässig umzusetzen und in kritischen Situationen jederzeit handlungsfähig zu bleiben.

Resilienz ist Teamarbeit

Erfolgreiche Wiederherstellungen gelingen nur dort, wo klare Strukturen bestehen. Unternehmen, die schnell wieder produktionsfähig waren, verfügten über definierte Abläufe, geschulte Mitarbeitende und getestete Notfallprozesse. Wesentlich ist nicht allein die Technologie, sondern das Zusammenspiel von Organisation, Prozessen und Kommunikation.

Dabei spielen auch scheinbar banale Fragen eine Rolle: Wer entscheidet in welchem Szenario? Wie kommuniziert man intern und extern im Fall eines Cybervorfalls? Welche Systeme werden zuerst wiederhergestellt? Fehler in der Koordination können aus einem begrenzten Schaden eine Unternehmenskrise machen.

Wer digital automatisiert, muss digital absichern

Intelligente Automatisierungssysteme, Industrie-4.0-Infrastrukturen und vernetzte Maschinen machen die Produktion effizienter und flexibler - aber auch angreifbarer. Die Zukunft industrieller IT liegt daher nicht in immer neuen Sicherheitsprodukten, sondern in einem durchdachten, ganzheitlichen Resilienz-Ansatz.

Industrieunternehmen, die heute in überprüfbare Schutzmaßnahmen, transparente Speicherlösungen und belastbare Recovery-Prozesse investieren, erfüllen nicht nur regulatorische Anforderungen. Sie sichern ihre Handlungsfähigkeit, bewahren kritische Daten und stärken ihre Position in einem zunehmend digitalisierten Markt. In einer Welt, in der ein Klick Maschinen stilllegen kann, wird Resilienz zur Voraussetzung für Produktivität und Vertrauen. ◄

Das neue Silent Brick System kombiniert NVMe-Performance, HDD-Wirtschaftlichkeit, hohe Skalierbarkeit und echten Air Gap. Der Slot-basierte Controller X nimmt bis zu 8 Silent Brick Pro mit je bis zu 96 TB (brutto) auf und lässt sich mit Silent Brick Max auf bis über 6 Petabyte (brutto) Gesamtkapazität erweitern.