

Operationale Resilienz im Zeitalter der Konnektivität

Neue Forschung zur Cyber-Resilienz in vernetzten Fertigungsumgebungen

Rockwell Automation

Die neue Realität der OT-Sicherheit

Industrieunternehmen vernetzen mehr Systeme, skalieren KI schneller und treiben den Betrieb in Echtzeit voran. Diese Investitionen schaffen Schnelligkeit und Flexibilität. Sie erhöhen auch das operationelle Risiko.

Neue Daten von Rockwell Automation zeigen eine Diskrepanz zwischen Vertrauen und betrieblicher Exposition.

Fast die Hälfte der Unternehmen (46 %) war im vergangenen Jahr von einem Cybervorfall betroffen, dennoch geben 90 % an, dass sie zuversichtlich sind, einen Cybervorfall eindämmen zu können. Mehr als ein Drittel (34 %) bezeichnet Cybersicherheit als eines der größten externen Wachstumshindernisse in den nächsten 12 Monaten.

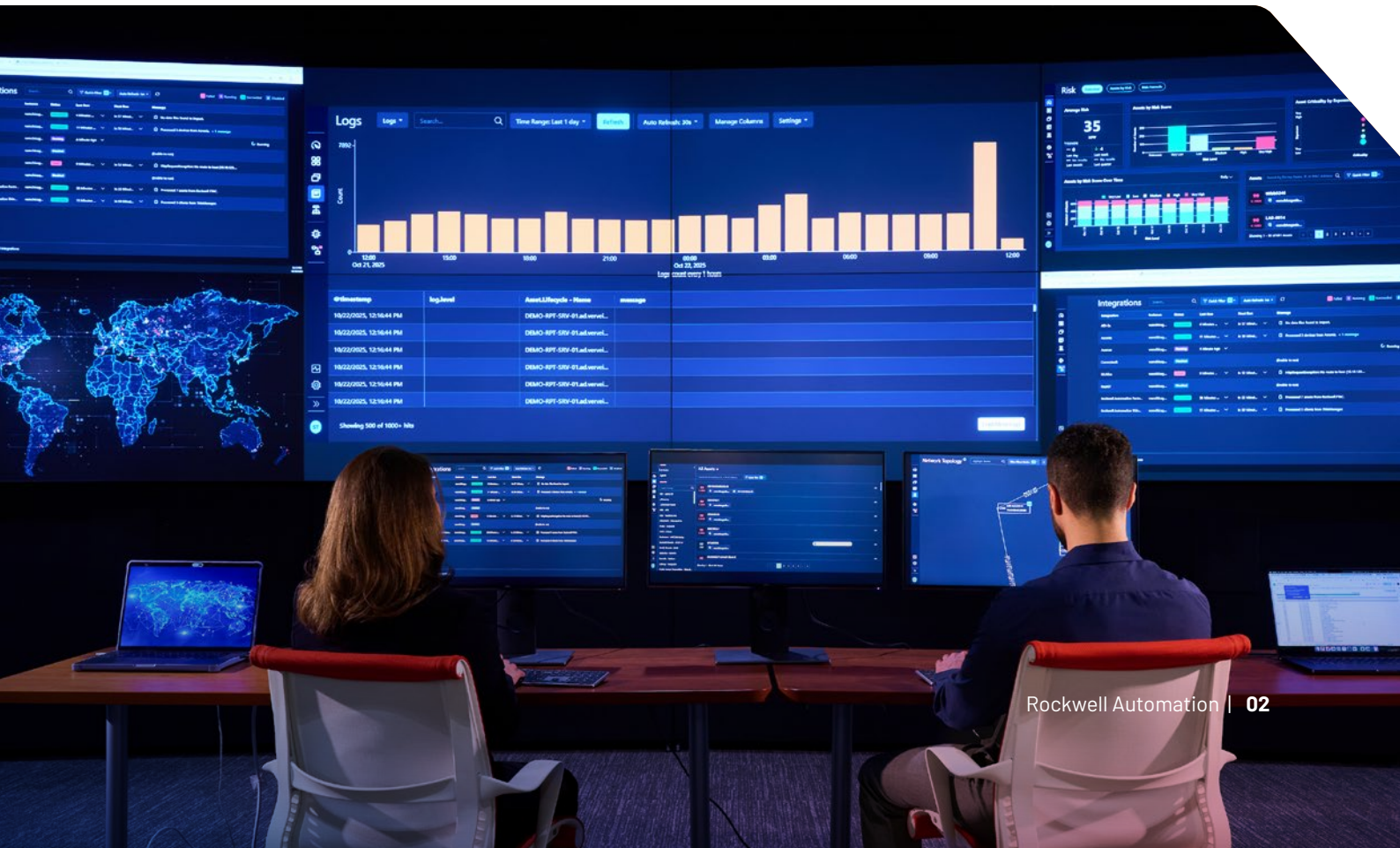
Trotzdem sind sich Unternehmen des Risikos bewusst und ergreifen Maßnahmen, um ihre Widerstandsfähigkeit – und ihr Vertrauen – zu stärken. 62 % haben bereits in Cybersicherheitsplattformen wie Asset-Inventarisierung, Systeme zur Angriffserkennung und sicheren Fernzugriff investiert. Cybersicherheit zählte auch zu den Top-Technologien, die in den letzten 12 Monaten eine Kapitalrendite generierten.

Das Problem ist nicht das Bewusstsein. Industrieunternehmen wissen, dass sich Cyberrisiken auf Betriebszeit, Kontinuität, Produktivität und Wachstum auswirken. Die Herausforderung besteht darin, den Betrieb abzusichern, der immer vernetzter und komplexer wird.

Die Akzeptanz von KI nimmt weiter zu. IT- und OT-Umgebungen konvergieren weiterhin. Die Betriebsdaten durchlaufen mehr Anlagen, Benutzer, Geräte und Anwendungen als je zuvor. Jede Verbindung schafft eine weitere Abhängigkeit. Jede Abhängigkeit schafft eine weitere Angriffsfläche.

Die gute Nachricht ist, dass sich Organisationen der Herausforderung stellen. Sie betrachten Cybersicherheit nicht mehr als eine separate IT-Initiative, sondern sehen sie zunehmend als Teil der operativen Leistungsfähigkeit.

Die Unternehmen, die die nächste Phase des industriellen Betriebs anführen, werden diejenigen sein, die Transparenz, eine sichere Architektur und Reaktionsfähigkeiten aufbauen, die die Produktion bei Störungen am Laufen halten.



Wachsendes Vertrauen durch Investitionen – aber reicht das aus?

Organisationen stehen nicht still. Sie investieren in die Technologien, Architekturen und Fähigkeiten, die zur Stärkung der Cyber-Resilienz erforderlich sind. Der nächste Schritt besteht darin, diese Investitionen in einem Cybersicherheitsprogramm zusammenzuführen, das die Transparenz kontinuierlich verbessert, Risiken reduziert und sich an die sich entwickelnden betrieblichen Anforderungen anpasst. Die Daten zeigen, worauf sich Organisationen heute konzentrieren.

Die wichtigsten Ergebnisse sind:

- IT/OT-Integrationspunkte gelten als besonders anfällig für Cybersicherheitsvorfälle und werden gleich hinter IT-Systemen und Unternehmensnetzwerken eingestuft. Investitionen in Cybersicherheit generierten in den letzten 12 Monaten eine der höchsten Kapitalrenditen.
- Cybersicherheit ist der zweitwichtigste ROI-Treiber unter den Technologieinvestitionen.

Diese Erkenntnisse deuten auf einen klaren Wandel hin: Unternehmen betten Cybersicherheit neben KI, Automatisierung, Cloud-Technologien und vernetzten Abläufen in umfassendere Strategien zur digitalen Transformation ein. Doch da Umgebungen zunehmend vernetzter werden, hängt die Resilienz davon ab, wie gut Organisationen Investitionen in koordiniertes Handeln umsetzen können.



62%

haben bereits in Cybersicherheitsplattformen investiert

45%

planen, in den nächsten 12 Monaten KI und maschinelles Lernen für die Cybersicherheit einzusetzen

35%

Mehr als ein Drittel der Industrieunternehmen bezeichnen die Cybersicherheit als eines der größten externen Wachstumshindernisse – nach dem Arbeitskräftemangel an zweiter Stelle in den nächsten 12 Monaten

37%

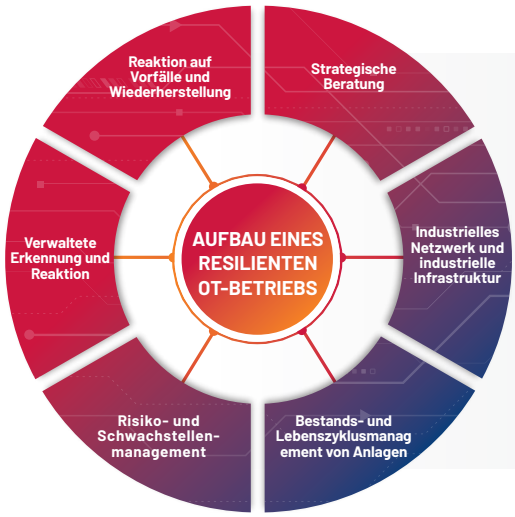
sagen, dass die Sicherung der IT/OT-Architektur in den nächsten fünf Jahren zu positiven Geschäftsergebnissen führen wird

Aufbau eines resilienten OT-Betriebs

Industrieunternehmen haben bei Investitionen in die Cybersicherheit erhebliche Fortschritte gemacht. Die nächste Herausforderung besteht darin, diese Investitionen in operationale Resilienz umzuwandeln.

Doch für stabile OT-Sicherheit braucht es mehr als Tools und Einzellösungen. Dies erfordert einen proaktiven, durchgängigen Ansatz, der auf weltweit anerkannte Rahmenwerke und Standards wie NIST, NIS2 und IEC 62443 ausgerichtet ist. Dies gibt Organisationen eine strukturierte Möglichkeit, die Sicherheitsreife zu verbessern und gleichzeitig gesetzliche Anforderungen zu erfüllen.

Die folgenden Fähigkeiten heben implementierte Maßnahmen führender Organisationen hervor und zeigen, wie dies in der Praxis aussieht.



Strategische Beratung

Entwickeln Sie eine risikobasierte Cybersicherheitsstrategie

Cyber-Resilienz beginnt mit dem Verständnis des Risikos im Kontext von operativen Prioritäten, Geschäftszielen und der organisatorischen Realität. Bevor Unternehmen Risiken effektiv reduzieren, die Resilienz verbessern oder Compliance-Anforderungen erfüllen können, benötigen sie einen klaren Überblick über ihre aktuelle Cybersicherheitsposition und die Lücken, die die größten Auswirkungen haben. Ohne diese Grundlage können Investitionen in die Cybersicherheit fragmentiert und reaktiv werden und sind schwer zu operationalisieren.

Organisationen, die strategische Beratungsdienstleistungen umsetzen, haben folgende Möglichkeiten:

- Identifizieren von Risiken, Festlegen von Prioritäten und Ausrichten der Investitionen auf Geschäftsergebnisse
- Ersetzen reaktiver, spontaner Sicherheitsentscheidungen durch eine priorisierte, risikobasierte Roadmap, die auf operative und geschäftliche Ziele abgestimmt ist
- Verschaffen eines Überblicks über die aktuelle Exposition von Anlagen, Schwachstellen, Prozesse und Governance-Praktiken, damit Ressourcen dort konzentriert werden können, wo sie die größte Wirkung erzielen
- Verbessern der Compliance-Vorbereitung, indem Sie Sicherheitslücken identifizieren und die Maßnahmen zur Behebung auf die geltenden Standards und Anforderungen abstimmen
- Schaffen einer internen Abstimmung zwischen IT, OT und der Führungsebene, die auf einem gemeinsamen Verständnis von Risiken, Prioritäten und messbaren Sicherheitsergebnissen beruht

Industrielles Netzwerk und industrielle Infrastruktur

Unternehmen modernisieren weiterhin ihre IT/OT-Architektur, da die Betriebsabläufe zunehmend vernetzt werden. Obwohl jede neue Verbindung das Cyber-Risiko erhöht, hilft eine verteidigungsfähige Architektur zu verhindern, dass aus Komplexität eine erweiterte Angriffsfläche wird. Führende Organisationen, die Cybersicherheit in das Design ihrer Betriebsabläufe integrieren, sind besser aufgestellt, um Risiken zu reduzieren und ihre Resilienz zu verbessern. Sie verbringen außerdem weniger Zeit mit der Reaktion auf Vorfälle und mehr Zeit mit der Förderung von Betriebsergebnissen.

Proaktive Organisationen haben folgende Möglichkeiten:

- Souveränes Vorantreiben der Initiativen zur digitalen Transformation und gleichzeitiges Schützen von kritischen Betriebssystemen
- Reduzieren der Wahrscheinlichkeit und der Auswirkungen von Störungen durch Netzwerksegmentierung, um Bedrohungen einzudämmen, bevor sie die Produktion beeinträchtigen
- Ermöglichen eines sicheren Fernzugriffs, der die betriebliche Flexibilität, Produktivität und Zusammenarbeit unterstützt, ohne unkontrollierte Einstiegspunkte zu schaffen
- Implementieren von Secure-by-Design-Architekturen, die das Risiko über den gesamten Lebenszyklus von Assets reduzieren
- Reduzieren langfristiger Sicherheitskosten, indem Sie Risiken proaktiv durch Architektur und Design angehen, anstatt durch reaktive Behebungsmaßnahmen

Bestands- und Lebenszyklusmanagement von Anlagen

Verschaffen Sie sich einen Überblick über Assets und Risiken

Eingeschränkte Sichtbarkeit ist eines der häufigsten Hindernisse beim Aufbau von Resilienz. Ohne einen vollständigen Einblick in die Umgebung – einschließlich Altsystemen, seriell angeschlossenen Geräten oder temporären Verbindungen – fehlt Unternehmen der Ausgangspunkt, der für die Planung und Umsetzung einer sinnvollen Risikominderung erforderlich ist.

Eine umfassende Anlagentransparenz eröffnet Organisationen folgende Möglichkeiten:

- Verstehen und Priorisieren von Cyber-Risiken in der gesamten Betriebsumgebung
- Reduzieren von blinden Flecken, die Betriebs-, Sicherheits- und Cybersicherheitsrisiken verursachen können
- Treffen schnellerer und fundierterer Entscheidungen, indem Sie verstehen, welche Assets miteinander verbunden sind, welche einem Risiko ausgesetzt sind und welche für die Produktion und den Geschäftsbetrieb am wichtigsten sind
- Beschleunigen der Bemühungen zur Risikominderung, indem Sie die Sanierungsmaßnahmen nach den betrieblichen Auswirkungen und nicht nur nach dem Schweregrad der Schwachstelle priorisieren
- Verbessern der betrieblichen Resilienz durch kontinuierliches Lebenszyklusmanagement der Anlagen, das zum langfristigen Erhalt einer sicheren und unterstützten Umgebung beiträgt
- Schaffen einer zuverlässigen Programmgrundlage für die Entwicklung kompensierender Kontrollen und anderer Komponenten für durchgängige Cybersicherheit

Risiko- und Schwachstellenmanagement

Priorisieren und beheben Sie die Risiken, die am wichtigsten sind

Organisationen können nicht alle Cyber-Risiken eliminieren, aber sie können ihre Sicherheitslage verbessern, indem sie die Geschwindigkeit stärken, mit der sie Bedrohungen identifizieren, priorisieren und darauf reagieren, bevor diese den Betrieb beeinträchtigen. Da der Industriebetrieb immer stärker vernetzt ist, hängt ein effektives Risikomanagement von kontextbezogener Transparenz, risikobasierter Entscheidungsfindung und einer nachhaltigen Betriebskontinuität bei Unterbrechungen ab.

Ein risikobasiertes Schwachstellenmanagement-Programm unterstützt Unternehmen bei Folgendem:

- Priorisieren der Behebung nach den betrieblichen Auswirkungen, statt nur nach Schweregrad
- Reduzieren der mittleren Zeit bis zur Behebung für alle OT-Assets
- Nachweisen messbarer Fortschritte bei der Einhaltung von IEC 62443, NIST CSF und NIS2
- Ermöglichen von fundierten Investitionsentscheidungen, indem Sie Investitionen in die Cybersicherheit auf die Risikotoleranz und die operativen Ziele des Unternehmens abstimmen

Verwaltete Erkennung und Reaktion

Aufrechterhaltung eines kontinuierlichen Bewusstseins für alle Betriebsabläufe

Da IT- und OT-Umgebungen zunehmend miteinander vernetzt werden, stehen Unternehmen vor der wachsenden Herausforderung, routinemäßige Sicherheitsereignisse von Bedrohungen zu unterscheiden, die den Betrieb stören könnten. Kontinuierliche Überwachung hilft, die wichtigsten Risiken zu verstehen, bevor sie zu Störungen führen.

Ein proaktives Erkennungs- und Reaktionsprogramm bietet Organisationen folgende Möglichkeiten:

- Beschleunigen der Erkennung und Reaktion durch die Aufrechterhaltung einer 24/7-Überwachung und kontinuierlichen Transparenz über IT- und OT-Umgebungen hinweg
- Ermöglichen einer schnelleren, fundierteren Entscheidungsfindung mit kontextbezogenen Einblicken, die Teams helfen zu verstehen, welche Bedrohungen sofortiges Handeln erfordern
- Schließen der Qualifikationslücke, indem Sie interne Fähigkeiten um dedizierte Expertise im Bereich OT-Sicherheit erweitern, ohne dass Kosten für den Aufbau und die Wartung eines vollständigen internen SOC anfallen
- Stärken der Wirksamkeit des Programms durch die Integration der Bedrohungserkennung mit dem Schwachstellenmanagement, der Reaktion auf Vorfälle, der Governance und den Bemühungen um eine kontinuierliche Verbesserung

Reaktion auf Vorfälle und Wiederherstellung

Eindämmen, wiederherstellen und verbessern

Wenn ein Cybersicherheitsvorfall auftritt, ist eine schnelle Reaktion entscheidend dafür, wie viel Schaden, Ausfallzeit und Kosten auf ein Unternehmen zukommen können. Die Eindämmung eines Vorfalls ist nur ein Teil der Herausforderung. Unternehmen müssen die Bedeutung der Wiederherstellungsbereitschaft verstehen, wenn es um die betriebliche Widerstandsfähigkeit geht. Wenn das Schlimmste eintritt, müssen sie in der Lage sein, die Dienste schnell wiederherzustellen und zum Normalbetrieb zurückzukehren.

Ein ausgereiftes Incident-Response-Programm bietet Organisationen folgende Möglichkeiten:

- Reduzieren der Auswirkungen von Cyber-Vorfällen durch vordefinierte, getestete Reaktions- und Eindämmungsverfahren
- Beschleunigung der betrieblichen Wiederherstellung durch Koordinieren von Reaktion und Wiederherstellung über IT-, OT- und Betriebsteams hinweg
- Minimieren der Ausfallzeiten durch eine verbesserte Wiederherstellungsbereitschaft für kritische Systeme
- Stärken des Vertrauens der Stakeholder durch klare Kommunikation, Governance und Incident-Management während und nach einem Ereignis
- Durchführen einer detaillierten Untersuchung von Vorfällen, um die eigentliche Ursache zu ermitteln und die gewonnenen Erkenntnisse anzuwenden, um die Cyber-Resilienz kontinuierlich zu stärken



Resilienz wird zu einem Wettbewerbsvorteil

Industrieunternehmen investieren massiv in Cybersicherheit, KI und vernetzte Abläufe. Diese Investitionen stärken zwar die Zuversicht, doch Technologie allein schafft keine Resilienz.

Die Organisationen, die den größten Nutzen aus der Cybersicherheit ziehen, werden diejenigen sein, die einen proaktiven, programmatischen Ansatz verfolgen. Indem sie von Anfang an Sichtbarkeit, risikobasierte Entscheidungsfindung, sichere Architekturen, kontinuierliche Überwachung und Wiederherstellungsbereitschaft in ihre Betriebsabläufe integrieren, können sie Betriebsrisiken reduzieren, die Produktion aufrechterhalten und dem Unternehmen ermöglichen, zuversichtlich voranzuschreiten.

In einem stärker vernetzten industriellen Umfeld geht es bei der Cybersicherheit nicht mehr nur um den Schutz von Anlagen. Es geht darum, widerstandsfähige Betriebsabläufe zu ermöglichen, die sich anpassen, wiederherstellen und weiterhin Geschäftswert liefern können.

Wenden Sie sich an Ihren Rockwell Automation-Ansprechpartner, um mehr zu erfahren.

Rockwell Automation

Sie finden uns auch hier

rockwellautomation.com — expanding **human possibility**®

AMERIKA: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: +1 414 382 2000
EUROPA/NAHER OSTEN/AFRIKA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgien, Tel: +32 2 663 0600
ASIEN/AUSTRALIEN/PAZIFIKRAUM: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
DEUTSCHLAND: Rockwell Automation GmbH, Parsevalstraße 11, 40468 Düsseldorf, Tel: +49 (0)211 41553 0
SCHWEIZ: Rockwell Automation AG, Industriestrasse 20, CH-5001 Aarau, Tel: +41(62) 889 77 77, Customer Service – Tel: 0848 000 277
ÖSTERREICH: Rockwell Automation, Kotzinastraße 9, A-4030 Linz, Tel: +43 (0)732 38 909 0

Allen-Bradley und expanding human possibility sind Marken von Rockwell Automation, Inc.
Marken, die nicht Rockwell Automation gehören, sind das Eigentum der jeweiligen Unternehmen.

Publikation GMSN-SP043A-DE-P – August 2026

Copyright © 2026 Rockwell Automation, Inc. Alle Rechte vorbehalten. Printed in USA.