Acronis

WHITEPAPER

Warum europäische Hersteller einen Plan für Unternehmensresilienz brauchen

Ausfallzeiten reduzieren, die Erfüllung von NIS 2 stärken und die Berechtigung für Cyberversicherungen

Kurzfassung

Europäische Hersteller stehen vor einer ganzen Reihe von Herausforderungen:

Ungeplante Ausfallzeiten sind eine der größten Bedrohungen für die Produktionsleistung in ganz Europa.

Die sich stetig weiterentwickelnde NIS-2-Richtlinie hat die Verantwortung für Geschäftskontinuität und Disaster Recovery auf die Ebene der Geschäftsleitung gehoben.

Gleichzeitig verlangen Cyberversicherer stärkere Nachweise für Resilienz, bevor sie Verträge abschließen.

Die Schwierigkeit besteht darin, dass diese Elemente nicht mehr getrennt voneinander auftreten. Ein einzelner Cyber-Security-Vorfall oder Katastrophenfall wirkt sich nun direkt auf den Betrieb, die Compliance und die finanzielle Erholung aus. Als Reaktion darauf müssen Hersteller über fragmentierte Backup-Strategien für ihre Operational-Technology-Umgebungen (OT) hinausgehen und einen echten Plan für Unternehmensresilienz einführen, der auf eine wiederherstellbare Produktion ausgerichtet ist.

Die Herausforderung für die Führungsebene: ein Vorfall, drei Auswirkungen

Viele Organisationen verwalten Backups, Compliance und Versicherungen immer noch getrennt voneinander. Theoretisch laufen diese Elemente bei einem Vorfall zusammen. Aber was passiert, wenn sie es nicht tun?

Wenn ein Hersteller die Produktion nicht auf kontrollierte und dokumentierte Weise wiederherstellen kann, hat das drei unmittelbare Folgen:

- Die Störung der Produktion und verpasste Lieferzusagen.
- Regulatorische Gefahren im Rahmen von NIS 2.
- Ein erhöhtes Risiko für strittige oder gekürzte Versicherungsansprüche.

Eine schwache Recovery-Bereitschaft führt daher nicht nur zu einem technisches Problem, sondern zu einem mehrschichtigen Geschäftsrisiko.

Die europäische Bedrohungslage und regionale Einblicke

Cybervorfälle stören schon heute Produktionsabläufe in ganz Europa, wobei Ransomware weiterhin die größte Bedrohung für Industrieumgebungen darstellt. Europäische Hersteller sind mit zusammenlaufenden Risiken konfrontiert. Ransomware-Gruppierungen nehmen die Produktionsbranche ins Visier, erhöhen die Zahl schwerwiegender Vorfälle und vergrößern die Anfälligkeit für Schwachstellen. Gleichzeitig verfügen viele kleine und mittlere Unternehmen (KMU), darunter auch Hersteller, nicht über ausgereifte Cyber-Security-Strategien und sind daher anfällig für Angriffe. Durch von Industrie 4.0 getriebene Initiativen hat sich auch die Angriffsfläche in OT-Umgebungen vergrößert, und viele Hersteller haben keine angemessenen Maßnahmen zum Schutz ihrer Daten ergriffen.

Sich von einem Cyberangriff zu erholen, ist teuer. Weltweit kostete eine durchschnittliche Datenkompromittierung in einer Industrieumgebung im Jahr 2025 laut IBM 5,0 Millionen US-Dollar.[1] Da Ransomware und andere Angriffe in Europa sowohl in ihrer Anzahl als auch in ihrer Schwere zunehmen, müssen Hersteller, genau wie andere KMU, eine wirksame Strategie für Schutz und Recovery entwickeln. Die Zahlen deuten darauf hin, dass sich die Lage verschlechtert, nicht verbessert.

Beispiele:

Europa: Laut dem Bericht „ENISA Threat Landscape 2025“ waren fast 15 % der im Bericht analysierten Ransomware-Angriffe auf die Produktion ausgerichtet, womit sie die am fünfthäufigsten angegriffene Branche von fast 20 im Bericht untersuchten Branchen war.[2]

Vereinigtes Königreich: Das britische National Cyber Security Centre (NCSC) berichtet, dass die Produktion zu den Branchen gehört, die am häufigsten Ziel von Ransomware sind.[3]

Deutschland: Any.run berichtete 2026, dass Angriffe auf deutsche Hersteller über Datenverlust hinausgingen und zu potenziellen Betriebsstillständen, physischen Schäden an Anlagen
sowie zu Störungen der Lieferkette führten. Grund sei, dass diese Hersteller Industrie-4.0-Technologien, IoT-Sensoren, operative OT und mit der Cloud verbundene Produktionssysteme integriert hätten. Da Mitarbeitende in der Produktion nur selten in Cyber Security geschult waren, erwiesen sich Social-Engineering-Angriffe als besonders wirksam.[4]

Frankreich: Die französische Cyber-Security-Behörde (ANSSI) erklärte in einem Bericht von 2026, dass französische Hersteller zu bedeutenden Zielen von sowohl staatlich unterstützten Störungen als auch Ransomware-Angriffen geworden seien. Der Bericht gab an, dass kleinere Hersteller besonders anfällig für digitale Sabotage waren.[5]

Italien: Ein Cyber-Security-Bericht von Telecom Italia stellte 2025 fest, dass italienische Produktionsunternehmen in den Jahren 2022–2024 Ziel von rund 26 % der Ransomware-Angriffe im Land waren.[6]

Nordische Länder: Mordor Intelligence berichtet, dass Industrie-4.0-Programme, die die OT-Angriffsflächen vergrößern, in den nordischen Ländern zu Investitionen in Cyber-Security-Lösungen mit einer beeindruckenden kumulierten jährlichen Wachstumsrate von mehr als 8 % führen. Hersteller reagieren auf die Risiken, indem sie IT- und OT-Abwehrmaßnahmen zusammenführen.[7]

Während OT-spezifische Statistiken weiterhin begrenzt sind, unterstreichen die verfügbaren nationalen Daten eine breitere Eskalation der Cyberrisiken in Produktionsumgebungen, einschließlich industrieller Systeme und KMU.

[1] IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, eine vom Ponemon Institute durchgeführte Studie, veröffentlicht im Jahr 2025, basierend auf der Analyse von 600 Organisationen in 16 Ländern zwischen März 2024 und Februar 2025.

[2] ENISA Threat Landscape 2025, Version 1.2, Agentur der Europäischen Union für Cybersicherheit, Januar 2026.

[3] National Cyber Security Centre (Vereinigtes Königreich). (2024). NCSC-Jahresrückblick 2024. GCHQ.

[4] ANY.RUN. (1. April 2026). Große Cyberangriffe im März 2026: OAuth-Phishing, SVG-Schmuggel, Magecart und mehr.

[5] Agence nationale de la sécurité des systèmes d’information. (11. März 2026). Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002). ANSSI.

[6] Telecom Italia (TIM) und Cyber Security Foundation. (12. Juni 2025). Cyber-Security-Bericht 2025. TIM Group.

[7] Mordor Intelligence, Analyse der Marktgröße und -anteile des Cybersecurity-Markts in den nordischen Ländern: Wachstumstrends und Prognosen (2026–2031), mit einer geschätzten Marktgröße von 14,92 Milliarden US-Dollar im Jahr 2026 und einem Wachstum auf 22,25 Milliarden US-Dollar bis 2031 (8,36 % kumulierte jährliche Wachstumsrate), veröffentlicht 2026.

Cyberangriffe auf die Produktion in Europa in der Praxis

In ganz Europa sind Cyber-Vorfälle in OT-Umgebungen längst keine isolierten IT-Ereignisse mehr. Sie sind Produktionsereignisse, die den Betrieb schwerwiegend stören und zu langen Ausfallzeit führen können. Aktuelle Beispiele sind:

- **Jaguar Land Rover:** Ein inzwischen berüchtigter Cyberangriff auf Jaguar Land Rover im Jahr 2025 störte die Produktion im Vereinigten Königreich für mehrere Wochen und verursachte Schätzungen zufolge Kosten von mindestens 50 Millionen britischen Pfund pro Woche,[8] was zudem zum Verlust von Arbeitsplätzen führte. Der Angriff zeigte, wie sich eine Störung der Unternehmens-IT direkt auf den Fabrikbetrieb auswirken kann.
- **Volkswagen Group France:** Im Oktober 2025 wurde die Volkswagen Group France Opfer eines Angriff der Qilin-Ransomware-Gruppe, der zur Exfiltration von rund 2.000 Dateien und 150 GB sensibler Daten führte.[9]
- **Dodd Group:** Im Jahr 2025 war der britische Rüstungskonzern Dodd Group das Ziel eines Cyberangriffs, der zu einem Leak sensibler Dateien des britischen Verteidigungsministeriums mit Informationen über Luftwaffen- und Marinestützpunkte führte.[10]

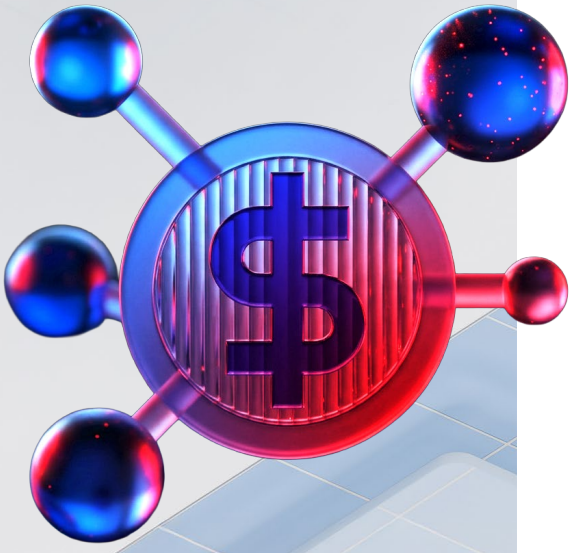
Was NIS 2 in der Praxis verlangt

Compliance bleibt ein zentrales Thema in OT-Umgebungen, in denen potenzielle finanzielle Strafen die Kosten ungeplanter Ausfallzeiten zusätzlich erhöhen können.
NIS 2 führt einen grundlegenden Wandel von Prävention hin zu nachweisbarer Resilienz ein.

Nach Artikel 21 müssen Organisationen nachweisen können, dass sie in der Lage sind, den Betrieb fortzuführen und eine wirksame Recovery zu leisten. Dazu gehören:

- Geschäftskontinuität und Disaster Recovery
- Backup-Management im Einklang mit operativen Anforderungen.
- Krisenmanagement- und Governance-Strukturen.

Die entscheidende Veränderung ist die Rechenschaftspflicht: Organisationen müssen nachweisen, dass Recovery in der Praxis funktioniert, nicht nur auf dem Papier. Damit ist die Recovery-Fähigkeit jetzt eine Compliance-Anforderung und nicht nur eine betriebliche Präferenz.



[8] BBC News, Cyberangriff auf Jaguar Land Rover stört Produktion und Lieferkette, veröffentlicht im September 2025.

[9] Cybernews. (16. Oktober 2025). Volkswagen France von Ransomware getroffen, Qilin-Gruppe beansprucht den Angriff für sich.

[10] Security Affairs. (20. Oktober 2025). Russische Lynk-Gruppe leakt sensible Dateien des britischen Verteidigungsministeriums, darunter Informationen zu acht Militärstützpunkten.

Was OT-Recovery unterscheidet

OT-Umgebungen bringen Komplexitäten mit sich, die traditionelle IT-Recovery-Ansätze nicht vollständig abdecken, darunter Altsysteme, eng gekoppelte Produktionsprozesse und strenge Neustartbedingungen, die die Reihenfolge der Recovery entscheidend machen.

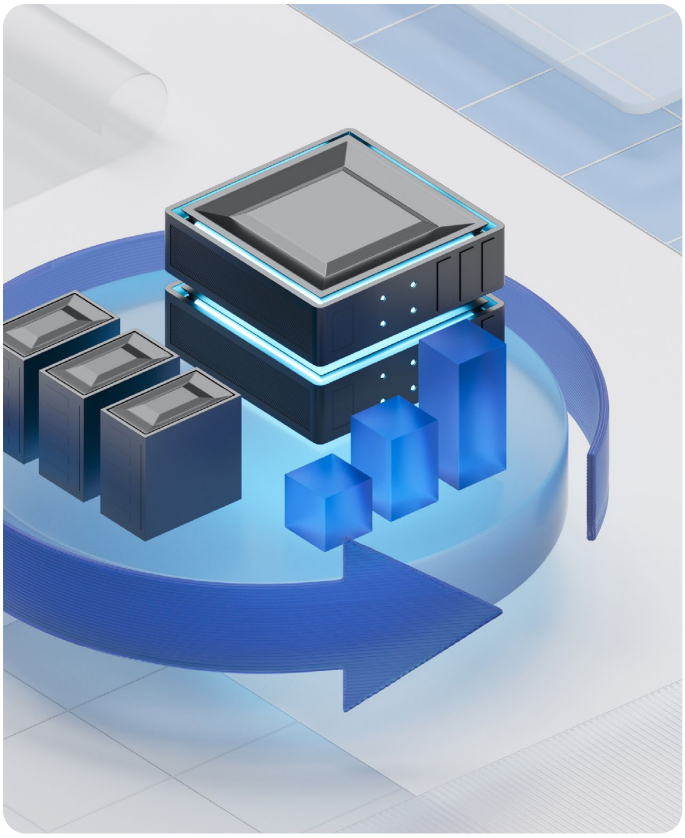
Daher hängt Resilienz in der Fertigung von der Wiederherstellung der Produktionsfähigkeit ab, nicht nur von der Wiederherstellung von Systemen oder Daten.

Von Backups zu Unternehmensresilienz

Ein Plan für Unternehmensresilienz umfasst weit mehr als nur Backups – er verbindet betriebliche Kontinuität, Compliance und Recovery in einem einzigen Rahmen.

Organisationen sollten mindestens Folgendes etablieren:

- Klare Governance über Standorte und Funktionen hinweg.
- OT-gerechte Recovery-Fähigkeiten.
- Regelmäßige Validierung von Recovery-Prozessen.



Das Ziel ist nicht nur, Daten wiederherzustellen, sondern dafür zu sorgen, dass Hersteller die Produktion schnell auf kontrollierte und vorhersehbare Weise wiederherstellen können.

Cyberversicherung und Verteidigungsfähigkeit

Anbieter von Cyberversicherungen prüfen Produktionsorganisationen zunehmend strenger, insbesondere im Hinblick auf das Risiko von Betriebsstörungen. Der Ausgang von Schadensansprüchen wird immer stärker davon beeinflusst, ob eine Organisation ihre Vorbereitung und die Ausführung der Recovery nachweisen kann.

Zu den wichtigsten Erwartungen gehören heute:

- Nachweise über definierte Kontinuitäts- und Recovery-Prozesse.
- Dokumentierte Recovery-Zeitpläne und -Maßnahmen.
- Angleichen von vertraglichen Zusagen und operativen Fähigkeiten.

Ohne diese Elemente laufen Organisationen Gefahr, in eine Grauzone bei Schadensfällen zu geraten, in welcher der Versicherungsschutz reduziert oder angefochten werden kann.

Was Führungskräfte in der Produktion als Nächstes tun sollten

Hersteller müssen Resilienz als Priorität für das Unternehmen und nicht als technisches Projekt behandeln.

Führungskräfte sollten sich auf drei sofortige Maßnahmen konzentrieren:

- Kritische Produktionsabhängigkeiten und Recovery-Risiken verstehen.
- Die Kontinuitätsplanung auf die Erwartungen von NIS 2 abstimmen.
- Einen strukturierten Plan für Unternehmensresilienz etablieren.

Dieser Wandel ermöglicht es Organisationen, das Risiko für Ausfallzeiten zu senken und gleichzeitig sowohl die Compliance als auch den finanziellen Schutz zu stärken.

Wie Acronis die OT-Resilienz unterstützt

Mit Acronis Cyber Protect für OT können Systeme mit einer einzigen Aktion wiederhergestellt werden, ohne dass dafür tiefgehendes IT-Fachwissen erforderlich ist. Insbesondere in Air-Gap-Umgebungen ist One-Click-Recovery eine unverzichtbare Funktion. Hersteller können Ausfallzeiten minimieren und die Geschwindigkeit der Recovery ohne Eingriffe oder Störungen maximieren.

Acronis Cyber Protect für OT ermöglicht es Herstellern, die Resilienz in komplexen Umgebungen zu stärken. Es unterstützt Organisationen dabei, die zusammenlaufenden Herausforderungen zu bewältigen:

- Schutz kritischer Systeme vor unerwünschten Ausfallzeiten.
- Validierung von Recovery-Prozessen und anderen für die Compliance wesentlichen Elementen.
- Erstellung der für Cyberversicherungen erforderlichen Nachweise.

Als Komponente der nativ integrierten Acronis Cyber Platform, die mehrere Cyber-Security-Funktionen in einer einzigen Konsole und an einem zentralen Management-Punkt vereint, ermöglicht Acronis Cyber Protect für OT Herstellern eine höhere Verfügbarkeit und die Reduzierung unerwünschter Ausfallzeiten sowie eine schnellere Recovery und eine stärkere Abstimmung zwischen betrieblicher Resilienz und der Verwaltung von Unternehmensrisiken.

WEITERE INFORMATIONEN