TAG

WARUM ACRONIS EIN FÜHRENDER ANBIETER VON CYBER-RESILIENZ FÜR OT-UMGEBUNGEN IST

DR. EDWARD AMOROSO
CEO, TAG INFOSPHERE

Acronis

WARUM ACRONIS EIN FÜHRENDER ANBIETER VON CYBER-RESILIENZ FÜR OT-UMGEBUNGEN IST

EDWARD AMOROSO, CEO, TAG

EINFÜHRUNG:

Seit Jahrzehnten steht der Begriff Cyber Security meist als Synonym für den Schutz der Informationstechnologie (IT) vor schädlichen Angriffen. Dementsprechend wurden Chief Information Security Officers (CISOs) ernannt, um die Führung in diesem etablierten Bereich zu übernehmen. In jüngerer Zeit wurde der Aufgabenbereich der Cyber Security jedoch auf weitere betriebliche, industrielle, physische und sonstige materielle Systeme ausgedehnt. Daraus hat sich eine neue Branche entwickelt, die wir als Operational Technology Security oder kurz OT-Sicherheit bezeichnen.

Da die OT-Sicherheit im Anschluss an die IT-Sicherheit entwickelt wurde, gibt es viele Gemeinsamkeiten bei den verwendeten Kontrollmechanismen. Das Gewinnen tieferer Einblicke und die Anwedung von Schadensbehebungsmaßnahmen sind typische Beispiele und stehen im Mittelpunkt von IT- und OT-Sicherheitsstrategien – was sich als hilfreich erwiesen hat, da die OT-Sicherheit organisatorisch immer mehr mit umfassenderen IT-Initiativen verschmilzt. Das spiegelt sich auch in der Zahl der CISOs wider, die heutzutage die volle Verantwortung für die OT-Sicherheit tragen.

Es ist jedoch zu erwarten, dass viele der Schwachstellen, die man von herkömmlichen IT-Sicherheitssystemen kennt, auch beim Schutz von Industrieanlagen auftreten werden. Die wohl offensichtlichste dieser Schwächen ist die typischerweise geringe Resilienz (Widerstandsfähigkeit), die viele OT-Systeme gegenüber Angriffen aufweisen. Ransomware ist ein typisches Beispiel dafür, wie selbst große Umgebungen komplett zum Stillstand gebracht werden können – was dann natürlich schwerwiegende Folgen für die Kund:innen hat.

Es gibt jedoch auch viele einzigartige Probleme, die im Zusammenhang mit OT-Sicherheit auftreten. Beispielsweise gibt es in vielen OT-Umgebungen kein geschultes Sicherheitspersonal vor Ort, sind viele ältere proprietäre Systeme in diesen Netzwerken vorhanden, und machen die oft anspruchsvollen Betriebsumgebungen es schwierig, Updates oder Patches zu installieren, ohne den laufenden Betrieb der Umgebung (z. B. einer Fabrik bzw. Produktionsstätte) zu beeinträchtigen.

In diesem Bericht wird erläutert, wie OT-Sicherheitsteams, die heute manchmal von CISOs geleitet werden, ihre operationale Resilienz verbessern können, indem sie sich auf eine Schlüsselfunktionalität konzentrieren: Backup und Recovery. Dieser Cyber Protection-Aspekt war auch früher schon eine Herausforderung für IT-Sicherheitsteams, da effektive Datensicherungslösungen eine genaue Kenntnis der Infrastruktur erfordern. Die meisten Anbieter, die in diesem Bereich tätig sind, haben sich jedoch traditionell eher auf den IT-Betrieb als auf die IT-Sicherheit konzentriert.

In Bezug auf OT-Umgebungen sind wir der Ansicht, dass eine Backup & Recovery-Funktionalität das wichtigste Element jeder Initiative zur Verbesserung der Sicherheit sind. Natürlich müssen auch andere Ziele verfolgt werden, wie z. B. möglichst gute Sicherheitsschulungen für das OT-Personals oder Bemühungen, die Anzahl vorhandener Altsysteme zu reduzieren. Wir vertreten jedoch die Ansicht, dass die größte Wirkung erzielt wird, wenn sich die OT-Sicherheitsfachkräfte auf eine Backup & Recovery-Funktionalität als Schlüsselfaktor für die Sicherheit von Prozessumgebungen konzentrieren.

Wir veranschaulichen diese Behauptung anhand der fortschrittlichen Lösungen für Cyber-Resilienz des kommerziellen Anbieters Acronis. Das Backup & Recovery-Konzept von Acronis, das für alle Arten von IT- und OT-Infrastrukturen geeignet ist, scheint gut gerüstet zu sein, um den zunehmenden Cyberbedrohungen zu begegnen, die sich gegen Industriebetriebe in Branchen wie Fertigung, Transport, Energie und Militär richten, in denen Unterbrechungen jeglicher Art unbedingt vermieden werden müssen.[1]

DER AKTUELLE STAND DER SICHERHEIT FÜR OT-SYSTEME

Wie oben bereits angedeutet, unterscheiden sich die Auswirkungen einer unzureichenden Resilienz zwischen IT- und OT-Infrastrukturen erheblich, denn Sicherheitsprobleme in OT-Umgebungen haben meist schwerwiegendere Folgen. Beispielsweise können Resilienzprobleme in industriellen Steuerungssystemen zum Ausfall von Sicherheitssystemen, zum Stillstand ganzer Produktionslinien oder zu Betriebsstörungen in Kernkraftwerken führen. Auch Szenarien, bei denen Menschenleben auf dem Spiel stehen könnten, sind vorstellbar.

Aus diesem Grund muss der Sicherheit in OT-Umgebungen eine hohe Priorität eingeräumt werden. Diese Umgebungen kämpfen jedoch seit jeher mit den Herausforderungen heterogener und proprietärer Technologien, die häufig mit veralteter Hardware und Legacy-Betriebssystemen einhergehen. Dies kann die Möglichkeiten zur Installation von Patches und Updates einschränken. Ganz zu schweigen von den engen Zeitfenstern für Backups in diesen Umgebungen, die oft nicht über ausreichende IT-Ressourcen oder geschultes IT-Personal verfügen.

Auch das Ziel, OT-Umgebungen durch ein Gateway zwischen IT- und OT-Umgebungen vor Hacker:innen zu schützen, konnte nicht erreicht werden. Das ursprüngliche Ziel, OT-Systeme durch die Schaffung eines IT/OT-Perimeters (eine Art Schutzzone oder Schutzgrenze) vor dem Internet zu schützen, scheiterte aus den gleichen Gründen, aus denen Perimeter immer scheitern: Sie ignorieren Insider-Bedrohungen, Zugriffsmöglichkeiten um den Perimeter herum, die Durchlässigkeit eines jeden Perimeters usw.

Der IT/OT-Gateway-Ansatz löst auch nicht die oben genannten Kernprobleme der OT-Sicherheit (wie proprietäre Systeme, kompliziertes Patching oder nicht gut in Sicherheitsfragen geschultes Personal). Die folgende Abbildung zeigt, dass diese Sicherheitsprobleme durch ein IT/OT-Gateway nicht gelöst werden. Auch unser Hauptaugenmerk wird hier nicht angesprochen: die Resilienz bei der OT-Sicherheit, für die hauptsächlich Backup & Recovery-Fähigkeiten erforderlich sind.

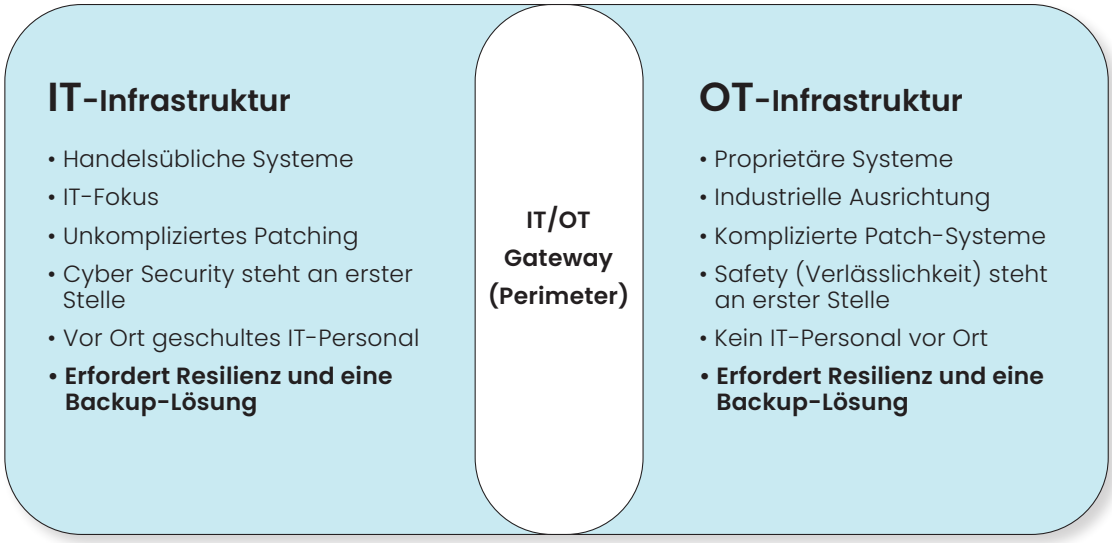

Abbildung 1. Herausforderungen beim Schutz von OT-Systemen

Wie bereits angedeutet, halten wir es für erforderlich, dass eine umfassende OT-Sicherheit für all diese Probleme eine Lösung bieten muss. Wir sind der Meinung, und werden dies nachfolgend noch erläutern, dass die Gewährleistung der Betriebskontinuität angesichts von Ransomware, Sabotage-Akten oder verheerenden Cyberangriffen das Hauptanliegen von modernen OT-Sicherheitsmaßnahmen sein sollte. Wir werden dies am Beispiel der kommerziellen Acronis Plattform und deren Unterstützung für OT-Sicherheit erläutern.

ACRONIS BACKUP & RECOVERY-LÖSUNGEN FÜR OT UND ICS

Unsere Erfahrung hat gezeigt, dass OT-Sicherheitsprogramme drei komplementäre Bereiche berücksichtigen sollten. Erstens sollten sie für mehr Sicherheitseinblicke in OT-Umgebungen sorgen, was häufig mithilfe kommerzieller Plattformen wie Claroty und Dragos geschieht. Die Erlangung vertiefter Sicherheitseinblicke ist von entscheidender Bedeutung. Daher lohnt es sich, genügend Energie darauf zu verwenden, dass dies tatsächlich gut funktioniert. Dazu gehören bessere Schulungen und möglicherweise ein stärkerer Fokus auf Cyber Range-Simulationen in OT-Umgebungen.

Zweitens glauben wir, dass die Führungskräfte ihre IT-Sicherheitsteams ermutigen sollten, in dem Maße, wie OT-Systeme in die IT integriert werden, auch mehr konvergente Kontrollmöglichkeiten zu erstellen. So sollte beispielsweise der Trend zu Zero Trust OT aufgegriffen werden, was bedeutet, dass mehr Betriebssysteme mit der Cloud und anderen herkömmlichen IT-Systemen verbunden werden. Auf diese Weise können IT-Kontrollen wie Cloud Native Application Protection Platforms (CNAPP) auf die OT-Infrastruktur ausgeweitet werden.

Drittens, und das ist der entscheidende Punkt, empfehlen wir den OT-Sicherheitsteams, sich mehr auf die operative Resilienz zu konzentrieren. In der Praxis bedeutet dies, dass die Kontinuität des Geschäftsbetriebs durch automatisierte Backup & Recovery-Lösungen sichergestellt werden muss. Dies gilt grundsätzlich natürlich genauso für alle IT-Systeme. Aber wie bereits erwähnt, kann eine Unterbrechung des OT-Supports weitaus schwerwiegendere Folgen haben (auch für die menschliche Sicherheit). Die Lösung von Acronis kann helfen, diese Probleme erst gar nicht aufkommen zu lassen.

Die Acronis Plattform deckt die wichtigsten Sicherheits- und Resilienzanforderungen für OT-Infrastrukturen ab. Das sind gute Nachrichten, denn Unternehmen sollten nicht gezwungen sein, ihre eigenen lokalen Backup & Recovery-Lösungen zu entwickeln, selbst wenn ihre Hardware und Software veraltet und proprietär ist. Folgende wichtige Funktionen der Acronis Suite sind für die Resilienz von OT-Umgebungen entscheidend:

1. **Schnelle Recovery von OT-Systemen** – Acronis bietet einen leistungsstarken Schutz für OT-Computer, was schnelle Wiederherstellungen ermöglicht und kostspielige Produktionsausfälle vermeidet. Diese Fähigkeit zur schnellen Wiederherstellung ist von entscheidender Bedeutung, um Ausfallzeiten zu minimieren und eine unterbrechungsfreie Produktion zu gewährleisten.
2. **Universelles Computer-Recovery** – Acronis Cyber Protect ermöglicht die schnelle und zuverlässige Wiederherstellung aller Computer – wozu auch herkömmliche Legacy-Systeme (bis hin zu Windows XP) gehören. Dies beinhaltet auch die Möglichkeit, ein System-Backup auf fabrikneuer Hardware wiederherstellen zu können Diese Funktion ist unerlässlich, um die Betriebskontinuität veralteter Legacy-Systeme zu gewährleisten (die in OT-Umgebungen noch oft anzutreffen sind).
3. **Anpassbare Backup-Pläne** – Acronis ermöglicht die Erstellung anpassbarer Backup-Pläne, die auf die spezifischen Anforderungen von OT- und ICS-Umgebungen zugeschnitten sind. So wird sichergestellt, dass kritische Daten und Systeme angemessen geschützt sind. Da OT-Infrastrukturen zunehmend mit KI und nachhaltigeren Bereitstellungsmethoden modernisiert werden, steigt auch die Nachfrage nach anpassbaren Lösungen.
4. **Integration in Drittanbieter-Applikationen** – Acronis bietet eine vereinheitlichte Backup & Recovery-Benutzeroberfläche mit zentraler Management-Konsole und der Möglichkeit zur Integration in Drittanbieter-Applikationen. Auch dies vereinfacht die Verwaltung und verbessert die Betriebseffizienz. Diese Fähigkeit ist besonders wichtig, da OT-Umgebungen eine besondere Herausforderung für Sicherheitsintegrationen darstellen.
5. **Optionen für die Datenhoheit** – um Compliance-Anforderungen an die Datenhoheit zu erfüllen, können Unternehmen zwischen einem eigenen lokalen Backup Storage oder den weltweiten Acronis Datenzentren wählen. Es besteht auch die Möglichkeit, Public Cloud Storages wie Amazon S3 oder Microsoft Azure als Backup-Speicherorte zu verwenden. Acronis entwickelt gemeinsam mit seinen Kund:innen die am besten geeignete Hosting-Lösung.

6. **Self-Service Recovery für Remote-Mitarbeiter:innen** – Acronis ermöglicht Mitarbeiter:innen an Remote-Standorten (an denen oft kein geschultes Technik-Personal vorhanden ist) Wiederherstellungen ganz einfach selbst auszuführen. Dank diesem sogenannten Self-Service Recovery können die IT-Teams entlastet und Betriebsausfälle schneller wieder behoben werden.

DIE ACRONIS PLATTFORM-ARCHITEKTUR

Die Acronis Cyber Protect-Plattform basiert auf einem Data Warehouse, in dem aktuelle, vergangene und wichtige OT-Unternehmensdaten aus anderen Quellen gespeichert und gesichert werden. In der OT-Umgebung können mehrere Konsoleninstanzen der Acronis Cyber Protect-Plattform mit mehreren zugehörigen Agenten installiert werden, die in der gesamten Umgebung zur Datensicherung und Datenwiederherstellung bereitgestellt werden. Die entsprechenden Metadaten werden von den Konsolen an das Data Warehouse gestreamt.

Es gibt Dashboards und Konsolen zur Überwachung aller Aspekte des Backup & Recovery-Prozesses für jede Cyber Protect-Bereitstellung sowie für den Acronis Centralized Monitoring Hub. Dieser Hub bietet historische Ansichten, anpassbare Berichte und eine Überwachung des laufenden Backup & Recovery-Prozesses. Ziel ist es, einen unterbrechungsfreien Betrieb bei Vorfällen, Angriffen und anderen Problemen zu gewährleisten, die die Resilienz von OT-Umgebungen beeinträchtigen (siehe Abbildung 2).

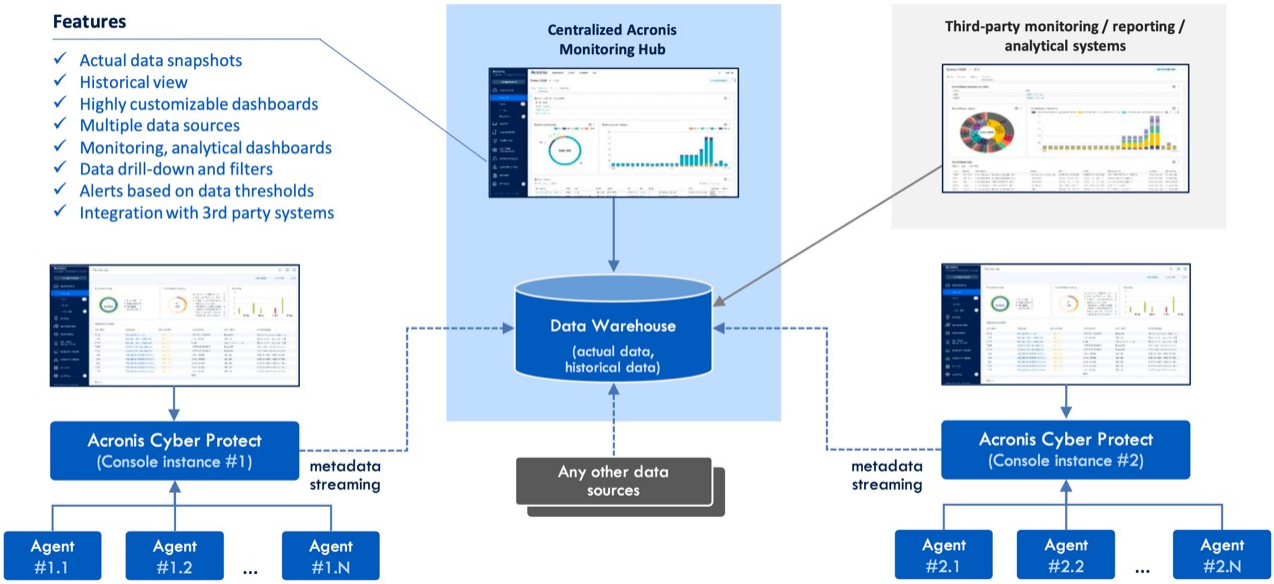

Abbildung 2. Systemarchitektur von Acronis

ACRONIS INTEGRATIONEN

Acronis Cyber Protect (beachten Sie die beiden Instanzen in der Abbildung) unterstützt Integrationen, indem es Backup, Disaster Recovery, KI-basierten Malware-Schutz, Remote-Unterstützung und Sicherheitstools in einer einzigen Plattform für (OT-)Sicherheitsteams zusammenfasst. Dank dieser Konsolidierung ermöglicht es jedem Unternehmen (einschließlich OT-Sicherheitsteams) verschiedene Cyber Protection-Aspekte über eine zentrale Benutzeroberfläche zu verwalten, wodurch die Komplexität reduziert und die Effizienz gesteigert wird.

Die flexible Architektur der Plattform sowie die umfassenden Steuerungsmöglichkeiten per API oder Befehlszeile unterstützen die Entwicklung und Integration von Drittanbieter-Applikationen sowohl durch Acronis als auch durch Drittanbieter (siehe die in Abbildung 2 dargestellten Drittanbieter-Feeds, die mit dem zentralen Data Warehouse verbunden sind). Dieses Design fördert ein dynamisches Ökosystem, in das zusätzliche Schutz-, Verwaltungs- und Automatisierungsdienste integriert werden können, wodurch sichergestellt wird, dass die Plattform an sich verändernde

Cyber Security-Landschaften angepasst werden kann. Diese Flexibilität stellt sicher, dass Unternehmen die Lösungen von Acronis auch in ihre vorhandenen Infrastrukturen integrieren können. Dies verbessert die allgemeine Widerstandsfähigkeit und Sicherheit, insbesondere in OT-Umgebungen.

DAS FORENSISCHE BACKUP VON ACRONIS

Acronis Cyber Protect enthält eine forensische Backup-Funktion, die nachfolgfende Analysen durch das Sammeln digitaler Beweise aus Laufwerk-Backups erleichtert. Diese Funktion ist von entscheidender Bedeutung für Unternehmen, die Compliance-Vorschriften einhalten und interne Untersuchungen effizient durchführen müssen. Sie ist aber auch sehr wichtig für OT-Umgebungen, da die Forensik bei der Identifizierung von Angriffen auf kritische Infrastrukturen und betriebsrelevante Dienste helfen kann.

Beim forensischen Backup von Acronis werden vollständige Laufwerk-Images erfasst, die neben aktivem Daten auch die Sektoren von unbelegtem Speicherplatz und Arbeitsspeicher-Abbildern (Memory Dumps) erfasst. Dieser gründliche Ansatz, der zunehmend zu einer generellen Anforderung in der OT-Sicherheit wird, stellt sicher, dass alle potenziell relevanten digitalen Beweise ordnungsgemäß gesichert werden. Dies erleichtert ausführliche Analysen nach einem Vorfall sowie die Einhaltung gesetzlicher oder anderer regulatorischer Auflagen.

Durch die Integration einer forensischen Datenerfassung in normale Backup-Abläufe ermöglicht Acronis Unternehmen die Aufrechterhaltung der Betriebskontinuität sowohl in IT- als auch in OT-Umgebungen und stellt gleichzeitig sicher, dass geschäftskritische forensische Informationen bei Bedarf sofort verfügbar sind. Diese Integration eliminiert die Notwendigkeit separater forensischer Datenerfassungsprozesse, optimiert den Betrieb und reduziert im Ernstfall das Risiko von Datenverlusten.

INTEGRIERTE DISASTER RECOVERY-FUNKTIONALITÄT VON ACRONIS

Acronis Cyber Protect bietet eine integrierte Disaster Recovery-Lösung, die nicht nur die Komplexität, sondern auch die Kosten minimiert. Durch die Kombination von Backup- und Disaster Recovery-Funktionen stellt die Plattform sicher, dass Unternehmen ihre Workloads selbst nach schwerwiegenden Vorfällen (wie Naturkatastrophen, menschlicher Sabotage, Cyberangriffen oder Hardware-Ausfällen) schnell wiederherstellen können. Wie bereits erwähnt, können diese Ereignisse schwerwiegende Auswirkungen auf OT-Systeme haben.

Die Disaster Recovery-Funktionalität ermöglicht das schnelle Hochfahren von IT- oder OT-Workloads im Desasterfall, die Erstellung von Runbooks zur Automatisierung der Recovery- und Test-Failover-Prozesse, um sicherzustellen, dass die Systeme im Ernstfall wie erwartet funktionieren. Diese Fähigkeiten sind zur Aufrechterhaltung der Geschäftskontinuität und zur Minimierung von Ausfallzeiten unerlässlich, insbesondere für Echtzeit-Applikationen, wie sie in OT-Umgebungen üblich sind.

Durch die Integration von Disaster Recovery-, Cyber Security- und Endpoint Management-Funktionalitäten bietet Acronis einen ganzheitlichen Cyber Protection-Ansatz. Diese Integration stellt sicher, dass alle Aspekte der IT-Infrastruktur eines Unternehmens geschützt sind, und fördert die Resilienz gegenüber einer Vielzahl möglicher Störungen. Sie erleichtert auch die Management-Aufgaben von CISOs, die sowohl für IT- als auch für OT-Produktionssysteme verantwortlich sind.

EINHALTUNG REGULATORISCHER AUFLAGEN

Neben der betrieblichen Notwendigkeit von Backup und Resilienz müssen sich OT-Sicherheitsteams zunehmend mit einer Vielzahl neuer externer Compliance-Regeln und anderer regulatorischer Rahmenbedingungen auseinandersetzen. Dies hat dazu geführt, dass die Einhaltung von Cyber Security-Vorschriften in OT-Umgebungen zu einem viel anspruchsvolleren Bestandteil von Unternehmenssicherheitsprogrammen geworden ist, da sie konvergierende Anforderungen umfasst, die sich mit der Zunahme der Bedrohungen weiterentwickeln.

Insbesondere stellen wir fest, dass globale Regulierungsbehörden die operationale Resilienz durch Rahmenwerke wie den Digital Operational Resilience Act (DORA) in der Europäischen Union und die Richtlinien des Basler Ausschusses für Bankenaufsicht betonen, was die Notwendigkeit robuster Cyber Security-Maßnahmen in kritischen Infrastruktursektoren unterstreicht. Die Lösungen von Acronis helfen, diese regulatorischen Auflagen zu erfüllen, indem sie Unterstützung in den folgenden Bereichen bieten:

1. **Umfassende Risikomanagement-Frameworks** – Die Lösungen von Acronis ermöglichen es Sicherheitsorganisationen, anpassungsfähige Risikomanagement-Frameworks zu implementieren, die Resilienz regelmäßig zu testen und kontinuierlich mit Stakeholdern und Regulierungsbehörden zu kommunizieren. Auf diese Weise stehen sie im Einklang mit globalen IT- und OT-Rahmenwerken für betriebliche Resilienz.
2. **Incident Response-Planung** – Acronis hilft bei der Entwicklung schriftlicher Reaktionspläne auf Zwischenfälle, die entweder eigenständig oder Teil eines Business Continuity-Plans sind, um auf mögliche Cyberbedrohungen gut vorbereitet zu sein. Für viele OT-Sicherheitsteams ist dies Neuland, daher ist die Unterstützung von Acronis hier besonders hilfreich.
3. **Drittanbieter-Risikomanagement** – Die Integrationsfähigkeiten von Acronis ermöglichen eine zuverlässige Kontrolle von Drittanbietern. Diese Funktion wird von den Aufsichtsbehörden als entscheidend für die betriebliche Resilienz hervorgehoben. Wie bereits erwähnt, kann die Cyber-Integration in Drittanbieter-Applikatioinen eine Herausforderung darstellen, da sie in der Vergangenheit entweder komplett ignoriert oder vernachlässigt wurde.

FÜHRENDE ANBIETER VON OT- UND ICS-AUTOMATISIERUNGSLÖSUNGEN VERTRAUEN AUF ACRONIS

Die Backup & Recovery-Lösungen von Acronis werden von den weltweit größten Anbietern von OT- und ICS-Plattformen eingesetzt, was die entscheidende Rolle von Acronis bei der Gewährleistung von Resilienz in OT- und Industrieumgebungen unterstreicht. Branchenführer (wie ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation oder Yokogawa) integrieren Acronis Cyber Protect in ihre Plattformen – entweder als White-Label- oder Co-Branding-Lösung – und ermöglichen ihren Kund:innen so eine betriebliche Resilienz. Die Tatsache, dass diese globalen Giganten Acronis als Standardlösung einsetzen, zeugt von der Zuverlässigkeit, Flexibilität und Marktführerschaft der Plattform im Bereich Backup & Recovery für OT-Umgebungen.

FAZIT UND AKTIONSPLAN FÜR OT-SICHERHEITSTEAMS

Wir sind der Meinung, dass sich die Backup- und Recovery-Lösungen von Acronis gut für alle Kund:innen eignen, die die Resilienz und Sicherheit ihrer OT-Infrastruktur verbessern möchten. Mit schnellen Wiederherstellungsfunktionen, der Unterstützung von Legacy-Systemen, anpassbaren Backup-Plänen sowie der Einhaltung gesetzlicher Vorschriften unterstützt Acronis Unternehmen bei der Aufrechterhaltung der Betriebskontinuität und der Compliance mit sich ändernden globalen Standards für betriebliche Resilienz.

Wir raten CISOs, die mit dieser Verantwortung betraut sind, oder jedem anderen Management- oder Führungsteam, das sich mit Cyber-Resilienz für OT befasst, sich umgehend mit Acronis in Verbindung zu setzen, um mehr über diese Fähigkeiten seiner Lösungen zu erfahren. Unser TAG-Team steht Ihnen auch gerne jederzeit zur Verfügung, um Sie bei Ihren Bemühungen zu unterstützen, einen tieferen Einblick in dieses und verwandte Themen im Bereich Cyber Security und künstliche Intelligenz zu gewinnen. Wir freuen uns darauf, von Ihnen zu hören.

[1] Wir sind den technischen und Führungsteams von Acronis sehr dankbar, dass sie uns dabei geholfen haben, die verschiedenen Risiken zu verstehen, die sie in den OT-Umgebungen ihrer Kund:innen beobachten. Das Acronis Team hat uns Zugang zu ihren Produktdokumentationen gewährt und dabei geholfen, nützliche Einblicke in ihre Produkt-Roadmaps für IT- und OT-Sicherheit zu gewinnen.

ÜBER TAG

TAG ist ein renommiertes Forschungs- und Beratungsunternehmen, das Tausenden von kommerziellen Lösungsanbietern und Fortune 500-Unternehmen Einblicke in und Empfehlungen für die Bereiche Cyber Security, künstliche Intelligenz und Klimawissenschaften bietet. TAG wurde 2016 gegründet und hat seinen Hauptsitz in New York City. Das Unternehmen widersetzt sich dem Trend zu „Pay-for-Play"-Forschung, indem es unvoreingenommene und fundierte Beratung, Marktanalysen, Projektberatung und personalisierte Inhalte anbietet – alles aus der Perspektive von Praktiker:innen.

Copyright © 2025 TAG Infosphere, Inc. Die Vervielfältigung, Verbreitung oder Weitergabe dieses Berichts ist ohne schriftliche Genehmigung von TAG Infosphere nicht gestattet. Das in diesem Bericht enthaltene Material gibt die Meinungen der Analyst:innen von TAG Infosphere wieder und sollte nicht als unbedingte Tatsachenbehauptung ausgelegt werden. Es wird keine Gewähr für die Richtigkeit, Nützlichkeit, Genauigkeit oder Vollständigkeit dieses Berichts übernommen.