Veröffentlicht am:
25. Februar 2025
Autorin:
Hollie Hennessy, Principal Analyst

On the Radar: Acronis bietet eine Backup & Recovery-Lösung für Cyber-Resilienz in OT-Umgebungen

Zusammenfassung

Katalysator

Das Angebot von Acronis im Bereich OT (Operational Technology) konzentriert sich auf den Aspekt „Wiederherstellen“ im Cyber Security-Puzzle. Es bietet Backup-, Recovery- und Data Protection-Funktionalitäten für OT-Umgebungen, um die Cyber-Resilienz zu verbessern. Der gute Ruf, den Acronis im Bereich OT-Sicherheit genießt, wird durch das starke Partner- und Channel-Netzwerk weiter gefestigt.

Einschätzung von Omdia

Die OT-Sicherheit umfasst mehrere Ziele – wovon ein spezielles schnelle Wiederherstellungen nach Vorfällen oder Angriffen sind. In Umgebungen mit geschäftskritischer operationaler Infrastruktur ist Geschäftskontinuität vielleicht noch wichtiger als in manchen IT-Umgebungen. Dies liegt an den regulatorischen Anforderungen, denen viele Unternehmen unterliegen, die kritische Infrastrukturen betreiben, und an den oft erheblichen finanziellen Auswirkungen oder potenziellen Schäden, die durch Ausfallzeiten verursacht werden.

Einen effektiven, erprobten und getesteten Backup & Recovery-Plan zu haben, ist in jeder Umgebung unerlässlich. Aber auch der beste Schutz kann Angriffe nicht ausschließen. Zu wissen, was in einem solchen Fall zu tun ist, und betroffene Systeme schnellstmöglich wieder zum Laufen zu bringen, sollte daher ein

wesentlicher Bestandteil jeder Cyber Security-Strategie sein. Regelmäßige Backups sind neben schnellen und effizienten Wiederherstellungsprozessen für exfiltrierte Daten von entscheidender Bedeutung.

Das Backup & Recovery-Angebot von Acronis wird hauptsächlich über indirekte Vertriebskanäle angeboten. Es bietet Service Providern und industriellen Anbietern die Möglichkeit, Backup & Recovery-Funktionen in ihre Services und Plattformen zu integrieren – und stellt darüber hinaus Unternehmen mit OT-Fokus direkt eine Punktlösung zur Verfügung.

Warum sollten Sie Acronis auf Ihrem Radar haben?

Acronis hat OEM-Partnerschaften (Original Equipment Manufacturer) geschlossen und ist die eingesetzte Backup & Recovery-Lösung für eine Vielzahl führender Anbieter von Automatisierungslösungen in den Bereichen Fertigung, Gesundheitswesen und Energie. Das Acronis Produkt unterstützt die Einhaltung gesetzlicher Vorschriften (wie NIS2) und Standards (wie ISA/IEC 62443). Darüber hinaus kann es das Produktangebot von Anbietern industrieller Automatisierung verbessern, da sie ihren Kund:innen einen zuverlässigeren und vertrauenswürdigeren Service bieten können. Das Know-how von Acronis im Backup & Recovery-Bereich hat es ermöglicht, eine Lösung zu entwickeln, die den Anforderungen industrieller Umgebungen und dort immer noch eingesetzter Legacy-Systeme gerecht wird.

Marktkontext

Der Markt für OT-Sicherheit wird von den Bereichen Asset Management, Monitoring sowie Incident Detection & Response dominiert. Und viele der führenden Anbieter in diesem Bereich bieten Lösungen für alle oder die meisten dieser Bereiche an. Darüber hinaus benötigt der Markt zusätzliche Fähigkeiten, um sowohl den regulatorischen Anforderungen als auch den Bedürfnissen von Industrie- und OT-orientierten Unternehmen gerecht zu werden.

Geschäftskontinuität ist (egal ob aus sicherheitstechnischen, betrieblichen oder finanziellen Gründen) in diesen Umgebungen von größter Bedeutung. Daher ist es wichtig, Datenschutzverletzungen oder Angriffe zu erkennen und bekannten Bedrohungen vorzubeugen. Zur Bewältigung des letztgenannten Aspekts wurden zusätzliche Lösungen entwickelt, entweder in Form von präventiver Automatisierung oder in Form von proaktiveren Ansätzen wie Risiko- und Schwachstellen-Management, Simulation von Sicherheitsverletzungen und Angriffen sowie Angriffsflächen-Management.

Da aber kein System unfehlbar ist, muss es auch weiterhin die Fähigkeit zur System-Wiederherstellung nach Vorfällen geben. Dieser Teil des Marktes konzentriert sich auf Cyber-Resilienz. Er umfasst Tools und Services für Schadensbehebungsmaßnahmen, für Forensik-Backups und zur Wiederherstellung von Daten bzw. Systemen. Dies sind alles Bereiche, in denen die Lösungen von Acronis gut für OT geeignet sind.

Eine gute Orientierungshilfe für die Cybersicherheitsanforderungen kritischer (und eigentlich aller) Unternehmen ist das NIST Cybersecurity Framework (CSF) 2.0. Ursprünglich auf kritische Infrastrukturen ausgerichtet, findet das Framework inzwischen weite Verbreitung und Anwendung, auch wenn sein Geltungsbereich inzwischen weiter gefasst ist. Die aktualisierte Version des Frameworks umfasst verschiedene Funktionen:

- Identifizieren
- Schützen
- Erkennen

- Reagieren
- Wiederherstellen
- Die neueste Ergänzung: Governance

Produkt/Service im Überblick

Die Data Protection-Funktionen von Acronis umfassen im Wesentlichen zwei Bereiche: „Backup“ und „Disaster Recovery“. Beide sind Teil der Acronis Cyber Protect-Plattform. Zu den Funktionen gehören:

- Vollständiges Image-Backup eines laufenden Systems mit ausfallsicherem Patching (d. h. es wird ein Image-Backup erstellt, bevor Patches für das System oder eine Applikationen installiert werden)
- Self-Service mit „One-Click Recovery“
- Universal Restore ermöglicht Wiederherstellungen auf beliebiger Hardware oder zu jedem Hypervisor
- Instant Restore ermöglicht es, ein System schon zu booten und auszuführen, während der Wiederherstellungsprozess im Hintergrund noch läuft
- Unveränderliche Backups für mehr Sicherheit
- Unterstützt Windows, Linux und andere Betriebssysteme/Applikationen, (einschließlich Legacy-Versionen wie Windows XP, die in Industrieumgebungen noch häufig im Einsatz sind)
- Antimalware-Scans und Antivirus-Updates als Bestandteil von Wiederherstellungsprozessen
- Vollständig integrierte Disaster Recovery-as-a-Service-Funktionalität

Acronis Cyber Protect ist auf OT-Umgebungen zugeschnitten, das es Installationen und Backups live durchführt, ohne dass die Systeme offline geschaltet oder neu gestartet werden müssen. Darüber hinaus unterstützt die Acronis Lösung bei Bedarf auch Wiederherstellungen auf fabrikneuer Hardware. Dies geschieht über den Acronis Cyber Protect-Agenten, der je nach Situation und Anforderungen des Kundenunternehmens mit oder ohne Malware-Schutz installiert werden kann.

Die Wiederherstellung wird durch die One-Click Recovery-Technologie vereinfacht, sodass auch Personen ohne IT- oder Sicherheitskenntnisse betroffene Systeme wiederherstellen können. Dies ist besonders bei abgelegenen oder verteilten Umgebungen wichtig (wie etwa Bohrinseln), die schwer zu erreichen sind – und in zeitkritischen Szenarien (wie etwa beim Wiederanfahren einer Produktionslinie). Es ist auch möglich, Daten durch einen Neustart aus einem lokalen Laufwerk-Backup oder aus der Acronis Cloud wiederherzustellen. Darüber hinaus werden die gesicherten Daten automatisch auf Malware und neueste Viren gescannt.

Alle Erkenntnisse und Kontrollen laufen in einem zentralen Dashboard (dem Centralized Acronis Monitoring Hub) zusammen. Das Dashboard nutzt Metadaten zur Analyse und zur Integration mit Drittanbieter-Applikationen.

Unternehmensinformationen

Hintergrund

Acronis wurde 2003 in Singapur gegründet und hat seit 2008 seinen Hauptsitz in der Schweiz. Heute beschäftigt das Unternehmen mehr als 1.800 Mitarbeiter:innen in 45 Ländern. Acronis unterstützt mehr als 750.000 Unternehmen in 150 Ländern.

Aufbauend auf seinen Wurzeln im Bereich Data Protection hat der Anbieter in den letzten Jahren ein beträchtliches Wachstum verzeichnet und bietet seinen Partnern und Kund:innen eine Reihe von Cyber Security-Produkten an. Mit der Acronis Cyber Protect-Plattform hat das Unternehmen zudem Pionierarbeit bei der Zusammenführung dieser beiden Bereiche geleistet.

Mit Acronis Labs legt Acronis einen starken Fokus auf Forschung und Entwicklung. Acronis Labs beschäftigt über 500 Ingenieur:innen, von denen mehr als 20 promoviert haben, und hält über 200 Patente, die dem Unternehmen seit seiner Gründung in den letzten 17 Jahren erteilt wurden. Die Threat Research Unit (TRU) von Acronis veröffentlicht zudem regelmäßig Erkenntnisse und Entdeckungen im Zusammenhang mit aktuellen und neuen Cyberbedrohungen.

Im August 2024 wurde bekannt gegeben, dass EQT (eine europäische Private-Equity-Gesellschaft) eine Mehrheitsbeteiligung an Acronis zu einem geschätzten Preis von 4 Mrd. USD erwerben wird. Der Abschluss der Transaktion wird für das erste oder zweite Quartal 2025 erwartet. Zuvor hatte Acronis über 500 Mio. USD von Investoren wie CVC Capital Partners, BlackRock und Goldman Sachs erhalten.

Aktuelle Position

Acronis verfügt über eine Reihe von Cyber Security-Technologien, die über eine reine Backup & Recovery-Funktionalität in OT-Umgebungen hinausgehen. Dazu gehört auch eine neu eingeführte XDR-Lösung (Extended Detection & Response) sowie eine Unterstützung durch generative KI-Assistenten. Das Portfolio des Anbieters umfasst im Wesentlichen folgende Bereiche:

- Data Protection (siehe oben)
- Cyber Security (Endpunkt-Sicherheit, Malware-Schutz, EDR/XDR usw.)
- Endpunktverwaltung (Patch- und Schwachstellen-Management, Remote-Zugriff usw.)

Acronis verkauft zwar einen Teil seiner Produkte direkt an Endkund:innen, der primäre Vertriebsweg verläuft jedoch indirekt über Vertriebspartner, einschließlich Reseller, Managed Service Provider (MSPs) und OEMs. Im Bereich der industriellen Automatisierung gehören dazu eine Reihe von Herstellern, wie ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation und Yokogawa.

Acronis bietet auch eine Freemium-Version seiner Plattform an. Erweiterte Funktionen werden nutzungsbasiert abgerechnet.

Zukunftspläne

Obwohl Acronis plant, seine KI-Plattform um weitere Cyber Security-Funktionen zu erweitern, hat das Unternehmen nicht die Absicht, die Bereiche IoT (Internet of Things) und OT damit abzudecken.

Wichtigste Fakten

Tabelle 1: Datenblatt: Acronis

Produktname	Acronis Cyber Protect	**Produktklassifikation**	Endpunktschutz und Backup/Recovery
Versionsnummer	Version 16	**Freigabedatum**	Februar 2024
Abgedeckte Branchen	Fertigungsindustrie Gesundheitswesen Forschungslabore (Biopharma-Branche) Öl- und Gasindustrie Stromerzeugung/Energie Transportwesen Automobilbranche Einzelhandel Bildungseinrichtungen/ Behörden Baubranche	**Abgedeckte Regionen**	Nordamerika Mittel- und Südamerika EMEA APAC
Größe der Zielunternehmen	Enterprise, mittelgroß, KMU	**Lizenzoptionen**	Software-Dauerlizenzen oder -Abonnementlizenzen
URL	www.acronis.com https://www.acronis.com/de-de/products/cyber-protect-enterprise/	**Vertriebsweg(e)**	Direkt
Hauptsitz	Schaffhausen, Schweiz	**Anzahl der Mitarbeitenden**	ca. 2.000

Quelle: Omdia

Analysten-Kommentar

Die zahlreichen Innovationen von Acronis und die Spezialisierung auf den Bereich „Data Protection und Recovery“ haben zu einem attraktiven Angebot für industrielle Umgebungen geführt. Die Lösung bietet mehrere Optionen für Deployment sowie Backup & Recovery und ermöglicht so Flexibilität und die Erfüllung individueller Kundenanforderungen. Viele der Anbieter von OT-Sicherheitslösungen, mit denen Service Provider oder Anbieter von industriellen Automatisierungssystemen zusammenarbeiten können, bieten keine Datenwiederherstellungsfunktionalität an, was eine große Chance für Acronis darstellt. Die Konkurrenz von Acronis im Bereich Datenwiederherstellung konzentriert sich eher auf die IT-Seite dieses Geschäfts. Die Mitbewerber verfügen auch nicht über die Spezialisierung, die Acronis in industriellen

Umgebungen bieten kann, und den guten Ruf, den sich das Unternehmen durch ein hohes Maß an Integration und enge Partnerschaften mit führenden industriellen OEMs erworben hat.

Das Angebot von Acronis für den indirekten Vertriebskanal und seine Partner ist jedoch die umfassendere Plattform. Diese erfüllt keine OT-Sicherheitsanforderungen, die über Wiederherstellungsfunktionen hinausgehen, und plant dies derzeit auch nicht. Die MSP- oder MSSP-Partner (Managed Security Service Provider) von Acronis konzentrieren sich mehr auf die Bereitstellung von IT-Services für Endbenutzer:innen. Darüber hinaus würde der Einstieg in den IoT/OT-Bereich mit einer Security Operations-Lösung aufgrund des Geräteverhaltens und der proprietären Protokolle wahrscheinlich einen erheblichen Entwicklungsaufwand erfordern. Die Plattform würde es den Partnern ermöglichen, wichtige IT-Sicherheitsfunktionen anzubieten, aber sie würden sich wahrscheinlich an andere Anbieter von OT-Sicherheitslösungen wenden, wenn es um Funktionen wie Erkennung, Prävention und Transparenz für Industrieunternehmen geht. Die führenden Unternehmen im Bereich OT-Sicherheit konzentrieren sich derzeit nicht auf den Bereich „Data Protection und Recovery“. Es besteht jedoch die Möglichkeit, dass diese Anbieter versuchen werden, diese Lücke zu schließen, was zu mehr Wettbewerb führen würde.

Anhang

On the Radar

„On the Radar“ ist eine Serie von kurzen Forschungsberichten über Anbieter, die innovative Ideen, Produkte oder Geschäftsmodelle auf den Markt bringen. Es lohnt sich, „On the Radar“-Anbieter im Auge zu behalten, da diese das Potenzial haben, den Markt zu verändern, weil ihre Herangehensweise, jüngsten Entwicklungen oder Strategien wegweisend und interessant für Käufer:innen und Nutzer:innen von Technologie sein könnten.

Weiterführende Literatur

Omdia Market Radar: OT Cybersecurity Platforms, 2025 (Januar 2025)

2025 Trends to Watch: IoT Cybersecurity (September 2024)

„Xage Security gibt eine neue Partnerschaft mit Armis und Yokogawa Engineering Asia für sichere Remote-Zugriffe bekannt“ (September 2024)

Omdia Secure Industrial Networks Survey 2023: Overall Findings (Dezember 2023)

Autor:in

Hollie Hennessy, Principal Analyst, IoT Cybersecurity

askananalyst@omdia.com

Zitiervorschriften

Bitte wenden Sie sich an citations@omdia.com für externe Zitierungen und die Nutzung von Forschungsergebnissen und Daten von Omdia.

Beratung von Omdia

Wir hoffen, dass Ihnen diese Analyse hilft, fundierte und kreative Geschäftsentscheidungen zu treffen. Sollten Sie weitere Fragen haben, steht Ihnen das Beratungsteam von Omdia gerne zur Verfügung. Für weitere Informationen zu den Beratungsleistungen von Omdia kontaktieren Sie uns bitte direkt unter consulting@omdia.com.

Copyright-Hinweis und Haftungsausschluss

KONTAKT

omdia.com

askananalyst@omdia.com