Schutz für kritische Infrastrukturen

Wie Sie eine kontinuierliche Versorgung mit Strom, Wasser, Erdgas und erneuerbaren Energien sicherstellen

Was auf dem Spiel steht

Versorgungsunternehmen sorgen für vieles mehr als nur dafür, dass das Licht nicht ausgeht. Sie stellen sicher, dass Krankenhäuser mit Notstrom versorgt werden, das Trinkwasser sicher ist, Haushalte im Winter mit Gas beliefert werden und die Rettungsdienste einsatzbereit sind. Fällt ein Versorgungsunternehmen aus, hat das Auswirkungen auf viele Bereiche. Auch auf andere Sektoren.

Bei von staatsnahen Hackergruppen verursachten Vorfällen wurde deutlich, dass es ihnen um die Störung des Betriebs und nicht um Datendiebstahl geht. Ein Beispiel ist der Bedrohungsakteur „Volt Typhoon", der 300 Tage lang unentdeckt in einem US-amerikanischen Strom- und Wasserversorgungsunternehmen aktiv war und dort die OT-Betriebsabläufe und die Netzstruktur ausspionierte.[1] Das FBI und die CISA haben bestätigt, dass dies kein Einzelfall ist. Versorgungsunternehmen sind zu einem Hauptziel für staatlich unterstützte Cyberkriminelle, Ransomware-Gruppen und andere Akteure mit zerstörerischer Absicht geworden.

Beliebte Ziele sind abgelegene Umspannwerke, Wasserpumpstationen oder ländliche Stromerzeugungsstandorte, da dort in der Regel kein IT-Personal vor Ort ist und die nächste Hilfe oft mehrere Stunden entfernt ist. Für die Wiederherstellung der Stromversorgung, des Wasserdrucks oder der Gasversorgung einer Gemeinde bleibt nur ein Zeitfenster von wenigen Minuten, nicht von mehreren Tagen.

Was wir aus dem Angriff auf den US-Wasserversorger gelernt haben

Im Jahr 2024 wurde der größte US-amerikanische Wasserversorger Opfer eines Cyberangriffs. Zwar waren die im Betrieb befindlichen Systeme nicht betroffen, es kam jedoch zu Ausfällen bei der Abrechnung und das Portal musste abgeschaltet werden. Ziel des Angriffs waren die IT-Systeme, auf die die OT-Systeme angewiesen sind, darunter Active Directory, Historians, GIS, OMS und die Abrechnung.[2]

[1] https://www.securityweek.com/chinas-volt-typhoon-hackers-dwelled-in-us-electric-grid-for-300-days

[2] https://www.amwater.com/press-room/press-releases/corporate/american-water-reactivating-systems-after-cyber-event-10102024

Die Bedrohungslage

Im vergangenen Jahr war jedes fünfte ICS-/OT-Unternehmen von einem bestätigten Cybervorfall betroffen. Es gab keine Vorwarnung. Die bestätigten Vorfälle betrafen die OT-Systeme, wobei 40 % direkte Betriebsstörungen verursachten und bei fast jedem fünften die Behebung mehr als einen Monat in Anspruch nahm. Für Versorgungsunternehmen ist diese lange Behebungsdauer keine bloße statistische Größe. Sie bedeutet Tage ohne zuverlässige Strom-, Wasser- oder Gasversorgung für die betroffenen Gemeinden.

1 von 5

ICS-/OT-Unternehmen war im vergangenen Jahr von einem Cybervorfall betroffen.

SANS State of ICS/OT Security 2025

40 %

dieser Vorfälle führten zu Betriebsstörungen, die sich auf die Produktion, die Service-Bereitstellung oder den öffentlichen Betrieb auswirkten. In 37,9 % der Fälle war Ransomware der Auslöser.

SANS State of ICS/OT Security 2025

19 %

der OT-Vorfälle konnten 2025 erst nach einem Monat komplett behoben werden. Die Bedrohungserkennung hat sich verbessert. Die Wiederherstellung bleibt jedoch die Achillesferse.

SANS State of ICS/OT Security 2025

Kleine und mittlere Versorgungsunternehmen gelten als attraktive Ziele. Oft verfügen sie über keine eigenen Cybersicherheitsteams und nur über begrenzte Ressourcen für die Wiederherstellung.

Die Lösung: Eine lokale Wiederherstellung, für die keine IT-Kenntnisse nötig sind

Acronis Cyber Protect für OT bietet OT-Systemen in der Versorgungsbranche Cyber-Resilienz auf IT-Niveau, ohne den laufenden Betrieb zu beeinträchtigen. Wenn sich in einem entfernten Umspannwerk, einer Pumpstation oder einem Kraftwerk ein Vorfall ereignet, ist zwar möglicherweise Automatisierungs- oder leitendes Betriebspersonal vor Ort, jedoch kein Cybersicherheitsteam. Die Wiederherstellungsabläufe sind so konzipiert, dass die Personen vor Ort sie selbst durchführen können, mit minimaler Abhängigkeit von externen Verbindungen oder dem Eingreifen der IT-Abteilung.

Backup ohne Ausfallzeit
Vollständiges Image- und Datei-Backup ohne Neustarts und Ausfallzeiten. Der Sektor-für-Sektor-Modus wird für proprietäre OT-Dateisysteme automatisch aktiviert. Es werden VSS-konsistente Snapshots für alle SCADA- und Historian-Systeme mit Multivolume-Konfigurationen erstellt.

One-Click Recovery für OT-Personal
Autorisiertes Vor-Ort-Personal (z. B. Ingenieur:innen für den Umspannwerkbetrieb, leitendes Betriebspersonal in Wasserkraftwerken, Schichtleiter:innen) kann einen geführten Wiederherstellungs-Workflow anwenden. Damit lässt sich ein ausgefallenes System in den letzten bekannten fehlerfreien Zustand zurücksetzen. Dadurch verkürzt sich die Wiederherstellungszeit – je nach den Bedingungen vor Ort – von Stunden oder Tagen auf wenige Minuten.

Bare-Metal Recovery und Universal Restore
Ermöglicht die automatische Wiederherstellung auf identischer oder abweichender Hardware. Universal Restore installiert die richtigen Treiber, ohne dass eine manuelle Neukonfiguration erforderlich ist. Das ist besonders wichtig, wenn der ursprüngliche Industrie-PC nicht mehr verfügbar oder veraltet ist.

Sichere und verifizierte Wiederherstellung
Um das Risiko einer Re-Infektion von SCADA- oder HMI-Systemen zu verringern, werden alle Backup-Images vor der Wiederherstellung auf Malware überprüft und validiert. Werden Bedrohungen erkannt, werden diese markiert und im Rahmen des Wiederherstellungsprozesses entfernt.

Air-Gap- und Offline-Anlagen
Alle Komponenten werden lokal bereitgestellt. Der Management Server läuft vollständig offline. Die Malware-Datenbank wird ohne Internetzugang aktualisiert. Die Agenten gewährleisten für weitere 30 Tage Schutz, falls der Management Server nicht erreichbar ist.

Unveränderlicher Backup Storage
Backup-Archive können nicht gelöscht, geändert oder durch Ransomware verschlüsselt werden – selbst dann nicht, wenn die Anmeldedaten kompromittiert wurden. Zur Erfüllung regulatorischer Vorschriften werden mithilfe der Governance- und Compliance-Modi Aufbewahrungsfristen von bis zu 10 Jahren durchgesetzt.

Altsysteme: Wir schützen, was andere Anbieter bereits aufgegeben haben

Die Betriebsdauer von OT-Anlagen von Versorgungsunternehmen beträgt 30 Jahre und mehr. Die computergestützten Systeme, mit denen sie verwaltet werden – darunter HMIs, SCADA-Server und Engineering-Workstations – laufen oft auf Betriebssystemen, für die die großen Anbieter bereits vor Jahren den Support eingestellt haben.

Windows 10 in OT-Umgebungen: Wie Sie Lifecycle-Risiken managen[3]

Versorgungsunternehmen verwenden auf ihren OT-Workstations häufig verschiedene Windows 10-Versionen mit unterschiedlichen Support-Zeiträumen. Während einige bereits nicht mehr unterstützt werden, erreichen andere 2027, 2029 oder später wichtige Lifecycle-Meilensteine. Das Upgraden oder Patchen dieser Systeme ist alles andere als eine Routineaufgabe. Es kann kostspielige Neuvalidierungen auslösen, lizenzierte SCADA-/HMI-Software lahmlegen oder OEM-Supportverträge ungültig machen. Acronis mindert diese Risiken, indem imagebasierte Backups mit einer Positivliste für Applikationen kombiniert werden. Dadurch wird der Betrieb von Altsystemen abgesichert, wenn eine sofortige Migration auf ein neueres Betriebssystem nicht möglich ist.

Acronis bietet vollständigen Backup- und Recovery-Support für Windows XP SP1/SP2/SP3 bis hin zu Windows Server 2025, für Linux Kernel 2.6.9 bis 5.19 sowie für alle gängigen Hypervisoren. Somit werden alle möglichen Betriebssystemgenerationen in OT-Umgebungen unterstützt.

Recovery und Wiederherstellung sind nicht dasselbe

In Versorgungsunternehmen kann eine Verwechslung dieser beiden Begriffe die kontinuierliche Versorgung beeinträchtigen und im schlimmsten Fall sogar die öffentliche Sicherheit gefährden.

In diesem Kontext bedeutet **„Recovery"**, die Frequenzregelung oder den Wasserdruck schnell wiederherzustellen – und zwar ausgehend vom jeweils letzten verfügbaren, einwandfreien Zustand. Die Aufrechterhaltung oder Wiederherstellung eines – wenn auch nur teilweisen – Betriebs, durch den beispielsweise die Stromversorgung eines Krankenhauses gewährleistet wird, hat höchste Priorität.

„Wiederherstellung" bedeutet die sichere Rückversetzung des gesamten zertifizierten Systems in einen bekannten, funktionsfähigen Zustand, ohne dass dabei erneut Malware oder Datenbeschädigungen eingeführt werden.

Acronis unterstützt sowohl das Recovery als auch die Wiederherstellung. One-Click Recovery sorgt für eine rasche Wiederaufnahme des Betriebs und ermöglicht es autorisiertem Personal, die Wiederherstellung eigenständig vor Ort einzuleiten. Spezielle IT-Fachkräfte müssen dafür nicht hinzugezogen werden. Die validierten, forensischen Backups ermöglichen eine vollständige und verifizierte Wiederherstellung. Bevor Backup-Images verwendet und bereitgestellt werden, wird ein Malware-Scan durchgeführt. Zudem werden Blockchain-beglaubigte Beweismittel zur Nachverfolgbarkeit für Untersuchungen und Audits nach einem Vorfall bereitgestellt.

Laut dem SANS-Bericht „State of ICS/OT Security 2025" werden mittlerweile fast die Hälfte aller OT-Vorfälle innerhalb von 24 Stunden entdeckt. Bei 19 % dauert es jedoch mehr als einen Monat, bis der normale Betrieb wieder vollständig hergestellt ist. Die Bedrohungserkennung hat sich verbessert. Die Wiederherstellung bleibt jedoch die Achillesferse.

[3] https://learn.microsoft.com/de-de/windows/release-health/release-information

Was Acronis in Versorgungsunternehmen schützt

Versorgungssektor	Von Acronis geschützte Systeme und Daten
Strom: Erzeugung, Übertragung und Verteilung, Netzrand	SCADA-/EMS-Server, Steuerungs-PCs für Umspannwerke, HMI-Workstations, DER-/Mikronetz-Steuerungen, BESS-Standortsteuerungen und Historian-Server. Zu den geschützten Daten gehören Betriebssystem-Images, SCADA-/HMI-Konfigurationen, Alarmlogik, Historian-Datenbanken und technische Projektdateien.
Wasser und Abwasser	SCADA-Systeme für die Wasseraufbereitung, HMI-Workstations, Steuerungs-PCs für Pumpen und Hebewerke sowie Überwachungssysteme für Wasserspeicher. Geschützte Daten umfassen Betriebssystem-Images, Konfigurationen der Aufbereitungsprozesse, die Steuerungslogik der Pumpen und behördliche Meldedaten.
Erdgasverteilung	Server für die Pipeline-Überwachung, PCs in Kompressorstationen, PCs in Reglerstationen, SCADA-Server und Custody-Transfer-Systeme. Zu den geschützten Daten gehören Prozesskonfigurationen, Überwachungsdaten, Kalibrierungsdateien und Pipeline-Betriebsprotokolle.
Erneuerbare Energien: Wind, Sonne, Wasserkraft, Biomasse und grüner Wasserstoff	PCs zur Steuerung von Turbinen und Wechselrichtern, Anlagenmanagement-Server, BESS-Managementsysteme und Systeme zur Umgebungsüberwachung. Zu den geschützten Daten gehören Steuerungssoftware, Standortkonfigurationen und Betriebsdaten.
IT-Systeme, auf die OT angewiesen ist	Active Directory/DNS, Jump-Hosts, Historians (IT-seitig), GIS, OMS, AMI/MDMS, Abrechnung und Kundenportale. Zu den geschützten Daten gehören System-Images, Konfigurationsdaten sowie Kunden- und Betriebsdaten.

SIEM-Integration: Mithilfe der lokalen Acronis SIEM-Integration können Backup-, Sicherheits- und RMM-Alarme über Syslog an SIEM-Lösungen von Drittanbietern gesendet werden. Dadurch können OT- und Sicherheitsteams Vorfälle in allen geschützten Umgebungen zentral erfassen und verwalten.

Compliance und Qualitätssicherung

Acronis unterstützt Versorgungsunternehmen dabei, Beweismittel für Recovery-Pläne und Backup-Validierungsprotokolle zu sammeln, Testergebnisse und Aufbewahrungskontrollen wiederherzustellen sowie Nachweise für die Risikobewertung von Zulieferern zu sichern. All dies stärkt die Audit-Readiness, die in allen wichtigen regulatorischen Vorschriften gefordert wird. Acronis ist nach IEC 62443-4-1 zertifiziert.

NERC CIP (Nordamerika)

Mithilfe von Backup-Validierungsprotokollen und forensischen Backup-Daten lassen sich Nachweise für die Dokumentation von CIP-009 Recovery-Plänen erbringen. Diese Funktionen sind für den Betrieb in vollständig isolierten Netzwerken ohne Cloud-Abhängigkeit konzipiert.

NIS-2-Richtlinie (Europa)

Unterstützt die Erfüllung der Anforderungen von Artikel 21 in Bezug auf Geschäftskontinuität und Backup-Management. Unveränderliche Backups und konfigurierbare Aufbewahrungsfristen entsprechen den NIS-2-Vorgaben zu Data Protection und Recovery-Readiness.

IEC 62443 (weltweit)

Zertifiziert gemäß IEC 62443-4-1 für sichere SSDLC-Praktiken (Secure Software Development Life Cycle). Live-Backups ohne Betriebsunterbrechung sowie Integritätsprüfungen erfüllen die in der Norm festgelegten Anforderungen an die Verfügbarkeit von Ressourcen und die Betriebskontinuität.

Europäische Cyberresilienz-Verordnung

Eine SSDLC-Zertifizierung kann OEMs dabei unterstützen, die Sicherheitsbewertungen für Zulieferer zu erfüllen, die im Rahmen der Europäischen Cyberresilienz-Verordnung für den Beschaffungsprozess von Versorgungsunternehmen immer wichtiger werden.

Hinweis: Acronis kann Nachweise für Recovery-Pläne und die Audit-Readiness bereitstellen. Die Verantwortung für die Einhaltung gesetzlicher Vorschriften liegt jedoch weiterhin beim Betreiber.

OEM-Partner und Integratoren

Acronis Cyber Protect für OT ist als White-Labeling-, Co-Branding- oder Referenzlösung erhältlich. Dadurch können OEM-Partner und Integratoren von Steuerungssystemen Cyber-Resilienz direkt in ihre OT-Produktkataloge für Versorgungsunternehmen integrieren.

Acronis arbeitet weltweit mit OEMs und Technologiepartnern aus der OT-Branche zusammen, darunter ABB, Emerson, GE Vernova, Honeywell, Rockwell Automation, Schneider Electric und Yokogawa.

Für OEM-Partner

- Native Integration von One-Click Recovery: Werden Sie Resilienz-Partner statt nur Hardware-Lieferant.
- Reduziert das Volumen reaktiver Supportanrufe sowie die Reisekosten für Technikereinsätze bei typischen Recovery-Szenarien.
- Ermöglicht wiederkehrende, resilienzbasierte Managed Services und höhere Umsätze.
- Die Zertifizierung nach IEC 62443-4-1 ist entscheidend für die Beschaffung durch Versorgungsunternehmen und die Einhaltung der Europäischen Cyberresilienz-Verordnung.

Steuerungssystem-Integratoren

- Ermöglicht die Bereitstellung von SCADA-/HMI-/OT-Servern mit Recovery-Add-on.
- Standardisiertes Wiederherstellungsverfahren für alle bereitgestellten Systeme in Versorgungsunternehmen.
- Verringert den Supportaufwand nach der Inbetriebnahme und SLA-Risiken.
- Ermöglicht die Einführung wiederkehrender Resilienz-Services im Projekt- und Managed Service-Angebot.
- Kann als Referenzlösung oder als Co-Branding-Produkt neben Ihrer Integrationslösung verkauft werden.

Sind Sie bereit, die Infrastruktur zu schützen, auf die sich die Menschen verlassen?

Dann vereinbaren Sie eine Live-Demonstration mit dem Acronis OT-Team oder Ihrem OEM-Partner.

SPRECHEN SIE MIT UNSEREM OT-TEAM

Acronis

Erfahren Sie mehr auf acronis.com