Acronis Cyber Protect für die Öl-, Gas- und Energiebranche

Eine speziell entwickelte Cyber-Resilienz-Lösung für kritische Sektoren

Kurzfassung

Die Öl-, Gas- und Energiebranche ist auf PC-basierte OT-Systeme (Operational Technology) angewiesen, um Energie sicher zu erzeugen, zu übertragen, zu speichern und zu verteilen. In diesen Umgebungen gibt es besondere Herausforderungen: Dazu gehören Legacy-Systeme mit langer Lebensdauer, Standorte mit eingeschränkter Konnektivität und eine geringe Toleranz gegenüber Ausfallzeiten. Gleichzeitig werden OT-Systeme auch zunehmend zum Ziel von Ransomware.

Acronis Cyber Protect für OT wurde entwickelt, um sichere Backups und schnelle Wiederherstellungen zu gewährleisten und somit die Resilienz im Betrieb von OT-Systemen sicherzustellen, ohne dass die Produktion unterbrochen werden muss. Die Lösung unterstützt Unternehmen dabei, validierte Systemzustände wiederherzustellen, die Wiederherstellungszeit zu verkürzen und die Recovery- und Audit-Anforderungen industrieller Cybersicherheitsstandards zu erfüllen.

Automatisierungsanbieter vertrauen auf Acronis

YOKOGAWA · Honeywell · GE VERNOVA · ABB · EMERSON

Warum Acronis für die Öl-, Gas- und Energiebranche?

- Minimale Auswirkung auf Systemleistung
- Offline- / Air-Gap-Anlagen
- Schnelle Wiederherstellung auf fabrikneuer Hardware
- Backup-Validierung / Malware-Scans
- One-Click Recovery
- Unterstützung für alte Betriebssysteme
- Universal Restore
- Unveränderlicher Speicher + Replikation + Verschlüsselung

Acronis Cyber Protect für OT wurde speziell für die in OT-Umgebungen wichtigen Aspekte entwickelt. Dazu gehören Verfügbarkeit, Benutzerfreundlichkeit, Wiederherstellbarkeit, Prävention, die Unterstützung von Legacy-Systemen und gemischten Umgebungen sowie die Möglichkeit einer Wiederherstellung durch das vorhandene Betriebspersonal für abgelegene und vom Netzwerk getrennte Anlagen.

Geschäftswert

Vorteile für den Betrieb:

- Minimale MTTR (Mean Time to Recovery) für kritische OT-Systeme
- Aufrechterhaltung der Produktionskontinuität
- Geringeres Risiko durch Wiederherstellung validierter Systemzustände

Risiko und Markenschutz:

- Geringe Wahrscheinlichkeit für die Wiederherstellung von unsicheren oder kompromittierten Systemzuständen
- Nachweis von Cyber-Resilienz und Recovery-Readiness gegenüber internen Governance-Organen, Partnern und Aufsichtsbehörden

Auswirkungen auf die Gesamtbetriebskosten:

- Geringere Betriebsausgaben (OPEX) durch Minimierung von Ausfallzeiten und Vereinfachung der Wiederherstellung kritischer OT-Systeme
- Optimierung der Kapitalkosten (CAPEX) durch Verlängerung des Lebenszyklus von Legacy-Systemen und Sicherstellung ihrer Wiederherstellbarkeit auf Ersatzhardware

Mehrwert für OEMs und Partner:

- Integration von Resilienz in ausgelieferte Systeme
- Geringerer Support-Aufwand nach der Auslieferung
- Wiederkehrende Umsätze durch Resilienz-Services und Lifecycle-Support

Abgedeckte Branchen

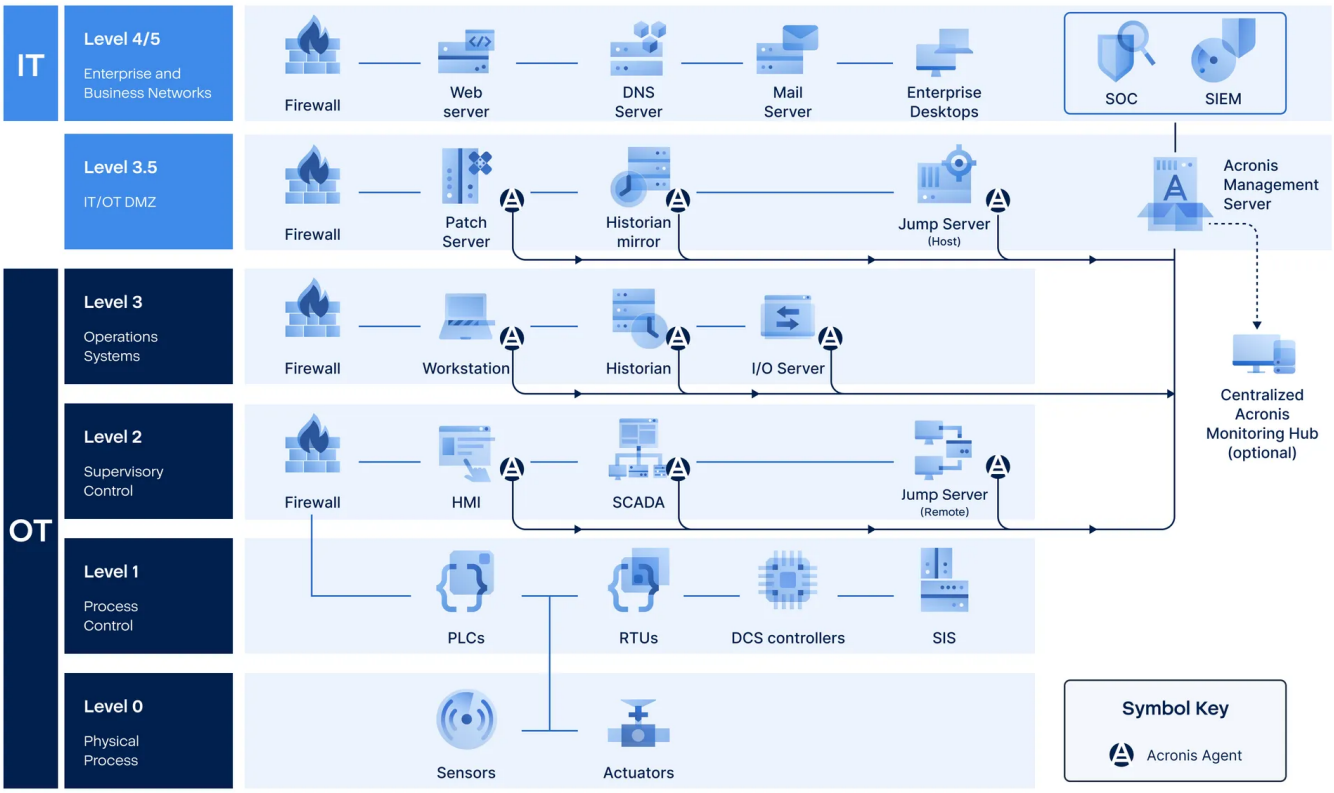
Energie- und Stromerzeugung:		
Stromerzeugung (thermische Energie, Kernenergie, Wasserkraft, Windkraft, Solarenergie, Biomasse und Energie aus Abfall)	Übertragung und Verteilung (Übertragungsnetze einschließlich Hochspannungs-Gleichstrom-Übertragungssysteme (HGÜ), Umspannwerke und Verteilungsnetze)	Netzrand und dezentrale Energie (Dezentrale Energie-Ressourcen [DER], Mikronetze, Batteriespeichersysteme [BESS]).
Öl und Gas:		
Upstream-Prozesse (Exploration, Bohrungen, Offshore-/Onshore-Förderung, Erdgasförderung und Feldverarbeitung)	Midstream-Prozesse (Gasverdichtung und -transport, Pipelinetransport, Speicherterminals, Verflüssigung und Transport von Erdgas [LNG])	Downstream-Prozesse (Raffinerie, petrochemische und chemische Produktion, GtL-Verfahren (Gas-to-Liquids), LNG-Regasifizierung)

Herausforderungen beim Betrieb von OT-Umgebungen in der Öl-, Gas- und Energiebranche

Herausforderung	Warum das wichtig ist
Sehr hohe Ausfallkosten	Ausfälle können Sicherheitsrisiken, Produktionsverluste, Service-Störungen und regulatorische Risiken verursachen. Eine schnelle Wiederherstellung ist entscheidend.
Cyber Security	Ransomware und gezielte Cyberangriffe stellen eine immer größere Gefahr für kritische OT-Systeme dar. Dazu zählen u. a. SCADA-, HMI- und Historian-Systeme sowie Engineering-Workstations.
Standorte mit eingeschränktem Netzwerkzugang und Air-Gap-Anlagen	An abgelegenen und verteilten Standorten kann die Konnektivität eingeschränkt sein. Ein kontinuierlicher Betrieb, segmentierte Netzwerke und Altsysteme erschweren die Installation von Patches. Daher müssen Backups und Wiederherstellungen lokal durchgeführt werden können.
Veraltete Betriebssysteme und Hardware	Viele OT-Systeme laufen auf veralteten Windows- oder Linux-Versionen bzw. auf an bestimmte Anbieter gebundenen Images. Upgrades sind bei diesen Systemen riskant oder sogar verboten.
Anfällige und deterministische Systeme	Betriebskritisch: OT-Umgebungen erfordern eine strenge Kontrolle über Neustarts, Software-Updates, die Agenten-Bereitstellung sowie Änderungen der Konfiguration. Der Schutz darf die Systemleistung nur minimal belasten, muss vorhersehbar sein und darf den Betrieb nicht beeinträchtigen.
Begrenzter IT-Support vor Ort	In der Regel ist an verteilten Standorten nur Betriebs- oder OT-Personal in der Anlage verfügbar. Die Wiederherstellung muss daher auch ohne speziellen IT-Support vor Ort einfach und schnell möglich sein.
Hohe Compliance- und Sicherheitsstandards	OT-Unternehmen sehen sich mit steigenden Anforderungen in Bezug auf Recovery-Readiness, Nachprüfbarkeit und Lieferkettensicherheit konfrontiert. Diese müssen mit den industriellen Cybersicherheitsstandards in Einklang stehen.
Anbieterabhängigkeit	Proprietäre OEM-Software, lizenzierte Images und hardwarespezifische Konfigurationen können die Handlungsoptionen einschränken, die Kosten erhöhen und Migrationen, Wiederherstellungen sowie Neuinstallationen erschweren.

Welche Systeme und Daten schützt Acronis Cyber Protect?

OT-Bereich	Geschützte Systeme	Geschützte Daten
Kern-OT und ICS	SCADA-Server/-Clients, HMI-Workstations, Operator-Stations für Prozessleitsysteme (PLS), Engineering-Workstations, Historian-Systeme und OT-Anwendungsserver	Betriebssystem-Images, Anwendungsarchitektur, SCADA-/HMI-Konfigurationen, Historian-Datenbanken, Alarmlogik und Betriebsparameter
Energieinfrastruktur	Steuerungs-PCs für Umspannwerke, HGÜ-/FACTS-Server, DER-/Mikronetz-Steuerungen, BESS-Standortsteuerungen und Server für das Lademanagement von Elektrofahrzeugen	Standortsteuerungssoftware, Konfigurationsdateien, Betriebsdaten, Gerätetreiber und Wiederherstellungsimages
Öl- und Gasindustrie	Pipeline-Überwachungsserver, Leckerkennungssysteme, PLS-/SCADA-Systeme für Raffinerien sowie Steuerungs-PCs für Turbomaschinen und Custody-Transfer-Systeme	Prozesskonfigurationen, Überwachungsdaten, Kalibrierungs- und Tuningdateien sowie Betriebsprotokolle
Engineering und Digitalisierung	Engineering-PCs, CAD-/CAM-Workstations, Simulationssysteme, Asset-Management-Server und Digital Twin-Plattformen	Engineering-Projektdateien, Zeichnungen, Modelle, Dokumentationen, Konfigurations-Repositorys sowie IP-sensible Projektdaten
OT DMZ (Demilitarized Zone) und unterstützende Systeme	Jump-Hosts, Datenerfassungsserver, Authentifizierungs-/Sicherheitsserver und zwischengeschaltete OT-/IT-Systeme	Gateway-Konfigurationen, Protokolle, System-Images und Richtlinien-/Konfigurationsdaten



*List of protected systems not exhaustive

SIEM- und SOC-Transparenz: Mithilfe der lokalen Acronis SIEM-Integration können Alarme und Ereignisse zu Backups, Sicherheit und RMM per Syslog oder Dateiexport an SIEM-Lösungen von Drittanbietern weitergeleitet werden. Dadurch können OT- und Sicherheitsteams Sicherheitsvorfälle in allen geschützten Umgebungen zentral überwachen und verwalten.

Wie schützt Acronis OT-Systeme?

OT-optimiertes Backup: Vollständige Image- und Datei-Backups mit geringem Bedarf an Systemressourcen, die für laufende OT-Systeme geeignet sind und meist keine geplanten Ausfallzeiten erfordern.

Speziell entwickelt für segmentierte und Air-Gap-Anlagen: Unterstützt den Offline-Betrieb und die lokale Speicherung (SAN, NAS, dedizierte Speicherzonen). Kann so bereitgestellt werden, dass es mit der Segmentierung des OT-Netzwerks und eingeschränkter Konnektivität kompatibel ist.

Sichere und verifizierte Wiederherstellung: Durch Backup-Validierung, Integritätsprüfungen und optionale Malware-Scans von Wiederherstellungspunkten wird das Risiko verringert, kompromittierte Systeme wiederherzustellen.

Wiederherstellung durch das Betriebspersonal: Dank geführter, vereinfachter Wiederherstellungsabläufe können OT-Teams Systeme vor Ort schnell wiederherstellen. Das ist besonders hilfreich an Standorten ohne IT-Personal oder ohne Remote-Zugriff.

Hardwareunabhängige Wiederherstellung: Um den Betrieb aufrechtzuerhalten, wenn die ursprünglichen Industriecomputer veraltet oder nicht mehr verfügbar sind, ist eine Wiederherstellung auf neuer oder abweichender Hardware (einschließlich P2P, P2V und V2P)* möglich.

Unterstützt sicherheitskritische OT-Systeme und Sicherheitssysteme:
In der Öl-, Gas- und Energiebranche hat Sicherheit oberste Priorität. Um einen sicheren Betrieb zu gewährleisten, sind Sicherheitssysteme wie Triconex, DeltaV SIS und Honeywell Safety Manager auf unterstützende, PC-basierte Engineering-Workstations, Konfigurations-Repositorys, Wartungssysteme, Dokumentationssysteme, Historian-Schnittstellen und Server angewiesen.

Acronis Cyber Protect für OT konzentriert sich auf den Schutz und die Wiederherstellung dieser PC-basierten Systeme. Im Falle von Hardware-Fehlern, Beschädigungen, Ransomware-Angriffen oder Betriebsstörungen können diese mithilfe von Acronis in einen validierten, funktionsfähigen Zustand zurückversetzt werden. Dadurch unterstützt Acronis die Cyber-Resilienz in sicherheitskritischen OT-Umgebungen und sorgt gleichzeitig für eine klare Abgrenzung zwischen Cyber-Resilienz und funktionaler Sicherheit.

Acronis schützt alle PC-basierten OT-Systeme – von der XP-Ära bis hin zu aktuellen Systemen

Acronis unterstützt auch alte Betriebssysteme, von denen sich andere Anbieter bereits verabschiedet haben:

Windows

- Windows Server 2003 SP1, R2 und höher, 2008/2008 R2, 2012/2012 R2, 2016, 2019, 2022 (außer Nano)
- Windows Small Business Server 2003/2003 R2, 2008, 2011
- Windows Home Server 2011
- Windows MultiPoint Server 2010, 2011, 2012
- Windows Storage Server 2003, 2008/2008 R2, 2012/2012 R2, 2016
- Windows XP Professional SP1, SP2, SP3
- Windows 7, 8/8.1, 10 (außer RT), 11 (alle Editionen)

Linux

- Kernel 2.6.9 bis 5.19
- RHEL 4.x, 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Ubuntu 9.10 bis 23.04
- Fedora 11 bis 31
- SUSE Linux Enterprise Server 10, 11, 12, 15
- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4–7.7, 8.0–8.8, 8.11, 9.0–9.8, 10.x, 11.x
- CentOS 5.x, 6.x, 7.x, 8.x*
- Stream 8*, 9*
- Oracle Linux 5.x, 6.x, 7.x, 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- CloudLinux 5.x, 6.x, 7.x, 8.x*
- ClearOS 5.x, 6.x, 7.x
- AlmaLinux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- Rocky Linux 8.x*, 9.0*, 9.1*, 9.2*, 9.3*
- ALT Linux 7.0

* Das System kann von einer physischen in eine physische Umgebung (P2P), von einer physischen in eine virtuelle Umgebung (P2V) oder von einer virtuellen in eine physische Umgebung (V2P) wiederhergestellt werden. Dadurch ist die Wiederherstellung auch dann gewährleistet, wenn der ursprüngliche Industriecomputer oder dessen genaue Hardware nicht mehr verfügbar ist.

Wichtige Anwendungsfälle

Ausfall eines OT-Systems	Ransomware- oder Malware-Angriff	Patch oder Hersteller-Update fehlgeschlagen	Ausfall von Engineering-Stationen	Ausfall einer Remote- oder Offshore-Anlage
Aufgrund eines Laufwerk- oder Mainboard-Fehlers ist ein Steuercomputer ausgefallen. Um den Betrieb rasch wieder aufzunehmen, können Sie das gesamte System schnell wiederherstellen, ohne es neu aufbauen zu müssen.	Um einen malwarefreien Systemzustand wiederherzustellen und das Risiko einer Reinfektion zu verringern, werden die betroffenen Systeme isoliert und aus validierten, sauberen Backups wiederhergestellt.	Führt eine Änderung zu Instabilität oder unsicherem Verhalten, kann das System in seinen letzten bekannten, fehlerfreien Betriebszustand zurückversetzt werden.	Stellen Sie Engineering-PCs und Projekt-Repositorys wieder her, um Neukonfigurationen, die mehrere Wochen dauern können, zu vermeiden und eine sichere Änderungskontrolle zu gewährleisten.	Ermöglichen Sie eine Wiederherstellung vor Ort, die nicht vom Internet oder VPNs abhängig ist. Dies ist insbesondere für Unterstationen, Verdichteranlagen, Bohrinseln und andere abgelegene Produktionsstandorte von Vorteil.

Wiederherstellungsworkflows nach Ausfallursache

Acronis Cyber Protect für OT bietet zahlreiche Wiederherstellungsoptionen. Dadurch können Teams je nach Ursache des Ausfalls, standortbezogenen Einschränkungen und betrieblichen Prioritäten den sichersten und schnellsten Wiederherstellungsworkflow auswählen.

Ausfallursache	Empfohlener Wiederherstellungsworkflow	Acronis Funktionen	Typisches Personal
Versehentliches Löschen oder Beschädigung einer begrenzten Anzahl von Dateien	Granulare Wiederherstellung (Wiederherstellung von Dateien bzw. Ordnern)	Gezielte Wiederherstellung einzelner Dateien (z. B. Projektartefakte, Konfigurationsdateien, Berichte), ohne dass das gesamte System rekonstruiert werden muss. Minimiert die Auswirkungen auf den Betrieb und vermeidet unnötige Änderungen an der OT-Workstation oder dem OT-Server.	Steuerungs-/ Automatisierungsingenieur:in oder OT-/ICS-Ingenieur:in
Teilweiser Ausfall oder Fehlkonfiguration einer Applikation (das System bootet aber noch)	Rückversetzung auf den letzten bekannten, funktionsfähigen Zustand (Wiederherstellungspunkt)	Wenn ein Patch fehlgeschlagen ist, ein Update des Herstellers Probleme verursacht hat oder ein Konfigurationsfehler aufgetreten ist, können Sie das System auf einen validierten Wiederherstellungspunkt zurücksetzen. Dadurch werden OT-Applikationen wieder in einen vorhersehbaren Betriebszustand versetzt.	Steuerungs-/ Automatisierungsingenieur:in oder OT-/ICS-Ingenieur:in
System kann nicht booten (Laufwerksausfall, beschädigtes Betriebssystem, Ransomware-Angriff)	Wiederherstellung auf fabrikneue Hardware (bootfähiges Notfallmedium: Linux oder WinRE)	Starten Sie das System mit dem Acronis Notfallmedium und stellen Sie das vollständige Image (Betriebssystem, Programme, Treiber und Daten) wieder her. Dadurch wird das System in einen bekannten, fehlerfreien Betriebszustand zurückversetzt, ohne dass eine manuelle Neuinstallation erforderlich ist.	OT-/ICS-Ingenieur:in oder geschulte:r Standorttechniker:in
Hardware-Fehler (kein identisches Ersatzgerät verfügbar)	Wiederherstellung auf abweichender Hardware (Universal Restore)	Stellen Sie das System-Image auf Ersatzhardware wieder her und integrieren Sie die erforderlichen bootkritischen Treiber (z. B. für Speichercontroller/ Chipsätze), um ältere, herstellerspezifische OT-Stacks wieder in Betrieb zu nehmen. Dies ist erforderlich, wenn die ursprünglichen Industriecomputer veraltet oder nicht mehr verfügbar sind.	OT-/ICS-Ingenieur:in oder Standorttechniker:in (ggf. mit IT-Kenntnissen)
Ausfall einer entfernten Anlage (eingeschränkter oder kein IT-Zugriff)	Wiederherstellung durch das Betriebspersonal (One-Click Recovery)	Mithilfe geführter, vereinfachter Wiederherstellungsabläufe kann das Anlagenpersonal OT-Systeme lokal und sicher wiederherstellen, ohne dass IT-Kenntnisse erforderlich sind. Dadurch werden Ausfallzeiten deutlich verkürzt, da lange Reisezeiten entfallen und kein Fernzugriff nötig ist.	Betriebspersonal, Schichtleiter:in oder Standorttechniker:in
Ransomware- oder Malware-Angriff (Reinfektionsrisiko während der Wiederherstellung)	Sichere Wiederherstellung (Wiederherstellungspunkte werden auf Malware überprüft/ Backup-Validierung)	Um das Risiko einer Wiederherstellung kompromittierter Images zu verringern, werden Backups validiert und Wiederherstellungspunkte vor der Wiederherstellung auf Malware überprüft. Dadurch wird eine sichere Wiederherstellung des OT-Systems in einen funktionsfähigen und malwarefreien Zustand gewährleistet.	OT-/ICS-Ingenieur:in und OT-Sicherheitsverantwortliche:r

Ausfallursache	Empfohlener Wiederherstellungsworkflow	Acronis Funktionen	Typisches Personal
Virtualisierte OT-Workloads müssen am schnellsten wiederhergestellt werden (sofern eine Virtualisierung zulässig ist)	Schnelle Wiederherstellung mithilfe von Standby-VMs	Sofern Virtualisierungen zulässig sind, können Sie OT-Workloads als VMs wiederherstellen. Dadurch verkürzt sich die Zeit bis zur Wiederaufnahme des Betriebs und es sind vollständige Validierungsschritte möglich, ohne dass die Produktion beeinträchtigt wird.	OT-Plattform-/ Virtualisierungsingenieur:in (OT und IT gemeinsam)
Nachweis der Wiederherstellbarkeit für Audits, Wartungen und Resilienzanforderungen	Verifizierte Wiederherstellbarkeit (Backup-Validierungen und Boot-Prüfungen)	Um die Wiederherstellbarkeit von Backups zu validieren, können Sie Integritätsprüfungen durchführen und die Bootfähigkeit überprüfen. So stellen Sie sicher, dass kritische OT-Systeme innerhalb der vorgeschriebenen Recovery-Ziele wiederhergestellt werden können.	OT-/ICS-Ingenieur:in in Zusammenarbeit mit den Verantwortlichen für OT-Sicherheit/-Compliance

Die Wiederherstellungsworkflows für unterschiedliche Ausfallursachen ermöglichen es OT-Teams, Ausfallzeiten zu minimieren, unnötige Systemänderungen zu vermeiden und den Betrieb wieder in einen validierten Zustand zurückzusetzen, der den Standortrichtlinien sowie den Richtlinien zur Änderungskontrolle entspricht.

Einhaltung von Compliance- und Sicherheitsstandards

Acronis Cyber Protect für OT erfüllt die üblicherweise in Cybersicherheitsprogrammen für die Energiewirtschaft und die Industrie zum Tragen kommenden Anforderungen an die Recovery-Readiness, die Nachweispflichten und die Lieferkettensicherheit. Dazu gehört die Erfüllung der Recovery-Readiness-Anforderungen gemäß der Norm IEC 62443, regionaler Vorschriften wie NIS 2 sowie der Resilienz-Anforderungen gemäß den Vorschriften für kritische Infrastrukturen. Des Weiteren umfasst es die Entwicklung branchenspezifischer Recovery-Pläne und deren Test sowie die Erfüllung der Anforderungen an die Lieferkettensicherheit und die sichere Produktentwicklung. Letztere gewinnen im Rahmen der europäischen Cyberresilienz-Verordnung für OEMs zunehmend an Bedeutung.

GDPR NIS2 NIST IEC NERC CIP CRA

Wie Acronis Cyber Protect die Compliance sicherstellt

- Verifizierter Wiederherstellung-snachweis
- Verschlüsselte Backups mit Aufbewahrungsrichtlinien
- Kontrollierte Wiederherstellungsverfahren
- SSDLC-Verfahren zur Unterstützung von Lieferantenbewertungen

IEC 62443-4-1 CERTIFIED

Acronis ist nach IEC 62443-4-1 zertifiziert

Die Zertifizierung nach IEC 62443-4-1 bestätigt, dass Acronis bei der Softwareentwicklung den Secure Software Development Life Cycle (SSDLC) anwendet und somit die industriellen Anforderungen erfüllt. Dadurch können Unternehmen der Öl-, Gas- und Energiebranche ihre lieferkettenbezogenen Sorgfaltspflichten erfüllen, Lieferkettenrisiken verringern und sich der Zuverlässigkeit der OT-Resilienzlösungen von Acronis sicher sein.

Zusammenfassung

Acronis Cyber Protect ermöglicht die sichere, planbare und schnelle Wiederherstellung kritischer OT-Systeme ohne Betriebsunterbrechung und erfüllt gleichzeitig die steigenden Anforderungen an industrielle Cybersicherheit und Recovery-Readiness.

Acronis

Erfahren Sie mehr auf acronis.com