Garantire il funzionamento dei servizi pubblica utilità

Proteggere le infrastrutture dedicate a energia elettrica, acqua, gas naturale ed energie rinnovabili

La posta in gioco

I servizi di pubblica utilità non si limitano a tenere accese le luci. Mantengono gli ospedali in funzione con l'alimentazione di emergenza, garantiscono che l'acqua sia sicura da bere, fanno arrivare il gas alle abitazioni in inverno e consentono ai servizi di emergenza di intervenire. Quando un servizio pubblica utilità fallisce, non fallisce da solo. Coinvolge altri settori.

Gruppi collegati agli Stati hanno dimostrato che l'obiettivo è l'interruzione operativa, non il furto di dati. Volt Typhoon ha trascorso 300 giorni senza essere rilevata all'interno di un servizio di energia elettrica e acqua degli Stati Uniti, eseguendo il mapping delle procedure operative OT e della topologia della rete.[1] L'FBI e la CISA hanno confermato che il modello non è isolato: i servizi di pubblica utilità sono diventati un obiettivo primario ugualmente per aggressori collegati agli Stati, per gruppi ransomware e per attacchi distruttivi.

È più probabile che queste interruzioni operative si verifichino in una sottostazione isolata, in una stazione di pompaggio dell'acqua o in un impianto di generazione rurale, dove non è presente alcun tecnico informatico e lo specialista più vicino potrebbe trovarsi a ore di distanza. La finestra temporale per ripristinare l'alimentazione elettrica, la pressione dell'acqua o il flusso del gas a una comunità si misura in minuti, non in giorni lavorativi.

La lezione dell'azienda idrica americana

Nel 2024, il più grande servizio pubblico idrico degli Stati Uniti ha subito un attacco informatico che non ha colpito i sistemi operativi, ma ha costretto alla sospensione della fatturazione e alla chiusura del portale. In quest'ambito rientrano anche i sistemi IT da cui dipende l'OT, inclusi Active Directory, historian, GIS, OMS e fatturazione.[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

Il panorama delle minacce

Un'organizzazione ICS/OT su cinque ha subito un incidente informatico confermato nell'ultimo anno. Nessun avviso. Gli incidenti confermati hanno colpito i sistemi operativi, con il 40% che ha causato un'interruzione operativa diretta e quasi uno su cinque la cui risoluzione ha richiesto più di un mese. Per le aziende che erogano servizi di pubblica utilità, quel divario di ripristino non è una statistica. Significa giorni senza fornitura affidabile di elettricità, acqua o gas alle comunità che ne dipendono.

Una su cinque

organizzazioni ICS/OT ha subito un incidente informatico nell'ultimo anno.

SANS State of ICS/OT Security 2025

Il 40%

di quegli incidenti ha causato un'interruzione operativa, che ha interessato produzione, erogazione di servizi o attività pubbliche. Il 37,9% ha avuto origine da ransomware.

SANS State of ICS/OT Security 2025

Il 19%

degli incidenti OT ha richiesto più di un mese per essere ripristinato nel 2025. Il rilevamento è migliorato. Il ripristino completo rimane il divario critico.

SANS State of ICS/OT Security 2025

Le piccole e medie aziende di servizi di pubblica utilità vengono descritte come "target rich but cyber poor" ovvero obiettivi di alto valore senza team dedicati di cyber security e con risorse limitate per recuperare.

La soluzione: un ripristino che funziona dove il tuo team non riesce ad arrivare

Acronis Cyber Protect for OT offre una resilienza digitale di livello IT agli ambienti OT delle aziende di servizi di pubblica utilità senza interrompere le attività in corso. È progettato su una realtà operativa fondamentale: quando si verifica un incidente in una sottostazione remota, in una stazione di pompaggio o in un sito energetico, la persona più vicina al sistema potrebbe essere un ingegnere dell'automazione o un supervisore di turno, non uno specialista di cyber security. I flussi di lavoro di ripristino sono progettati per funzionare direttamente in loco, con una dipendenza minima dalla connettività esterna o dall'intervento di personale specializzato.

Backup senza interruzioni operative

Backup completo dell'immagine e a livello di file senza riavvii e senza interruzione operativa. La modalità settore per settore si attiva automaticamente per i file system OT proprietari. Snapshot omogenei VSS su configurazioni SCADA e historian multi-volume.

Ripristino con un clic per gli operatori

Il personale locale autorizzato, tra cui gli ingegneri delle sottostazioni, i responsabili delle attività idriche e i capiturno, può seguire un flusso di lavoro guidato per il ripristino, in modo da riportare un sistema in avaria all'ultimo stato funzionante conosciuto, contribuendo a ridurre i tempi di ripristino da ore o giorni a minuti, a seconda delle condizioni del sito.

Bare-metal e Universal Restore

Recupera automaticamente su hardware diverso o sostitutivo. Universal Restore installa i driver corretti senza bisogno di una riconfigurazione manuale, il che è fondamentale quando il PC industriale originale è obsoleto o non disponibile.

Ripristino sicuro e verificato

Le immagini di backup vengono analizzate alla ricerca di malware e convalidate prima del ripristino completo, contribuendo a ridurre il rischio di reinfettare un sistema SCADA o HMI ripristinato. Le minacce rilevate vengono segnalate e possono essere rimosse come parte del flusso di lavoro di ripristino.

Funzionamento air-gap e offline

Tutti i componenti vengono distribuiti in locale. Il management server funziona completamente offline. Le definizioni anti-malware si aggiornano senza accesso a Internet e gli agenti continuano a offrire protezione per 30 giorni se il management server non è raggiungibile.

Storage di backup immutabile

Gli archivi di backup non possono essere eliminati, modificati o crittografati dal ransomware, anche se le credenziali vengono compromesse. Modalità Governance e Compliance con periodi di conservazione fino a 10 anni per gli obblighi normativi.

Sistemi legacy: proteggere ciò che altri hanno abbandonato

Le risorse OT dei servizi di pubblica utilità operano per 30 anni o più. I sistemi informatici che le gestiscono, tra cui HMI, server SCADA e workstation di progettazione, spesso utilizzano sistemi operativi che i principali fornitori hanno smesso di supportare già da anni.

Windows 10 in OT: gestione del rischio del ciclo di vita[3]

Molte workstation OT dei servizi di pubblica utilità eseguono ancora edizioni di Windows 10 con tempistiche di supporto diverse. Alcune non sono più supportate, mentre altre raggiungeranno il traguardo del loro ciclo di vita nel 2027, nel 2029 o più avanti. Aggiornare o applicare le patch a questi sistemi spesso non è una semplice operazione di routine; può comportare costose procedure di riconvalida, compromettere il funzionamento del software SCADA/HMI con licenza o invalidare i contratti di supporto OEM. Acronis funge da controllo compensativo, abbinando backup basato su immagine con la whitelist delle applicazioni per contribuire a gestire i sistemi legacy in modo più sicuro quando la migrazione immediata del sistema operativo non è fattibile.

Acronis offre un supporto ampio e completo per backup e ripristino da Windows XP SP1 / SP2 / SP3 fino a Windows Server 2025, kernel Linux 2.6.9 a 5.19 e tutti i principali hypervisor, coprendo ogni generazione di OT.

Ripristino operativo e ripristino completo: non sono la stessa cosa.

Negli ambienti dei servizi di pubblica utilità, confondere questi due termini costa la continuità del servizio e, nei casi peggiori, la sicurezza pubblica.

Ripristino operativo significa ripristinare rapidamente il controllo della frequenza o riprendere la pressione dell'acqua da qualunque stato convalidato sia disponibile. Le operazioni parziali che mantengono alimentato un ospedale non sono uno stato di guasto. Sono la prima missione.

Ripristino completo significa riportare in sicurezza l'intero stack del sistema certificato a una baseline notoriamente funzionante, senza reintrodurre malware o corruzione.

Acronis supporta entrambi. One-Click Recovery contribuisce a garantire una rapida continuità operativa, consentendo al personale autorizzato di avviare il ripristino completo in sede senza intervento di specialisti. Il backup convalidato e di livello forense supporta un ripristino completo e verificato, inclusa la scansione delle immagini di backup alla ricerca di malware prima dell'uso e la fornitura di prove con catena di custodia certificate su blockchain per l'indagine post-incidente e l'audit.

Secondo il report SANS State of ICS/OT Security 2025, mentre quasi la metà degli incidenti OT viene rilevata entro 24 ore, il 19% richiede più di un mese per essere ripristinato completamente. Il rilevamento è migliorato. Il ripristino completo rimane il divario critico.

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

Ciò che Acronis protegge su tutta la rete di servizi di pubblica utilità

Ambiente dei servizi di pubblica utilità	Sistemi e dati protetti da Acronis
Energia elettrica: generazione, trasmissione e distribuzione, periferia della rete	Server SCADA / EMS, PC di controllo di sottostazione, workstation HMI, controller DER / microgrid, controller di sito BESS, server historian. I dati protetti includono immagini del sistema operativo, configurazioni SCADA / HMI, logica degli allarmi, database historian e file di progetto di ingegneria.
Sistemi idrici e di acque reflue	SCADA per il trattamento dell'acqua, workstation HMI, PC di controllo di pompe e stazioni di sollevamento, sistemi di monitoraggio dei serbatoi. I dati protetti includono immagini del sistema operativo, configurazioni del processo di trattamento, logica di controllo delle pompe e dati di reporting normativo.
Distribuzione di gas naturale	Server di monitoraggio delle condotte, PC delle stazioni di compressione, PC delle stazioni di regolazione, server SCADA, sistemi di trasferimento di custodia. I dati protetti includono configurazioni di processo, dati di monitoraggio, file di calibrazione e record operativi della pipeline.
Energia rinnovabile: eolica, solare, idroelettrica, biomassa e idrogeno verde	PC controller di turbine / inverter, server di gestione dell'impianto, sistemi di gestione BESS, monitoraggio ambientale. I dati protetti includono software di controllo, configurazioni del sito e dataset operativi.
Sistemi IT da cui dipende l'OT	Active Directory / DNS, jump host, historian (lato IT), GIS, OMS, AMI / MDMS, portali di fatturazione e dei clienti. I dati protetti includono immagini di sistema, dati di configurazione, record dei clienti e operativi.

Integrazione SIEM: l'integrazione SIEM in locale di Acronis inoltra avvisi di backup, sicurezza e RMM ai SIEM di terze parti tramite syslog, per aiutare i team OT e di sicurezza a centralizzare la consapevolezza degli incidenti in tutti gli ambienti protetti.

Conformità e assicurazione

Acronis aiuta le aziende di fornitura di servizi di pubblica utilità a generare prove del piano di ripristino operativo e record di convalida del backup, risultati dei test di ripristino completo e controlli di conservazione, e a garantire la documentazione di garanzia dei fornitori necessaria per essere pronti agli audit secondo i principali standard di riferimento. Acronis è certificata secondo la norma IEC 62443-4-1.

NERC CIP (Nord America)

Può contribuire a fornire prove per la documentazione del piano di ripristino operativo CIP-009 tramite record di convalida del backup e dati di backup forense. Progettato per operare in reti completamente isolate senza dipendenze dal cloud.

Direttiva NIS 2 (Europa)

Può contribuire alle aspettative dell'Articolo 21 in materia di continuità operativa e gestione del backup. I backup immutabili e i periodi di conservazione configurabili si allineano all'intento della NIS 2 in materia di protezione dei dati e preparazione al ripristino operativo.

IEC 62443 (globale)

Certificata secondo la norma IEC 62443-4-1 SSDLC. Backup non invasivi in tempo reale e verifica dell'integrità si allineano con i requisiti di disponibilità delle risorse e di continuità nel framework IEC 62443.

Cyber Resilience Act dell'UE

La certificazione del ciclo di vita dello sviluppo sicuro può supportare le valutazioni di garanzia dei fornitori OEM, sempre più richieste negli appalti del settore dei servizi di pubblica utilità nell'ambito del CRA dell'UE.

Nota: Acronis supporta la documentazione relativa ai piani di ripristino operativo e la preparazione agli audit. La conformità a qualsiasi framework normativo rimane responsabilità dell'operatore.

Partner OEM e integratori

Acronis Cyber Protect per OT è disponibile come soluzione white label, in co-branding o venduta come riferimento, che consente ai Partner OEM e agli integratori di sistemi di controllo di integrare direttamente la resilienza digitale OT nei portafogli dei propri sistemi per i servizi di pubblica utilità.

Acronis collabora con produttori OEM e Partner tecnologici del settore industriale in ambienti OT in tutto il mondo, tra cui ABB, Emerson, GE Vernova, Honeywell, Rockwell Automation, Schneider Electric e Yokogawa.

Per i Partner OEM

- Integra One-Click Recovery in modo nativo. Diventa un Partner per la resilienza, non solo un fornitore di hardware.
- Aiuta a ridurre il volume delle chiamate di supporto reattivo e i costi di trasferta degli ingegneri per i comuni scenari di ripristino operativo.
- Consente servizi gestiti ricorrenti di resilienza e un aumento dei ricavi contrattuali.
- Certificato IEC 62443-4-1, che sta diventando sempre più determinante negli acquisti delle aziende fornitrici di servizi di pubblica utilità e nella conformità al CRA dell'EU.

Per gli integratori di sistemi di controllo

- Include il ripristino operativo come parte della fornitura di server SCADA / HMI / OT.
- Standardizza le procedure di ripristino su tutti i sistemi di servizi di pubblica utilità forniti.
- Riduce il carico di supporto post-deployment e la responsabilità SLA.
- Aggiunge servizi ricorrenti di resilienza ai portfolio di progetto e di servizi gestiti.
- Vende come riferimento o in co-branding insieme all'attività di integrazione.

Sei pronto a proteggere l'infrastruttura da cui dipendono le comunità?

Parla con uno specialista OT di Acronis o con il tuo Partner OEM per organizzare una demo dal vivo.

PARLA CON UN ESPERTO DI OT

Acronis

Per saperne di più, visita acronis.com