TAG

PERCHÉ ACRONIS È LEADER NELLA RESILIENZA INFORMATICA DELLE TECNOLOGIE OPERATIVE (OT)

DR. EDWARD AMOROSO,
CEO, TAG INFOSPHERE

Acronis

PERCHÉ ACRONIS È LEADER NELLA RESILIENZA DIGITALE DELLE TECNOLOGIE OPERATIVE (OT)

EDWARD AMOROSO, CEO, TAG

INTRODUZIONE

Per decenni, Cyber Security è stato sinonimo soprattutto di protezione delle tecnologie informatiche (IT) dagli attacchi potenzialmente dannosi. Per questo motivo, è stato istituito il ruolo di Chief Information Security Officer (CISO). Più di recente, tuttavia, la Cyber Security si è estesa fino a includere sistemi operativi industriali, fisici e tangibili, dando vita al nuovo settore che si occupa della sicurezza delle tecnologie operative (OT).

Emersa successivamente alla sicurezza IT, la sicurezza OT ne condivide molte tipologie di controlli. Il miglioramento della visibilità e la distribuzione di misure di mitigazione, ad esempio, sono centrali per le strategie di sicurezza dell'IT e dell'OT, e ciò è utile perché la sicurezza OT, a livello delle organizzazioni, continua a fondersi con le iniziative IT più ampie. A dimostrazione di ciò, oggi molti CISO sono anche pienamente responsabili della sicurezza OT.

Come prevedibile, tuttavia, molti dei punti deboli presenti nei tradizionali piani per la sicurezza IT si ritrovano nella sicurezza industriale. Il più evidente è probabilmente la fragile resilienza che molti sistemi OT manifestano durante un attacco. Il ransomware, ad esempio, è riuscito ad arrestare completamente grandi ambienti operativi, con gravi conseguenze per i clienti.

I contesti della sicurezza OT presentano tuttavia problemi specifici, che nella maggior parte degli ambienti OT sono generalmente legati alla mancanza di personale interno specializzato in sicurezza, alla presenza di un mix di sistemi proprietari obsoleti nelle reti e alle difficoltà specifiche degli ambienti operativi, che non consentono l'applicazione delle patch o degli aggiornamenti senza incidere sulle attività in esecuzione (ad esempio, in una fabbrica o in un impianto di produzione).

Questo report intende illustrare come i team di sicurezza OT, oggi spesso guidati dai CISO, possano migliorare la propria resilienza operativa focalizzandosi sulle funzionalità chiave di backup e ripristino. Si tratta di un aspetto della Cyber Protection che ha sempre rappresentato una sfida per i team di sicurezza IT, perché le soluzioni efficaci richiedono una conoscenza approfondita dell'infrastruttura e la maggior parte dei fornitori che operano in questo ambito si sono tradizionalmente occupati delle operazioni IT anziché della sicurezza.

Riteniamo che backup e ripristino siano gli elementi chiave di qualsiasi iniziativa che punti a migliorare la sicurezza degli ambienti OT. Ovviamente, è necessario definire obiettivi complementari per formare meglio il personale OT in materia di sicurezza e ridurre il numero di sistemi legacy in uso. La nostra tesi, tuttavia, è che il miglior rapporto qualità-prezzo si ottiene quando gli ingegneri della sicurezza OT si focalizzano su questo elemento chiave nell'ambiente di produzione.

Negli esempi del presente documento, utilizzeremo le moderne soluzioni di resilienza digitale del fornitore commerciale Acronis. L'approccio dell'azienda al backup e al ripristino in qualsiasi tipo di infrastruttura, sia IT che OT, sembra essere adeguato alle minacce informatiche in evoluzione che puntano a colpire l'operatività di settori industriali come quello manifatturiero, i trasporti, la produzione di energia ed elettricità, il settore militare, che non possono accettare interruzioni di alcun tipo.[1]

SICUREZZA ATTUALE DEI SISTEMI OT

Come accennato, le conseguenze di una resilienza inadeguata differiscono tra infrastrutture IT e OT, perché in molti casi i problemi della sicurezza operativa possono avere ripercussioni più gravi. Ad esempio, la mancata resilienza di un sistema di controllo industriale potrebbe causare il malfunzionamento di un sistema di sicurezza, l'interruzione di una linea di produzione o un problema operativo in una centrale nucleare. Non è difficile immaginare situazioni che comportano la potenziale perdita di vite umane.

È quindi indiscutibile che negli ambienti OT la sicurezza debba essere una priorità assoluta. È tuttavia proprio in questi ambienti che le complessità causate da tecnologie eterogenee e proprietarie, spesso con hardware e sistemi operativi obsoleti, si acuiscono. Ciò limita la possibilità di applicare patch e aggiornamenti, per non parlare delle finestre di backup restrittive tipiche di questi ambienti, spesso carenti di risorse IT adeguate o di esperti qualificati.

Il tentativo di isolare gli ambienti OT dagli hacker con un gateway tra gli ambienti IT e OT non si è dimostrato efficace. L'obiettivo iniziale di nascondere i sistemi OT da Internet creando un perimetro IT/OT non è stato raggiunto, per ragioni intrinseche al concetto stesso di perimetro: non vengono riconosciute le minacce interne, non vengono individuati i percorsi di accesso intorno al perimetro, viene ignorata la natura permeabile di qualsiasi perimetro, ecc.

Inoltre, l'approccio al gateway IT/OT non tiene conto delle problematiche di sicurezza OT sopra elencate e relative ai sistemi proprietari, alla complessità del patching, al personale non qualificato in materia di sicurezza, ecc. L'immagine seguente evidenzia come questi problemi di sicurezza non siano risolti dai gateway IT/OT, che non coprono nemmeno il nostro principale argomento, ovvero la resilienza della sicurezza degli ambienti OT che richiede funzionalità di backup e ripristino.

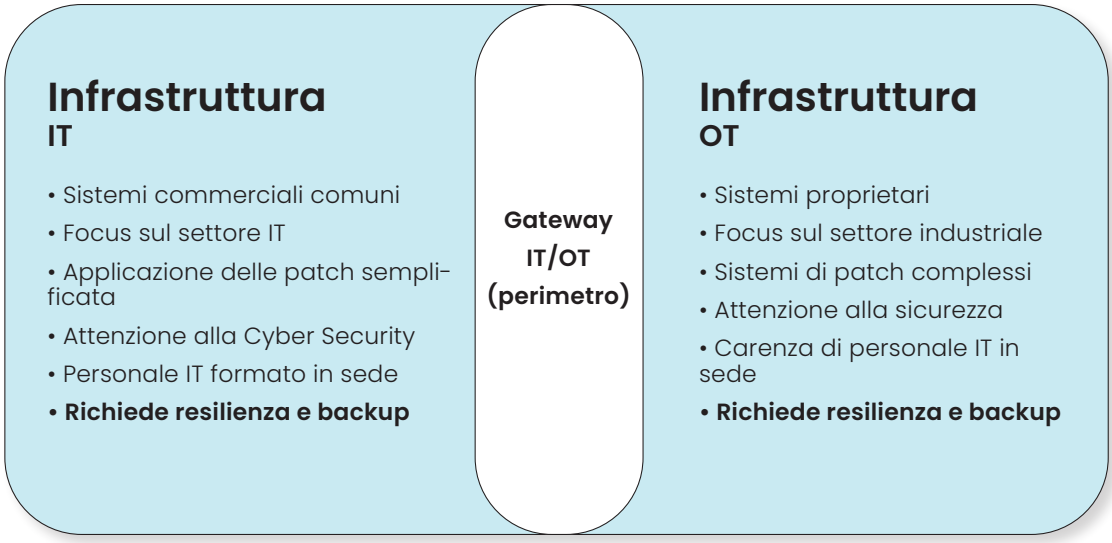

Figura 1. Sfide alla sicurezza dei sistemi OT

Come suggerito, riteniamo che per ottenere una sicurezza OT completa sia necessario individuare soluzioni per tutti i problemi indicati. Riteniamo inoltre, e lo spiegheremo più avanti, che l'obiettivo principale delle moderne soluzioni di sicurezza OT deve essere la continuità operativa in caso di ransomware, sabotaggi o attacchi informatici distruttivi. Illustreremo questo approccio nel contesto della piattaforma Acronis commerciale e del supporto che offre alla sicurezza OT.

SOLUZIONI ACRONIS PER IL BACKUP E IL RIPRISTINO PER AMBIENTI OT E ICS

La nostra esperienza suggerisce che i programmi di sicurezza OT devono coprire tre aree complementari. In primo luogo, è necessario garantire la visibilità dell'ambiente OT, in genere ottenuta tramite piattaforme commerciali come Claroty e Dragos. La visibilità è essenziale e occorre investire energie per migliorarne il funzionamento pratico, prevedendo, ad esempio, una formazione migliore e incrementando le simulazioni negli ambienti cyber range OT.

In secondo luogo, riteniamo che i responsabili debbano chiedere ai team di sicurezza IT di creare controlli più convergenti quando i sistemi OT si integrano con quelli IT. È necessario, ad esempio, adottare l'approccio Zero Trust per l'OT, presupponendo che sempre più sistemi operativi si connettono al cloud e ad altri sistemi IT tradizionali. Ciò consente di estendere i controlli IT, come le piattaforme di protezione delle applicazioni cloud-native (CNAPP), in modo che coprano anche l'infrastruttura OT.

Il terzo punto, forse il più importante, è raccomandare ai team di sicurezza OT di concentrarsi maggiormente sulla resilienza operativa. In pratica, significa garantire l'operatività continua avvalendosi di soluzioni di backup e ripristino automatizzate. Ovviamente ciò vale anche per i sistemi IT, ma come suggerito prima, l'interruzione del supporto OT può avere conseguenze molto più gravi, anche in termini di sicurezza delle persone; la soluzione Acronis può aiutare a evitare questi problemi.

La piattaforma Acronis offre una valida copertura dei requisiti di sicurezza e resilienza più adatti all'infrastruttura OT. È una buona notizia, perché i team aziendali non devono occuparsi di sviluppare una propria soluzione di backup e ripristino locale, anche in presenza di hardware e software obsoleti e proprietari. In particolare, le funzioni chiave della suite Acronis ed essenziali per la resilienza dell'OT, includono quanto segue:

1. **Ripristino rapido dei sistemi OT.** Acronis offre protezione ad alte prestazioni, consentendo il ripristino rapido dei computer OT per evitare costose interruzioni degli impianti produttivi. Questa funzionalità di ripristino rapido è fondamentale per ridurre al minimo i tempi di fermo e mantenere la continuità operativa.
2. **Ripristino universale dei sistemi.** Acronis Cyber Protect garantisce un ripristino rapido e affidabile di qualsiasi computer, compresi i sistemi legacy risalenti all'epoca di Windows XP, con opzioni per il ripristino bare-metal. Questa funzionalità è essenziale, perché garantisce la continuità anche in presenza di sistemi obsoleti, ancora comuni negli ambienti OT.
3. **Piani di backup personalizzabili.** Acronis consente di personalizzare i piani di backup in base alle esigenze specifiche degli ambienti OT e ICS, garantendo un'adeguata protezione dei dati e dei sistemi critici. L'esigenza di personalizzazione cresce con la modernizzazione delle infrastrutture OT, che utilizzano l'AI e metodi di distribuzione più sostenibili.
4. **Integrazione con strumenti di terze parti.** Acronis offre una visualizzazione unificata delle attività di backup e ripristino, con opzioni di controllo centralizzato e di integrazione con strumenti di terzi, semplificando la gestione e migliorando l'efficienza operativa. Negli ambienti OT l'integrazione della sicurezza rappresenta una sfida notevole, pertanto questa funzionalità è particolarmente importante.
5. **Opzioni di sovranità dei dati.** Per garantire la conformità ai requisiti di sovranità dei dati, le organizzazioni possono scegliere uno storage in sede o utilizzare i data center globali di Acronis, con opzioni come Amazon S3 e Microsoft Azure. Acronis collabora con i propri clienti per individuare la soluzione di hosting più adatta.
6. **Ripristino self-service per i lavoratori a distanza.** Acronis offre opzioni di ripristino self-service per chi lavora da remoto, consentendo anche al personale non tecnico di avviare i processi di ripristino, decentralizzando efficacemente il carico di lavoro dell'IT e accelerando il ritorno all'operatività dopo un incidente di sicurezza.

ARCHITETTURA DELLA PIATTAFORMA ACRONIS

La piattaforma Acronis Cyber Protect è basata su un data warehouse nel quale sono archiviate e protette le origini dei dati OT attuali, storici e di altro tipo dell'azienda. In uno stesso ambiente OT è possibile installare più istanze della console di Acronis Cyber Protect, effettuando il deployment di più agenti associati per l'acquisizione e il ripristino dei dati. I metadati vengono trasmessi dalle console al warehouse.

Per ogni deployment di Cyber Protect e per Acronis Centralized Monitoring Hub sono disponibili dashboard e console che tengono sotto controllo tutti gli aspetti dei processi di backup e ripristino. L'hub fornisce visualizzazioni cronologiche, con report e monitoraggio personalizzabili anche mentre le attività di backup e ripristino sono in corso. L'obiettivo è, ovviamente, quello di garantire il funzionamento continuo in caso di incidenti, attacchi e altri problemi di resilienza (vedere Figura 2).

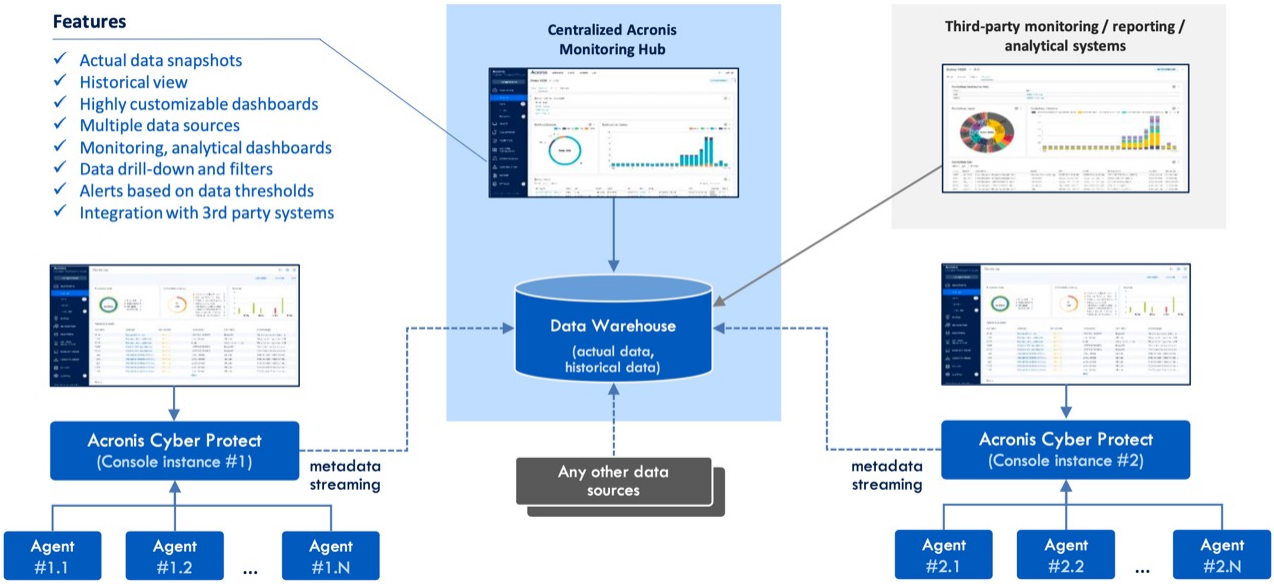

Figura 2. Architettura del sistema Acronis

INTEGRAZIONI ACRONIS

Acronis Cyber Protect (si notino i due esempi di console raffigurati nell'immagine) supporta l'integrazione unificando backup, disaster recovery, protezione anti-malware basata su AI, assistenza remota e strumenti di sicurezza in una singola piattaforma per il team di sicurezza, anche in ambito OT. Questo consolidamento consente a qualsiasi azienda, inclusi i team di sicurezza OT, di gestire vari aspetti della Cyber Protection tramite un'unica interfaccia, riducendo la complessità e migliorando l'efficienza.

L'architettura flessibile della piattaforma, le interfacce di programmazione delle applicazioni e della riga di comando supportano lo sviluppo e l'integrazione di applicazioni di Acronis e di terze parti (si notino i feed di terzi raffigurati in Figura 2 che si connettono al data warehouse centralizzato). Questo modello favorisce un ecosistema dinamico in cui è possibile integrare servizi aggiuntivi di protezione, gestione e automazione, garantendo che la piattaforma rimanga adattabile ai contesti di Cyber Security in continua evoluzione. La flessibilità permette alle organizzazioni di integrare le soluzioni Acronis nelle infrastrutture esistenti, migliorando la resilienza e la sicurezza complessiva, soprattutto negli ambienti OT.

BACKUP FORENSE ACRONIS

Acronis Cyber Protect include una funzionalità di backup forense progettata per semplificare le analisi future acquisendo prove digitali dai backup di disco, un aspetto strategico per le organizzazioni che devono gestire i requisiti di conformità e condurre le indagini interne in modo efficiente. È essenziale anche per gli ambienti OT, dove i dati forensi possono aiutare a individuare gli attacchi destinati alle infrastrutture critiche e ai servizi di base.

Il processo di backup forense di Acronis prevede l'acquisizione di immagini complete del disco, compresi i dati attivi, lo spazio disponibile e i dump di memoria. Questo approccio scrupoloso, che va emergendo come requisito di sicurezza OT, garantisce che tutte le potenziali prove digitali siano correttamente conservate per facilitare eventuali analisi approfondite successive agli incidenti, a supporto degli obblighi legali e normativi.

Integrando l'acquisizione dei dati forensi nelle regolari routine di backup, Acronis consente alle organizzazioni di mantenere la continuità operativa e di garantire informazioni forensi prontamente disponibili se e quando necessario, sia negli ambienti IT che in quelli OT. Questa integrazione evita l'implementazione di processi separati per l'acquisizione dei dati forensi, ottimizzando le operazioni e riducendo il rischio di perdita di dati durante gli incidenti.

DISASTER RECOVERY INTEGRATO ACRONIS

Acronis Cyber Protect offre una soluzione di disaster recovery integrata che riduce al minimo complessità e costi. Combinando funzionalità di backup e disaster recovery, la piattaforma garantisce alle aziende il ripristino rapido dei workload in caso di emergenze naturali, errori umani, attacchi informatici o guasti hardware. Come detto sopra, nel contesto dei sistemi OT questi eventi possono avere gravi conseguenze.

Le funzionalità di disaster recovery includono avvio rapido dei workload IT o OT in caso di emergenza, runbook per l'automazione dei processi di ripristino e failover di prova che garantiscono il corretto funzionamento dei sistemi durante un'emergenza. Si tratta di fattori essenziali per assicurare la continuità operativa e ridurre i tempi di fermo, in particolare per le applicazioni real-time, molto diffuse negli ambienti OT.

Integrando il disaster recovery con la gestione degli endpoint e la Cyber Security, Acronis offre un approccio olistico alla Cyber Protection garantendo la protezione di tutti gli aspetti dell'infrastruttura IT e promuovendo la resilienza contro un'ampia gamma di possibili interruzioni operative. Inoltre, rende più semplice la gestione per i CISO responsabili dei sistemi di produzione IT e OT.

ALLINEAMENTO AI REQUISITI NORMATIVI

Oltre alla necessità operativa di backup e resilienza, i team di sicurezza OT devono garantire il rispetto di requisiti di conformità e dei quadri normativi esterni in continuo aggiornamento. Il risultato è che la conformità alla Cyber Security OT è diventata un'attività molto impegnativa dei piani di sicurezza aziendale, perché include requisiti convergenti che si evolvono di pari passo all'aumentare delle minacce.

Più specificamente, osserviamo una maggiore attenzione delle autorità di regolamentazione globali verso la resilienza operativa, attraverso quadri normativi come il Digital Operational Resilience Act (DORA) nell'Unione europea e le linee guida del Comitato di Basilea per la vigilanza bancaria, che sottolineano la necessità di rafforzare le misure di Cyber Security nei settori infrastrutturali critici. Le soluzioni Acronis supportano il rispetto di questi requisiti normativi fornendo supporto nelle aree seguenti:

1. **Quadri di gestione dei rischi completi**. Le soluzioni Acronis consentono alle organizzazioni di sicurezza di adottare framework di gestione dei rischi adattabili, di testare regolarmente la resilienza e di mantenere un canale di comunicazione aperto con le parti interessate e i regolatori, in linea con i quadri di resilienza operativa globali per l'IT e l'OT.

2. **Pianificazione dell'incident response.** Acronis offre assistenza alla redazione di piani di incident response, sia autonomi sia come parte di un piano di continuità operativa, garantendo alle aziende di essere preparate alle potenziali minacce informatiche. Essendo questa una nuova attività per molti team di sicurezza OT, il supporto di Acronis è particolarmente utile.
3. **Gestione dei rischi di terze parti.** Le funzionalità di integrazione di Acronis consentono una supervisione efficace delle applicazioni di terze parti, un componente critico della resilienza operativa evidenziato anche dalle autorità di regolamentazione. Come detto, l'integrazione digitale con i prodotti di terzi può essere complessa perché in passato è stata ignorata o sottovalutata.

I FORNITORI DI AUTOMAZIONE OT E ICS DI PUNTA SI AFFIDANO AD ACRONIS

L'adozione delle soluzioni di backup e ripristino di Acronis da parte dei principali fornitori globali di piattaforme OT e ICS ne conferma il ruolo strategico nel garantire la resilienza degli ambienti OT e industriali. Aziende leader del settore, come ABB, Emerson, Siemens, Schneider Electric, Rockwell Automation e Yokogawa, integrano Acronis Cyber Protect nelle proprie piattaforme, sia come soluzione white label sia in co-branding, garantendo ai propri clienti la resilienza operativa. Il fatto che questi giganti globali abbiano scelto Acronis come standard è la prova dell'affidabilità, della flessibilità e della posizione di leadership nel settore del ripristino e del backup in ambito OT.

CONCLUSIONI E PIANO D'AZIONE PER I TEAM DI SICUREZZA OT

Riteniamo che le soluzioni di backup e ripristino di Acronis siano particolarmente adatte per i clienti che intendono migliorare la resilienza e la sicurezza delle proprie infrastrutture OT. Grazie alle funzionalità di ripristino rapido, al supporto per i sistemi legacy, a piani di backup personalizzabili e all'allineamento con i requisiti normativi, Acronis favorisce il mantenimento della continuità operativa e il rispetto degli standard globali in continua evoluzione per la resilienza operativa.

Ai CISO a cui è affidata questa responsabilità, o a qualsiasi altro team di gestione o dirigenziale che si occupa di resilienza digitale per l'OT, suggeriamo di contattare Acronis per saperne di più sulle funzionalità offerte. Il team di TAG è a disposizione dei lettori interessati ad approfondire questo e altri argomenti correlati alla Cyber Security e all'intelligenza artificiale. Saremo lieti di fornire il nostro aiuto.

[1] Siamo particolarmente grati al team tecnico e dirigenziale di Acronis per averci aiutato a comprendere i vari rischi riscontrati negli ambienti OT gestiti dai loro clienti. Il team Acronis ci ha fornito l'accesso alla documentazione del prodotto e ci ha aiutato a ottenere informazioni utili sui futuri sviluppi dei prodotti per l'IT e per l'OT.

INFORMAZIONI SU TAG

TAG è una consolidata società di ricerca e consulenza che fornisce informazioni e raccomandazioni in materia di Cyber Security, intelligenza artificiale e scienze del clima a migliaia di fornitori di soluzioni commerciali e ad aziende della classifica Fortune 500. Fondata nel 2016 e con sede a New York, TAG si distingue nel settore della ricerca commerciale offrendo orientamenti e linee guida, analisi di mercato, consulenze sui progetti e contenuti personalizzati, imparziali, approfonditi e orientati al punto di vista del professionista.