WHITE PAPER

Demistificare il modello Zero Trust nell'OT

Passare dall'attendibilità implicita al modello Zero Trust

Executive Summary

Non molto tempo fa, le reti di tecnologia operativa (OT) utilizzate in ambienti come le fabbriche e le infrastrutture critiche erano isolate in "air-gap", ovvero non erano collegate a Internet. Oggi, però, i mondi un tempo isolati dell'OT e dell'informatica (IT) sperimentano una maggiore interconnessione grazie alla trasformazione digitale e al supporto per una forza lavoro carente o remota. Questa connettività può migliorare la produzione attraverso la condivisione dei dati e nuovi strumenti basati su cloud che consentono alle organizzazioni di sfruttare un nuovo valore commerciale.Uno dei principali svantaggi della convergenza IT/OT, tuttavia, è che le minacce informatiche in continua evoluzione possono ora accedere più facilmente agli ambienti OT precedentemente isolati in "air-gap", mettendo a repentaglio i vantaggi di questa integrazione.

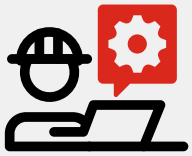
I sistemi OT sono particolarmente vulnerabili perché sono stati progettati in modo da considerare implicitamente attendibile tutto quello che si trova all'interno dei loro ambienti. Le organizzazioni devono quindi passare a un modello di sicurezza informatica Zero Trust, che verifichi continuamente l'attendibilità di utenti e dispositivi controllando gli accessi in base alle informazioni contestuali.

L'evoluzione del modello Zero Trust nell'OT

Storicamente, i progettisti, i costruttori, i produttori e gli operatori dei sistemi IACS (Industrial Automation And Control System) sapevano cosa poteva essere considerato attendibile e cosa no in termini di protezione dei propri sistemi. Potevano presumere che i loro sistemi non avrebbero eseguito qualcosa di pericoloso per l'operatore umano o per la linea di produzione. La maggior parte delle tecnologie IACS sono state progettate basandosi sul concetto ipotetico di attendibilità implicita, il che significava che tutte le connessioni effettuate all'interno del perimetro OT isolato in "air-gap" erano al sicuro da tutte le minacce informatiche che proliferavano nel mondo esterno. Per molti anni, questa strategia di sicurezza basata sull'attendibilità implicita ha funzionato con successo principalmente perché i sistemi OT erano isolati dall'Internet pubblico.

Inoltre, gli asset ICS (Industrial Control System) sono tipicamente realizzati per durare a lungo. Le tecnologie impiegate possono continuare ad essere utilizzate per 20 anni o più. Spesso ci sono solide giustificazioni commerciali (oltre a requisiti di sicurezza e affidabilità) per continuare a utilizzare le apparecchiature ICS più obsolete.[2] Inoltre, non si è mai considerato un futuro in cui le connessioni esterne ai sistemi OT diventassero una necessità comune.

Gli ambienti OT sono sempre più connessi con le reti IT (nota anche come convergenza IT/OT o Industria 4.0), il che può offrire nuovi vantaggi strategici, tra cui l'utilizzo di funzionalità cloud-native e il miglioramento del processo decisionale in prima linea grazie all'utilizzo di dati provenienti da sistemi IT e OT.[3] Questa convergenza può inoltre ridurre i requisiti di spazio, eliminare l'hardware fisico, accorciare i tempi di distribuzione, migliorare i risparmi sui costi, incrementare le prestazioni e ridurre le risorse dei reparti IT e OT in compartimenti stagni.[4] Ma queste connessioni bucano anche l'air-gap OT, sgonfiando così le false nozioni di attendibilità implicita e sicurezza dei sistemi ICS fin dall'ideazione.



"Non solo gli ambienti IT sono spesso necessari per configurare e gestire i dispositivi OT, ma sono anche il luogo in cui i dati chiave devono essere raccolti, normalizzati, elaborati e segnalati in modo che l'organizzazione possa gestire efficacemente le proprie risorse OT. Questa capacità di collegare le reti aziendali e industriali soddisfa un'esigenza aziendale. Tuttavia, con la migrazione di un maggior numero di risorse IT verso ambienti basati su cloud, le risorse OT sono ora esposte a sfide di sicurezza informatica che in precedenza non esistevano".[1]

Tre quarti delle organizzazioni OT hanno segnalato almeno un'intrusione nell'ultimo anno. Le intrusioni di malware (56%) e phishing (49%) continuano ad essere i tipi di incidenti più comuni segnalati; quasi un terzo degli intervistati ha dichiarato di essere stato vittima di un attacco ransomware.[5]

La progressiva affermazione del modello Zero Trust nella sicurezza informatica

A livello concettuale, il termine "Zero Trust" sposta l'idea della sicurezza da un approccio di "attendibilità implicita" a uno stato di "violazione presunta", in cui nulla è considerato attendibile se prima non viene verificato.

In termini più pratici, Zero Trust si riferisce a un modello di sicurezza in cui agli utenti e ai dispositivi non viene più concesso automaticamente l'accesso in base alla posizione della rete, ma ci si concentra sulla valutazione dell'attendibilità in base alle singole transazioni. I gradi di accesso possono essere concessi agli utenti e ai dispositivi verificati in base ai fattori contestuali della richiesta. La riverifica o la rivalutazione delle autorizzazioni è frequente.

Gli approcci all'implementazione di un modello Zero Trust possono variare notevolmente e anche alcuni acronimi delle soluzioni più comuni possono confondere senza definizioni dettagliate.

- **Una soluzione ZTA (Zero Trust Access)** si concentra sull'identificazione e sulla supervisione di quali utenti e dispositivi accedono alla rete. Poiché un numero sempre maggiore di utenti lavora da remoto e i dispositivi Industrial-Internet-of-Things (IIoT) proliferano negli ambienti OT, le organizzazioni devono verificare continuamente tutti gli utenti e i dispositivi che accedono a dati e applicazioni.
- **Una soluzione ZTNA (Zero Trust Network Access)** si riferisce all'accesso alle applicazioni in cui nessun utente o dispositivo è ritenuto attendibile per accedere a un'applicazione a meno che non dimostri le proprie credenziali. Il modello ZTNA è spesso citato come una naturale evoluzione dei tradizionali tunnel VPN, in cui si presuppone che tutto quello che supera i controlli del perimetro di rete sia attendibile. A differenza di una VPN, ZTNA estende il modello Zero Trust oltre la rete e riduce la superficie di attacco nascondendo le applicazioni da Internet.

Negli Stati Uniti, l'interesse per l'implementazione dei principi Zero Trust è aumentato dopo un ordine esecutivo del 2021 della Casa Bianca che mirava a garantire l'adozione di prassi di sicurezza di base in tutte le agenzie e a far migrare il governo federale verso un'architettura Zero Trust.[6]

Quali problemi può risolvere il modello Zero Trust?

Un'implementazione efficace del modello Zero Trust può rispondere a diverse esigenze pressanti di sicurezza informatica che le organizzazioni si trovano ad affrontare oggi:

- Consentire la piena mobilità del personale senza interrompere le normali operazioni o influenzare le policy di controllo degli accessi implementati
- Unificare la strategia di sicurezza dell'organizzazione in termini di utenti, asset e (indirettamente) applicazioni, indipendentemente dalla loro ubicazione fisica
- Contribuire a impedire che le minacce informatiche si diffondano lateralmente all'interno dell'organizzazione rivalutando continuamente l'identità e l'approccio di utenti e dispositivi in base ad ogni singola sessione

Problematiche legate all'implementazione del modello Zero Trust nell'OT

La strada che porta dall'attendibilità implicita al modello Zero Trust non è priva di ostacoli o complicazioni. Per implementare efficacemente una soluzione Zero Trust come ZTA in un ambiente OT, I responsabili della sicurezza potrebbero trovarsi ad affrontare questioni specifiche riguardanti il funzionamento dei sistemi ICS nell'ambiente OT e tutti gli aspetti relativi alla sicurezza.

1. Il linguaggio delle garanzie offerte da qualsiasi fornitore di automazione attuale limita o pone paletti a quello che può accadere sulla rete? Si tratta di un problema abbastanza frequente che dovrebbe essere esaminato in anticipo.
2. Le tecnologie ZTA sono compatibili con le tecnologie legacy presenti negli ambienti OT? È necessario tenere conto della longevità dei sistemi ICS (cicli di vita di oltre 20 anni).
3. I proprietari degli asset dipendono spesso da integratori di sistemi e produttori di apparecchiature originali (OEM) per l'integrazione e la messa in servizio. Sono preparati all'introduzione di tecnologie ZTA che potrebbero stravolgere i sottosistemi attualmente integrati e messi in servizio?
4. I produttori di apparecchiature originali e gli integratori di sistemi possono anche richiedere l'accesso remoto come parte della garanzia o dei contratti di gestione e manutenzione (O&M) di terzi.
5. In genere, gran parte dello stack tecnologico ICS/OT è privo di interfaccia, rendendo impossibile l'interazione con l'utente. Gli indirizzi IP sono spesso statici e sarebbe difficile immaginare di autenticare nuovamente una connessione con un dispositivo senza interfaccia utente. La soluzione ZTA può supportare questa particolare limitazione degli ambienti OT?
6. Poiché gli ambienti OT sono storicamente isolati in "air-gap", a volte si affidano a password statiche anziché a quelle gestite in Active Directory (AD) con policy di gestione delle credenziali sicure.
7. Alcuni componenti OT (ad esempio, controllori logici programmabili [PLC], interfacce uomo-macchina [HMI]) potrebbero non supportare le tecnologie o i protocolli necessari per integrarsi completamente con un'implementazione ZTA. Di conseguenza, un approccio ZTA potrebbe non essere pratico per alcuni dispositivi o sistemi OT.
8. Alcune tecnologie ICS all'interno dell'ambiente OT possono essere designate per operazioni di sicurezza e possono richiedere un accesso tempestivo e ininterrotto ai sistemi per eseguire le funzioni di sicurezza. Pertanto, l'implementazione di una soluzione ZTA per tali sistemi ICS non deve ostacolare gli aspetti di sicurezza dell'infrastruttura.

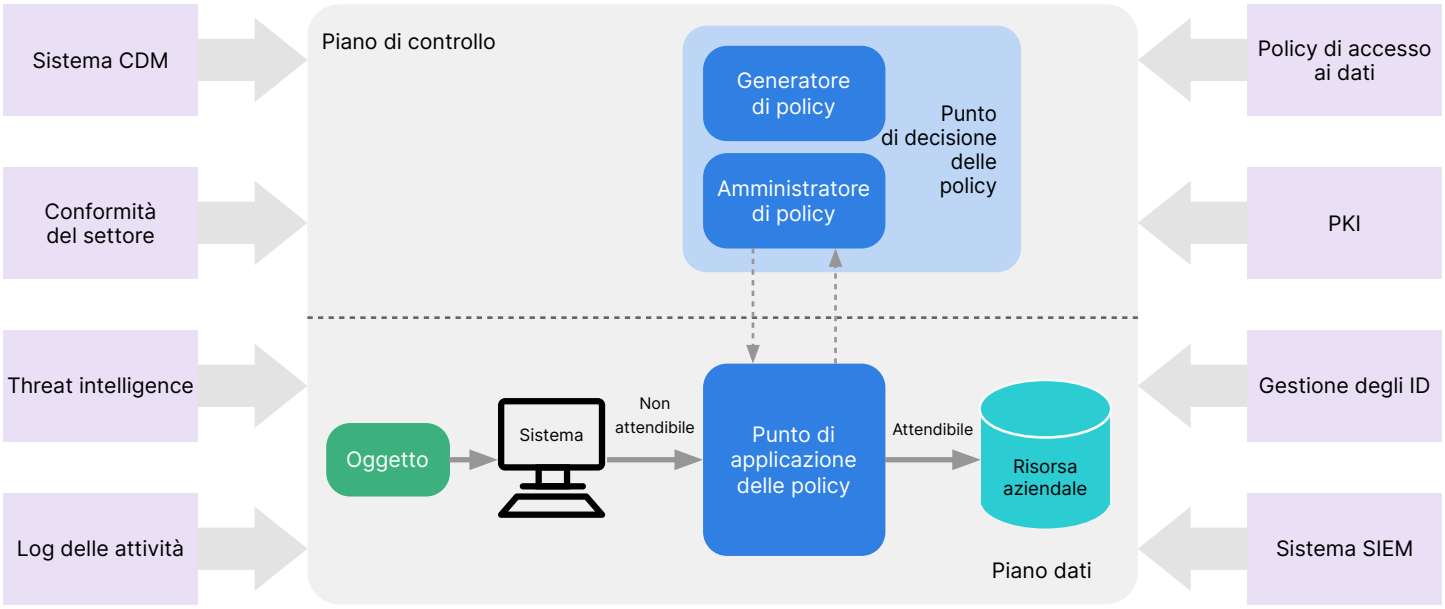
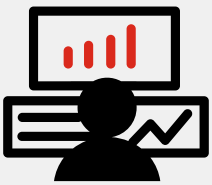


Figura 1: componenti logici del modello Zero Trust core secondo NIST SP 800-207[7]

Un'altra problematica fondamentale per l'implementazione del modello Zero Trust negli ambienti IT/OT interconnessi è che le organizzazioni devono stabilire identità distinte tra le due parti dell'azienda. Per distribuire al meglio la tecnologia ZTA, è necessaria una soluzione in grado di far convergere le operazioni di sicurezza per due aree di gestione che si incontrano con priorità diverse. Mantenere centri operativi di sicurezza (SOC) separati per IT e OT aumenta la complessità e i rischi potenziali quando si tratta di gestire le risorse e le policy in entrambi gli ambienti, di raccogliere e analizzare i dati provenienti da sistemi IT e OT e di eseguire azioni di correzione in caso di intrusioni informatiche.

L'acquisizione e la manutenzione di soluzioni Zero Trust richiederà anche un know-how interno e risorse operative per la gestione delle registrazioni e dei controlli di accesso. In combinazione con budget limitati, molte organizzazioni attualmente possono avere difficoltà a trovare, assumere e fidelizzare il personale di sicurezza qualificato necessario per distribuire e gestire le soluzioni Zero Trust. In questi casi, può essere importante considerare se un fornitore offre l'opzione di servizi di supporto dedicati.



Il numero di responsabili della sicurezza OT che considerano l'approccio alla sicurezza della propria organizzazione "estremamente maturo" è sceso dal 21% al 13% quest'anno, suggerendo la presenza di una crescente consapevolezza tra i professionisti OT, oltre che di strumenti più efficaci per l'autovalutazione delle capacità di sicurezza informatica.[8]

Il percorso verso il futuro inizia oggi

Con l'accelerazione della convergenza IT/OT, i leader della sicurezza devono passare a un modello Zero Trust per mantenere i loro ambienti OT al sicuro da interruzioni dovute a eventi di sicurezza interni o esterni. Il percorso odierno per distribuire il modello Zero Trust nell'OT è triplice:

- **Persone:** è necessario iniziare a sensibilizzare gli utenti sui rischi della convergenza IT/OT e formarli su come le soluzioni Zero Trust possono contribuire a proteggere l'organizzazione dalle minacce opportunistiche.
- **Processo:** l'era della sicurezza basata sull'attendibilità implicita nell'OT ormai è un ricordo del passato. Tutte le policy e i protocolli di sicurezza devono ora essere basati sull'attendibilità verificata contestualmente e costantemente riverificata. Le organizzazioni hanno bisogno di un controllo completo e continuo su chi e cosa si trova nella rete, compresi i fornitori di automazione e i service provider.
- **Tecnologia:** occorre valutare le soluzioni Zero Trust per gli ambienti OT e tenere presente che possono avere un impatto anche sulla supply chain più ampia. Per questo motivo, è opportuno cercare un fornitore di sicurezza Zero Trust con solide partnership in tutto l'ecosistema tecnologico.

[1] "IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems", Carnegie Mellon University, 18 luglio 2022.

[2] Ibid.

[3] "Converge IT and OT to turbocharge business operations' scaling power", McKinsey & Company, 28 giugno 2022.

[4] "Report sullo stato della tecnologia operativa e della sicurezza informatica nel 2023", Fortinet, maggio 2023.

[5] Ibid.

[6] "How to Create a Comprehensive Zero Trust Strategy", Fortinet, 15 maggio 2023.

[7] "SP 800-207: Zero Trust Architecture", NIST, agosto 2020.

[8] "Report sullo stato della tecnologia operativa e della sicurezza informatica nel 2023", Fortinet, maggio 2023.

ottobre 31, 2023 12:51 PM

2177370-0-0-IT