Piattaforma di sicurezza di prossima generazione per infrastrutture critiche

Le moderne sfide per la protezione dei sistemi di controllo delle infrastrutture critiche

SCADA e i sistemi di controllo industriale (ICS), utilizzati per automatizzare i processi su infrastrutture critiche, come utenze e trasporti, hanno subito trasformazioni rivoluzionarie negli ultimi decenni. Quelli che una volta erano un insieme di soluzioni isolate e proprietarie basate su protocolli seriali, sono diventati sistemi altamente interconnessi, che sfruttano il protocollo internet e le soluzioni commerciali per ottimizzare le operazioni e ridurre i costi. Questa integrazione tra IT e OT (intesa come tecnologia operativa) ha portato numerosi vantaggi, ma la modernizzazione ha anche aumentato il rischio di minacce informatiche che possono mettere a repentaglio la disponibilità del processo e il benessere del personale, dei cittadini, dei sistemi economici e dell'ambiente. Questo fattore di rischio, combinato con l'espansione delle minacce e degli scenari di regolamentazione, ha incrementato gli oneri di protezione delle infrastrutture critiche a carico dei titolari delle risorse. Ecco alcune di queste sfide:

- Ottenere visibilità granulare sul traffico di rete operativo, a livello di applicazione e di utente, per confermare un uso corretto o anomalo
- Segmentare le reti con controlli di accesso sufficienti a limitare i vettori di attacco estranei e interni e, al contempo, soddisfare requisiti prestazionali rigorosi
- Proteggere sistemi commerciali privi di patch dalle minacce informatiche note e ridurre i tempi di inattività causati da incidenti informatici o attività di patching
- Prevenire gli attacchi informatici avanzati che utilizzano metodi Zero Day per interrompere la produzione, compromettere l'integrità delle informazioni o procedere alla sottrazione degli IP
- Gestire reti e prodotti di sicurezza per gli endpoint distribuiti e disallineati
- Rispettare le normative e fornire in modo efficiente informazioni per gli audit

I sistemi di controllo – Sfide e iniziative:

- Ridurre la frequenza e la gravità degli incidenti informatici a mantenere tempi di inattività e sicurezza elevati
- Adeguarsi a obiettivi prestazionali rigorosi
- Abilitare un accesso sicuro da reti di supporto aziendali e di terzi
- Proteggere i sistemi privi di patch durante cicli di manutenzione prolungati
- Endpoint e rete lavorano in sinergia per prevenire gli attacchi avanzati
- Conformità normativa

Oggi, per proteggere efficacemente le reti SCADA e ICS sulle infrastrutture critiche, è necessario un approccio alla sicurezza moderno.

Le soluzioni puntuali tradizionali non gestiscono le esigenze dei moderni sistemi SCADA/ICS

Purtroppo, le soluzioni legacy sono inadatte ad affrontare queste sfide, per diversi motivi. Dal punto di vista della sicurezza di rete, le architetture di sicurezza esistenti sono spesso basate su firewall di tipo stateful inspection, che forniscono visibilità e controllo degli accessi solo a livello di porte e indirizzi IP. Questi sistemi sono inefficaci per confermare che il traffico legittimo, come i protocolli ICS, le applicazioni storiche e di automazione e le applicazioni infrastrutturali come SSH, sia effettivamente l'unico presente. Analogamente, non sono in grado di evidenziare la presenza di traffico collegato ad applicazioni o protocolli non consentiti o dannosi. Data la mancanza di controllo a livello di utente, inoltre, non supportano i controlli di accesso basati sui ruoli previsti dagli standard di sicurezza ICS. E, naturalmente, i firewall di tipo stateful inspection non verificano i contenuti né bloccano minacce quali exploit e malware.

Le organizzazioni cercano di risolvere il problema distribuendo più soluzioni scollegate, come appliance per l'ispezione di applicazioni/contenuti, IPS e sandboxing, ma questo approccio genera un'ulteriore serie di problematiche. Innanzitutto, le prestazioni calano vertiginosamente su ogni dispositivo aggiuntivo che deve rielaborare i pacchetti: questa situazione è inaccettabile all'interno di sistemi di controllo che richiedono prestazioni elevate e latenza ridotta. Molte organizzazioni sono costrette a distribuire i componenti aggiuntivi in modalità passiva, di solo rilevamento, che non aiuta a ridurre e a prevenire gli attacchi. La proliferazione di componenti comporta anche una riduzione della produttività e un rischio di errore più elevato per gli amministratori della sicurezza SCADA che devono eseguire il provisioning di questi dispositivi. Inoltre, l'analisi forense diventa più difficile per la presenza di numerosi silos di informazioni scollegati tra loro. Ciò determina un aumento dei tempi e delle iniziative necessari per analizzare e risolvere gli incidenti informatici, lasciando le organizzazioni esposte e il servizio non disponibile per periodi di tempo prolungati.

Presentano problemi anche i prodotti endpoint legacy, che finora hanno funzionato separatamente dalla sicurezza della rete. Questi sono fondamentalmente in grado di affrontare solo le minacce con firme, stringhe e comportamenti noti, ma non riescono a prevenire gli attacchi che utilizzano exploit e malware mai visti prima. Dati gli elevati rischi collegati alla protezione delle infrastrutture critiche, le soluzioni di sicurezza devono essere in grado di prevenire tutti gli attacchi, anche di tipo Zero Day, per garantire l'integrità del processo e mantenere tempi di attività e sicurezza elevati.

La piattaforma di sicurezza di prossima generazione di Palo Alto Networks®

Per affrontare queste sfide e proteggere con efficacia le infrastrutture critiche, è necessario un approccio completo e dirompente, ovvero un approccio basato su piattaforma. La piattaforma di sicurezza enterprise di Palo Alto Networks elimina le complessità tipiche dei prodotti singoli per firewall, IPS, IDS, filtraggio URL, antivirus per endpoint e altro ancora. La nostra piattaforma di sicurezza di prossima generazione realizza questa visione di una protezione completa integrando tre elementi fondamentali:

- Il **firewall di nuova generazione**[1], con il suo innovativo motore di classificazione a 7 livelli, non solo offre visibilità granulare sul traffico anche per i protocolli, le applicazioni e gli utenti ICS ma, in qualità di dispositivo di applicazione, consente agli utenti di segmentare la rete mediante policy aziendali intuitive che riducono l'impronta dell'attacco. Il traffico consentito risulta ulteriormente protetto tramite il blocco a livello nativo delle minacce conosciute, come exploit di software e protocolli ICS, virus e spyware e mediante il sandboxing delle minacce sconosciute, analizzate e bloccate rapidamente mediante misure di protezione generate in modo automatico. La sicurezza può essere estesa anche agli ambienti virtuali e mobili, sempre più ampiamente distribuiti nei sistemi di controllo, per migliorare l'efficienza.
- La prevenzione endpoint avanzata, Traps, assicura che il punto di ingresso per la maggior parte delle minacce avanzate, l'host, sia al sicuro. Utilizza un approccio dirompente alla prevenzione, bloccando le tecniche sottostanti utilizzate da exploit e malware nella relativa catena di attacco. Si tratta di un approccio diverso rispetto a quello, inefficace e complesso, delle soluzioni endpoint tradizionali, che considerano solo il crescente repository di firme, stringhe e comportamenti noti, per cercare di scoraggiare gli attacchi Zero Day.
- Il cloud di intelligence sulle minacce analizza e mette in correlazione l'intelligence da tutte le funzioni di sicurezza della piattaforma (il filtraggio URL, la sicurezza mobile, la prevenzione minacce/IPS e il motore di esecuzione virtuale o sandbox, WildFire™) e dai contributi confermati della community. WildFire rileva immediatamente i malware prima sconosciuti e comunica i risultati alla piattaforma, per la generazione automatica delle firme. Tutta l'intelligence sulle minacce viene distribuita alla rete e agli endpoint per garantirne la protezione. Attacchi noti, Zero Day e avanzati, incluse APT, possono tutti essere bloccati dall'endpoint al data center. Tutto questo avviene automaticamente, riducendo i carichi operativi e il tempo di risposta dell'organizzazione.

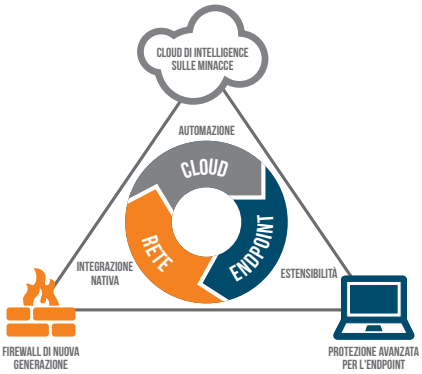

Figura 1: Piattaforma di sicurezza di rete di prossima generazione di Palo Alto Networks

Vantaggi della piattaforma di sicurezza per la rete dei sistemi di controllo

La piattaforma di sicurezza enterprise di Palo Alto Networks offre numerosi vantaggi per le reti dei sistemi di controllo:

- **Visibilità e intelligence incrementate:** non solo la piattaforma identifica il traffico di rete dell'impianto con il livello di granularità maggiormente intuitivo di protocolli (ad esempio Modbus, DNP3, CIP EtherNet IP), applicazioni (ERP/database, Historian), utenti e contenuti, ma fornisce anche il rapporto contestuale tra le informazioni, in modo intrinseco. Questo consente alle organizzazioni di verificare facilmente se la rete dell'impianto viene utilizzata in modo conforme alle esigenze di business e alle policy, e di rispondere rapidamente qualora venga rilevato un uso anomalo.

- **Impronta dell'attacco ridotta:** le capacità di segmentazione avanzate consentono la creazione di aree di sicurezza e l'applicazione dei controlli di accesso basati sui ruoli, a privilegio minimo, come previsto dallo standard IEC 62443. Non solo in questo modo si riduce la superficie di attacco impiegata dalle entità dannose, ma si minimizza anche il rischio di incidenti informatici involontari. Grazie a questa funzionalità di creazione di micro-segmenti, i titolari delle risorse possono garantire un accesso esterno sicuro a utenti aziendali, fornitori e partner, nonché un utilizzo sicuro all'interno dell'OT.
- **Prevenzione delle minacce completa:** le minacce informatiche possono avere origine sulla rete o a livello di host (HMI, server di automazione, workstation), e possono essere conosciute o sconosciute. La nostra piattaforma applica un approccio di difesa profondo, che assicura il blocco delle minacce, anche quelle mai viste prima, anziché la loro semplice rilevazione nei diversi punti di origine. Questo riduce drasticamente il potenziale di messa a rischio del processo, che si tratti di una problematica minima, come un'infezione accidentale da una variante rehashed di SQL Slammer, o di qualcosa di più mirato, come la prossima campagna Energetic Bear. Data l'estensione delle finestre di manutenzione dei sistemi di controllo, spesso superiori a 12 mesi, la capacità fornita da Traps di proteggere i sistemi vulnerabili, privi di patch o unpatchable, da attacchi Zero Day e malware tra un'attività di patching e l'altra, diventa irrinunciabile.
- **Migliore capacità di soddisfare le norme e gli standard:** che si tratti di definire i perimetri di sicurezza elettronica CIP NERC, di distribuire il nucleo NIST Cybersecurity Framework, o semplicemente di fornire il livello granulare di registrazione del traffico e amministrativa richiesto dai revisori aziendali, la nostra piattaforma offre tutti i controlli, le funzioni e i dettagli sul traffico necessari per l'adeguamento agli standard.
- **Operazioni più efficienti, riduzione della complessità:** limitando l'impronta dell'attacco e bloccando le minacce informatiche, le organizzazioni possono non solo migliorare la sicurezza, ma anche ridurre i tempi di inattività, perché gli incidenti informatici da risolvere sono meno numerosi, e perché l'approccio adottato dalla protezione endpoint avanzata richiede una minore attività di patching. Inoltre, la nostra architettura esclusiva riduce il carico amministrativo, semplificando la manutenzione e la configurazione di policy, offrendo gestione centralizzata e automatizzando l'intelligence sulle minacce.

Informazioni aggiuntive su sistemi di controllo del traffico, minacce e rischi

Con più di 19.000 clienti in oltre 120 paesi e diversi settori, oltre 75 aziende Fortune 100 e le pubbliche amministrazioni più avanzate al mondo si affidano a Palo Alto Networks per migliorare la propria condizione di sicurezza informatica. Informatevi oggi stesso su come sfruttare la nostra piattaforma per proteggere la vostra infrastruttura critica e garantire l'operatività e la sicurezza. Richiedete una valutazione e un report AVR (Application Visibility and Risk, Visibilità e rischi delle applicazioni) gratuiti, per ottenere una visione dettagliata delle modalità di utilizzo della rete dei vostri sistemi di controllo (applicazioni, protocolli ICS, URL, file), e dei relativi rischi potenziali. Informatevi su Traps, la nostra rivoluzionaria tecnologia per la protezione avanzata degli endpoint, e scoprite come previene gli attacchi, anche quelli sconosciuti, garantendo la protezione dei sistemi legacy privi di patch, diffusi nell'ambito dei sistemi di controllo.

Report AVR (visibilità e rischi delle applicazioni) - http://connect.paloaltonetworks.com/avr-alt

Traps - Protezione avanzata per l'endpoint - http://go.paloaltonetworks.com/traps

---

[1] *Leader Magic Quadrant di Gartner Group per i firewall enterprise negli ultimi tre anni.*

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Telefono: +1.408.753.4000
Vendite: +1.866.320.4788
Assistenza: +1.866.898.9087

www.paloaltonetworks.com

PAN_WP_ESPCI_102914