Steve Rawlins

Proteggiamoci dagli attacchi

Per i sistemi di automazione industriale, la connettività stabile di dati è oggi tanto importante quanto la funzionalità di controllo di base. Le piattaforme che forniscono sicurezza informatica integrata e difesa approfondita sono il modo migliore per difendere le soluzioni altamente connesse

Fig. 1 - Una maggiore integrazione di OT e IT, combinata con un uso diffuso di dispositivi wi-fi mobili, rende i dati più accessibili che mai, ma offre anche opportunità agli hacker

Le piattaforme di automazione industriale non forniscono più solo funzionalità di base, ma sono oggi chiamate a svolgere importanti funzioni di aggregazione e analisi dei dati dell'Internet of Things Industriale (IIoT). Ogni dispositivo sta diventando più smart e più interconnesso di quanto lo sia mai stato prima e mette a disposizione dati preziosi, che devono però essere accessibili dove e quando serve. Per trarne il massimo valore è necessaria una connettività trasparente e senza soluzione di continuità, dall'impianto fino al cloud. L'Internet e le risorse informatiche aziendali di livello superiore sono essenziali nella trasmissione ed elaborazione dei dati.

Tuttavia, il costante aumento delle capacità e della connettività genera maggiori preoccupazioni per la sicurezza informatica. I dispositivi digitali OT (Operational Technology) di livello industriale possono essere costruiti per resistere agli agenti esterni meglio delle loro controparti IT, ma i dispositivi IT godono di un notevole vantaggio nel fornire misure di cybersecurity. La connettività Internet e l'adozione del wi-fi negli impianti spalancano le porte ai malintenzionati che vogliono accedere a tutti i tipi di risorse digitali OT. Mentre in passato la disponibilità di dispositivi digitali industriali era di importanza primaria, oggi la riservatezza e l'integrità hanno un ruolo ugualmente importante.

Una cybersecurity adeguata non può essere semplicemente aggiunta, e questo articolo spiega perché è essenziale che le piattaforme di automazione offrano protezioni integrate di tipo Defense in Depth. Descrive inoltre funzionalità come l'uso di firmware firmato e crittografato digitalmente utilizzando i ben noti standard aperti, il Secure Boot, le password utente e OEM crittografate, le comunicazioni crittografate con protocollo OPC-UA Secure e altro ancora. Queste sono alcune delle caratteristiche richieste per un approccio 'Secure by Design', ed è perciò importante che chi le implementa insista nell'includerle nelle piattaforme di automazione.

Come siamo arrivati a questo punto

Le preoccupazioni legate alla sicurezza informatica dei sistemi di automazione industriale si sono intensificate per numerosi fattori dovuti a decisioni passate. Mentre le risorse digitali sono state implementate in ambito industriale per oltre tre decenni, l'importanza della cybersecurity è stata riconosciuta solo recentemente. Effettivamente, quando sono stati utilizzati i primi dispositivi, non esistevano veramente pratiche di sicurezza informatica. La massima protezione presa in considerazione a quel tempo era di isolare i dispositivi, creando isole di automazione

relativamente difficili da accedere fisicamente e senza un'accessibilità estesa tramite la rete. Questo era un approccio di progettazione sicuro a quel tempo, perché basato sulle tecnologie disponibili, ma sicuramente inaccettabile per soddisfare le esigenze delle aziende di oggi. La verità è che, mentre le installazioni più recenti e i retrofit hanno la possibilità di utilizzare dispositivi digitali più sicuri, molti asset obsoleti e poco sicuri restano in funzione per decenni, senza aggiornamenti di sicurezza e a volte senza alcun supporto disponibile. Nel frattempo, le minacce cibernetiche sono aumentate e diventate più sofisticate. Con le reti wireless e i dispositivi USB, l'isolamento fisico non è semplicemente più praticabile. Anzi, è in diretto contrasto con la necessità di un accesso legittimo completo a tutti i tipi di dispositivi digitali industriali, soprattutto a quelli particolarmente intelligenti che possono fornire dati importanti.

Riconoscere la necessità di cybersecurity è indispensabile, ma aggiungerla semplicemente ai dispositivi esistenti non è la soluzione giusta, perché è un po' come aggiungere una porta d'acciaio chiusa a chiave a una scatola di cartone per tenere lontani gli intrusi dal suo contenuto. Dato che molti protocolli e dispositivi sono stati progettati senza pensare alla sicurezza nei livelli fondamentali dei sistemi OT, mancano loro i meccanismi basilari di difesa cibernetica e quindi nessun patch può correggerli. I provvedimenti di cybersecurity devono invece essere integrati in maniera appropriata per fornire una difesa avanzata di tipo Defense in Depth.

Fig. 2 - I prodotti e sistemi PACSystems di Emerson forniscono una gamma di misure di cybersecurity, assicurando che le soluzioni di automazione e informatiche siano dotate di Defense in Depth per resistere ai vettori di attacco

Perché alcuni schemi di cybersecurity sono problematici

Ai fornitori industriali di dispositivi digitali va riconosciuto il merito di aver progressivamente cercato negli anni di incorporare la cybersecurity. Alcuni fornitori hanno provato le loro strategie personali, ma dato che l'arena commerciale IT ha conquistato un enorme vantaggio in questo ambito, anche gli approcci più validi non hanno attecchito in questo settore. In effetti, le misure personalizzate o proprietarie sono considerate meno sicure di quelle basate su standard aperti, che in genere hanno origine dalla tecnologia dell'informazione.

In alcuni casi, i produttori di dispositivi hanno implementato la cybersecurity utilizzando un chipset proprietario associato a un proprio firmware. Gli elementi proprietari non sono facilmente controllabili da esperti industriali, e sono costantemente esposti al rischio di attacchi informatici. E una volta che le aziende interne sviluppano un firmware di sicurezza informatica, devono impegnarsi a curarlo e ad aggiornarlo continuamente per garantire la protezione dei prodotti interessati. Ciò significa che devono farsi carico di trovare tutti i punti deboli e di risolvere i problemi senza soluzioni di verifica e assistenza da parte della community. In questi casi è praticamente impossibile porre rimedio a un hardware obsoleto senza sostituire completamente il dispositivo, e utilizzare un vecchio firmare crea vulnerabilità inaccettabili non essendo in grado di affrontare le tipologie di attacchi più recenti.

Un altro problema molto più grave riguardante le misure di cybersecurity proprietarie è che il provider deve anche stabilire misure protettive per distribuire gli aggiornamenti. Anche se il piano di sicurezza cibernetica dell'hardware e del software è realizzabile, gli hacker dotati di competenze sufficienti sviluppano a volte metodi per creare un proprio firmware modificato, che viene utilizzato per aprire la porta alla pirateria informatica. In certi casi è difficile per gli utenti fidarsi di futuri aggiornamenti firmare, ma allo stesso tempo gli aggiornamenti sono necessari per proteggersi da nuove minacce.

Anche se può sembrare non intuitivo, gli standard aperti forniscono un approccio più sicuro.

Gli standard aperti riducono i rischi

Mentre alcuni fornitori industriali hanno acquistato algoritmi di hashing proprietari e altri metodi, la soluzione migliore per l'industria è seguire le migliori pratiche comprovate e ampliamente utilizzate del settore commerciale IT, che ha una maggiore base di dispositivi digitali installati rispetto al mondo industriale. La tecnologia operativa OT può sfruttare il meglio di ciò che ha sviluppato il mondo IT e imparare meglio dai suoi errori.

Per esempio, alcuni fornitori industriali offrono tutte le applicazioni firmware e software tramite un repository curato a cui hanno facile accesso gli utenti qualificati. Ognuno di questi pacchetti software è crittografato digitalmente e firmato utilizzando strategie industriali standard e standard aperti, incluse chiavi pubbliche e private. In questo modo si utilizzano metodi comprovati e sicuri per fornire aggiornamenti importanti ai clienti, sfruttando il meglio di ciò che ha dimostrato di funzionare. Con strumenti aperti in mano agli utenti, il personale di progettazione e assistenza è pronto per il successo. Si può scaricare sempre il software più attuale, confermare che sia verificato digitalmente e installarlo nel dispositivo di destinazione o nel computer. È inoltre possibile confermare che la giusta versione verificata digitalmente sia in un dispositivo di destinazione come un PLC/PAC o un edge controller, in modo che gli utenti possano controllare il loro sito invece di continuare a utilizzare versioni obsolete per anni per paura di aggiornare i loro sistemi. Notare che esiste una differenza tra crittografia e cybersecurity. La crittografia in questo caso riguarda il metodo di consegna, che serve ad assicurare di avere ottenuto il giusto firmware/software.

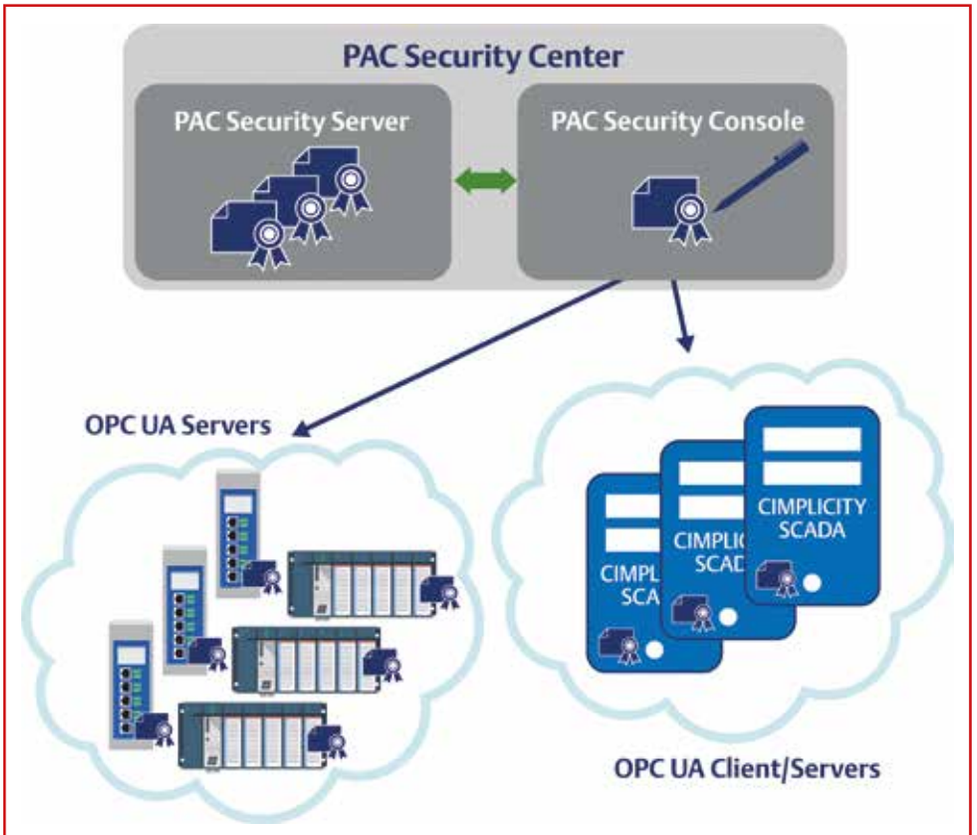

Fig. 3 - Basandosi su standard aperti e protocolli industriali comprovati, i prodotti e le piattaforme Emerson tipo il PAC Security Center aiutano i clienti a creare e mantenere installazioni sicure da attacchi cibernetici

Una volta inserito il firmware/software corretto, gli utenti possono installarlo ed essere certi di avere la versione sicura più recente. La cybersecurity è un argomento molto più ampio, con la crittografia come sottosistema. Questo esempio mostra però un metodo di adozione che può essere applicato a tutti i principi di sicurezza informatica e a bisogni specifici.

Ricerca di più livelli di difesa

Gli utenti devono cercare piattaforme industriali che hanno incorporato altre tecnologie di cybersecurity aperte e standard quando acquistano un sistema di sicurezza di tipo Defense in Depth per i loro progetti (figura 2). Per esempio, alcune piattaforme industriali usano la tecnologia Trusted Platform Module (TPM), che è un microcontroller dedicato che esegue compiti di crittografia e autenticazione. Funzionalità come la TPM sono un esempio di cosa può essere incorporato in un prodotto per far fronte alla sicurezza in tutti i livelli, cercando di rendere le cose più sicure possibili, pur fornendo la funzionalità di cui i clienti hanno bisogno.

Secure Boot è un altro aspetto chiave che può essere incorporato nei dispositivi digitali e con il quale il firmware controlla che il boot loader e tutte le immagini software associate siano firmati con una chiave crittografica autorizzata dal fornitore del prodotto. Come standard di sicurezza sviluppato dall'industria dei PC e utilizzato dalla Unified Extensible Firmware Interface (UEFI) assieme a un Bios, il Secure Boot impedisce ai dispositivi di essere violati dagli hacker o di essere modificati per fornire un accesso segreto.

Gli sviluppatori, e specialmente gli OEM, vogliono essere sicuri che le loro piattaforme informatiche e di automazione industriale offrano password criptate con l'abilità di bloccare e crittografare le applicazioni. Questo ha in parte a che fare con la protezione della proprietà intellettuale e con la prevenzione di modifiche non autorizzate in campo, ma password efficaci e bloccaggio delle applicazioni servono anche come livelli addizionali di cybersecurity che ne impediscono la modifica da parte di individui non autorizzati. Allo stesso modo, quando i prodotti di automazione necessitano di comunicare tra loro o con risorse informatiche di livello superiore, si preferiscono protocolli di comunicazione industriali crittografati come OPC-UA Secure (figura 3). Le pratiche e le procedure di progettazione rappresentano un aspetto importante dei sistemi di sicurezza informatica. I fornitori principali di automazione testano i loro prodotti per assicurarsi che resistano contro le minacce alla sicurezza informatica. I progettisti devono rispettare gli standard industriali ampiamente accettati, tipo la norma ISA/IEC 62443, che definisce i requisiti e i processi coinvolti nell'implementazione e manutenzione dei sistemi industriali di automazione e di controllo cyberprotetti. Utenti proattivi verificheranno i loro impianti per confermarne le prestazioni continue.

Ottenere soluzioni Secure by Design

La connettività sicura dall'impianto fino al cloud non è più una sottigliezza per l'automazione industriale e per i sistemi di elaborazione dati, bensì un imperativo. I prodotti OT tradizionali non erano semplicemente costruiti per fornire il livello di cybersecurity che deve accompagnare questa connettività estesa. Gli hacker prendono sempre più di mira gli ambienti OT per una serie di motivi e l'industria deve essere preparata. La cybersecurity aggiuntiva, o ancora peggio la cybersecurity personalizzata creata in modo inefficiente, lascia le strutture operative vulnerabili agli attacchi che possono paralizzare la produzione, costare un sacco di soldi o introdurre addirittura rischi per la sicurezza e l'ambiente. Gli standard aperti, e soprattutto quelli sviluppati e forniti dall'ampia base delle tecnologie IT, forniscono la risposta migliore per l'industria OT. Gli sviluppatori devono costruire le loro soluzioni di automazione basandosi su questi tipi di standard, utilizzando prodotti performanti con funzionalità di sicurezza integrate, come per esempio firmware/software firmati digitalmente e crittografati, Secure Boot e password/applicazioni criptate. Seguendo un approccio sicuro e multilivello, gli sviluppatori e gli OEM possono garantire la migliore cybersecurity possibile per la loro automazione e le soluzioni IIoT.

Emerson - www.emerson.com