Sicurezza

Fonte: www.womensecuritysociety.co.uk

MANTENERE LA SICUREZZA NELLE RETI IBRIDE

di **Simone Castelli**

UNA DIFESA CON UN APPROCCIO MULTILIVELLO PUÒ AIUTARE A PROTEGGERE AMBIENTI DI PRODUZIONE ETEROGENEI DOVE CONVIVONO DIVERSE MACCHINE AUTOMATICHE E SISTEMI DI CONTROLLO DI PROCESSO

Negli ambienti dove convivono processi continui e processi discreti, molto spesso convivono anche le più svariate rete di comunicazione, proprio perché la tradizionale differente architettura di sistemi di controllo e delle tecniche di automazione ha facilitato la proliferazione di tecnologie di base differenti, oppure sviluppate in periodi storici diversi.

In tali ambienti, non è raro imbattersi in soluzioni di rete tipiche del mondo PLC, magari pluriformitore, affiancate da reti che affondano le loro radici nelle tecnologie tipiche del controllo di processo.

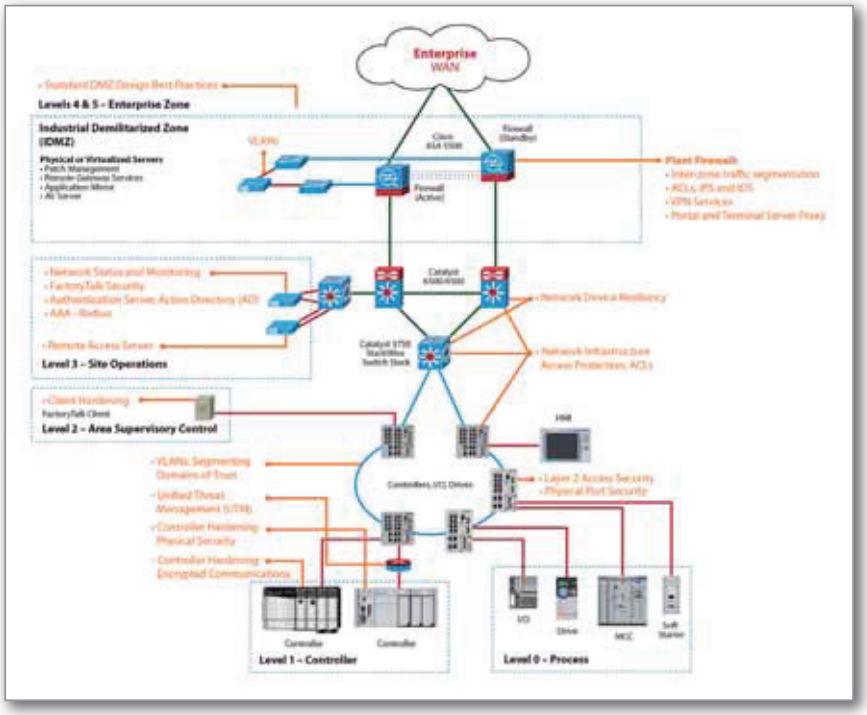
La spinta all'integrazione tra i due mondi dell'automazione discreta e del controllo di processo crea inevitabilmente punti di contatto tra le varie reti di comunicazioni installate, che potenzialmente possono far insorgere nuovi rischi di esposizione a minacce non considerate in precedenza quando le reti erano isolate.

Difesa con approccio multilivello

Nessuno ha la bacchetta magica per garantire in modo semplice e documentabile la sicurezza totale di un insieme di reti di comunicazioni, ma vale certamente la pena seguire alcune buone pratiche per la minimizzazione dei rischi di sicurezza applicabili a tutte le reti, a maggior ragione quando le tecnologie di rete possono essere diverse tra loro.

Una delle metodologie frequentemente suggerite è quella di adottare tecniche di difesa multilivello, ossia applicate ai vari aspetti tecnologici e organizzativi che impattano sull'intera organizzazione aziendale. In sostanza, si tratta di cercare di introdurre elementi di sicurezza e metodologie di prevenzione dei rischi in vari punti della 'piramide' organizzativa e operativa. Ad esempio, anziché concentrare tutte le proprie attenzioni sulla sola installazione di un efficace firewall nel punto di contatto tra rete interna di fabbrica e rete di comunicazione di ufficio, operazione certamente necessaria, ma che in caso di 'crollo' del 'muro di difesa' esporrebbe l'intera rete interna al rischio indiscriminato di attacco, meglio distribuire il più possibile i meccanismi di difesa su più livelli, onde costruire una serie di barriere concentriche di protezione e segregando tra loro nel limite del possibile le varie zone da proteggere, nell'ottica di confinare un'eventuale intrusione in un'area la più piccola possibile, senza mettere a repentaglio l'intero sistema. Concretamente, è pertanto necessario sia gestire con accuratezza l'accesso fisico alle reti, sia l'aspetto organizzativo della distribuzione delle password o delle procedure di aggiornamento di software e firmware delle apparecchiature. A tal proposito, sarebbe ben poco utile installare un firewall di ultima generazione per proteggersi da attacchi esterni se chiunque potesse scavalcare facilmente un cancello e collegarsi alla rete di fabbrica interna con un portatile o uno smartphone senza essere rilevato.

L'approccio multilivello alla sicurezza deve pertanto prevedere attenzioni molteplici, a partire dal controllo dell'accesso fisico delle persone ai componenti critici. A cominciare dalla comuni di attività di portineria, fino al controllo degli accessi alle aree sensibili dell'impianto, risulta utile tracciare e segregare le aree accessibili mediante meccanismi di controllo e identificativi elettronici, con l'obiettivo di

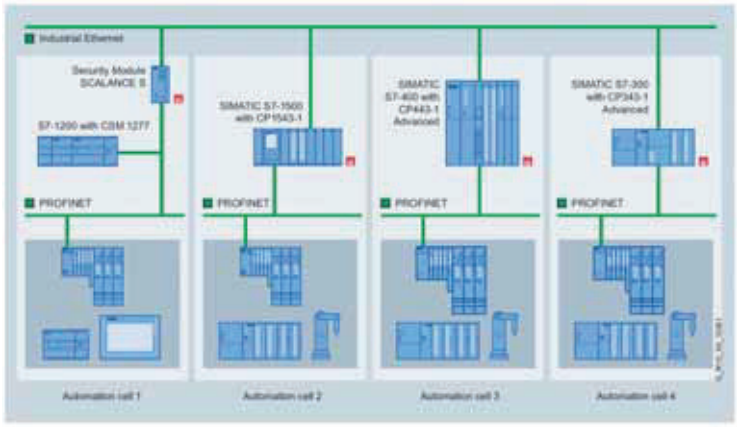


Esempio di architettura di protezione multilivello illustrata da Rockwell Automation che abbraccia l'intera struttura di un sito produttivo

mantenere lontane persone interessate a introdurre intenzionalmente malware o a carpire informazioni sensibili.

Reti con celle segmentate

I firewall sono un elemento essenziale per proteggere le applicazioni di produzione da accessi autorizzati provenienti dalla rete d'ufficio aziendale o dall'esterno. La segmentazione delle rete in più sottoreti permette di aumentare il livello di protezione perimetrando le celle produttive in modo tale da poterle proteggere individualmente creando un secondo 'muro di protezione' a valle di quello principale. Inoltre, la protezione delle celle permette di proteggersi dalle intrusioni provenienti dall'interno della rete di fabbrica stessa. Il concetto di protezione delle celle prevede di suddividere le aree dell'impianto in celle di automazione semiautonome, all'interno delle quali i dispositivi coinvolti possono comunicare tra loro. L'accesso viene controllato all'interno della cella nel punto di contatto con il resto della rete mediante un dispositivo hardware di tipo firewall, che protegge dagli attacchi provenienti da fonti extra-cella. I dispositivi all'interno delle cella protetta possono comunicare con l'esterno, ad esempio con altre celle di produzione presenti nello stesso impianto, oppure con dispositivi esterni alla fabbrica, tramite dei canali con protocolli sicuri realizzati tramite reti private virtuale dedicate (VPN). Qualora si verificasse un incidente di sicurezza, il danno verrebbe confinato all'interno di una singola cella, anziché propagarsi immediatamente sull'intera rete. Un'altra tecnica di segmentazione molto utile è l'adozione di una zona cosiddetta demilitarizzata (DMZ), ossia una porzione di rete che ospita server raggiungibili solo in modalità unidirezionale, affinché sia impedita la comunicazione diretta tra reti esterne e rete interna di fabbrica, ma garantendo comunque lo scambio di dati sicuro tra interno ed esterno tramite il loro deposito e consultazione sui server collegati alla rete DMZ.



Esempio di segmentazione della rete a livello di singola cella produttiva per mitigare i rischi di intrusione illustrato da Siemens

Crittografia e sicurezza fisica

L'evoluzione dell'elettronica ha facilitato l'adozione di tecniche crittografiche integrandole a basso costo all'interno dei dispositivi fisici, dalle schede di rete ai PLC o ai dispositivi intelligenti di vario tipo collegabili in rete. Pertanto, un ulteriore livello di sicurezza può essere efficacemente ottenuto abilitando la sola presenza di comunicazioni crittografate all'interno della rete di fabbrica, che riduce notevolmente il rischio di attacchi dall'interno e aiuta a identificare tentativi di accesso non autorizzati. Oggi le tecniche di crittografia sono disponibili per numerosi sistemi di comunicazione classici, sia come modulo da inserire all'interno di PLC o interfacce di rete, sia come blocco funzionale software attivabile nei vari applicativi che comunicano via rete. Oltre che mediante l'attivazione della crittografia, le reti a livello fisico possono anche essere rese più sicure riducendone i punti di accessibilità fisica. Ad esempio, qualora sui dispositivi siano presente porte di comunicazione non utilizzate, la buona pratica suggerisce di disattivarle, onde evitare di offrire punti di ingresso disponibili per attività non autorizzate.

Gestione password

La sicurezza di una rete passa anche dalla gestione delle credenziali necessarie per autenticare il personale e gli applicativi necessari ad eseguire attività di configurazione, manutenzione e monitoraggio. Si tratta di un aspetto trasversale a tutta l'organizzazione aziendale che obbliga a scelte difficili che coinvolgono le tecnologie, l'organizzazione e le scienze umane. Una gestione centralizzata di password e credenziali solitamente permette di allestire un'infrastruttura più robusta per obbligare al rispetto delle regole di complessità della password e per tracciare eventuali cambiamenti o tentativi di accesso non autorizzati. Una gestione eccessivamente rigida rischia, però, di compromettere la sua accettabilità da parte degli utilizzatori coinvolti. Non c'è niente di peggio per la sicurezza che il rispetto formale di tutte le regole sul cambio regolare e complessità delle password per poi trovarsi dei 'post-it' con le credenziali di accesso incollate agli apparati o sotto la scrivania.