di **Matteo Marino**

Rafforzare la sicurezz

La numerosità e la gravità delle conseguenze degli attacchi degli ultimi anni nei confronti delle aziende evidenzia come esista una cyber battaglia silenziosa che le organizzazioni devono abituarsi a combattere quotidianamente

Le tecniche, gli obiettivi e gli effetti dei 'cyber attacchi' verso le realtà aziendali sono fortemente cambiati negli ultimi anni rispetto al passato: l'osservazione dei dati statistici dovrebbe sensibilizzare tutto il comparto industriale che, forse, non è ancora completamente consapevole della necessità di doversi difendere. La situazione in essere conduce alla neces-

La parola agli esperti

Per confrontarci con chi affronta il tema quotidianamente abbiamo chiesto a due esperti del settore come Giancarlo Carlucci, product manager Plant Solutions, PLC, Networks & I/O di Schneider Electric, e Roberto Beccalli, product manager Servo & Motion di Mitsubishi Electric di fornirci il loro punto di vista.

La prima questione che gli abbiamo posto riguarda le nuove esigenze del mercato che avranno impatto sulle scelte complessive del settore.
"Vediamo crescere molto l'attenzione legata alle tematiche di sicurezza che sorgono dall'adozione in ambito industriale della comunicazione di rete con sviluppi che trasformano l'infrastruttura industriale, tradizionalmente chiusa, in un ambiente maggiormente aperto, oltre che integrato con altre reti attive in azienda popolate da molti dispositivi" ha sottolineato Carlucci. "Tale condizione aumenta i rischi, si tratta quindi di integrare elementi di cyber security nelle soluzioni offerte al mercato". Per Beccalli "il mercato oggi richiede totale integrazione dei sistemi, semplicità di impiego, risparmio energetico e soprattutto sicurezza sulle macchine. Gli investimenti delle aziende sono infatti molto concentrati su due principali punti: risparmio energetico e sicurezza. La sfida infatti è quella di riuscire a costruire macchine sempre più performanti che ottimizzino l'energia impiegata ma soprattutto che siano sicure proteggendo l'incolumità delle persone che operano sulla macchina stessa.

Abbiamo anche chiesto come le nuove tendenze e i comportamenti sociali stiano cambiando il panorama della sicurezza hardware e software.
Carlucci ha posto in evidenza il forte impatto della diffusione, anche in ambito industriale, di modalità operative nate nel mondo consumer. Ci si riferisce per esempio alla crescente diffusione di tablet e smartphone come strumenti di lavoro: "Oggi anche noi di Schneider Electric offriamo ai nostri clienti la possibilità di operare con questi device, per esempio per interagire con le interfacce HMI da remoto, per monitorare i processi, erogare o richiedere servizi di assistenza. Questo ha delle implicazioni di sicurezza, perché tali dispositivi devono essere protetti adeguatamente e gli utenti devono essere educati per farne un uso il più sicuro possibile". Infatti molto spesso si leggono sui giornali notizie di gravi infortuni che subiscono gli operatori di vari settori. E anche "nel mondo manifatturiero, i rischi sono moltissimi" sostiene Beccalli "e spesso le persone si infortunano per malfunzionamenti della macchina oppure per negligenza delle stesse persone che non rispettano le indicazioni di sicurezza. Per limitare al massimo gli infortuni e con l'obiettivo di azzerarli, i governi intervengono con leggi e norme sempre più severe le quali per essere applicate necessitano che le aziende fornitrici di prodotti, anche di automazione, concentrino i propri reparti R&D nello sviluppo di soluzioni più adatte, sicure e affidabili sia hardware sia software".

Giancarlo Carlucci, product manager Plant Solutions, PLC, Networks & I/O di Schneider Electric

Ci siamo chiesti poi quali fossero nell'ultimo anno gli interventi più

a dove conta

www.morguefile.com

sità di un ripensamento generale riguardo alle misure di sicurezza e al tipo di comunicazione industriale da porre in atto, così come di tutte le procedure per assicurarne la stabilità.
Oggi sia i produttori sia gli operatori di automazione industriale si trovano inevitabilmente di fronte a un oggettivo e quanto mai reale pericolo, che non può più essere solo osservato.

Gestire i rischi

Numerosi studi effettuati in tutto il mondo dimostrano come i rischi legati alla presenza di minacce alla sicurezza industriale stiano aumentando esponenzialmente e l'industria dell'automazione e controllo sta cercando di seguire tale evoluzione per difendersi al meglio. Per affrontare le minacce in modo adeguato ed efficace gli esperti consigliano di progettare i sistemi mantenendo sempre una visione d'insieme, che permetta di migliorare il controllo 'end to end' durante tutte le trasmissioni dati dal livello di fabbrica a quello business e, orizzontalmente, fra i vari strati organizzativi. Di contro, gli hacker investono i loro sforzi verso le tecnologie maggiormente diffuse, per avere una più elevata probabilità di apportare danni alle aziende in modalità estensiva una volta intercettate le falle

Roberto Beccalli, product manager Servo & Motion di Mitsubishi Electric

importanti dal punto di vista tecnologico che hanno contribuito a innovare il comparto.

"Una delle scelte più importanti per un'azienda è l'adozione del giusto mezzo per le comunicazioni" conclude Carlucci. "È sempre più importante adottare standard in grado di supportare le necessità in termini di traffico dati e integrazione di device anche di differenti fornitori. Una delle tecnologie che è praticamente diventata convenzione nell'industria è lo standard Ethernet come mezzo di comunicazione tra dispositivi anche eterogenei. Oggi questa tecnologia pervade le soluzioni per i clienti e rende possibile la convergenza tra IT e OT (Operational Technology). I benefici sono numerosi, per esempio poter misurare i consumi energetici associati alla produzione aumentandone l'efficienza produttiva o rendere fattivo il concetto di smart grid e smart city per una utility". Per Beccalli "le funzioni di sicurezza richieste sono aumentate e sono in rapido incremento.
Safe Torque Off, Safety Limited Speed, Safety Operation Stop ecc. vengono ormai integrate di serie in sistemi ridondanti che garantiscono la massima sicurezza delle macchine e degli impianti. In crescendo anche la gestione della sicurezza tramite reti dedicate oppure standard ma aggiornate per supportare pienamente le funzioni di sicurezza stesse".

Le scelte per affrontare il futuro sono sempre diverse. Sentiamo quali sono le scelte di tipo tecnologico, organizzativo e gestionale di Mitsubishi dalla voce di Beccalli.

"Ovviamente un leader mondiale come Mitsubishi Electric investe molto in termini di sicurezza a prescindere da eventuali leggi o norme. L'azienda, infatti, ha come principale obiettivo la sicurezza delle persone che impiegano i suoi prodotti. Tutti i prodotti di automazione di Mitsubishi Electric integrano, infatti, funzioni di sicurezza in grado di arrivare al livello massimo SIL4 Categoria 3 e PLe, offrendo quindi soluzioni complete che soddisfano pienamente le richieste di alte performance, risparmio energetico e appunto sicurezza" sostiene Beccalli.

Provando a dare voce agli imprenditori e manager del settore. Abbiamo chiesto cosa vorrebbe un rappresentante di Mitusbishi che il Sistema Italia facesse per supportare le aziende.

"Le nostre imprese sono sempre più soggette ad attacchi esteri, soprattutto da parte di quei paesi in grado di offrire soluzioni simili a un prezzo molto più competitivo. Per riuscire a rimanere 'attraenti' sul mercato mondiale le nostre aziende devono investire in tecnologia e qualità non potendo competere ad armi pari con alcuni paesi stranieri dove i costi sono molto inferiori. Per contro, per essere un passo avanti rispetto alla concorrenza, sono necessari numerosi investimenti che dovrebbero essere pienamente supportati dal Sistema Italia, finanziando almeno in parte i progetti e aiutando gli imprenditori nella commercializzazione all'estero. Purtroppo ciò avviene molto raramente, lasciando i nostri imprenditori soli sul mercato e diminuendo quindi la nostra competitività a scapito di paesi stranieri che, invece, supportano le loro imprese nonostante non siano qualitativamente di alto livello" conclude Beccalli.

attraverso cui applicare gli attacchi. È una tendenza sempre più diffusa nel mondo industriale quella di estendere la pervasività delle reti informatiche a tutti i livelli aziendali, da quello di produzione a quello strategico, assicurando un accesso immediato per il personale alle informazioni e alle applicazioni essenziali, oltre che il collegamento tra i sistemi e il controllo integrato dei processi. Le reti industriali e i loro sistemi sono progettati tipicamente per fornire gestibilità e controllo con la massima affidabilità, tuttavia non sempre sono pronti per un'efficace gestione delle minacce provenienti da reti esterne o interne. L'integrazione dei sistemi basati su IP con quelli industriali tradizionali richiede l'installazione di soluzioni di sicurezza di rete ad hoc, per rispondere alle esigenze di ambienti che spesso sono caratterizzati da condizioni non compatibili con i tipici strumenti di salvaguardia della sicurezza impiegati in ambito IT. L'estensione dell'ICT all'area industriale apporta vantaggi irrinunciabili, ma tale processo dovrebbe essere affrontato con la dovuta attenzione. Sorvolando pure sulle questioni di carattere infrastrutturale, che devono tenere in considerazione la specifica architettura dei sistemi, la vera sfida per le organizzazioni sta nella determinazione di un livello di affidabilità degli apparati pari al 100% ottenendo al contempo la protezione completa dalle minacce e mantenendo un adeguato compromesso tra gestibilità, costi ed efficacia. Il mantenimento dei livelli di affidabilità target non è sempre un'impresa semplice a causa di numerosi fattori, come l'uso di protocolli di comunicazione aperti, la permanente esposizione degli apparati a causa della gestione realtime attraverso WAN, l'obsolescenza dei dispositivi non più compatibili con i più evoluti software di sicurezza, l'utilizzo di sistemi e apparecchiature industriali non progettati per la gestione della sicurezza di rete e il controllo da remoto. Alcune tendenze, inoltre, rendono ancora più difficile il mantenimento del necessario livello di sicurezza, per esempio la veloce evoluzione delle minace e dei target da parte degli hacker, che negli ultimi anni hanno dimostrato di poter aggredire anche ambienti apparentemente impenetrabili, così come l'inarrestabile esposizione a Internet, facilitata dalla diffusione di soluzioni mobili che aumentano i potenziali veicoli di accesso e il numero stesso degli accessi.

Trade off

La scelta della soluzione ottimale dal punto di vista dei costi dovrebbe considerare alcuni aspetti, in primo luogo il fatto che il personale delle organizzazioni deve essere in grado di effettuare il deployment dei sistemi attraverso dispositivi semplici da installare e apparati preconfigurati. La gestione dovrebbe poi poter essere eseguita completamente da remoto per più dispositivi contemporaneamente, semplificando le operazioni per le organizzazioni distribuite su più siti. Una gestione centralizzata costituisce un fattore cruciale per ridurre i costi, offrendo numerosi vantaggi, come la coerenza di configurazione, la riduzione degli errori introdotti da attività eseguite manualmente e la riduzione dei tempi di set up per far fronte a nuove minacce. Il controllo remoto riduce inoltre i periodi di vulnerabilità, favorendo la conformità alle practice e alle normative di sicurezza, la gestione degli eventi coordinati, l'analisi e il reporting consolidato. Infine, è preferibile scegliere una soluzione di sicurezza 'all in one' che includa più funzioni di sicurezza per tutti i dispositivi installati.

Requisiti funzionali di base

Quali sono dunque i requisiti funzionali di base che un'implementazione dovrebbe rispettare per assicurare gli standard di sicurezza? Innanzitutto, l'affidabilità deve essere senza compromessi. Data la natura degli ambienti industriali è essenziale per i dispositivi di sicurezza rispettare una progettazione robusta e capace di adattarsi alle condizioni di operatività tipiche dell'ambito manifatturiero, ossia in presenza di polveri, temperature estreme, umidità, vibrazioni. I dispositivi devono essere durevoli, quindi avere indici di Mtbf (Mean Time Between Failure) estremamente elevati, e le parti in movimento, come ventole e hard disk, dovrebbero essere limitate. Da una prospettiva di rete, poi, l'affidabilità è fondamentale. Pertanto i dispositivi di sicurezza dovrebbero presentare caratteristiche di alta disponibilità e ridondanza, come failover attivo-attivo o attivo-passivo a un secondo del dispositivo, routing dinamico, dial-up di backup e interfacce WAN ridondanti per stabilire percorsi alternativi. La pervasività delle minacce, la natura business critical della produzione o le reti mission critical distribuite dovrebbero determinare scelte che includano funzionalità di sicurezza integrata. Pertanto, alcuni aspetti riguardanti la sicurezza sono da considerare essenziali, come: firewall multilayer, in grado di effettuare un controllo degli accessi su tutta la rete; filtraggio attraverso 'white list', che assicurino la verifica e la prevenzione delle intrusioni; interruzioni del servizio per accessi non consentiti; gateway antivirus, anti malware e anti spyware per impianti con accesso diretto alla rete Internet; VPN (Virtual Private Network) con standard di criptografia e opzioni di identificazione. Un altro capitolo relativo alle funzionalità di base riguarda l'efficienza ed efficacia della gestione dei sistemi. Una buona gestione integrata dovrebbe comprendere l'impiego di interfacce intuitive e semplici da usare, monitoring realtime e troubleshoting, logging e reporting globale, interfacce di gestione remota, omogeneità dei dispositivi e upgrade automatici. La compatibilità costituisce, infine, un aspetto da non trascurare durante tutto il ciclo di vita dei sistemi. avendo effetti diretti da una prospettiva sia sistemica, sia economica. Soluzioni di sicurezza industriali dovrebbero infatti poter essere installate in qualsiasi configurazione di rete senza richiedere modifiche sostanziali alle infrastrutture esistenti.

Schneider Electric - www.schneider-electric.it
Mitsubishi Electric - it3a.mitsubishielectric.com/fa/it