## Cambiamenti nel mondo della sicurezza di rete

**I requisiti di sicurezza per le reti Ethernet industriali stanno rapidamente migrando dalle reti Enterprise al controllo di processo e ad altri ambienti industriali. I recenti problemi causati dal malware Stuxnet hanno dato la sveglia a tutti, e ora abbiamo bisogno di valutare con occhi nuovi come venga gestita la sicurezza nelle reti industriali. John Browett di CLPA analizza le minacce potenziali alla sicurezza delle reti industriali e come mitigarle.**

Nella marcia verso la scelta della tipologia Ethernet come rete industriale preferita, le considerazioni relative alla sicurezza della rete sono state in qualche modo trascurate. Ciò nonostante, la possibilità che le reti vengano compromesse sia dall'esterno che dall'interno di una data struttura sono molto reali.

Naturalmente, è difficile proteggere un'azienda dai rischi di hacking deliberato dall'interno: si tratta più di un problema di sicurezza del personale che di un problema di sicurezza generale della rete. In ogni caso, delle considerazioni di sicurezza sensate devono prendere in considerazione anche la possibilità che il personale possa accidentalmente collegare un dispositivo errato alla parte sbagliata di una rete, o che degli utenti non autorizzati si trovino in grado di regolare parametri chiave di processo senza rendersi conto di cosa stiano facendo. Inoltre, mentre le aziende iniziano a rendersi conto dei vantaggi offerti dall'accesso remoto agli impianti, ad esempio monitorando i processi tramite browser Web standard, si stanno anche aprendo alla possibilità di abuso della rete da parte di terzi.

In particolare, l'incidente molto pubblicizzato dello scorso anno col virus Stuxnet, che aveva attaccato i sistemi SCADA (Supervisory Control And Data Acquisition), ha dimostrato come la tipica architettura di controllo degli impianti di produzione abbia punti deboli e vulnerabilità per quanto riguarda la sicurezza. Ciò ha portato diverse aziende a mettere in dubbio i metodi tradizionali utilizzati per muovere le informazioni tra gli impianti e il livello aziendale.

Il virus Stuxnet ha cambiato il punto di attacco alle aziende dalla parte superiore, apparentemente molto sicura, al medio livello, in qualche modo più vulnerabile. A questo livello, spesso vediamo sistemi di controllo basati su PC con poca o senza alcuna sicurezza implementata, mentre alcune tecnologie vengono ancora utilizzate nonostante le ben note vulnerabilità.

I problemi di sicurezza a questo livello e al livello dei dispositivi negli impianti di produzione vengono esacerbati dal fatto che, spesso, la collaborazione tra il reparto IT e i reparti di controllo tecnico di un'azienda è limitata. Inoltre, , le minacce alla sicurezza dei sistemi di automazione e le relative responsabilità non sono sempre riconosciute con grande chiarezza all'interno della comunità tecnica e di controllo. In particolare, il caso aziendale per la sicurezza dei sistemi aziendali non è sempre ben chiaro e la comprensione dei fattori di rischio per i sistemi di automazione è limitata.

La spinta generale verso le tecnologie di rete aperte, e specialmente verso Ethernet, come mezzo in grado di dare alle aziende l'agognata libertà di scegliere le migliori tecnologie di controllo, ha esacerbato ulteriormente le minacce alla sicurezza. Gli utenti vogliono standardizzazione, flessibilità e possibilità di scelta, e tutto ciò viene offerto grazie a protocolli aperti standardizzati. Purtroppo tutto questo ha un costo che solo ora sta iniziando ad essere compreso: i protocolli aperti sono meno robusti e più vulnerabili agli attacchi. Per contro, le vecchie reti proprietarie erano molto robuste, proprio grazie alla loro non standardizzazione, ma molto meno flessibili e finivano per limitare le scelte di produzione.

Analizzando allora quello che offrirebbe la rete industriale ideale, possiamo creare un elenco di desiderata che offre la robustezza del vecchio combinata con la flessibilità del nuovo. Questo elenco di desiderata include un cablaggio comune, connettori standardizzati, standard aperti, facilità di configurazione, sicurezza massima possibile e ridotta vulnerabilità agli attacchi.

Pensando a come potremmo adattare l'Ethernet industriale in modo da soddisfare quanto richiesto dall'elenco di desiderata, vale la pena di rivisitare la nostra definizione di Ethernet, dato che non c'è singola parola nel linguaggio della rete che sia stata così male utilizzata in quanto ombrello sotto il quale includere le tecnologie, standard e applicazioni più

disparate. E il luogo migliore da cui iniziare è lo stesso modello OSI a sette layer.

Il layer 1, quello fisico, definisce tutte le specifiche elettriche e fisiche dei dispositivi. In particolare, definisce la relazione tra un dispositivo e il mezzo fisico. Il layer 2 è quello del data link, che garantisce i mezzi funzionali e procedurali per trasferire i dati tra entità di rete e rilevare ed eventualmente correggere gli errori che possono verificarsi sul layer fisico. È a questo livello che Ethernet è definito come protocollo di rete in base allo standard IEEE 802.3.

Negli anni, Ethernet è diventato sinonimo della suite TCP/IP, ma uno non implica necessariamente l'altro. IP è definito sul layer di rete (layer 3) del modello OSI. Questo layer offre i mezzi funzionali e procedurali per il trasferimento di sequenze di dati di lunghezza variabile da una fonte a una destinazione tramite una o più reti. Il layer di trasporto (layer 4) garantisce il trasferimento trasparente dei dati tra utenti finali, e definisce TCP e UDP.

Il layer di sessione (layer 5) controlla le connessioni tra computer, mentre quello di presentazione (layer 6) trasforma i dati in modo da fornire un'interfaccia standard per il layer di applicazione (layer 7) in cima al modello. È a questo livello che troviamo le applicazioni tipiche come FTP, HTTP, RTP, SMTP, SNMP ed altre ancora. In breve, quando si tratta di lavorare come architettura di comunicazione nelle reti industriali, Ethernet può ben poco senza i layer sovrastanti.

Non tutte le offerte di Ethernet industriale implementano lo stack Ethernet allo stesso modo. Sul layer di applicazione, le diverse organizzazioni per l'Ethernet industriale implementano i propri kernel e protocolli, che definiscono gran parte dei vantaggi funzionali delle relative tecnologie. Ciò nonostante, dal punto di vista della sicurezza quello che è veramente interessante sono i layer inferiori, più vulnerabili.

In base al modello a sette layer, basta che un layer ceda a un attacco per compromettere l'intero sistema di comunicazione, potenzialmente anche senza che gli altri layer si rendano conto dell'esistenza di un problema. La sicurezza è solida solo quanto l'anello più debole della catena.

Ci sono diversi prodotti di sicurezza discreti disponibili che funzionano bene, ma uno dei problemi maggiori nell'arena industriale è l'implementazione di sistemi di sicurezza strettamente integrati senza incorrere in costi eccessivi né imporre livelli di complessità che rendano il sistema difficile da manutenere e complicato in termini di assistenza. Inoltre, le soluzioni di sicurezza standard commercialmente disponibili sono raramente adatte al rigori degli ambienti industriali.

In termini di tecnologia di rete, è stato fatto molto per rendere il layer 2 più sicuro, ma nelle implementazioni più classiche dell'Ethernet industriale, è stato fatto ben poco per affrontare le debolezze del layer di rete (layer 3) e del layer di trasporto (layer 4). Come per l'implementazione Ethernet per uffici, la gran parte delle tecnologie Ethernet industriali sono sempre centrate su IP al layer 3 e TCP/UDP al livello 4.

Gran parte degli impianti Ethernet industriale implementano la sicurezza perimetrale (servizi firewall) nei punti in cui si collegano ad altre reti per garantire la protezione su questi layer più vulnerabili. I firewall filtrano gli indirizzi IP sorgente e di destinazione e i numeri di porta del protocollo (ad esempio le porte TCP e UDP) per limitare ulteriormente il traffico che può accedere a una rete Ethernet. Il filtraggio dei pacchetti può essere implementato anche tra comunità di rete conosciute, e in alcuni casi il filtraggio ha a che vedere con indirizzi di dispositivo e porte di applicazione molto specifici in modo da garantire un layer di sicurezza all'accesso univoco per un dispositivo e un applicazione collegati. Tuttavia, nonostante questo, nelle implementazioni classiche di Ethernet industriale, i layer 3 e 4 sono sempre molto vulnerabili agli attacchi.

Per CC-Link il discorso è diverso. CC-Link IE (Control and Communication Link Industrial Ethernet) è stato sviluppato da CLPA come rete gigabit Ethernet completamente integrata per l'automazione industriale, definendo così la nuova soglia per gli standard aperti per l'Ethernet industriale. CC-Link IE combina il meglio delle diverse tecnologie esistenti per applicarlo ad un sistema di rete industriale ottica oppure in rame con architettura ridondante, che consente di trasferire i dati in maniera estremamente veloce e affidabile tra dispositivi di campo ed altri controller, tramite collegamenti Ethernet. La velocità di segnalazione di 1 Gbps ridefinirà le aspettative degli utenti e le capacità dei sistemi; si tratta di un valore più che sufficiente a soddisfare le attuali necessità di comunicazione in tempo reale dell'attuale settore manifatturiero.

Ci sono varianti di CC-Link in grado di affrontare i requisiti di controllo a tutti i livelli della rete di automazione. Al livello di controllo, abbiamo CC-Link IE Control. Al livello dei dispositivi, abbiamo CC-Link IE Field e CC-Link IE Motion. E, ovviamente, c'è la stretta integrazione con fieldbus CC-Link.

È fondamentale la differenza tra CC-Link IE e le implementazioni convenzionali, grazie alla definizione di un "Protocollo in tempo reale" aperto all'interno dei layer dello stack. Grazie a questo approccio nell'implementazione di questi layer nello stack Ethernet, CC-Link IE realizza i benefici elencati dai nostri desiderata per le tecnologie di rete.

Utilizza connettori Ethernet standard, è facile da configurare ed è molto robusto. Inoltre, è uno standard aperto, quindi gli utenti godono di libertà di scelta nella selezione delle migliori tecnologie per la componentistica. Fondamentale dal punto di vista della sicurezza è che offre per sua natura la massima sicurezza possibile, ed è quindi meno suscettibile di attacchi. Questi sono vantaggi significativi rispetto ad altre implementazioni di Ethernet industriale. Il fattore differenziante chiave è una knowledge base aperta ma controllata per la tecnologia di rete. Di conseguenza, mentre le aziende in buona fede possono implementare la tecnologia su base aperta, i "cattivi" avranno maggiori difficoltà ad infiltrarsi.

I requisiti di sicurezza per le reti Ethernet industriali continuano ad evolversi, con sempre più requisiti sofisticati che stanno rapidamente migrando dalle reti Enterprise al controllo di processo e ad altri ambienti industriali. Ovunque si trovino installazioni di rete, le aziende devono verificare la probabilità di attacchi alla rete nonché il rischio associato ad ogni attacco. In qualsiasi caso, al crescere dell'importanza della sicurezza, le aziende devono cercare di mitigare, ridurre o eliminare i rischi secondo quanto richiesto in ciascun ramo della topologia di rete. Grazie al suo approccio aperto agli standard e alla tecnologia di comunicazione proprietaria, l'implementazione CC-Link IE di Ethernet industriale rappresenta un'opzione molto interessante nella spinta alla massimizzazione ed ottimizzazione della sicurezza di rete.

## Informazioni su CLPA

CLPA (CC-Link Partner Association) è un'organizzazione internazionale i cui membri sono oltre 1.700 aziende in tutto il mondo. L'obiettivo comune dei partner è la promozione dello sviluppo tecnologico e dell'adozione della famiglia di tecnologie aperte di rete CC-Link. Sono ormai disponibili più di 1.200 prodotti, offerti da oltre 250 fabbricanti. CC-Link è già il principale protocollo fieldbus industriale in Asia e sta diventando sempre più diffuso in Europa e in America. La sede europea è in Germania, con uffici in tutto il continente.

---

## Editor Contact

DMA Europa Ltd. : Glenda Terenzi

Tel: +44 (0)1299 405454
Fax: +44 (0)1299 403092
Web: www.dmaeuropa.com
Email: glenda.terenzi@dmaeuropa.com

## Company Contact

CLPA Europe : John Browett

Tel: +44 (0)776 833 8708
Fax: +49 (0)2102 532 9740
Web: www.the-non-stop-open-network.com
Email: john.browett@clpa-europe.com