UNO SGUARDO SUGLI STRUMENTI DI CYBER SECURITY PIÙ DIFFUSI

Wireless e cyber security industriale: opportunità e rischi

La connessione in rete, cablata o wireless, moltiplica l'efficienza di impianti e macchinari che possono essere gestiti in remoto e godono dell'accesso rapido ad informazioni e dati. Se crescono le minacce informatiche, aumenta anche la disponibilità di soluzioni e strumenti per la sicurezza.

A cura del Gruppo Specialistico Wireless Industriale di Anie Automazione

I controlli industriali si stanno integrando sempre di più con tecnologie dell'informazione distribuita. Stazioni HMI, PLC, DCS e strumenti per la configurazione e la manutenzione tecnica in loco sono supportati da hardware e tecnologie standard disponibili a chiunque sul mercato. Ethernet e Internet sono diventati molto popolari anche nell'ambito di impianti industriali.

I sistemi di controllo stanno iniziando a integrare sistemi di comunicazione wireless (Wi-Fi, ZigBee, Bluetooth ecc.). Queste tendenze riducono i costi degli impianti, non sono necessari cablaggi fisici con linee in rame o fibra ottica. Le espansioni dell'impianto o l'aggiunta di un modulo nel macchinario sono ottenute in modo veloce aumentando le funzionalità e incrementando l'integrazione con le varie parti della produzione o processo.

Ancora più evidenti sono i vantaggi offerti dalla rete Internet: gli impianti e i macchinari possono essere raggiungibili da remoto in pratica ovunque siano installati a livello mondiale.

Le stesse tendenze di **apertura e interconnettività** dei sistemi hanno fatto diminuire le protezioni da minacce esterne, rendendoli più vulnerabili alle intrusioni informatiche da parte di persone non autorizzate o con intenzioni di compiere reati. Gli attacchi più pericolosi possono portare al danneggiamento della produzione, creando blocchi ai sistemi di controllo, oppure alla sottrazione della cosa più preziosa all'interno di una struttura industriale e cioè le informazioni sensibili quali progetti e know-how oltre che alla divulgazione di archivi storici con i dati aziendali sensibili.

Gli effetti che ne derivano non sono solamente di perdita economica della produzione compromessa, ma in alcuni casi è in pericolo la sicurezza stessa degli operatori e delle infrastrutture, effetto dovuto alla perdita di controllo del macchinario o del processo.

Questi aspetti riguardanti sicurezza e danno economico, a volte ingente, sono molto sentiti dai proprietari e gestori di impianti e macchinari.

I *cyber attack* sono sempre più frequenti proprio per la promiscuità della rete Internet.

Reti prettamente IT di gestione dati, reti private domestiche, reti industriali di gestione automazione di fabbrica sono tutte virtualmente collegate ad un'enorme rete globale che è Internet.

Un caso comune

Ad esempio i PC portatili sono molto vulnerabili. Vediamo di seguito uno scenario molto comune oggi a livello industriale.

Un dipendente si collega con il proprio PC alla rete aziendale con tutte le sicurezze offerte dal *firewall server* di rete; vengono controllate password e identificativo utente ad ogni accesso rete, inoltre *antivirus* e *antispyware di rete* proteggono da virus software e programmi maligni che aprono ponti di collegamento a intrusi esterni. Tutto questo crea un ambiente protetto e sicuro con mezzi di protezione sempre aggiornati ed efficienti. Appena il dipendente si collega a reti wireless pubbliche o al proprio *access point* di casa, decadono tutti i meccanismi di sicurezza che erano propri del collegamento Lan presso l'ufficio dell'azienda.

Non è detto che il PC portatile non possa essere stato infettato da virus software o essere stato vittima dell'installazione indebita di un pro-

►

A FIL DI RETE
www.anieautomazione.it

gramma *spyware* o *trojan*.
Sia i virus che i programmi maligni creano teste di ponte per collegamenti esterni non autorizzati, forzando dall'interno i sistemi di sicurezza. È indispensabile l'implementazione di una strategia per la cyber security ottimizzata contro intrusioni e attacchi cibernetici.

Ambienti wireless e protezioni

Bisogna distinguere due principali tipi di reti industriali. Le Lan wireless di fabbrica con una classe di IP comune principalmente usate per connessioni locali ethernet punto-punto o con struttura client access point. Le Wan cioè le connessioni che escono dall'ambito della fabbrica che sfruttando Internet si connettono a PC o server remoti.

ANIE Automazione
e il gruppo specialistico Wireless

Il gruppo specialistico Wireless Industriale fa parte di ANIE Automazione, Associazione Italiana Automazione e Misura (www.anieautomazione.it), e vi partecipano i principali fornitori di tecnologia ed esperti del settore. Il gruppo nasce con le seguenti finalità: diffondere informazioni chiarificatrici su caratteristiche e applicabilità della tecnologia wireless; interfacciarsi con enti deputati alla regolamentazione dell'uso delle varie apparecchiature per condividere e supportare gli sviluppi normativi; quantificare e studiare il mercato.

Nel caso delle reti Lan wireless di fabbrica per proteggere il collegamento i sistemi più efficaci e comunemente usati sono le password di connessione rete.
Attualmente sono due le tipologie di chiavi di protezione maggiormente utilizzate: Wep e WPA.
La chiave Wep è stata introdotta e resa ufficiale nel 1999 ed è oggi diventata obsoleta e poco sicura. Ad oggi si consiglia infatti l'utilizzo della chiave WPA che, essendo di recente introduzione, garantisce una maggiore protezione e tutela dei dati.

L'evoluzione di questo sistema di protezione è **la chiave WPA2**, che si sta affermando come nuovo standard di sicurezza per le connessioni wireless.
I dispositivi wireless per uso industriale, quali Access Point, devono sicuramente gestire il protocollo 802.11i e nello specifico WPA2 a 128-bit.
Nascondere il nome della rete wireless in modo che non sia visibile a tutti è un altro provvedimento sicuramente da impostare nell'access point. Questa funzione aumenta la sicurezza contro le connessioni non autorizzate e prende il nome di **SSID Hiding**.
Il sistema **IEEE 802.1X/Radius** permette di avere i dati cioè le credenziali dei soggetti abilitati a collegarsi all'Access Point wireless; oltre alla maggior sicurezza si ha un unico database con i dati utenti, **l'amministratore IT può gestire gli accessi in modo centralizzato** e in un **unico file**.
Impostare dei filtri sul transito dei pacchetti dati fissando l'identità di chi può trasmettere e quindi è abilitato al transito dei dati aumenta la sicurezza della connessione wireless. Questa funzione prende il nome di *packet access control & filtering*.
Solo i dispositivi abilitati possono collegarsi ad un access point e farvi transitare i dati.

VPN per l'industria

Nel caso delle reti Wan wireless di fabbrica con collegamenti esterni attraverso Internet o per reti Lan wireless di fabbrica particolarmente riservate e importanti, esiste un sistema di sicurezza e riservatezza della comunicazione dati ancora più avanzato delle semplici password.
Questo sistema è reso possibile dall'implementazione della **VPN (Virtual Private Network)**.
Con tale meccanismo si crea un tunnel di collegamento virtuale che sfrutta i normali protocolli di trasporto dati TCP o UDP nel quale transitano gli stessi criptati.
Le chiavi di decodifica risiedono nei due end point: il PC client e il router server.
Il PC client si collega al router server e poi da quest'ultimo si ottiene l'accesso a PLC o PC remoti. Le chiavi di decodifica dati contenute nei certificati rimangono nel PC client e nel router server, non vengono trasmesse. Quindi i dati in transito anche se intercettati, non possono essere de-criptati poiché l'intruso non possiede i certificati corretti.
Ad oggi **il tunnel VPN che utilizza i certificati** è ritenuto il sistema più sicuro per trasmettere dati che devono rimanere privati, anche e soprattutto attraverso Internet.

Vi sono molti software *open source* che permettono di implementare una VPN sfruttando appunto i certificati e dando quindi la possibilità di creare soluzioni personalizzate estremamente flessibili alle funzionalità richieste e libere da ogni royalty.
I certificati vengono creati da un'autorità virtuale che è l'unico ente abilitato a rilasciarli con le relative chiavi di codifica criptatura dati.
Ad oggi **i router per uso industriale hanno a bordo le funzionalità per gestire i protocolli VPN** e la gestione dei relativi certificati.

Firewall e Nat

Un altro componente fondamentale e necessario a bordo dei router industriali è la funzione di **firewall**, cioè la possibilità di **decidere le regole di transito dati**. Vengono lasciati passare i dati provenienti da fonti stabilite ad esempio un indirizzo IP ritenuto affidabile e vengono bloccati tutti gli altri dati non compresi nelle suddette regole.
Altro esempio è il blocco di protocolli particolari quali i Ping di test provenienti da indirizzi IP esterni. Questo sistema è anche chiamato **firewall hardware**, aumenta la sicurezza e rafforza le azioni dei firewall software residenti nei server o PC end point. In ambito industriale spesso gli end point di collegamento sono PLC o HMI che non hanno a bordo un firewall software: ecco che il firewall hardware del router assume un'importanza vitale.
Altra funzione molto importante del router è la funzione **Nat Network Address Translation**: in pratica si **nasconde l'indirizzo IP privato** cioè interno della rete Lan locale, presentando alla rete Wan esterna un altro indirizzo IP stabilito.
In pratica chi riceve il pacchetto dati pensa che siano provenienti dall' indirizzo IP Wan pubblico.
Gli IP interni con la funzione Nat rimangono raggiungibili se si conoscono o da comunicazioni broadcast indirizzate a tutti gli IP.
Anche in quest'ultimo caso è necessario combinare la funzione Nat alla protezione offerta dal firewall hardware.

Soluzioni diversificate

In conclusione, per avere una rete aziendale veramente conforme ai criteri di sicurezza imposti dalla cyber security, bisogna **implementare più sistemi di sicurezza distribuiti**. La frammentazione e la personalizzazione delle misure di sicurezza, aumentano le probabilità di inviolabilità della rete.
Ogni ramo della rete deve avere una protezione specifica e personalizzata.
A questo scopo i **router industriali distribuiti** con tutte le loro funzioni di sicurezza assolvono il compito di proteggere ogni segmento di rete.
La combinazione con protezione software nei server e nei PC quali firewall software e antivirus completano il quadro di protezioni attuate.