La sicurezza nelle reti industriali

Massimo Giussani (*)

Fonte: Vimar

Il termine 'sicurezza' si presta alla traduzione di due differenti vocaboli inglesi, pur se simili nel significato: 'safety' e 'security'. Nel contesto dell'automazione industriale, il primo è più legato a un concetto di protezione da guasti, danni, errori, incidenti che possono mettere in pericolo l'incolumità degli impianti o del personale. Il concetto di security, invece, è maggiormente improntato alla gestione degli accessi e alla protezione delle informazioni. Il fatto che in italiano sia possibile tradurre questi due lemmi con un unico vocabolo è indicativo di una compenetrazione dei significati, che riflette una sovrapposizione di ambiti applicativi.

È imprudente ritenere sicura una rete industriale per il solo fatto che non mostra connessioni palesi con il mondo esterno

Anche se ci si limita al contesto delle sole reti telematiche, il termine security copre una vasta gamma di discipline volte a tutelare la riservatezza, l'integrità e l'accessibilità (la cosiddetta 'triade' CIA: Confidentiality, Integrity, Availability) delle informazioni elaborate o memorizzate dai sistemi digitali. I molteplici aspetti della security contemplano la creazione e la messa in pratica di una politica della sicurezza, il controllo degli accessi e la configurazione degli elementi dell'infrastruttura di rete e dei sistemi di elaborazione con il duplice scopo di impedire che informazioni di valore vengano carpite all'azienda e che dati malevoli (codice dannoso o false informazioni) vengano introdotti causando danni.

La messa in sicurezza di una rete, sia essa aziendale o industriale, richiede una serie di passi la cui singola importanza non deve essere sottovalutata. Innanzitutto, è necessaria un'attenta valutazione dei rischi, che permetta di identificare le aree vulnerabili e i possibili rimedi; successivamente, si stila una 'policy' di sicurezza, stabilendo le misure che possono essere prese per incrementare la sicurezza della rete e i comportamenti da tenere per evitare di inficiarne i benefici. Da non sottovalutare è la fase di salvataggio delle informazioni, tra i quali sono da includere i dati di configurazione dei dispositivi sul campo. La fase più importante, però, sembrerebbe anche scontata: mettere in pratica le misure stabilite, facendo rispettare in maniera rigorosa da tutti i dipendenti la policy di sicurezza intrapresa. Verifica, manutenzione e aggiornamento rappresentano le facce della quinta fase della gestione di una rete sicura.

Vulnerabilità delle reti industriali

Un impianto produttivo tipo dispone di almeno due tipologie distinte di rete: una aziendale tradizionale, cosiddetta da ufficio, che viene impiegata per la contabilità e la gestione d'impresa in generale; una di controllo, che si trova sul piano di fabbrica e si occupa della produzione vera e propria, generalmente comunicando con i sistemi di datalogging e di gestione d'impresa.

La rete industriale integra tutta una serie di componenti che hanno una lunga storia d'immunità agli attacchi informatici provenienti dall'esterno. Il motivo è che in passato questi dispositivi erano quasi esclusivamente componenti proprietari gestiti da sistemi operativi creati su misura, spesso privi di

connessione con il mondo esterno. Un sistema di questo tipo era 'sordo', ma allo stesso tempo invulnerabile alle minacce dei moderni hacker. Con l'introduzione delle architetture aperte sul piano di fabbrica si è avuto lo spiacevole effetto collaterale di esporre anche la rete di controllo industriale agli attacchi informatici. Per quanto gli studi in merito siano scarsi e facciano riferimento a una casistica ancora limitata e necessariamente parziale, è significativo il fatto che il numero di attacchi sia aumentato rapidamente in corrispondenza del passaggio al nuovo millennio. La spiegazione di questo va cercata nel massiccio rinnovo del parco macchine associato alla risoluzione del problema Y2K (Anno 2000): i nuovi sistemi dotati di interfacce e protocolli aperti, come Ethernet e la suite TCP/IP, e di sistemi operativi commerciali, quali Windows, sono divenuti visibili e vulnerabili agli attacchi esterni.

Anche l'origine degli attacchi informatici alle aziende pare aver subito un'inversione di tendenza negli ultimi anni: la maggioranza non è portata a termine dall'interno, da impiegati scontenti, ma arriva dall'esterno, spesso sottoforma di agenti automatici che non mirano specificamente all'applicazione industriale, ma la colpiscono come se si trattasse di un sistema informatico tradizionale. A peggiorare le cose ci si mette il fatto che le reti industriali, in particolar modo quelle più vicine al campo, presentano una topologia e un assortimento tale di componenti eterogenei da rendere impraticabile l'adozione di misure di protezione capillari. Per difficoltà di cablaggio, per obsolescenza di alcune unità o per le difficoltà di aggiornamento, che comporterebbero l'arresto della produzione, è più facile trovare componenti esposti agli attacchi in una rete di processo che in una d'ufficio. A conferma di ciò, i rapporti sugli attacchi a questo tipo di rete fanno spesso riferimento a virus e 'malware', che su Internet hanno da tempo esaurito il proprio ciclo di vita. È questo un segnale di come molte aziende non mettano correttamente in pratica le politiche di sicurezza, ritenendo erroneamente di essere al sicuro dagli attacchi dei virus e dei 'worm' che affliggono la rete Internet pubblica.

Le fonti del contagio

Il falso senso di sicurezza degli utenti industriali è spesso causato dall'erronea convinzione di avere un sistema di controllo sconnesso dalle reti esterne, pertanto non suscettibile di attacchi. In realtà, i punti di accesso a una rete posta sul piano di fabbrica sono molteplici anche quando la rete è protetta da un firewall (figura 1). Un esempio sono le connessioni che possono avvenire dietro le protezioni perimetrali, come lo scambio di dati diagnostici con il portatile di un tecnico che sta analizzando un guasto. Sebbene venga connesso alla rete interna, separata dal mondo esterno, il notebook, la cui gestione della sicurezza non è controllata dall'impresa, può essere stato esposto agli attacchi di più virus prima di entrare in azienda. Anche un notebook interno potrebbe essere utilizzato impropriamente dai dipendenti, se non si è fatta debita formazione riguardo ai rischi relativi alla sicurezza. CD, DVD e penne USB, usati per trasferire file da computer non sicuri ai sistemi sicuri della rete di controllo, sono un'altra fonte di potenziali infezioni, ma possono anche essere usati per carpire dati riservati, se il loro uso non viene debitamente limitato.

Le connessioni wireless sono per loro natura maggiormente esposte al rischio d'intercettazione, dato che non è necessario accedere fisicamente al sistema informatico e nemmeno trovarsi in azienda per carpire informazioni non debitamente criptate. L'adozione di protocolli di cifratura avanzati e il monitoraggio capillare del traffico da e verso le stazioni wireless possono ridurre i rischi provenienti da questa porzione di rete.

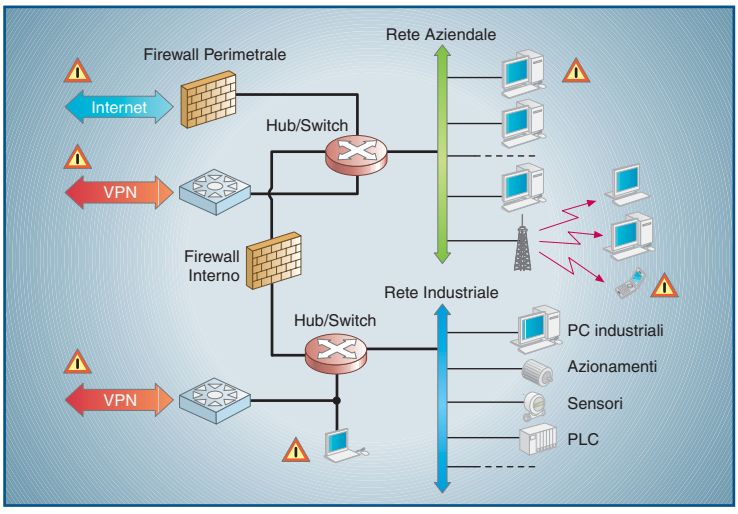

Figura 1 - Una normale rete aziendale presenta tutta una serie di punti d'accesso sfruttabili per carpire informazioni e immettere codice malevolo, arrivando anche alla rete di fabbrica

Le connessioni alle reti proprietarie di fornitori o produttori non sono sotto il diretto controllo dell'azienda per quanto riguarda le misure di sicurezza: è necessario trattarle come se fossero 'ostili', filtrando opportunamente il traffico in ingresso e in uscita. Le reti private virtuali (VPN) sono sicure solo se tutti i nodi della rete sono debitamente protetti; in caso contrario, diventano un mezzo per veicolare, paradossalmente in maniera sicura su connessioni criptate, virus e worm che possono attaccare l'infrastruttura di rete e compromettere irrimediabilmente la sicurezza del sistema.

Non vanno poi trascurati i comportamenti azzardati da parte del personale, che magari in buona fede sceglie scientemente di scavalcare le misure di sicurezza per collegarsi a Internet o inviare messaggi di posta.

Protezione della rete

Le reti industriali necessitano, dunque, anch'esse di una protezione che va al di là del singolo firewall. Va tuttavia os-

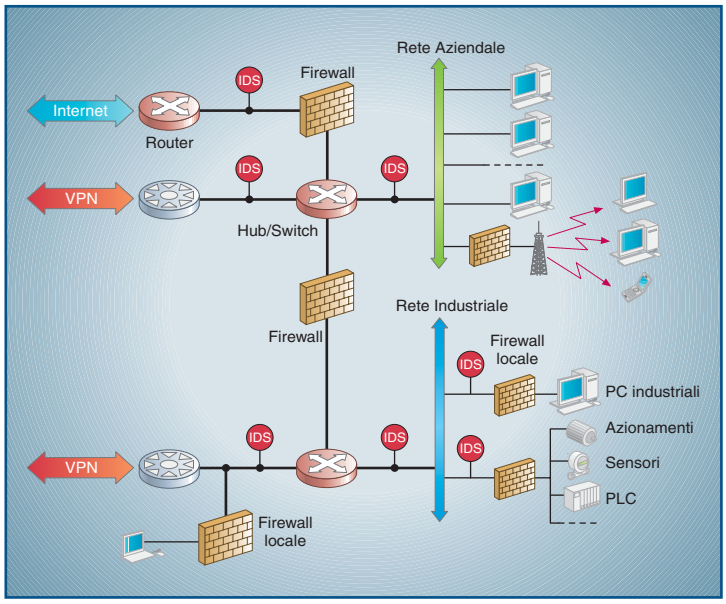

Figura 2 - L'impiego di router, firewall e agenti di rilevamento delle intrusioni (IDS) a più livelli dell'infrastruttura di rete permette di incrementarne il livello di sicurezza, aumentando però la complessità di cablaggio e manutenzione

servato che, per la loro particolare costituzione, queste reti presentano problematiche di sicurezza che si differenziano da quelle di una normale rete informatica aziendale. Se un sistema di tale tipo può andare incontro al rischio di una perdita di dati, mitigabile ricorrendo a salvataggi periodici, i rischi di un'intrusione malevola in un sistema di controllo industriale contemplano l'interruzione della produzione, pericoli per l'incolumità del personale e dei macchinari e persino incidenti che possono coinvolgere la popolazione o l'ambiente. Le differenze si manifestano anche sul piano tecnico, dato che i dispositivi che popolano una rete di controllo sono in genere molto diversi tra loro per tipologia ed evoluzione tecnologica. Sul piano di fabbrica trovano posto PC industriali per la supervisione e il controllo di processo, postazioni di lavoro per il controllo di qualità e la diagnostica, server che ospitano gli archivi storici della produzione, dispositivi di controllo distribuito più o meno intelligenti, oltre ovviamente ad azionamenti e sensori vari.

Il livello di sofisticazione tecnologica è altrettanto variegato e per alcune tipologie di dispositivo soluzioni di protezione decentrate come l'installazione di firewall software ('personal firewall'), agenti di rilevamento intrusione (IDS, Intrusion Detection System) e programmi antivirus sono addirittura improponibili. La complicazione del cablaggio, le difficoltà di aggiornamento e il rischio di un'interruzione della produzione per operazioni di manutenzione sui singoli nodi hanno portato alla creazione di sistemi di protezione che fanno da tramite, nella maniera meno invasiva possibile, tra interi segmenti della rete di processo e le connessioni verso la rete aziendale o le stazioni wireless. Questi 'centri di distribuzione' sono in grado di mettere in atto misure attive e passive di analisi del traffico e provvedono a smistare i dati di processo verificandone mittenti, destinatari e contenuti.

La rete di controllo può essere dotata di una singola protezione perimetrale, con il duplice vantaggio di non richiedere cablaggi aggiuntivi e di poter essere messa in opera senza fermi macchina (figura 3). Per incrementare il livello di sicurezza si può adottare una soluzione di protezione perimetrale frazionata, che isola i sottosistemi principali per mezzo di un dispositivo che funge da nodo di smistamento (figura 4). L'alterazione della topologia rende però inevitabile mettere mano al cablaggio delle sottoreti con tutte le conseguenze del caso. Una protezione ancora più capillare richiederebbe interventi dedicati per ciascun sottosistema, con firewall hardware e agenti di rilevamento delle intrusioni installati nei punti chiave della rete. Lo svantaggio di un simile approccio è ovviamente rappresentato dai costi d'installazione e manutenzione.

L'importanza di una buona politica della sicurezza

La protezione della rete industriale è strettamente correlata a un'adeguata protezione della rete aziendale e dei dispositivi dell'infrastruttura di rete: se un hacker prende il controllo di un router o di uno switch, potrà causare danni a prescindere dal livello di protezione che si trova più a valle. Questi dispositivi possono infatti essere utilizzati per creare false identità, intercettare i pacchetti in transito e inviarli surrettiziamente a terzi. È dunque necessario tenere aggiornati i sistemi operativi di router e switch e dotarli di software in

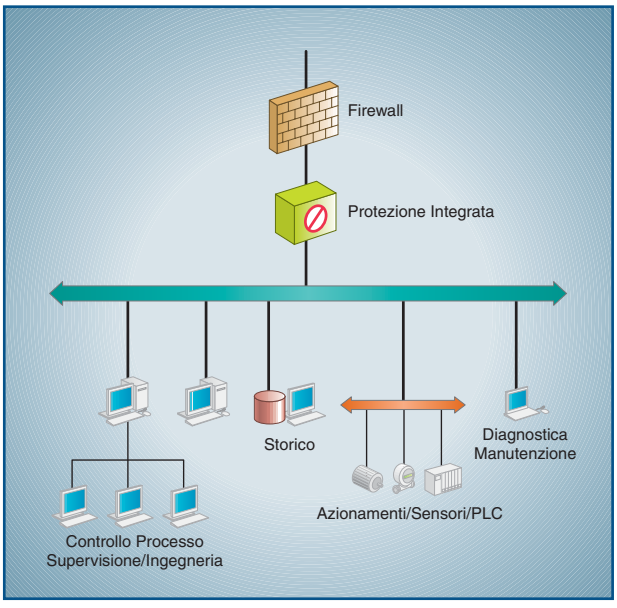

Figura 3 - Un compromesso tra sicurezza e costi è rappresentato da una protezione perimetrale della rete di controllo, per mezzo di un dispositivo che incorpora i principali servizi di sicurezza e disaccoppia la rete di controllo da quella aziendale connessa all'esterno

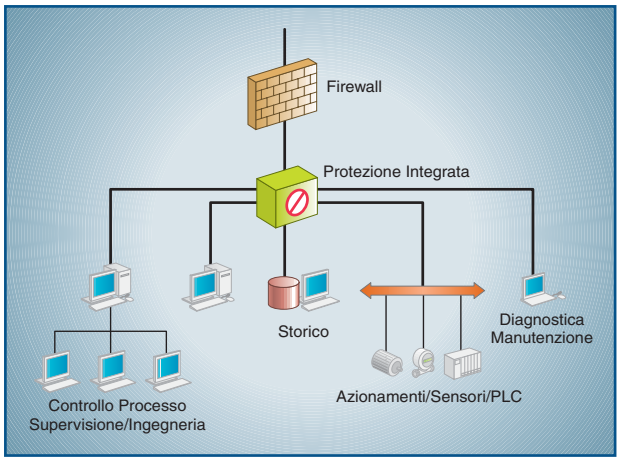

Figura 4 - Disaccoppiare i singoli sottosistemi della rete di controllo è possibile con una soluzione di protezione perimetrale frazionata: occorre ricablare parte dell'impianto con possibilità di un fermo macchina durante la fase d'installazione

grado di gestire le minacce provenienti dall'esterno. Per minimizzare la vulnerabilità dei sistemi operativi dei PC connessi in rete è necessario provvedere a disabilitare tutti i servizi che non vengono espressamente utilizzati, chiudendo anche tutte le porte non strettamente necessarie. La messa in sicurezza del sistema operativo, dei programmi di navigazione sul Web, dei client di posta elettronica e delle altre applicazioni che si interfacciano con l'esterno deve essere effettuata prima di connettere il PC a una rete sicura.

Tutti questi accorgimenti contribuiscono a creare una rete più sicura, ma diventano inutili senza la collaborazione attiva del personale dell'azienda, che deve essere opportunamente sensibilizzato sulle problematiche inerenti la sicurezza e si deve impegnare a rispettare diligentemente la policy adottata.

È questo l'anello più debole della catena: impiegati che usano password 'deboli' scritte su post-it messi in bella mostra sul bordo del monitor; dipendenti che inseriscono chiavette USB per provare l'ultimo gioco scaricato dalla rete domestica, con relativo carico di malware, dopo aver disabilitato l'antivirus personale, perché "rallentava il sistema"; personale tecnico che dal piano di fabbrica si collega direttamente a Internet per scaricare una patch, scavalcando fisicamente il firewall. È compito della dirigenza fare in modo che tutti gli impiegati siano debitamente informati sul significato delle misure di sicurezza intraprese e sulle conseguenze che eludere tale misure può comportare.

Il ricorso a riunioni periodiche sulla sicurezza e a questionari può aiutare a far prendere coscienza del problema e a verificare l'effettiva consapevolezza dei rischi connessi. ■

(*) Bibliografia: Tanenbaum, Andrew S., "Reti di calcolatori", 4ª edizione, Pearson Italia
Cole, Eric; Conley, James W., "Network Security Bible", Wiley
AA.VV., "Inside Network Perimeter Security", SAMS
Byres, Eric; Leversage, David; Kube, Kate "Security incidents and trends in Scada and Process industries"