I bus di sicurezza

Ilaria De Poli

I tragici avvenimenti di questi ultimi anni, dall'11 settembre americano, a Madrid, a Londra, solo poco tempo fa, hanno fatto sì che tutti noi prendessimo piena coscienza dell'importanza della sicurezza. Guerre e pericoli che sembravano ormai far parte del passato, o che pensavamo legate a realtà lontane dalla nostra quotidianità, a civiltà ritenute ancora 'poco sviluppate', a interessi di altre parti del mondo, sono venute invece a bussare alla nostra porta, più vicini che mai. Ci siamo resi conto di quanto ogni questione legata alla sicurezza sia da considerarsi 'globale', non più localizzabile in una singola parte del globo, non più confinabile entro un perimetro prestabilito. E questo non solo da un punto di vista 'materiale': Internet e il cyberspazio sono infatti luoghi, virtuali, nei quali la sicurezza è di importanza fondamentale e sempre più lo sarà quanto più la vita di apparati strategici, industrie, intere amministrazioni statali sarà affidata al corretto funzionamento di sistemi di controllo e gestione sofisticati e automatizzati, dove la tecnologia svolge un ruolo cruciale.

Safety e security: due priorità dalle quali dipende non solo la sicurezza dei dati trasmessi in rete, ma l'esistenza stessa della fabbrica

Questo discorso vale anche e ancora di più per le aziende, qualsiasi sia il loro business e a qualunque livello dell'infrastruttura di rete, da quello informatico di gestione, a quello della produzione e dei processi, coinvolgendo dunque fieldbus e reti di fabbrica :"Oggi non esiste più, se mai c'è stato, un 'dentro' la fabbrica separato da un 'fuori' pericoloso", ha sottolineato Gigi Tagliapietra di Clusit, associazione italiana per la sicurezza informatica, in occasione del seminario intitolato "La security nei sistemi di controllo e automazione nelle reti e infrastrutture", promosso da Anipla e coordinato da Enzo Maria Tieghi di Vision Automation. Con l'avvento, infatti, della cosiddetta 'fabbrica virtuale', dove tutti i processi sono connessi in rete e alle reti sono collegati produttori, fornitori, clienti e collaboratori, nulla può più dirsi totalmente 'al sicuro'.

Una volta che i pirati informatici sono penetrati in un apparato, tutti i sistemi ad esso collegati sono a rischio

Attacco e difesa

Le tipologie di 'attacco' che una rete industriale può subire sono, come nell'informatica, svariate e colpiscono le informazioni nelle loro caratteristiche fondamentali di integrity (integrità), ossia accuratezza e completezza, availability (disponibilità), cioè possibilità di accedere ai dati quando necessario, e confidentiality (riservatezza). Virus e worm, ad esempio, causano i 'denial of service' in grado di bloccare gli apparati e rendere le informazioni non disponibili; altri atti di sabotaggio modificano o cancellano i dati, ledendone l'integrità; i 'furti', infine, possono riguardare ricette e brevetti. "L'intrusione è una qualsiasi attività anomala che si verifica in rete", afferma Andrea Cogliati di Ultimo-Byte-Gotech. "Essa reca sempre danno al sistema-azienda, indipendentemente dall'intenzione dell'autore". Per 'complicare la vita' a chi attacca le reti informatiche, chiunque egli sia, lo faccia per trarne profitto, per amor di sfida, o con intenzioni terroristiche, occorre prendere provvedimenti sia dal punto di vista tecnologico, introducendo filtri di accesso e firewall, progettando architetture su più livelli, di cui alcuni inaccessibili, slegati dalle reti di comune utilizzo, sia organizzativo, pianificando adeguate procedure aziendali di accesso e autorizzazione, nonché formando il personale in modo che possa intervenire tempestivamente in caso di pericolo, anche disconnettendo i sistemi della rete aziendale.

"Spesso gli apparati di fabbrica vengono attaccati 'dalla porta d'ingresso', partendo dall'alto per arrivare al basso", afferma Al Cooley di Verano, azienda statunitense specializzata in sistemi di sicurezza. Ad esempio, le VPN, le connessioni wireless o via Web che consentono ai PC di tecnici e collaboratori di entrare nel sistema aziendale per effettuare controlli da remoto, opere di

manutenzione o altro sono veri e propri 'cavalli di Troia', tramite i quali hacker e virus hanno facile accesso alle reti e ai fieldbus. Basti pensare a un qualsiasi sistema di controllo di processo distribuito connesso via bus alla periferia di campo. Le informazioni viaggiano dal basso fino ai livelli di fascia alta dell'azienda, ai gestionali SAP e ERP e a reti informatiche Intranet e Internet. Una volta penetrato uno strato, anche gli altri risultano scoperti, in preda al 'pirata' virtuale. A volte, poi, le strategie di difesa sono inefficaci per trascuratezza o leggerezza dei gestori, per cui i firewall non sono impostati in modo corretto, o i software di protezione non sono aggiornati.

"Se i PC di alcuni uffici", insiste Cooley, "sono collegati a infrastrutture pubbliche, reti di aziende partner, società sorelle, specialisti e consulenti, il pericolo aumenta". Per ovviare a ciò occorre studiare architetture di rete dove i livelli più bassi dell'impianto e del campo non siano mai accessibili dall'esterno. "È anche consigliabile innalzare delle barriere lungo la 'periferia' dell'impianto", ribadisce Cooley. "Si possono usare sistemi d'allarme che segnalano la presenza di file o processi nuovi, mai registrati prima, dato che il mondo industriale è meno dinamico di quello IT e file o procedure diverse dalle consuete dovrebbero subito far insospettire".

"Nel momento in cui le reti industriali sono diventate parte integrante del Web, la sicurezza al 100% semplicemente non è più esistita", concorda Tagliapietra. "Si è venuto a creare una sorta di 'varco' che consente facile accesso a sistemi industriali spesso critici", afferma Pasquale Fanelli di Invensys. "Il punto è che le reti industriali non sono state create per difendersi, perciò non sono pronte a farlo. Quindici anni fa non si pensava a rendere le operazioni d'impianto sicure, bensì più efficienti ed efficaci", insiste Cooley. Perciò oggi risulta estremamente semplice violare le reti di aziende ad esempio di processo, che spesso operano in zone a rischio di esplosione o utilizzano sostanze tossiche, come le chimiche e petrolchimiche. Si possono sabotare i comandi di valvole o, in generale, modificare i dati trasmessi dal campo, senza che i sistemi d'allarme rilevino l'intrusione, o che gli apparati di controllo registrino una qualche anomalia nei sistemi produttivi, mettendo a repentaglio la vita degli addetti, la sicurezza dei beni e dell'ambiente.

I rimedi che vengono dai bus

Conscio dei pericoli ai quali è esposto, il mondo industriale si è fatto via via più sensibile al problema della sicurezza delle reti di campo e degli apparati di fabbrica nel loro insieme, come dimostra l'intervento di Antonio Augelli di Siemens sulla sicurezza dei sistemi in occasione del recente Profibus Day organizzato a Brescia da PNO (Profibus Network Organization). "Quando si parla di system security si intende discutere sia di 'safety', sicurezza funzionale, ossia il corretto funzionamento di sistemi e apparecchiature, sia di 'security', ossia i principi di base per l'implementazione dei requisiti tecnici per la sicurezza informatica nella comunicazione dei dati, includendo l'integrità dei messaggi, la loro autenticità, le autorizzazioni di accesso ecc…".

Con 'stato di safety' si intende una condizione nella quale "il sistema è libero da pericoli e minacce inaccettabili per l'ambiente, i beni e le persone, attribuibili all'hardware o al software". Per assicurare questo tipo di condizione sono stati aggiunti alcuni layer di comunicazione allo standard Profibus DP di riferimento, creando il protocollo sicuro Profisafe. I sistemi finora installati con caratteristiche fail-safe sono circa 11 mila, mentre i nodi Profisafe attivi in impianti d'automazione sono circa 80 mila, destinati a ricoprire importanza sempre maggiore nel prossimo futuro considerando la chiara richiesta da parte del mercato di soluzioni di sicurezza efficaci su TCP/IP. PNO si è già messo all'opera istituendo tre gruppi di lavoro che stanno mettendo a punto un protocollo di rete sicuro per Ethernet, su Profinet I/O. In questo programma rientra la collaborazione di PNO con organismi quali TÜV e BIA (German institute for occupational safety). Un primo documento di bozza delle specifiche safety per Profinet è atteso in occasione della Fiera di Hannover, mentre la specifica finale si prevede sarà pronta per la fine del 2005.

Nelle reti d'automazione aperte agli standard IT è comunque fondamentale anche la questione della sicurezza intesa come security, data l'alta probabilità di atti di cyberterrorismo, cyberspionaggio, mailbombing/spam mail, virus, Web page defacement e attacchi tipo denial of service. Essi compromettono l'accesso alle reti d'automazione o l'integrità dei dati dal campo, essenziali per la produzione e la corretta gestione dei processi. Da questo punto di vista sono a disposizione degli utenti le Profinet Security Guideline, contenenti raccomandazioni per ridurre i rischi e suggerimenti che costituiscono la base per la certificazione dei componenti Profinet per la security. Per quanto concerne la certificazione, l'obiettivo di PNO è integrare le linee guida nello standard (IEC 61784-3 di IEC SC65C Wg13, ISA SP99), puntando anche sulla collaborazione con enti quali Namur, Vdma (German Engineering Federation) e Zvei (German electrical and electronic manufacturer's association).

Si suggerisce, ad esempio, l'inserimento di adeguati dispositivi esterni o integrati nelle interfacce di collegamento fra PLC e reti per proteggere le celle d'automazione connesse all'infrastruttura aziendale. ■

Anipla readerservice.it n. 20
Clusit readerservice.it n. 21
Invensys readerservice.it n. 22
PNO – Profibus Network Organization readerservice.it n. 23
Siemens readerservice.it n. 24
UltimoByte-Gotech readerservice.it n. 25
Verano readerservice.it n. 26
Vision Automation readerservice.it n. 27