La security IT nell'automazione

Armando Martin

La massiccia diffusione di risorse ICT nei sistemi di automazione espone gli stessi a rischi di attacchi informatici, usi inadeguati e ripercussioni negli impianti produttivi. La protezione dei dati e delle infrastrutture passa per politiche coordinate, investimenti e formazione continui, adesione alle normative. In Italia, come in Europa, occorre recuperare il gap esistente tra security IT e security industriale.

Quando nel 2000 a Maroochy Shire, in Australia, un ex-dipendente riuscì a introdursi nel sistema di telecontrollo di un impianto di depurazione provocando il riversamento nell'ambiente di circa 1.200.000 litri di liquami, erano probabilmente in pochi a porsi il problema della security in modo sistematico. Oggi Il tema della sicurezza informatica applicata ai sistemi di automazione e controllo è generalmente avvertito, non fosse altro per gli elevati costi dei fermi macchina, dei blocchi della produzione e della sospensione dei servizi provocati da malfunzionamenti, aggressioni remote e incidenti informatici. Il massiccio ricorso alle tecnologie ICT (Information Communication Technologies) ha avuto come conseguenza l'incremento della complessità e delle interdipendenze funzionali tra le diverse infrastrutture, al punto che un guasto o un'anomalia di natura accidentale o dolosa, possono facilmente propagarsi amplificando, a cascata, gli effetti negativi su tutto il sistema, fino a minacciare l'incolumità delle persone. La ricerca dell'efficienza e della continuità nelle reti industriali viene ottenuta sia con le tecnologie di prevenzione dei rischi della sicurezza fisica (Safety), sia con l'utilizzo di tecnologie dell'informazione (Security). In questi tempi, connotati da un crescente uso di tecnologie e sistemi aperti, dal sensore al PC, e da un'estensione dei protocolli di rete (TCP/IP, SNMP, Wi-Fi e altri ancora), il livello di rischio è aumentato soprattutto per l'introduzione di alcune tipiche minacce IT nelle reti di controllo industriale. Si rivela perciò inadeguata la semplice protezione "perimetrale" con firewall o attraverso soluzioni isolate e non coordinate. È necessario un approccio sistematico che analizzi tutte le fasi dei processi da controllare e prenda in considerazione tutti i punti potenzialmente vulnerabili della rete.

La sicurezza negli Scada e nelle reti di controllo

Troppo spesso i sistemi Scada (Supervisory Control And Data Acquisition), al centro della gestione delle informazioni nell'industria, sono percepiti e configurati in modalità disconnesse, poco o per nulla correlate ai rischi delle reti IP. Per altro verso, la condivisione dei canali di trasmissione (la rete Scada è spesso collegata o coincidente con la rete informatica d'ufficio), la crescente interoperabilità con le procedure aziendali e l'introduzione di sistemi operativi commerciali rendono i sistemi Scada vulnerabili. Il concorso di questi fenomeni determina un abbassamento generale del livello di sicurezza e varie ripercussioni economiche e pratiche per gli operatori e gli utenti. Va ricordato che gli Scada controllano processi e infrastrutture critiche (centrali elettriche, reti di fornitura di gas o acqua, reti di comunicazione e trasporto) non solo attraverso il software di supervisione o il livello HMI (Human Machine Interface), ma anche tramite le periferiche PLC, DCS e RTU che controllano i singoli impianti. D'altra parte proprio la sottovalutazione delle conseguenza pratiche di un livello di sicurezza inadeguato ha provocato negli ultimi anni alcuni incidenti piuttosto clamorosi: la diffusione di un virus informatico nel sistema di monitoraggio di una centrale nucleare in Ohio, l'attacco del 2005 alle reti informatiche dei grandi network di informazione americani, le azioni di sabotaggio delle reti di controllo di impianti pertrolchimici in Venezuela e in Siberia, oltre a una preoccupante sequenza di attività di hackeraggio, spionaggio industriale e di cyber-terrorismo. Se alcune delle spiegazioni di fondo possono attribuirsi alle politiche di abbattimento dei costi perseguite attraverso la standardizzazione e la convergenza delle tecnologie (ad esempio l'uso di PC standard, sistemi operativi legacy, connessioni Ethernet, TCP/IP, Wi-Fi, cablaggio strutturato ecc.), d'altro canto vi è ancora una forte barriera culturale da abbattere. La presenza di protocolli di comunicazione privi di autenticazione, cifratura e firma elettronica è una prassi ancora molto diffusa. Come non è infrequente imbattersi in sistemi Scada le cui basi dati sono "in chiaro", scarsamente strutturate a livello di log e accounting. Per non parlare delle disinvolte modalità di gestione remote e via web, spesso caratterizzate da configurazioni prive di backup e piani di recupero dati. Ovvio che queste situazioni rendono tali sistemi vulnerabili a virus, worm, anomalie, oltre ai potenziali effetti a catena dovuti agli errori non controllati. Dunque, se da un lato i produttori di Scada e sistemi di controllo dovrebbero aumentare e differenziare le proposte, gli utilizzatori dovrebbero ancor più fortemente investire in formazione dei lori manager e operatori, e soprattutto attuare credibili politiche di security e controllo. È quindi fondamentale l'implementazione di sistemi integrati basati su reti ad accesso

limitato VPN/VLan/DMZ (Virtual Private Network/Virtual Local Area Network/Demilitarized Zone) che comprendano dispositivi di sicurezza fisica, impiego di adeguati patch, antivirus, firewall, content filter, tecniche di ridondanza e backup. Senza trascurare la cura della qualità del servizio e la gestione della documentazione. Una buona politica di security deve prevedere l'adozione di infrastrutture di tipo AAA (Authentication, Authorization and Accounting), l'utilizzo di tecniche di criptazione dei dati, la disabilitazione dei servizi di rete inutilizzati, la gestione di regolari test di sicurezza con un metodo appropriato e secondo standard riconosciuti. In aggiunta, per proteggere le utenze tipiche del controllo industriale (PLC, DCS, RTU) in rete, occorre adottare un modello di firewall "distribuito" in modo che il singolo controllore abbia un proprio gate di accesso sotto costante controllo. Il sistema così concepito può proteggere ogni dispositivo in modo indipendente dagli altri. Particolare attenzione va riservata, inoltre, all'utilizzo di sistemi di comunicazione wireless (es. Wi-Fi e Bluetooth) nelle reti Scada. Anche in questo caso la policy complessiva, la scelta dell'hardware e della configurazione di rete (in grado di supportare protocolli "sicuri" come Wep, Radius, Weca) si rivelano aspetti fondamentali.

Il ruolo degli standard

Quasi impossibile tracciare in poche righe il panorama normativo della cybersecurity, in particolare nei sistemi di controllo e nelle certificazioni Scada. Un ruolo centrale è comunque rivestito dalla famiglia Iso 27000 il cui obiettivo è quello di fornire un modello e una guida dettagliata per ridurre l'esposizione delle imprese ai rischi collegati alla sicurezza delle informazioni. Tali standard affrontano i temi della gestione dei rischi, le problematiche di metrica e misurazione, l'efficacia dei sistemi di sicurezza e le metodologie di attuazione. Dal 2005 lo standard Iso 27000 ha sostituito e integrato lo standard BS7799, il cui contenuto è ancora alle fondamenta delle misure di sicurezza informatica e si compone di due parti: la prima, ripresa nel 2000 dalla Iso/IEC 17799, suggerisce "best-practice" per implementare un programma per la sicurezza delle informazioni; la seconda elenca i processi e i controlli necessari per implementare un sistema certificato di gestione della sicurezza informatica. Altro pilastro normativo della security è la Iso/IEC 15408, più nota come "Common Criteria", che consente di verificare se le esigenze dell'utente, descritte attraverso un insieme di requisiti di alto livello (PP, protection profile), sono soddisfatte sulla base dei requisiti e delle specifiche utilizzate dal produttore per l'implementazione di un determinato prodotto (ST, Security Target). Recentemente alcuni governi hanno adottato specifiche politiche di sicurezza contro le minacce di natura informatica. Ad esempio il governo americano ha indicato come priorità nazionale l'incremento del livello di cyber-security degli Scada e dei DCS, mentre il governo britannico ha incaricato l'autorevole CPNI (Centre for the Protection of National Infrastructure) di attivare forme di cooperazione nei confronti degli utilizzatori di sistemi Scada e DCS.

Uno scenario in continua evoluzione

Il modello Isa S99 resta il principale riferimento per l'implementazione della security nelle più comuni piattaforme software industriali (Scada, Mes, ERP, CRM, Supply Chain ecc.). Ma per la security di cui si occupano il reparto IT e il CSO (Chief Security Officer), il mercato offre ulteriori strumenti ad hoc. Spiega Enzo Maria Tieghi, membro votante Isa S99, promotore di numerose giornate di studio Anipla sul tema sicurezza e amministratore delegato di Vision Automation (società che distribuisce e supporta prodotti e tecnologie per la cybersecurity di reti e sistemi di controllo e automazione): "Possiamo dire che oggi sono finalmente disponibili metodologie e tecnologie che consentono di adottare contromisure adeguate per i rischi informatici di reti e sistemi di fabbrica. Alcune aziende, tra le quali Industrial Defender e Vision Automation, hanno studiato sistemi per la protezione di sistemi DCS, Scada, PLC ecc. Inoltre, mediante una opportuna segmentazione delle reti e segregazione dei server (MES, DBMS di supply chain ecc.) con DMZ ed altre tecniche, è possibile isolare e protegge i sistemi di controllo dalla propagazione di eventuali problemi informatici sulle reti". Non mancano però le resistenze, soprattutto in termini di approccio al problema. La security "industriale" spesso è percepita in modo distorto e non sufficientemente distinto da quella applicata ai servizi e alla business information. Precisa Tieghi: "È probabilmente il 'rischio' l'aspetto che più differenzia la security 'industriale' dalla security 'IT'. Infatti di solito la preoccupazione maggiore dell'IT è la perdita di dati e informazioni a causa di problemi di Integrità-Disponibilità-Riservatezza. Il rischio principale che soggiace alla security industriale è la eventuale 'perdita del controllo' che potrebbe procurare fermi impianto, inefficienze, buchi in produzione, scostamenti rispetto ai parametri di qualità, fino ad arrivare a problemi per l'incolumità dell'impianto, delle persone e dell'ambiente". Di fatto, però, le aziende e gli operatori si decidono a investire in sicurezza più che altro sulla spinta delle regolamentazioni forzate e dell'inquadramento legislativo. "Pensiamo infatti – chiarisce Tieghi – a quanti hanno iniziato ad usare antivirus e firewall sulle reti d'ufficio, solo dopo l'obbligo imposto dalla legge sulla privacy e dal DPS (Documento Programmatico sulla Sicurezza) in essa contemplato Del resto il Roi (Ritorno sull'Investimento) della sicurezza è spesso impossibile da determinare. Spesso è più convincente una BIA (Business Impact Analysis) o una BLA (Business Loss Analysis) che risponda ad alcune domande, del tipo: mi posso permettere che si fermino gli impianti e la produzione a causa del rischio informatico; che impatto potrebbe avere un incidente che porti ad una rottura di un macchinario, un danno all'operatore, o un inquinamento dovuto ad un malfunzionamento di un PC o un PLC?". Che dire infine del livello di implementazione della security nel nostro paese? Secondo Tieghi "L'Italia, ma anche l'Europa, stanno correndo ai ripari ed iniziando a percorrere una strada per recuperare il tempo perso: recentemente esperti hanno stimato in almeno 5 anni il gap esistente tra security IT e security industriale".

readerservice.it - n. 35