Tutorial


Fonte: www.metrolic.com

SOA: L'AUTOMAZIONE DI QUARTA GENERAZIONE - PARTE 2

LE PROBLEMATICHE LEGATE ALLA SICUREZZA INFORMATICA SONO RILEVANTI ANCHE PER LE RETI DI AUTOMAZIONE: LE ARCHITETTURE WEB-BASED SI DIMOSTRANO PIÙ AFFIDABILI E MENO VULNERABILI IN CASO DI GUASTO

di **Micaela Caserza Magro, Paolo Pinceti (*)**

I problemi di sicurezza tipici di un sistema di automazione industriale sono costituiti dall'accesso non consentito e dalla diffusione di software 'maligno', il cosiddetto malware. Le conseguenze tipiche di un sistema danneggiato da malware sono: l'impossibilita tra host di comunicare su di una rete a pacchetto a causa dell'alto traffico generato da host la cui sicurezza sia stata compromessa; crash dei sistemi operativi degli host compromessi e relativa necessità di riavvii o shutdown; raccolta ragionata di informazioni sensibili e loro invio verso destinazioni non designate, o installazioni di back-door che abilitano il controllo dell'host da parte di soggetti non autorizzati.

Per prevenire un'infezione da malware è raccomandabile limitare il più possibile i mezzi di propagazione (vettori) utilizzati da questo tipo di software applicando una serie di regole progettuali e comportamentali. Occorre, prima di tutto, impedire ogni traffico email, instant messaging, IRC entrante verso gli host della rete del sistema di automazione; poi, se per motivi operativi si rende necessario usare sistemi di messaggistica, questi devono essere installati su host distinti all'interno delle control room, non collegati alla rete del sistema di automazione ma direttamente alla rete dell'azienda o alla rete esterna (Internet). Inoltre, come per l'email la navigazione su pagine Web arbitrarie deve essere limitata: usare firewall e VPN per garantire il collegamento a pochi siti pre-approvati è una scelta più che ragionevole. I sistemi di Drive Sharing che permettono di spostare i dati da e per la rete del sistema di controllo devono essere bloccati da firewall e i PC portatili devono installare le ultime patch del proprio sistema operativo e applicazioni; i malware scanner devono essere installati e aggiornati e tutti i sistemi devono abilitare solo servizi e user account realmente utilizzati. Oltre a ciò, il dataflow deve essere progettato con cura, in modo che nessuna richiesta transiti dall'esterno della rete di controllo verso i sistemi che vi stanno all'interno. In questo caso un semplice firewall potrebbe chiudere tutto il traffico entrante.

Se alcuni servizi devono obbligatoriamente girare dentro la rete di controllo è opportuno, se si controllano sia i client sia i server, spostare le porte TCP dai valori usuali, noti a tutti. È oltretutto utile usare VPN per restringere l'accesso solo a client autorizzati e creare zone di contenimento attraverso l'uso di firewall tradizionali e locali (personal firewall).

Misure precauzionali in una struttura three-tier

Rifacendosi alla struttura three-tier si può distinguere tra le misure precauzionali prese per il livello di business e quelle prese per il livello di presentazione. Per quanto riguarda il business tier, essendo il sistema monolitico e centralizzato sugli application server, le precauzioni si limitano a proteggere il server dall'accesso fisico, a non fornire accesso locale all'application server e ad abilitare su di esso solo i servizi strettamente necessari. Più ampio invece il discorso relativo ai thin client, sui quali l'accesso è effettuato tramite l'immissione di credenziali quali username e password ed è impedita l'introduzione di dispositivi e supporti esterni quali CD/DVD, dispositivi USB ecc.

Nel caso usuale di sistemi di controllo con connessioni alla intranet aziendale, l'accesso in ingresso al sistema di automazione avviene esclusivamente mediante il protocollo di sicurezza https, che utilizza di default la porta 443. Per accedere dalla intranet al sistema di controllo sono inoltre presenti meccanismi di autenticazione e crittografia, nonché politiche di sicurezza che devono essere seguite dagli operatori.

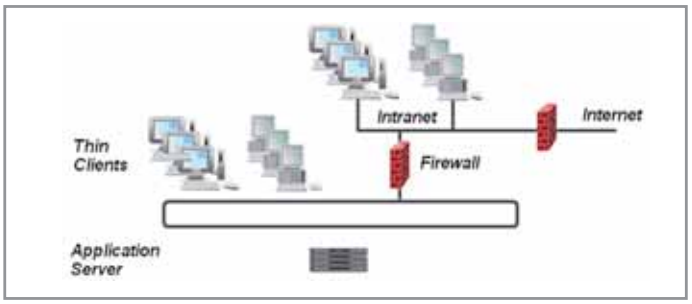

Figura 6 - PCS connesso alla rete intranet aziendale

Laddove Internet venga utilizzata da thin client remoti per il collegamento all'impianto, la connessione avviene attraverso VPN, che consente una connessione sicura attraverso il gateway di accesso alla rete. Discorso diverso per i thin client su dispositivi portatili mobili, dove la VPN viene implementata via etere e meccanismi di protezione aggiuntivi (livello di sicurezza WPA, WiFi protected access) vengono

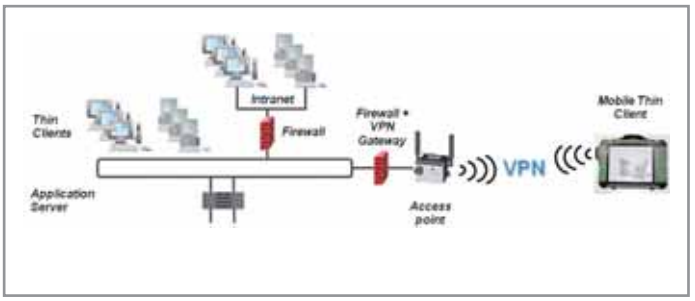

Figura 7 - Thin client su dispositivi portatili

applicati tra il thin client mobile e l'access point collegato al gateway, che è situato sulla rete del sistema di controllo.

La 'fidatezza' dei sistemi Web-enabled

Numerosi concetti concorrono nel termine 'fidatezza' (brutta traduzione italiana del termine inglese 'dependability'): affidabilità, manutenibilità, disponibilità, sicurezza. Spesso ci si riferisce a questi concetti con l'acronimo Rams (Reliability, availability, maintainability and safety), che identifica l'approccio sistematico con cui vengono valutate le grandezze prima citate. È evidente come la fidatezza sia, insieme alle prestazioni, il parametro fondamentale di un qualsiasi PCS. Al fine di perseguire un'analisi anche solo parzialmente quantitativa delle prestazioni di fidatezza di un sistema è necessario definire quello che in sede di normativa internazionale e nazionale viene chiamato 'mission profile', dove vengono identificati i modi di funzionamento o stati del sistema. Nello specifico, ogni stato del sistema è caratterizzato dalle funzioni che devono essere eseguite, dai parametri e limiti ammessi per ogni funzione identificata e, infine, dalle condizioni ambientali e di funzionamento dell'intero sistema.

Di seguito viene definita una modellazione semplificata di un PCS, utile per considerazioni relative alla fidatezza:

- funzionamento normale: è il corretto funzionamento, in cui tutti i servizi e le funzioni del sistema sono attivi e accessibili da parte dell'utente;
- funzionamento degradato: una o più funzioni non critiche del sistema sono fuori servizio e/o non possono essere fruite dall'utente, invece le funzioni critiche per il compimento della missione del sistema sono ancora funzionanti e accessibili dall'utente;
- funzionamento in allarme: una o più funzioni critiche sono fuori servizio, ma per ognuna delle funzioni critiche guaste esiste una configurazione ridondante che è entrata in servizio;
- guasto: il sistema non è più in grado di portare a termine una o più funzioni. Le funzioni svolte dal sistema vengono classificate in 'critiche' o 'non critiche'; le prime sono funzioni senza le quali il sistema non è in grado di portare a termine la sua missione. Le funzioni non critiche sono invece quelle che non pregiudicano in modo sostanziale la missione del sistema. Quando mancano si ha un funzionamento 'degradato'.

Riferendosi all'architettura tipica di un PCS si possono identificare i seguenti sottosistemi: campo (sensori e attuatori intelligenti), comunicazione di campo (fieldbus tra il campo e il controllo), controllo (esegue i loop di regolazione, le sequenze e in generale processa i dati provenienti dal campo), database manager (contiene il database real-time del sistema), comunicazione verso la sala controllo (permette lo scambio dati tra il controllo di processo e i sistemi di supervisione e d'interfaccia uomo/macchina), sala controllo (è la parte in cui i servizi di più alto livello, rispetto alla regolazione, vengono resi disponibili all'utente).

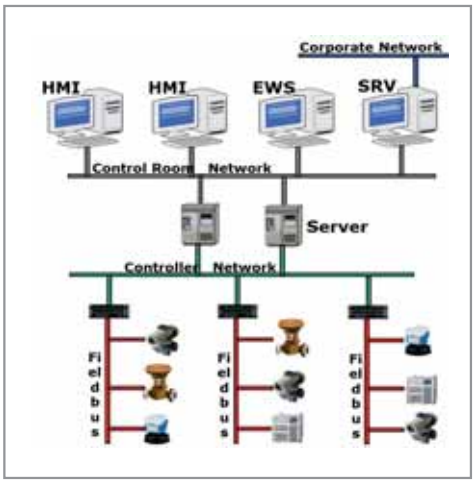

Figura 8 - Architettura di un sistema PCS

Un sottosistema include sia le funzionalità hardware, sia quelle software. Si possono identificare due tipi di guasti (si veda figura 9); il primo è il 'guasto critico', che interessa un sottosistema, o una parte di esso, coinvolto nello svolgimento di una funzione critica. Partendo dallo stato normale un guasto critico porta il sistema in condizioni di guasto, per cui è persa una funzione essenziale. Se invece le funzioni critiche sono supportate da configurazioni ridondanti, il guasto porta il sistema in condizione di allarme, in quanto la funzione è svolta dal canale di riserva, ma non è più disponibile un back-up. Il guasto 'non critico', invece, interessa un sottosistema, o una parte di esso, coinvolto per la definizione di una funzione ritenuta non critica per il sistema: dallo stato normale un guasto non critico porta il sistema nello stato degradato.

È necessario prevedere per le funzioni critiche una configurazione ridondante o di stand-by al fine di garantire la robustezza del sistema rispetto al primo guasto (sicurezza N-1). Gli interventi di riparazione riportano il sistema in stato normale.

A titolo di esempio, la tabella 1 identifica le funzioni tipiche di un PCS classificandole secondo la criticità o meno della funzione stessa.

Le architetture di PCS convenzionali presentano un'architettura con-

cettuale di tipo distribuito: in sala controllo si ha una macchina dedicata per ogni funzione (supervisione, HMI, diagnostica ecc.). Ognuna di queste macchine accede al database server per ottenere i dati provenienti dal campo ed elaborarli autonomamente; su ogni macchina gira l'applicativo specifico, oltre ai driver di comunicazione necessari. Se la funzione è considerata critica, per fornire continuità alla funzione svolta anche al verificarsi di un primo guasto è necessario avere una macchina ridondante, con le stesse caratteristiche e lo stesso software applicativo.
Al contrario, un'architettura di PCS Web-based utilizza un approccio

Funzione	Critica	Non Critica	Sottosistema
HMI	☼		Sala controllo
Gestione allarmi	☼		Sala controllo
Historian		☼	Sala controllo
Trend		☼	Sala controllo
Comunicazione verso ERP		☼	Comunicazione
Gestione eventi	☼		Sala controllo
Controllo di processo: parti impianto critiche	☼		Controllo
Controllo di processo: parti impianto non critiche		☼	Controllo
Comunicazione verso campo	☼		Comunicazione
Diagnostica		☼	Sala controllo

Tabella 1: Classificazione delle funzioni di un PCS

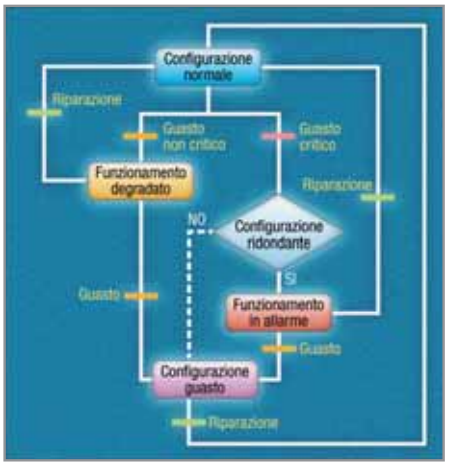

Figura 9 - Tabella delle transizioni degli stati di un sistema

centralizzato: vi è un unico server su cui girano tutte le applicazioni di più alto livello, mentre le macchine in sala controllo sono thin client, che non necessitano l'installazione di applicativi software e/o driver dedicati per svolgere la funzione loro assegnata. Questo significa che ciascun client può rendere disponibile qualsiasi funzione, purché l'utente abbia i diritti di accesso. Questo implica un aumento di affidabilità e disponibilità dell'intero sistema. In questa configurazione i tempi per la riparazione sono praticamente nulli, infatti i client sono tra loro tutti intercambiabili. La configurazione che si viene a creare è una configurazione 'k-su-n': servono k client in servizio per assolvere a tutte le n funzioni previste. Anche la disponibilità aumenta di conseguenza: il tempo per sostituire una macchina generica, che operi come client, è molto inferiore rispetto a configurare una macchina dedicata per una certa funzione.
Il nuovo concetto di sistema risulta dunque più affidabile e disponibile rispetto a un PCS realizzato secondo un'architettura software convenzionale, pur offrendo gli stessi servizi ed essendo interfacciato con lo stesso campo e lo stesso controllo.
Il cuore di un sistema Web-based è evidentemente l'application server. Se questo ha un guasto, l'intero sistema è in condizione di guasto. Proprio per il ruolo centrale che assume è necessario realizzare l'application server impiegando una macchina particolarmente robusta in termini di disponibilità, come può essere un server fault-tolerant, i cui tempi di downtime medi sono dell'ordine di 30 s/anno (disponibilità del 99,9999%). Per comparazione, un server convenzionale ha una disponibilità intorno al 99,9% cui corrisponde un downtime di circa 9 ore/anno. La centralizzazione delle funzionalità critiche e non del sistema consente di aumentarne l'affidabilità perché riduce il problema a una singola macchina, molto più facilmente gestibile che non un cluster di macchine in rete.

I benefici offerti da una piattaforma SOA

Il mondo IT è oggi fortemente orientato verso l'impiego di Service Oriented Architecture per i benefici che offrono nell'integrazione di sistemi complessi. Allo stesso modo si può senz'altro pensare di migrare sui PCS le stesse tecnologie informatiche che da un lato offrono prestazioni molto elevate, dall'altro consentono una più agevole apertura verso l'integrazione del PCS nel sistema di IT aziendale. Quando declinata per un PCS la SOA si caratterizza per: interfaccia con il campo totalmente digitale, attraverso una rete di comunicazione ridondata; impiego globale delle tecniche di programmazione object oriented; architettura di sistema Web based secondo il modello three tier standard per le applicazioni Web; centralizzazione di tutte le applicazioni di control room su un server ridondato (application server) che rappresenta il business tier del sistema. E ancora: utilizzo per tutte le funzionalità di control room di macchine standard (PC, PDA, laptop ecc.) senza software aggiuntivo (thin client); intercambiabilità

Funzione	Critica	Non Critica	Sottosistema
HMI	☼		Aut. Server
Gestione allarmi	☼		Aut. Server
Historian		☼	Aut. Server
Trend		☼	Aut. Server
Comunicazione verso ERP		☼	Comunicazione
Gestione eventi	☼		Aut. Server
Controllo di processo: parti impianto critiche	☼		Aut. Server
Controllo di processo: parti impianto non critiche		☼	Aut. Server
Comunicazione verso campo	☼		Comunicazione
Diagnostica		☼	Aut. Server

Tabella 2: Classificazione delle funzioni di un PCS di tipo Web-based

piena di tutte le macchine d'interfaccia utente; elevata sicurezza informatica grazie all'impiego di un'unica piattaforma sulla quale girano tutte le applicazioni (Java o altre); elevata fidatezza del sistema grazie alla semplificazione dell'architettura hardware e software, in particolare grazie all'implementazione del business tier su un'unica macchina centralizzata e alla realizzazione di un presentation tier accessibile da thin client; infine, interfaccia nativa per le applicazioni informatiche aziendali.

(*) Fonti: Paolo Pinceti, "Scada per Sistemi Elettrici", Franco Angeli Editore; Samuel M. Herb, "Understanding distributed processor systems for control", ISA 1999; Bela G. Liptak, "Instrument engineers' handboosk. Process software and digital networks", CRC Press, 2002; Jonas Berge, "Software for automation: architecture, integration and security", ISA 2005; International Standard ISO/IEC 15408:2005 - Information technology - Security techniques - Evaluation criteria for IT security; IEC 61078, "Analysis techniques for dependability - Reliability Block Diagram and boolean methods", 2006:05; IEC TR 62380, "Reliability data handbook - Universal model for reliability prediction of electronics components, PCBs and equipment", 2004-08; CEI 56-50, "Terminologia sulla fidatezza e sulla qualità del servizio", 1997-05; Stratus ftServer W Series 4300 system boasts of edge technology, price/performance leadership, and breakthrough online software upgrade capability", www.stratus.com/news/2005 /20050912.htm; M. Hecht, "Reliability/availability modelling and prediction for e-commerce and other internet information systems", Ieee Annual reliability and maintainability symposium, 2001