Tre paradigmi di Citel per la sistemistica informatizzata di gestione della sicurezza fisica in architettura aperta

di Nils Fredrik Fazzini, general manager Citel spa

Visto successo del concetto PSIM (Physical Security Information Management) e l'improvvisa fioritura dell'offerta di prodotti "PSIM" in Italia nel volgere di pochissimo tempo, nei due numeri precedenti di **essecome** avevamo fatto delle precisazioni e distinzioni riguardo ai requisiti necessari per collocare una soluzione di supervisione nella classe PSIM.

E poiché Citel ha svolto un ruolo pionieristico ultradecennale per l'informatizzazione della sicurezza fisica, può sentirsi legittimata a supportare l'utenza nella valutazione dell'offerta dei PSIM dell'ultima ora in funzione dei contenuti e a prescindere dalle etichette; e in questo senso ricordando **la necessità di integrare il paradigma di IHS con criteri oggettivi di valutazione non basati sulla sola aderenza nominale ai requisiti**, essendo questi espressi in maniera particolarmente sintetica. A integrazione dei 7 requisiti, una valutazione prudente – come un sistema informatizzato richiede – si baserà quindi sulla diffusione nel mercato, sull'organico di progettazione e supporto, sul livello di utilizzo raggiunto dagli utenti e la loro soddisfazione e, infine, sulla dinamica dell'evoluzione delle soluzioni a catalogo negli anni, sia di piattaforma che applicativa.

Le precisazioni da parte di Citel sono iniziate con l'articolo sul n. 4/2015 di essecome, in cui si riprendevano recenti commenti di IHS che implicitamente ricordavano che **il PSIM non corrisponde affatto a un semplice software di su-pervisione allarmi** ma consiste in un vero e proprio **sistema informatizzato di gestione**.

Siamo quindi in una situazione di mercato in cui, dopo la fiammata iniziale di interesse, si pone il problema di **come oggettivizzare il concetto di "classe PSIM"** e di come modulare le sue valenze significative in modo – se non altro – di collocare i diversi prodotti di mercato in una scala di valori la più utile e oggettiva possibile.

L'idea di Citel in proposito è che un concetto oggettivo e facilmente condivisibile da prendere a riferimento nella pratica aziendale è quello del ***sistema informatico dipartimentale*** per la sicurezza fisica, e che per considerarlo tale a tutti gli effetti, sia necessario soddisfare **tre paradigmi**:

(1) naturalmente il **PSIM** definito da IHS, con i suoi requisiti purché adeguatamente sviluppati e argomentati professionalmente in chiave informatica;

(2) l'**Ecosistema dinamico**, ovvero il crogiuolo delle funzionalità ad uso dell'utente, alimentato continuamente dalla sinergia con utenti e partner di integrazione; una fonte sinergica di soluzioni senza la quale è dimostrato che l'evoluzione dei processi di un sistema informatico resta al palo; e infine

(3) la **sistemistica professionale**, cioè l'infrastruttura tecnica che, indipendentemente dalle distanze, assicura l'acquisizione dei dati, attiva i processi che generano eventi e situazioni, alimenta la circolazione di informazioni e comandi a fini operativi, assicurando la conformità alla normativa e ai vincoli di compliance e di buone pratiche.

PSIM ed Ecosistema sono stati trattati nei numeri 3 e 4 di Essecome mentre la **sistemistica professionale** viene trattata qui di seguito.

IL TERZO PARADIGMA DI CITEL:
LA SISTEMISTICA PROFESSIONALE DI TELE GESTIONE - CARATTERISTICHE E VINCOLI

Naturalmente, in questa sede non si tratta la gestione da parte di chi è presente sulla scena dell'evento, ma di coloro che – indipendentemente dalla loro collocazione fisica - sono addetti al monitoraggio e all'attivazione dell'intervento, da chi è responsabile delle decisioni operative in caso di escalation e, infine, da chi è il responsabile ultimo (o delegato) in rappresentanza dell'impresa, non solo ai fini della sicurezza in senso stretto ma anche degli aspetti di *safety* e di *business continuity*.

La gestione adeguata di tale catena nei due sensi richiede un'**intelligenza opportunamente distribuita** sia per la generazione di informazioni attendibili e facilmente fruibili, sia per l'attivazione di reazioni automatiche immediate o telegestite da remoto: In tutti i casi deve assicurare la circolazione di flussi informativi e operativi lungo una filiera che prescinde dalle distanze fisiche.

Una filiera che deve garantire un **livello omogeneo di continuità del trasporto dei dati e di protezione della loro integrità** a fini di telegestione lungo tutto il percorso, rispettando precisi vincoli di affidabilità intrinseca.

"Telegestione" vuol dire in pratica la possibilità di agire a distanza quasi come se si fosse presenti sul posto, sia in termini di rilevazione a distanza dell'accaduto che, nei limiti dell'impiantistica disponibile, per l'accertamento e per il primo intervento. E se questo è l'obiettivo, occorre creare le **condizioni tecniche necessarie, sia sul posto da proteggere, che in Control Room e nella connessione** tra di essi e con altri aventi causa.

Condizioni tecniche necessarie che si riassumono - al di là delle funzionalità - nell'**affidabilità intrinseca della struttura per la sicurezza**. Con il corollario per cui senza un grado adeguato di affidabilità intrinseca, livello per livello, la **telegestione potrebbe rivelarsi un rimedio peggiore del male**.
Nel seguito sono riportate in sintesi le condizioni da

creare per ottenere una **sistemistica di telegestione della sicurezza fisica adeguata ai vari livelli**, dal sito da proteggere a quello della governance. Da sottolineare che **le soluzioni basate sulla normativa CEI 79/5 (liv. 2) e 79/6 permettono di rispettare al massimo grado le raccomandazioni riguardanti il livello rete dati tra sito e Control Room**.

Livello: **sito da proteggere**
- densità e distribuzione adeguata in campo di sensori singolarmente indirizzati e correlabili per ottenere una precisa localizzazione delle singole segnalazioni, anche per ottenere reazioni di verifica opportunamente mirate e immediate come la video-ispezione
- connessioni garantite e monitorate nel campo locale tra sensore e centrale di gestione eventi, con l'elaborazione di correlazioni tra sensori per:
  - generare eventi il più possibile qualificati per tipo e attendibilità, tali da azzerare i falsi negativi (allarme ignorato) ma anche a minimizzare i falsi positivi (falso allarme);
  - ridurre al minimo gli interventi di risorse fisiche di verifica sul posto;
  - supportare chi dovesse comunque intervenire sul posto con informazioni inizialmente mirate ed eventualmente aggiornate nel corso dell'operazione,

anche con dispositivi di informatica personale connessi in rete.
- protezione fisica individuale della persona che interviene sul posto per verifiche di anomalie non altrimenti verificabili in orari di chiusura o comunque in condizioni di isolamento (eventualmente nel rispetto del DL 81 sulla safety del lavoratore).

Livello: **rete dati tra sito e Control Room**
- certezza della trasmissione immediata nei due sensi
- salvaguardia dell'integrità delle informazioni trasmesse

Livello: **Control Room interna o Centro Servizi**
- garanzia della ricezione integrale e immediata di quanto trasmesso
- garanzia del trattamento tempestivo e appropriato dell'evento e possibilità di commutazione della gestione
- alert in caso di timeout lungo tutto il processo: l'inizio della gestione, l'attivazione dell'intervento, la conclusione, la generazione del report
- per ogni evento trattato: reporting oggettivo, tracciato, completo, documentato, non manipolabile, non cancellabile se non da determinati livelli di responsabilità, generato anche automaticamente dall'attività stessa dell'operatore
- Time-Line di esecuzione delle attività di gestione dell'evento a fini work-flow per l'operatore e per la ricostruzione passo-passo del trattamento e delle azioni intraprese

Livello: **rapporti con terze parti di intervento**
- ingaggio semi-automatico della terza parte da coinvolgere per quello specifico evento come FFOO, vigilanza, manutentore, ecc.
- possibilità di ingaggio automatico in determinate condizioni di rischio
- possibilità di ingaggio automatico per time-out dell'azione dell'operatore
- coinvolgimento di terze parti mediante messaggistica documentata, anche multimediale, per consentire a chi interviene di avere un quadro contestualizzato e neutro della situazione

Livello: **Direzione, audit, governance, indagini forensi**
- accesso istantaneo al quadro complessivo - anche di una pluralità di siti - della gestione degli eventi in corso
- accesso alla base dati di tutti gli eventi, del loro trattamento e del reporting, anche multimediale, compresi video-clip e snap-shot associati all'evento
- accesso a posteriori ad ogni fase dell'evento, a partire dalla sua generazione, con la ricostruzione facilitata su Time-line dell'intero processo di trattamento dell'evento e del reporting
- retrieval con estrazione e trasmissione di singoli eventi ed elementi della gestione agli aventi causa per valutazioni ed azioni, compresi i fornitori di servizi
- possibilità di misurare la tempestività e la produttività della gestione di un singolo o gruppi di siti in base a indici specifici ed eventuale visualizzazione di cruscotti di sintesi.

CONTATTI: CITEL SPA
Tel. +39 02 2550766
www.citel.it