IoT, sicurezza fisica e sicurezza informatica: convergenza o interdipendenza? - Prima puntata

a cura della Redazione

L'Internet of Things è un tema di estrema importanza per la sicurezza, in ogni sua declinazione (attiva, passiva, security, safety, fisica, informatica…). Gli scenari sottostanti alla sua diffusione - in parte già ben chiari, in parte ora solo intuibili - potranno venire percepiti come opportunità da cogliere e/o rischi da evitare ma, di sicuro, interesseranno chiunque operi nella sicurezza, a qualsiasi titolo: dal security manager alla guardia giurata, dal costruttore al progettista, dall'installatore all'assicuratore eccetera. Un tema di questo peso ci ha spinto a chiedere il parere ad alcuni protagonisti della scena della sicurezza, per aiutarci a "razionalizzarlo" e proporlo nel modo più adeguato ai nostri lettori, nel percorso di informazione dedicata che faremo da qui in avanti. Iniziamo con Citel Spa, la società italiana chevanta la maggiore presenza nei sistemi informatici della sicurezza fisica nella fascia della grande utenza, che certamente ha familiarità con la materia, considerando che è in continuo contatto con una clientela composta dalle principali banche, Poste Italiane, ENI, ENEL, SNAM, Finmeccanica e, quindi, dalle principali infrastrutture critiche del Paese.

Nell'editoriale di essecome n. 3/2015 "IoT, cancellato il confine tra la sicurezza fisica e quella logica" abbiamo riportato alcuni episodi criminosi e un rapporto di origine USA, che dimostrerebbero la caduta del confine tra sicurezza fisica e sicurezza logica. Cosa ne pensate di questa teoria? E, visto che ci siamo, possiamo fare chiarezza sui concetti che stanno dietro la terminologia e sulle implicazioni pratiche?
Parto dall'IOT, l'internet delle cose. Di sicuro, si può solo dire che se sempre più "cose" vengono connesse a una infrastruttura di per sé aperta come Internet, sarà il caso di implementare protezioni sempre più stringenti (anti-virus e anti-malware) per mitigare il rischio. Lo dimostra il fatto stesso che il rapporto citato nell'editoriale è di fonte Symantec e mi pare naturale che la società metta in evidenza questo aspetto. Peraltro, se c'è qualcuno che connette via Internet la sicurezza fisica di una infrastruttura critica a un centro di controllo e ci viene chiesto un parere, noi rispondiamo "no comment" nel senso che operiamo su altri livelli di sicurezza e proponiamo quindi di chiedere a utenti come SNAM o ENEL cosa ne pensano. Non mi è chiaro, invece, in base a quali argomenti si possa sostenere che il confine tra sicurezza fisica e logica sia stato cancellato grazie (o a causa) dello IoT. La domanda più generale sull'eventuale convergenza operativa ce la siamo già fatta più di una volta, senza però trovare una ragionevole motivazione né un'applicazione pratica. Per adesso, ci limitiamo a fare proposte di convergenza sulle *definizioni* dei due concetti e delle loro relazioni, che – lo ribadisco – non devono essere necessariamente di convergenza operativa se non sussistono delle oggettive basi tecniche e funzionali. Per cominciare, quella che non è "Sicurezza Fisica" nel nostro mondo si chiama "Sicurezza Informatica" e non "Logica", se non altro perché è la traduzione più vicina a quella dell'inglese "Cyber Security" che, ormai, ha prevalso su "Computer Security", anche secondo Wikipedia.

Gli addetti ai lavori del mercato italiano hanno le idee chiare a proposito della distinzione tra sicurezza fisica e sicurezza informatica e dei rispettivi contenuti?
Se parliamo di organizzazioni grandi e medio-grandi la risposta è affermativa. Non potrebbe essere diversamente: le responsabilità e le interazioni operative verso le strutture da proteggere e verso le fonti del rischio sono oggetto di politiche e procedure stringenti nei settori in cui operiamo. Aggiungo anche che incrociamo sempre più spesso i consulenti specializzati chiamati per i penetration test e per la certificazione della *compliance* per nuovi impianti o dispositivi che connettiamo alla rete dati. D'altra parte, i nostri più grandi utenti sono banche e infrastrutture critiche nel campo dell'energia, ed è scontato che noi siamo sempre di fronte a interlocutori ad elevata professionalità. Pertanto, nella nostra esperienza tutti gli addetti ai lavori operano in una chiarezza di competenze e di ruoli e, fino ad oggi, non abbiamo rilevato nessuna "zona grigia". Nelle organizzazioni di dimensioni minori o in settori dove i rischi sono più contenuti, c'è una certa varietà di situazioni, legata al tipo di settore e ai rischi prevalenti, ma comunque con una sensibilità e una preparazione decisamente accettabile e in crescita negli anni, grazie anche alla diffusione della cultura informatica nella sfera della persona, delle aziende e della società.

È possibile – in base ai rapporti con la grande utenza – definire oggettivamente le relazioni – anche indirette – tra sicurezza fisica e sicurezza informatica e individuare una terminologia neutra e di uso corrente?
Certamente, sono convinto che sia particolarmente opportuno, ma non vorrei limitarmi a un glossario, che non risulterebbe utile perché i termini sono legati a concetti da contestualizzare. Preferisco pertanto illustrare per punti il contesto PSIM, proponendo di **evidenziare in grassetto** la terminologia significativa o a rischio di ambiguità, spiegata in 3 punti:
1 – Citel realizza progetti di **sicurezza fisica che utilizzano strumenti informatici** e reti dati strutturate dell'utente per ottenere soluzioni di protezione dei suoi asset fisici (palazzi, sedi periferiche, stabilimenti, strutture commerciali, impianti di produzione energia, ecc.). Fin qui siamo nella sicurezza fisica che viene ottenuta usando strumenti informatici (il computer, il PSIM, le centrali di gestione eventi) **transitando su LAN e WAN** dell'utente per concentrare la gestione degli eventi in una control-room ma anche su posti operativi presso centri servizi o su apparati mobili.
2 – Quindi, il sistema informatico dipartimentale di sicurezza fisica, il PSIM Centrax nel caso di Citel, è connesso a LAN e WAN dell'utente utilizzando a livello centrale, secondo le dimensioni del progetto: una semplice Workstation oppure un insieme di Server, Posti di lavoro, Front-end, ecc.. Mentre in campo gli apparati che generano eventi sono raggiunti perché connessi ai router di una LAN che porta alla WAN. **La rete dati usata dal sistema informatico aziendale veicola quindi anche i dati di un PSIM che potrebbe introdurre delle vulnerabilità con un impatto potenziale sul sistema informatico gestionale dell'azienda.** Le vulnerabilità non sono quelle del software PSIM, ma quelle che (ad esempio attraverso una centrale di allarmi) potrebbero creare una sorta di pericolosa "porta di servizio" in un punto di una rete dati che per il resto è stata blindata da accessi non previsti. Il rischio per il sistema informatico gestionale non riguarda quindi il sistema Centrax in sé, ma deriva dalla eventualità dell'introduzione volontaria di **malware in rete che possa corrompere i dati gestionali trasmessi su LAN/WAN** o ne possa impedire la circolazione. Ma, se questo è un rischio originato dall'innesto di apparati del PSIM scelti dall'utente (intrusione, accessi, videosorveglianza, ecc.), non è altro che quello che accade ogni volta che qualsiasi altro sistema informatico dipartimentale dell'azienda (produzione, logistica, personale, ecc. con i relativi dispositivi specializzati da mettere in rete) viene innestato nella rete dati aziendale per ottenere un unico sistema informatico gestionale sempre più integrato.
3 - Ma l'azienda, che utilizza l'informatica per ogni processo produttivo e gestionale, ha anche l'esigenza di minimizzare i rischi di un attacco alla struttura fisica del Data Centre, cuore e sistema circolatorio dell'informatica aziendale. E, pertanto, si richiedono **misure di sicurezza fisica** che proteggano i computer, gli organi fisici di alimentazione e di comunicazione da attacchi esterni che ne possano bloccare il funzionamento interrompendo il servizio del sistema informatico e quindi l'operatività aziendale. **Pertanto, il cerchio si chiude constatando che in questo caso il PSIM, sistema di sicurezza fisica utilizzatore del Sistema Informatico anche contro attacchi di cyber security, in questo caso lo protegge da attacchi e incidenti di tipo fisico.**
Sembra un giuoco di parole ma serve a descrivere sinteticamente l'interdipendenza (non la convergenza!) della sistemistica di Sicurezza Fisica e della Sicurezza Informatica.