



**MASSIMO  
BECCHERLE**  
Direttore  
Commerciale  
Digitronica.IT

## SUPERVISIONE E DIALOGO TRA I SISTEMI PER PROTEGGERE IL VALORE DELL'AZIENDA



Massimo Beccherle

**C**on il crescere della competizione globale e lo svilupparsi di nuove forme di minacce esterne, la sicurezza ha guadagnato priorità fra le preoccupazioni di ogni azienda. Sia che si tratti di proteggere i dati, i processi o i prodotti, di difendere la proprietà intellettuale, o di salvaguardare le strutture, i luoghi di lavoro e di ricerca come di tutelarsi dalle intrusioni verificando la correttezza degli accessi, ormai il controllo totale è un'esigenza che ha assunto un'importanza centrale.

Fortunatamente oggi la diffusione delle più avanzate tecnologie telematiche viene incontro alle imprese e rende la sicurezza meno onerosa e più "friendly" dal punto di vista delle metodologie d'u-

so. Occorre però che l'evoluzione della sicurezza fisica proceda di pari passo con lo sviluppo della sicurezza logica, per evitare che i varchi che restano aperti in un comparto possano danneggiare anche l'altro.

La convergenza tra questi due mondi non è mai stata scontata: anzi, nell'epoca più pionieristica sembrava che le esigenze specifiche procedessero in parallelo senza il bisogno di incontrarsi per rendere il sistema più "stagno" e resistente alle minacce. Proprio su questa esigenza di far coincidere dapprima gli obiettivi e quindi i metodi Digitronica.IT ha fondato la propria filosofia di progettazione e di realizzazione di sistemi di sicurezza integrata.

Ricordiamo che all'origine della sicurezza fisica ci dev'essere sempre la concessione di un'autorizzazione all'accesso che inizia con un sistema identificativo (badge, pin, impronta,...) e termina con un

sistema attuativo che apre o chiude le porte e tutti gli altri sbarramenti fisici. Per accesso logico si intende invece una "porta virtuale", ovvero il rendere disponibile a un utente le informazioni, i dati e in generale i sistemi informativi che sono il patrimonio di un'azienda. Incrociando e sommando le singole sicurezze applicate a questi due ambienti, la sicurezza complessiva si moltiplica: da un lato un soggetto deve essere identificato e ricevere un'autorizzazione prima di accedere a uno spazio controllato, a un bene o a una qualunque altra risorsa azienda-

deve andare, con che funzioni, di quale livello di autorizzazioni dispone, per quanto tempo e così via.

Lo step successivo riguarda l'attuazione, ovvero chi regola l'accesso e secondo quali criteri. Ciò dipende in primo luogo dalle policy aziendali, che creano un processo decisionale e quindi operativo a cascata. Per quanto riguarda gli accessi fisici all'azienda, ad esempio, Digitronica.IT ha sviluppato un software applicativo, MultiAccess, per il monitoraggio delle persone che accedono a una struttura e che si muovono al suo interno, colle-

complessità è evidentemente aumentata con lo sviluppo della tecnologia. È chiaro quindi che le aziende e le strutture molto articolate devono risolvere ogni problema legato all'assenza di convergenza tra i due sistemi di sicurezza. In altre parole bisogna superare la difficoltà di identificare in maniera univoca un soggetto in entrambi i contesti, perché altrimenti non è possibile stabilire un parallelismo operativo tra i due tipi di accessi richiesti.

Emerge così con chiarezza la necessità di disporre di un sistema di supervisione che sia in grado di gestire tutte quelle operazioni che abbiano effetto in tempo reale sui vari sottosistemi. L'esempio tipico è l'abilitazione contemporanea di un nuovo nominativo aziendale sia per gli accessi fisici alla struttura che per gli accessi logici alla rete, come all'opposto la disabilitazione di un dipendente che cessa la sua collaborazione (situazione ancor più delicata, che richiede certezze assolute ed estrema rapidità di esecuzione).

Va qui sottolineato un altro elemento di potenziale fragilità del mondo aziendale: in molti casi, dalle piccole imprese ai grandi gruppi multinazionali, la sicurezza fisica e quella logica dipendono da strutture di vertice differenti e separate, che spesso non comunicano nemmeno tra loro e solo in pochi casi possono contare su una figura di supervisione. Abitualmente infatti il controllo degli accessi alla struttura fa capo alle direzioni Risorse umane o Servizi generali, mentre l'accesso alla rete è il più delle volte trattato come un problema di gestione di rete e quindi affidato alla direzione IT. Un sistema di supervisione sovra-

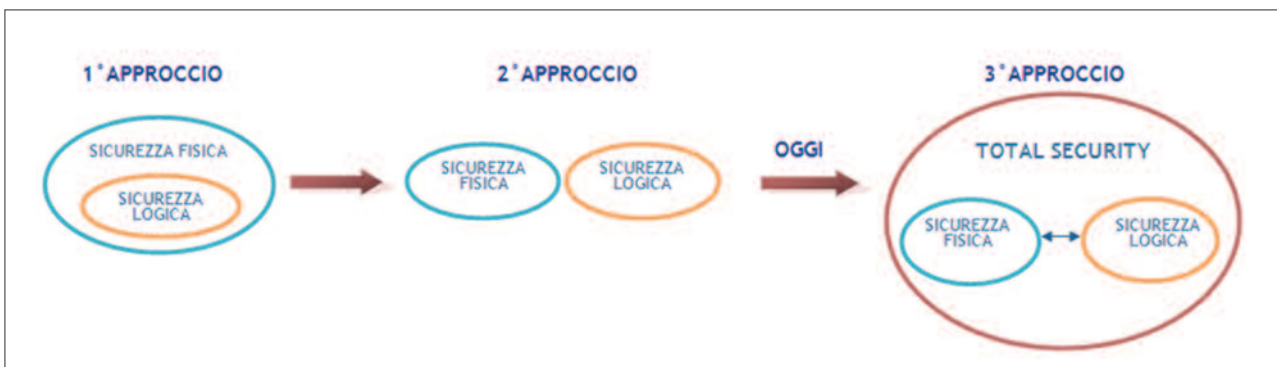
## **Una crescente convergenza tra sicurezza degli accessi fisici e logici è la nuova frontiera per la difesa delle strutture e delle reti.**

le; dall'altro lo stesso soggetto deve venire abilitato ad accedere anche ai dati e alle informazioni, i quali sono beni altrettanto preziosi ma intangibili, impalpabili.

Al punto d'incontro, cioè alla convergenza di questi due concetti, c'è quindi sempre una persona, che accede all'azienda sia fisicamente che in modo virtuale. Il primo passaggio della procedura consiste sempre nell'identificazione del soggetto: gli organi incaricati vengono a conoscenza di chi è la persona che deve accedere, dove

gato a lettori di badge che comandano le aperture.

Per garantire una sicurezza affidabile a tutta l'azienda, la stessa cosa deve avvenire in parallelo per gli accessi informatici, che sono ancora più delicati essendo invisibili e basato su una rete sempre più diffusa: la logica di fondo è la stessa (il sistema che detiene le informazioni deve verificare l'identità e le credenziali di chi chiede l'accesso, e solo ottenuta una risposta positiva può consentirlo, per tutta la rete o solo per alcuni livelli), ma la





stante che sia davvero efficace mette invece in comune le informazioni delle varie strutture e le trasmette a tutti gli interessati, e rende possibile la gestione degli accessi fisici e logici con una sola operazione, sia al momento dell'entrata in carico di un nuovo soggetto che alla sua uscita.

Ma vediamo in sintesi che cosa significa oggi incrociare le esigenze della sicurezza fisica con quelle della sicurezza logica, e quali soluzioni è più opportuno adottare. Come abbiamo visto, il problema principale è che non c'è adeguata convergenza tra i due sistemi, e chi regola l'accesso logico non dispone ancora dell'opportunità di crearsi dei "ponti" verso il controllo degli accessi fisici.

Il motivo più banale è che finora non ce n'era la mentalità: la sicurezza non era percepita come un valore da condividere e quindi non si riteneva necessario creare una adeguata rete per la circolazione delle informazioni. Adesso le cose stanno cominciando a cambiare, ma in qualche realtà aziendale il responsabile sicurezza si occupa soprattutto di quella fisica, ambientale, delle strutture e dei beni immobili (in sostanza come una sorta di "capo delle guardie"). E quando questa funzione dipende dalle Risorse umane, si tende naturalmente a porre più attenzione alle persone e agli accessi ai luoghi.

Invece la sicurezza logica, come abbiamo detto, è quasi sempre prerogativa della direzione IT, che riveste un ruolo più trasversale. Ma nonostante questo, e anche se il collegamento tra l'informatica e la sicurezza è ormai acquisito, non si è però ancora affermato il concetto di supervisione generale. Eppure anche grazie a una veloce evoluzione

dei sistemi esistono ormai software adeguati, capaci di dialogare con i sistemi di controllo degli accessi.

Il problema di fondo viene aggravato da un altro fattore: la nascita della cosiddetta informatica distribuita. Una volta bisognava essere fisicamente in una stanza per potersi sedere alla tastiera di un terminale, oggi invece si può accedere alla rete da qualunque punto diffuso sul territorio, non solo con il personal computer ma anche con un cellulare. La prima necessità è dunque concedere l'accesso alla rete solo alle persone "giuste".

Inoltre adesso nel sistema informatico risiedono – e non è un modo di dire – tante e tali informazioni da determinare la vita o la morte, il successo o il fallimento di una società. La rete aziendale, un'autentica biblioteca e cassaforte, sono custodite le idee e le risorse di tutti coloro che ci lavorano, ed essa va quindi protetta con le tecnologie più avanzate e la sua sicurezza va integrata con quella fisica.

E siccome al sistema si può accedere anche dall'esterno della sede aziendale, ecco perché serve un "guscio" esterno che protegga entrambi i sottosistemi attraverso una corretta e univoca identificazione, da condividere in tempo reale con tutta la struttura e i responsabili della sicurezza.

Digitonica.IT ha elaborato con SCS la sua risposta a questa esigenza. Il progetto è nato una decina di anni fa, quando ancora il concetto di convergenza tra sicurezza fisica e logica non era ancora universalmente acquisito. Il principio al quale ci si è ispirati è che occorre far confluire in un unico sistema le informazioni provenienti dai vari settori aziendali e dirette a più destinatari.

Con il tempo questa architettura si è sviluppata come sistema di supervisione degli accessi fisici e logici, fino a dar vita a un'ampia serie di prodotti riuniti in una suite. SCS, il sistema integrato che sovrintende alle procedure di gestione degli accessi e della sicurezza, è un software che concentra in un unico database i dati anagrafici e organizza le interfacce utente per favorire il dialogo tra le applicazioni.

In conclusione, lo sviluppo di una convergenza tra sicurezza fisica e logica è la sola risposta possibile a una crescente complessità delle minacce che un'impresa deve affrontare. Perciò i destinatari di questa nuova filosofia sono sia aziende piccole o medie che molto grandi: più che la dimensione in termini di addetti o di estensione sul territorio (che pure hanno una loro incidenza diretta sulla scelta del software applicativo e delle metodologie di attuazione) occorre tenere presente qual è la produzione di valore, o meglio ancora il "valore" della produzione.

In altre parole è necessario proteggere con la stessa cura sia una piccola azienda che lavora metalli pregiati o pietre preziose che una grande struttura la cui "miniera" è rappresentata dai dati e dalle informazioni, soprattutto se si tratta di un gruppo che opera nel campo della ricerca o dello sviluppo di processi o prodotti innovativi. In definitiva si può dire che mentre la sicurezza fisica deve la sua crescente efficacia a un sempre maggiore contenuto di software, dall'altra parte un operatore di sicurezza logica deve "difendere" il proprio perimetro virtuale di responsabilità con la stessa cura un tempo applicata al controllo degli accessi reali. ■