Passare a un sistema di controllo accessi ad architettura aperta, i vantaggi chiave

di Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc

Il mercato del controllo accessi è molto cambiato nell'ultimo decennio. In precedenza, i vecchi sistemi di controllo accessi (ACS) con hardware proprietario legavano le aziende a singoli fornitori e a soluzioni stagnanti. Oggi, l'arrivo di nuove tecnologie ha fornito una scelta più ampia di sistemi e componenti, che ha permesso di soddisfare esigenze mirate potenziando l'ACS preesistente.

Tuttavia, alcune aziende rimangono aggrappate a tecnologie ACS obsolete, pur conoscendone gli svantaggi. La paura dei costi associati alla migrazione scoraggia l'aggiornamento, inducendo a impiegare tempo e denaro nella manutenzione dei vecchi sistemi.

Alcuni vedono l'acquisto di un nuovo ACS esclusivamente come un esborso di capitale, ma non come un potenziale ritorno sull'investimento (ROI). Con tale premessa, non considerano opzioni alternative alla semplice manutenzione del sistema. Se ragionassero sull'aggiornamento con un approccio ROI, vedrebbero rapidamente i vantaggi, compresi quelli relativi ai costi. Migrando a un ACS unificato, basato su un'architettura aperta IP (come Security Center **Synergis**™ di Genetec), si può massimizzare l'investimento sulla sicurezza migliorando tutte le aree del business, dalla gestione delle presenze in tempo reale al monitoraggio dei perimetri.

Protezione del business

Un ACS unificato può fare molto di più del semplice bloccare e sbloccare le porte. Può tutelare persone e risorse aziendali più efficacemente e migliorare operazioni e capacità decisionali.

Synergis, per esempio, è in grado di aggregare e visualizzare dati in modo dinamico, con dashboard del tutto personalizzabili e che combinano i dispositivi live con rapporti, grafici e istogrammi. Ciò significa che il team di sicurezza, con una semplice occhiata, ottiene una visione unificata di ciò che avviene sul sito o all'interno dei sistemi. Tracciando segnali e informazioni chiave, le dashboard organizzano gli eventi in prospettiva. Per esempio, una dashboard che traccia gli allarmi attivi insieme ad altre metriche, tra cui il numero di clienti in attesa, può avvertire gli operatori quando una situazione va fuori controllo. Questo permette di identificare per tempo potenziali problemi e a scegliere le opportune contromisure.

Il vero costo dei sistemi legacy: indifesi contro la criminalità informatica

I vecchi sistemi, sono stati progettati per soddisfare le esigenze aziendali in un dato momento. Con l'evolversi delle esigenze e della tecnologia, possono diventare obsoleti. Alcuni, ad esempio, limitano la possibilità d'inserire nel sistema di sicurezza fisica novità come serrature wireless e credenziali mobili. Altri richiedono aggiornamenti e supporto costante solo per continuare a funzionare. I ricambi possono essere difficili da trovare e sono spesso costosi. Le opzioni che supportano software e hardware superati sono limitate. Inoltre, se l'ACS è proprietario e fortemente integrato nel sistema, può comportare ulteriori costi di manutenzione.

I sistemi di controllo accessi sono un importante strumento infrastrutturale, che tende ad essere trascurato come potenziale vettore di attacchi informatici. Poiché essi sono in genere collegati alla rete aziendale, se un criminale informatico riesce a violarli, non solo può aprire e chiudere le porte a piacimento, può anche ottenere il controllo su qualsiasi sistema collegato. Una volta che la rete è violata, tutti i dati sono vulnerabili, comprese le informazioni sensibili. I criminali cercheranno quelle in grado di generare il maggior

guadagno, quindi i dati personali di dipendenti e clienti o gli estremi finanziari dell'azienda. Compromettendo l'account Active Directory di un singolo utente, un criminale può mascherare gli account che ruba, rendendo impossibile per il sistema di sicurezza ritrovarli. Per proteggere dati e reti, le aziende hanno pertanto bisogno di un ACS all'altezza.

Aumentare il ROI

Per evitare battute d'arresto dovute a sistemi chiusi, occorre un ACS flessibile e aperto, che si evolva di pari passo con le esigenze aziendali, fornisca soluzioni aggiornate, permetta di arricchire i sistemi con le nuove tecnologie e sia capace di scalare attraverso hardware aggiuntivi, moduli software built-on e integrazioni software aperte con prodotti di terze parti. Synergis permette di personalizzare i sistemi, selezionando l'hardware che risponde a esigenze di sicurezza specifiche. Permette di risparmiare tempo e denaro riutilizzando l'hardware esistente piuttosto che migrare a un sistema completamente nuovo. Centralizza le operazioni in una singola piattaforma, riducendo i tempi di risposta e garantendo una sicurezza coerente in tutta l'organizzazione, attraverso l'automazione delle procedure operative.
Correlando i dati, Synergis fornisce anche una visione globale degli ambienti, permettendo al team di sicurezza di valutare e rispondere agli incidenti in modo rapido ed efficace.

Synergis aiuta a proteggere dal crimine informatico e a garantire la conformità

Synergis è costruito pensando alla sicurezza informatica. Protegge l'ACS in modo end-to-end, con tecnologie di smart card, protocolli di comunicazione bidirezionali sicuri tra lettore e controller e registri crittografici avanzati per comunicazioni protette su Internet.

Se combinato con **ClearID**, aiuta a gestire i diritti d'accesso temporanei e a rafforzarne le politiche, poiché il sistema permette solo a individui autorizzati di accedere alle aree protette. Questo è particolarmente importante per le aziende che operano in settori regolamentati, sottoposte a ulteriori politiche di sicurezza.
Un altro modo per consolidare la sicurezza è creare gruppi di controllo accessi e assegnare privilegi specifici a ognuno di loro, per un facile smistamento degli utenti. Ciò assicura che gli operatori abbiano accesso solo alle aree necessarie alle loro funzioni, mentre privilegi speciali possono essere accordati a dipendenti di livello superiore oltre al normale orario d'ufficio.
ClearID dispone inoltre di una funzione integrata di gestione dei visitatori, che semplifica i processi di check-in e check-out assegnando a ognuno diritti specifici, consentendo di creare in anticipo carte di controllo secondo privilegi pre-programmati.

Contatto:
Gianluca Mauriello,
Regional Sales Manager Italia, Genetec Inc.
Tel. +39 327 739 8560
www.genetec.com