MANUTENZIONE, AGGIORNAMENTI E SERVICE SONO ELEMENTI DECISIVI PER GARANTIRE L'AFFIDABILITÀ DEI SISTEMI DI SICUREZZA, A MAGGIOR RAGIONE QUANDO SI PARLA DI UN AMBITO VERTICALE COME LE INFRASTRUTTURE CRITICHE. GIANCARLO GIUNCA, SERVICE MANAGER DORMAKABA ITALIA, SA BENE COSA QUESTO SIGNIFICHI PER CHI SI OCCUPA DI CONTROLLO ACCESSI

Tecnologia, ma... non solo

di **Giacomo Longo**

Quando si parla di sicurezza, l'attenzione si concentra quasi sempre sulle tecnologie installate, ma molto meno su ciò che ne garantisce l'efficienza col passare del tempo: manutenzione, aggiornamenti e service.
Eppure è proprio qui che si gioca una parte decisiva dell'affidabilità del sistema, soprattutto in quei contesti sensibili (ospedali, data center o altre infrastrutture critiche) in cui la presenza di un impianto non adeguatamente gestito può tradursi in vulnerabilità operative o interruzioni che mettono a rischio la continuità delle attività e l'immagine dell'azienda.
Di come questo tema si declina per i professionisti che si occupano di sistemi di controllo accessi, abbiamo parlato con Giancarlo Giunca, Service Manager dormakaba Italia.

Negli edifici complessi e nelle infrastrutture critiche, il tema del service è diventato centrale quanto quello della tecnologia installata…
Al giorno d'oggi l'erogazione dei servizi di manutenzione e assistenza non è più un tema secondario rispetto alla tecnologia: si tratta di due facce della stessa medaglia.
Anche la soluzione tecnica più avanzata, se non supportata da un'assistenza adeguata e continuativa, perde la sua efficacia, con evidenti rischi per la sicurezza delle persone e degli asset che si vogliono proteggere. E non è questione soltanto di operatività: una violazione della sicurezza può tradursi in un danno reputazionale significativo, spesso ben più oneroso dell'intervento tecnico stesso. Nelle infrastrutture critiche questo concetto è ancora più evidente.
In un aeroporto, in un ospedale o in un sito produttivo, un varco che non funziona correttamente non rappresenta solo un disagio operativo: può compromettere protocolli di sicurezza, percorsi di emergenza, o la segregazione di aree ad accesso controllato. Il service, in questi ambienti, diventa parte integrante del sistema di sicurezza stesso.
C'è poi un altro aspetto che spesso viene sottovalutato: la complessità crescente delle soluzioni. I sistemi moderni integrano hardware, software, connettività e logiche legate alla cybersecurity. Mantenerli efficienti nel tempo richiede competenze che vanno ben oltre la semplice manutenzione meccanica. Il team deve quindi essere in grado di affrontare problemi complessi.
Per questo in dormakaba stiamo investendo molto sulla struttura del service, non solo in termini di tempi di risposta, ma nella qualità delle competenze, nella capacità di pianificare interventi preventivi e nel dialogo costante con il cliente. Perché il vero obiettivo non è riparare un guasto, è fare in modo che il guasto non impatti mai sulla continuità operativa del cliente.

Un service non strutturato crea vulnerabilità che si accumulano nel tempo, fino a manifestarsi nel momento peggiore possibile. Il nostro compito è fare in modo che quel momento non arrivi mai
Giancarlo Giunca, Service Manager dormakaba Italia

Nel caso di ospedali, data center, siti industriali o grandi hub logistici, quali sono i rischi concreti di un service non strutturato?
Quando parliamo di infrastrutture critiche, i rischi di un service non strutturato sono molto concreti e, in alcuni casi, possono avere conseguenze serie sulla sicurezza delle persone, non solo sulla continuità dei processi.
Per esempio, prendendo il caso di un ospedale, il controllo degli accessi presidia aree ad altissima criticità. Un sistema non manutenuto correttamente può generare anomalie nei permessi di accesso, consentire ingressi non autorizzati in aree protette o bloccare l'accesso al personale medico in situazioni di emergenza.
In un data center, la segregazione fisica degli spazi è parte integrante del modello di sicurezza. Un varco che non funziona correttamente, o un sistema di accesso con credenziali non aggiornate, possono vanificare investimenti in cybersecurity. La sicurezza fisica e quella digitale sono sempre più interconnesse.
In un sito industriale, ci sono spesso normative molto stringenti: basti pensare alle certificazioni GMP nel farmaceutico, che impongono una tracciabilità precisa degli accessi e una documentazione rigorosa degli interventi di manutenzione.
Un service non strutturato espone l'azienda non solo a rischi operativi, ma anche alla non conformità normativa, con impatti in termini di audit e certificazioni.
In un hub logistico, infine, la continuità operativa è tutto. Varchi automatici, porte scorrevoli e a battente automatizzate, che gestiscono il flusso di entrata e uscita di merci e persone su tre turni, 7 giorni su 7, non possono permettersi tempi di fermo non pianificati. Il rischio non è solo operativo, è sistemico. Un service non strutturato crea vulnerabilità che si accumulano nel tempo, fino a manifestarsi nel momento peggiore possibile. Il nostro compito è fare in modo che quel momento non arrivi mai.

Quanto incidono manutenzione preventiva e gestione del ciclo di vita dei sistemi sulla resilienza complessiva di un edificio?
La manutenzione preventiva e predittiva rappresenta un investimento sulla prevedibilità dei guasti. In un edificio complesso o in un'infrastruttura critica, poter prevedere quando un componente sta arrivando alla fine del suo ciclo di vita è un valore concreto.
Significa poter pianificare la sostituzione nel momento meno impattante per la continuità operativa del cliente, invece di gestire un guasto improvviso in una situazione critica.
C'è poi una dimensione economica che spesso viene trascurata. La manutenzione preventiva costa, ma le conseguenze economiche di un fermo in un'infrastruttura critica, in termini di ripristino di emergenza, sono sempre significativamente superiori. Quando aiutiamo il cliente a ragionare su questi numeri in modo trasparente, la percezione del valore della manutenzione preventiva cambia.
Inoltre, un sistema installato dieci anni fa può essere ancora funzionante, ma potrebbe non essere più aggiornabile, potrebbe avere vulnerabilità non più correggibili, potrebbe non essere integrabile con le nuove esigenze del cliente. Ignorare questo significa accumulare un debito tecnologico che prima o poi si paga.

Il nostro approccio è quello di affiancare il cliente con una visione pluriennale: una roadmap che mappa lo stato di salute di ogni componente del sistema, ne prevede il ciclo di vita e pianifica gli interventi di aggiornamento o sostituzione in modo coerente con il budget e le priorità del cliente.
Questo trasforma il service da una voce di spesa imprevedibile a un elemento pianificabile e controllabile.

Dal punto di vista normativo e delle responsabilità, cosa può comportare una gestione non adeguata dei sistemi di accesso?
Le implicazioni normative e di responsabilità in questo settore sono reali e significative e spesso vengono sottovalutate.
I sistemi di controllo accessi nelle infrastrutture critiche non sono semplici installazioni tecnologiche, sono parte integrante di un sistema di sicurezza che risponde a normative precise, che variano per settore ma hanno tutte un denominatore comune: richiedono che i sistemi siano mantenuti in efficienza, documentati e verificati nel tempo.
In ambito ospedaliero e sanitario, per esempio, esistono requisiti stringenti legati all'accreditamento delle strutture che impongono standard precisi sulla gestione degli accessi in aree sensibili. Una non conformità rilevata in sede di audit può mettere a rischio l'accreditamento stesso della struttura con conseguenze che vanno ben oltre il tema tecnico. In ambito farmaceutico, le normative GMP e le ispezioni delle autorità regolatorie come Aifa o Fda richiedono una tracciabilità rigorosa e documentata di chi accede a determinate aree produttive. Un sistema non manutenuto, con log non affidabili o accessi non correttamente profilati, può generare non conformità gravi in sede di ispezione.
In ambito aeroportuale e delle infrastrutture di trasporto, le normative di security imposte da Enac e dalle direttive europee sono molto precise sulla gestione degli accessi in "air side" o "land side". Una vulnerabilità in questi sistemi non rappresenta solo un problema tecnico: può avere implicazioni di sicurezza pubblica.
C'è poi una dimensione di responsabilità civile e contrattuale che riguarda direttamente chi gestisce questi impianti. Se un incidente di sicurezza dipende per esempio da una manutenzione non eseguita, le responsabilità possono ricadere sul conduttore dell'impianto. Oggi, in un contesto in cui la tracciabilità degli interventi è sempre più richiesta, non disporre di uno storico chiaro rappresenta già un fattore di rischio.

dormakaba affianca il cliente con una visione pluriennale: una roadmap che mappa lo stato di salute di ogni componente del sistema

Infine, con l'evoluzione normativa legata alla direttiva NIS2 - che estende gli obblighi di sicurezza anche alla componente fisica delle infrastrutture critiche - il perimetro di responsabilità si sta ulteriormente allargando. Chi gestisce sistemi di accesso in contesti critici deve iniziare a ragionare in un'ottica di compliance integrata, che mette insieme sicurezza fisica, sicurezza informatica e gestione del rischio in modo coordinato.
Una gestione non adeguata dei sistemi di accesso non espone solo a rischi operativi ma anche a rischi legali, normativi e reputazionali che possono avere conseguenze durature.

Guardando ai prossimi anni, quali competenze diventeranno indispensabili nei team service che operano sulla sicurezza degli edifici complessi?
I confini tra sicurezza fisica e sicurezza digitale si stanno via via dissolvendo. Dovremo investire molto sulla formazione dei nostri tecnici, consentendo loro di avere non solo una formazione meccanica ed elettrica ma anche una comprensione di base delle logiche software e dei protocolli di rete. Nei prossimi anni questa integrazione tra parti meccaniche controllate da intelligenza software diventerà ancora più profonda: i sistemi di controllo accessi saranno sempre più connessi e basati su cloud, quindi esposti a minacce che arrivano dal perimetro digitale prima ancora che da quello fisico. Non è possibile gestire la sicurezza fisica senza capire quella digitale, e viceversa.
Avremo bisogno di migliorare la nostra capacità di leggere e interpretare i dati. I sistemi moderni generano grandi quantità di informazioni: log di accesso, dati di utilizzo, anomalie comportamentali, segnali predittivi di guasto. Un team service moderno deve saper trasformare i dati in decisioni: anticipare un problema prima che si manifesti, individuare situazioni anomale, ottimizzare i piani di manutenzione sulla base di evidenze concrete. Questo richiede una mentalità analitica che in passato non era necessariamente richiesta ai tecnici di campo, ma che oggi diventa sempre più centrale.
La terza area di competenza è la conoscenza normativa e di compliance. Il quadro normativo si sta evolvendo rapidamente, tra NIS2, normative di settore e requisiti di certificazione sempre più rigorosi. Dobbiamo essere in grado, quindi, di affiancare il cliente anche su questo fronte, supportandolo nelle scelte tecniche per garantire che gli impianti siano sempre conformi.
C'è poi una competenza cui tengo in modo particolare, perché è quella più difficile da sviluppare e più facile da sottovalutare: la capacità relazionale e consulenziale. Il tecnico service del futuro non è solo qualcuno che risolve problemi tecnici, è qualcuno che sa dialogare con il facility manager, con il responsabile della sicurezza, con il CTO di un'azienda complessa. Sa tradurre concetti tecnici in linguaggio di business, sa identificare esigenze che il cliente non ha ancora saputo esprimere, sa costruire fiducia nel tempo. Questa dimensione consulenziale trasforma il service da funzione reattiva a funzione strategica.
A questo si aggiunge un altro elemento fondamentale: la stratificazione verticale delle competenze. Un team efficace non è composto da tecnici intercambiabili con competenze organizzate in modo esclusivamente orizzontale e trasversale su più funzioni, ma da una struttura verticale specializzata su più livelli, in cui responsabilità e profondità tecnica sono chiaramente definite.
Accanto a questo, diventa sempre più rilevante la specializzazione per contesto. Chi opera in un aeroporto deve conoscere non solo i sistemi che gestisce, ma anche la logica operativa di quell'ambiente: i flussi, le normative specifiche, le procedure di emergenza. La comprensione del contesto applicativo è parte integrante della qualità del service.
Infine, guardando ancora più avanti, vedo crescere l'importanza della capacità di lavorare con sistemi basati su intelligenza artificiale. La manutenzione predittiva, la gestione automatizzata degli accessi, il riconoscimento di anomalie comportamentali sono tutte aree in cui l'AI sta entrando in modo concreto.
I nostri team dovranno essere in grado di supervisionare questi sistemi, di interpretarne gli output e di intervenire quando la macchina da sola non basta.
In sintesi, il tecnico service del futuro sarà una figura ibrida: solida tecnicamente, capace di ragionare sui dati, consapevole del contesto normativo e in grado di relazionarsi con interlocutori diversi. Non è una figura facile da trovare ma è quella su cui stiamo investendo, perché siamo convinti che la qualità del service nei prossimi anni farà la differenza competitiva nel nostro settore.

6 COMPETENZE PER IL TECNICO SERVICE DEL FUTURO

- **FORMAZIONE NON SOLO MECCANICA ED ELETTRICA, ma con una comprensione di base delle LOGICHE SOFTWARE e dei PROTOCOLLI DI RETE**
- **Capacità di LETTURA E INTERPRETAZIONE DEI DATI GENERATI DAI SISTEMI DI SICUREZZA, in modo da saper trasformare le informazioni in decisioni**
- **CAPACITÀ DI LAVORARE CON L'INTELLIGENZA ARTIFICIALE, di supervisionare questi sistemi e interpretarne gli output**
- **CAPACITÀ RELAZIONALE E CONSULENZIALE, che permette di dialogare e comunicare con interlocutori e figure aziendali diverse**
- **Specializzazione per contesto e COMPRENSIONE DELL'AMBITO APPLICATIVO IN CUI SI VA AD AGIRE**
- **CONOSCENZA NORMATIVA E DI COMPLIANCE, per garantire al cliente la conformità degli impianti**