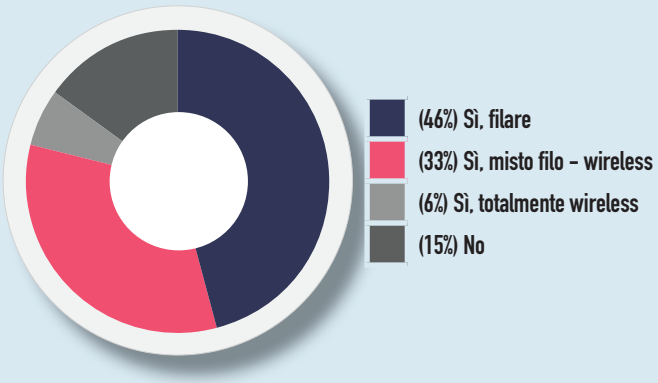
Ilaria Garaffoni

Nel controllo accessi semplicità vuol dire praticità

La tecnologia wireless sta trasformando ogni aspetto del nostro quotidiano: dalle cuffie per ascoltare la musica al pubblico trasporto, dai pagamenti all'accesso ad Internet. Non fanno eccezione ovviamente le modalità con cui entriamo, usciamo - e gestiamo - gli edifici, dal momento che sono sempre più diffuse tecnologie come Bluetooth Low Energy (BLE) e WiFi 6, lo standard wireless di ultima generazione che consente agli access point di supportare più connessioni in ambienti ad alta densità, offrendo più performance delle reti LAN wireless convenzionali, soprattutto per dispositivi Internet of Things. Ma a che punto è la transizione dai dispositivi meccanici tradizionali verso i sistemi elettronici di controllo degli accessi?

Secondo l'ultima indagine IFSEC "The Wireless Access Control Report 2023", il processo di transizione continua ormai inesorabilmente, ma non è più solo un fatto di sicurezza. La praticità – intesa come facilità di utilizzo e comodità sia per gli operatori che per gli utenti – gioca infatti un ruolo fondamentale nel processo. Il motivo più comune per l'adozione di credenziali di accesso mobile è risultata essere infatti proprio la convenience (praticità). Se dunque la sicurezza è ormai data per assunta, che devono fare i vendor per assicurare un'esperienza d'uso sempre più flessibile, adattabile e scalabile?

Avete un sistema elettrico di controllo accessi?



Fonte: "The Wireless Access Control Report 2023" (IFSEC Insider – Assa Abloy)

Accesso mobile superstar

Correlata alla transizione wireless, si staglia la tendenza verso forme di controllo dell'accesso basato su dispositivi mobili, leggi smartphone. Secondo gli analisti di Omdia, nel 2021 sono state scaricate quasi 29,8 milioni di "credenziali mobili" per il controllo degli accessi a livello globale e il numero è destinato a crescere ad una CAGR del 44,9% tra il 2021 e il 2026. Nessun'altra apparecchiatura del segmento Physical Access Control (PACS) potrebbe mai sperimentare un tasso di crescita minimamente comparabile a questo, trattandosi di dispositivi di massa, dichiaratamente B2C.
Sebbene raramente utilizzate come unica modalità di credenziale, le soluzioni di controllo accessi abilitate per dispositivi mobili continuano a crescere anche secondo l'indagine IFSEC: il 29% delle realtà intervistate ha infatti affermato di aver utilizzato credenziali mobili (+3% sul 2021).

I benefici

Maggiore praticità per utenti e amministratori e un ulteriore livello di sicurezza generato dagli stessi smartphone (che ormai quasi sempre richiedono un'autenticazione prima dell'uso, compresi riconoscimento facciale, impronte digitali o autenticazione a due fattori) sono tra i primi vantaggi. Anche qui la praticità è la motivazione all'acquisto più gettonata, davanti al costo e anche alla sicurezza. L'utente ha infatti sempre con sé il cellulare ed è improbabile che lo smarrisca, inoltre è difficile condividere le credenziali mobili con persone non autorizzate o clonare un accesso mobile. Gli utenti hanno anche considerato il fatto che le credenziali mobili sono un'opzione più sostenibile rispetto alle chiavi magnetiche. Tra i non tanti (il 19%) che hanno votato invece il costo come elemento ostativo all'acquisto, molti hanno specificato che in realtà il timore più grande relativo al costo era rappresentato dalla sostituzione delle apparecchiature esistenti. Il mercato offre però oggi molte soluzioni che si possono integrare con i sistemi preesistenti, quindi non occorre sempre rifare tutto l'impianto per abilitare i lettori alle tecnologie mobile. Inoltre si può eseguire l'aggiornamento verso soluzioni "mobile ready" per rendere il loro accesso mobile "futuribile" senza però dover sostituire tutto nell'immediato. Alcuni sistemi di controllo accessi ricevono regolarmente patch di aggiornamento software: l'implementazione di una soluzione di accesso mobile non comporta dunque necessariamente un rinnovo totale. Ad esempio, con lettori abilitati BLE (Bluetooth Low Energy), gli utenti possono passare al cellulare quando decideranno che sia effettivamente giunto il tempo di farlo, senza dover in futuro sostituire il lettore.

Principali vantaggi della tecnologia mobile

Fonte: "The Wireless Access Control Report 2023" (IFSEC Insider – Assa Abloy)

Controllo accessi wireless e sostenibilità

Si assiste di tempo ad una crescente consapevolezza del ruolo della sicurezza fisica nell'acquisizione degli obiettivi di sostenibilità perseguiti dalle aziende. In questo senso, il controllo degli accessi è spesso ritenuto il punto di partenza per gestire l'efficienza di una struttura, perché permette di calibrare illuminazione, alimentazione elettrica e HVAC in base al reale livello di occupazione delle diverse aree dell'edificio. I sistemi wireless di per sé possono ulteriormente contribuire alla causa perché sono più energeticamente efficienti rispetto alle controparti cablate: consumano infatti meno energia e richiedono meno manutenzione, oltre al fatto - non irrilevante - che contemplano meno elementi (vedi cavi elettrici e rame) da installare e manutenere. Il che significa anche meno trasferte in loco da parte di tecnici e manutentori. Se poi si usano sistemi abilitati al mobile per accedere all'edificio, si ridurranno i RAEE da smaltire: quando i cellulari raggiungeranno il loro fine vita, verranno smaltiti senza dover aggiungere anche badge o chiavi.

Ma l'utenza chiede di più

Gli utenti finali però vogliono di più: uno su tre (34%) crede che i sistemi dovrebbero essere autoalimentati (cioè senza batterie); il 37% vuole prodotti realizzati con un'alta percentuale di componenti e parti riciclabili; il 25% vuole meno imballaggi o imballaggi facilmente riciclabili e un buon 20% vuole implementare sistemi di controllo accessi dotati di certificazione di sostenibilità (come la dichiarazione Ambientale di Prodotto EPD, Environmental Product Declaration) o di specifiche di bioedilizia secondo protocolli ambientali come BREEAM o LEED.

Certamente i sistemi di controllo accessi sono la chiave per rendere un edificio più integrato ed efficiente dal punto di vista energetico. Parte di questo processo può comportare l'integrazione del sistema di controllo accessi in una piattaforma di Building Management Systems che consenta, ad esempio, di accendere luce, gas e raffrescamento nella tale scrivania/stanza/area dell'edificio solo quando il sistema di controllo accessi abbia autorizzato il tale soggetto ad accedere alla tale zona.

La sicurezza cyber, spina nel fianco

L'indagine IFSEC rivela una preoccupante ignoranza, tra gli operatori professionali del settore, delle più banali normative in materia cyber, come l'European Cybersecurity Act, la NIS2, il Product Security and Telecommunications Infrastructure (PSTI) Act o l'European Cyber Resilience Act.

Oltre la metà degli intervistati non risulta essere nemmeno a conoscenza di questi regolamenti né sapere dell'esistenza di certificazioni di sicurezza informatica. Il tutto in un contesto in cui, per contro, il 35% degli utenti ritiene che la loro scelta del sistema di controllo accessi possa contribuire a rafforzare anche significativamente la sicurezza informatica dell'azienda, giocando un ruolo di rilievo anche ai fini della *compliance* normativa. È evidente che, con tanti dispositivi di sicurezza fisica ormai permanentemente connessi, è imperativo che la cultura dei professionisti della sicurezza fisica debba estendersi anche alla cyber security... diversamente il sistema fisico di controllo accessi potrebbe diventare il punto d'accesso più facile da colpire per gli hacker.

Standard aperti: un must

Di fondamentale importanza per la determinazione all'acquisto è che il sistema di controllo accessi wireless sia integrabile in una soluzione di sicurezza completa. E non solo con altri impianti di security, ma in una più ampia piattaforma di gestione degli edifici (di per sé richiesta per gestire in modo efficiente le risorse energetiche in base alle presenze reali). L'utilizzo di open standard è quindi cruciale. Come emerge dal report di Omdia *Smart Buildings Intelligence Service,* l'evoluzione degli edifici intelligenti e l'integrazione dei sistemi hanno portato ad una crescita di sistemi elettronici di controllo accessi: oltre il 27% dell'hardware per sistemi di controllo accessi nel 2020 sarebbe infatti stato integrato in una piattaforma BMS o di gestione (PSIM).

CLOUD: sì o no?

Nel settore del controllo accessi il trend verso l'utilizzo del cloud – netto in altre aree della security fisica - è ancora frammentato. Se il 51% degli intervistati di IFSEC (erano il 65% nel 2021) dichiara infatti di utilizzare ancora server locali per il controllo accessi, solo uno su cinque (il 22%) ospita il proprio sistema localmente, ma usa comunque un sistema di gestione degli accessi basata su cloud. E solo il 12% degli intervistati (in aumento comunque di un punto percentuale sul 2021) si affida

ad un cloud di terze parti per i servizi ACaaS (controllo degli accessi come servizio).
Secondo IFSEC, il motivo principale per cui le aziende scelgono un provider SaaS o ACaaS esterno è per l'automatizzazione degli aggiornamenti di software e patch (39%). Tra gli altri vantaggi si annoverano la capacità di offrire sistemi di controllo accessi in tempo reale (38%), una scalabilità essenzialmente illimitata (29%) e un business model basato su canone, che non obbliga a forti investimenti in sistemi di controllo accessi che nel lungo periodo potrebbero non soddisfare più le necessità aziendali. Certamente, assieme ai vantaggi, gli utenti vedono anche i potenziali rischi di gestire la sicurezza nel cloud, tra i quali si staglia il timore di violazioni informatiche. Questa è la più grande preoccupazione di oltre un intervistato su quattro (28%); al secondo posto troviamo la privacy e la protezione dei dati (20%). È interessante notare che il 17% degli intervistati non mostra tuttavia alcuna preoccupazione: si tratta certamente di un indicatore di crescente fiducia nel cloud.

Ostacoli all'acquisto

Ma cosa frena l'utenza finale dall'acquistare un sistema elettronico di controllo accessi?
Il 41% degli intervistati ha risposto che le decisioni sulla security non vengono prese, e spesso nemmeno influenzate, da veri esperti di sicurezza; il 33% ha detto che la sicurezza non è ritenuta core business e il 30% che il budget è insufficiente (dato in calo comunque rispetto al 46% della scorsa edizione). Dati che non sorprendono, visto che un report datato 2022 dell'SRI - *Security Research initiative* – rileva che quando la funzione di security non ha potere decisionale (o non è *dotata di portafoglio,* come diremmo con un linguaggio ministeriale) – l'insufficienza del budget per la sicurezza diventa un ostacolo costante. Ma purtroppo nella stanza dei bottoni spesso non c'è sufficiente percezione delle reali minacce di sicurezza. Secondo il rapporto SRI, le possibilità di ottenere un budget adeguato crescono infatti se la funzione di security viene considerata fondamentale per il business (86%). Ma come devono fare i professionisti della sicurezza ad essere ascoltati, a diventare essenziali? Secondo la ricerca IFSEC, per la metà degli intervistati occorre saper evidenziare i rischi della non-sicurezza, mentre il 44% crede che i dati generati dai sistemi di sicurezza dovrebbero poter essere utilizzati come evidenze probatorie in altre aree del business, ad esempio nella gestione delle presenze per la gestione dei modelli di lavoro ibridi e per il miglioramento dell'efficienza energetica solo riscaldando e/o illuminando le aree dell'edificio occupate. Il 28% degli intervistati ritiene infine che per essere ascoltati occorre mettere in relazione la spesa per la sicurezza con la fornitura di dati e il miglioramenti ad altri reparti.
Inoltre, un intervistato su tre ritiene che il budget per la sicurezza fisica dovrebbe essere collegato ai budget informatici/IT (tema rispetto al quale i vertici sono ormai sempre più sensibili).

Come risolvere il problema budget?

- (52%) sottolineare i rischi del non raggiungimento degli obiettivi di sicurezza
- (44%) migliorare l'uso dei dati generati dai sistemi di sicurezza
- (34%) collegare il budget per la sicurezza fisica a quello per la sicurezza cyber

Fonte: "The Wireless Access Control Report 2023" (IFSEC Insider – Assa Abloy)

Misurabilità dei dati

Un punto molto sentito, in tutte le aree della security, è la necessità di misurare i benefici generabili da processi efficaci basati sui dati rilevati dagli impianti di sicurezza.
Un esempio in area TVCC: più alto è il *conversion rate* e meno si verificano furti cd. per opportunità. Quanti visitatori si trasformano in clienti è un dato estraibile ed analizzabile dalla videosorveglianza, ma di fatto incarna un KPI che esula dagli indicatori strettamente di security per migliorare le performance di un negozio. Bene, il controllo accessi ci dice non solo quante persone sono in un luogo, ma volendo – e al netto delle questioni privacy, comunque superabili seguendo correttamente la normativa – anche chi è presente in quel luogo. E se quel luogo fosse un'area restricted, magari accessibile solo con una specifica vestizione e attrezzatura, allora gli effetti sarebbero non solo di security ma anche di safety, e magari di sicurezza sanitaria. Aspetti sempre più intrecciati e di sempre maggior rilievo.