La Redazione

Controllo accessi: la gestione degli eventi

"Transiti regolari, utenti non riconosciuti, tentativi di ingresso non autorizzati. E poi: errori, anomalie, allerte, allarmi… In un sistema elettronico di controllo accessi gli eventi si susseguono a un ritmo incalzante. Informazioni da rilevare, catalogare, memorizzare, trasmettere, convertire, visualizzare, stampare, condividere con altri impianti di sicurezza, archiviare, ripescare… Una vita spesso breve ma intensa. Vediamo in sintesi le tappe principali.

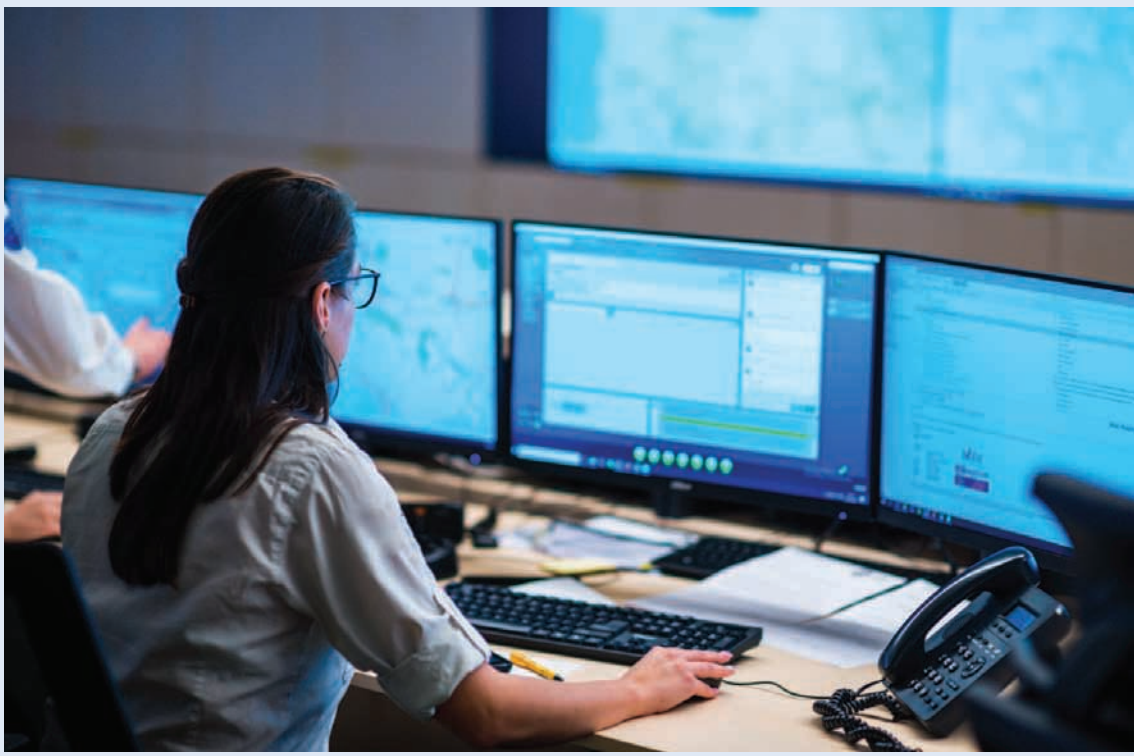
Un sistema elettronico di controllo accessi basato su badge, transponder o impronta biometrica – oltre a riconoscere gli utenti in automatico, verificare i diritti di ingresso, autorizzare o meno il transito, seguire il passaggio attraverso un varco (porta, tornello ecc.) – genera e gestisce centinaia di "eventi" diversi. L'evento è un'occorrenza che si verifica durante le fasi che caratterizzano il ciclo di accesso o, più raramente, nello stato di quiete. Disporre di informazioni puntuali e dettagliate su ciò che accade (o è successo) è essenziale sia per avere la situazione sotto controllo in tempo reale (e poter così intervenire in caso di emergenza) sia per eseguire a posteriori ricerche e analisi sui dati storicizzati, specie in occasione di un "incidente" (intrusione, furto, sabotaggio ecc.).

Di diversa natura

Gli eventi in gioco in un sistema elettronico di controllo accessi possono essere di diversa natura. Una prima tipologia comprende le occorrenze ordinarie. Tra queste: la segnalazione di un transito regolare nella direzione di ingresso dopo l'esito positivo di tutte le verifiche previste, l'uscita da un'area riservata senza identificazione automatica (azione sul pulsante lato interno o sul maniglione antipanico), le operazioni conseguenti a comandi manuali (sblocco permanente, blocco, messa in fuori servizio di un varco, tacitazione di un allarme) ecc. Una seconda categoria riguarda gli eventi che, pur configurandosi come anomalie, non richiedono particolare e immediata attenzione. Esempi: il tentativo di accesso eseguito da una persona non autorizzata, la rinuncia a transitare nonostante il varco sia stato sbloccato. Una terza classe, infine, la più importante, include gli eventi che devono essere subito presi in carico e trattati dal personale addetto alla sicurezza in quanto di particolare gravità: la digitazione di un PIN sotto stato di costrizione o i ripetuti tentativi di indovinare quello corretto, la forzatura di un varco o la manomissione di un lettore, la porta di una zona critica rimasta aperta e così via.

Vita breve ma intensa

L'evento, dal momento in cui si manifesta a quello in cui viene eliminato dagli archivi, ha spesso una vita breve ma intensa. In alcune situazioni, infatti, può spegnersi sul nascere (ad esempio quando l'informazione riguarda il transito di un VIP, da ignorare o cancellare all'instante) mentre in altre può subire una lunga serie di trattamenti. La prima tappa del viaggio inizia dal momento in cui l'evento nasce e termina quando viene notificato all'Unità Centrale (Host). Questa fase è gestita in autonomia dal Controller, ossia dall'unità elettronica che controlla gli accessi a uno o più varchi. I trattamenti a cui viene sottoposto si possono così ri-



Gli eventi relativi al controllo degli accessi vengono in genere visualizzati sullo schermo della stazione di lavoro del responsabile della sicurezza fisica oppure nella security room.

Tipo di eventi

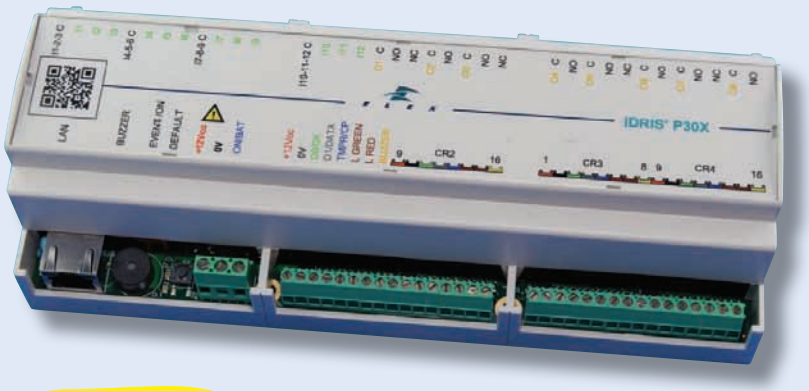
Tipo di evento	Alcuni esempi
Ordinario	Entrata autorizzata
	Uscita da comando manuale
	Blocco, sblocco varco e simili da comandi manuali
Trascurabile	Tentativo di accesso non autorizzato
	Varco non aperto in tempo
	Richiesta disattivazione impianto di allarme negata
Grave (da prendere in carico)	Tentativo di individuare il PIN
	Digitazione PIN sotto stato di costrizione
	Varco rimasto aperto dopo un transito
	Forzatura del varco
	Effrazione, rimozione lettore di credenziale
	Mancanza corrente (funzionamento a batteria)

Un sistema elettronico di controllo accessi al passo coi tempi può generare centinaia di eventi diversi. Molti di essi sono del tutto regolari, altri trascurabili. Alcuni, infine, oltre a richiamare l'attenzione dell'operatore addetto alla sicurezza, devono essere subito presi in carico e gestiti correttamente seguendo procedure appropriate.

Gestione e trattamento degli eventi

Fase	Gestore	Trattamento	Note
0		Manifestazione	Nascita dell'evento
1	Controller	Rilevazione	
		Analisi	Verifica validità
		Catalogazione	Abbinamento a una classe di eventi
		Creazione	Generazione del file
		Memorizzazione	Nel buffer locale (temporanea)
		Messa in attesa	Nell'impossibilità di notificarlo all'Host
		Cifratura	Del file
		Trasmissione	Trasferimento verso l'Host
2	Host	Ricezione	Presa in carico
		Notificazione	Al Controller, di avvenuta corretta ricezione
		Decrittazione	Del file
		Conversione	In un messaggio in chiaro, icona ecc.
		Visualizzazione	Sul monitor locale o su dispositivi mobili
		Stampa	
		Condivisione	Con altri sistemi di sicurezza
		Archiviazione	Storicizzazione
3	Host	Ripescaggio	In caso di incidenti (furti, sabotaggi ecc.)
		Rielaborazione	Analisi e statistiche
		Riarchiviazione	Per successive verifiche
		Distruzione	Cancellazione definitiva

Dal momento in cui si manifesta e viene rilevato, l'evento può essere veicolato e sottoposto a una serie di trattamenti gestiti dal Controller che sorveglia i varchi oppure dall'applicazione software che risiede su un Server o un PC. Gli eventi sono dati personali, da proteggere e conservare per il tempo strettamente necessario (GDPR).



Il Controller, ossia l'unità elettronica di controllo accessi che gestisce i varchi, rileva tutti gli eventi per poi notificarli all'Host dove risiede l'applicazione software (Courtesy Elex srl).

assumere: rilevazione, analisi (per determinare la validità dell'evento stesso), catalogazione (abbinamento a una determinata classe), creazione (del file), memorizzazione (locale), messa in stand-by (nel caso in cui manchi temporaneamente la connessione verso l'Host) e trasmissione (notificazione all'Unità Centrale in chiaro o cifrato). Una volta che l'Host ha ricevuto correttamente l'evento, provvede a prenderlo in carico per poi convertirlo (in un messaggio in chiaro, in una icona su una planimetria ecc.), visualizzarlo (sul monitor locale o su un dispositivo mobile), stamparlo, archiviarlo (per successive verifiche ed elaborazioni) ed eventualmente condividerlo con altri sistemi di sicurezza (antintrusione, videosorveglianza ecc.) o applicazioni software. Un evento archiviato può, a distanza di tempo, essere ripescato, rielaborato e infine distrutto.

Un cuore che batte

Durante l'orario di lavoro, specie nelle aziende e organizzazioni di medio-grandi dimensioni, un sistema elettronico di controllo accessi genera e gestisce migliaia di eventi. L'interscambio di dati fra i vari Controller e l'Host è continuo, concitato, intenso. Ma cosa succede quando di notte o nelle pause diurne tutto (o quasi) si ferma? A volte passano ore prima che accada qualcosa. Poiché il colloquio tra le parti cessa completamente, è difficile per l'Host capire se effettivamente non sta succedendo nulla o se uno o più Controller hanno smesso di funzionare. **Il sistema di monitoraggio dello stato di salute delle unità periferiche, noto da tempo nel mondo dell'informatica e adottato anche negli accessi, è il cosiddetto *HeartBeat*** (battito cardiaco). Il Controller, se non ha nulla da dire, notifica periodicamente all'Host un evento speciale a significare che è vivo e che tutto procede regolarmente.

GDPR, la spada di Damocle anche sugli eventi?

Un evento, ovvero il file che contiene tutte le informazioni (utente, data, ora, ubicazione, tipologia ecc.), **secondo un'interpretazione restrittiva della norma sulla privacy, è da considerarsi a ogni effetto un dato personale. Non tutti sono d'accordo.** Il fatto che la stringa di dati, ancorché eventualmente cifrata, non contenga informazioni *in chiaro* (come il nome e cognome del soggetto coinvolto) ma un semplice codice numerico individuale (tipicamente il numero di badge), giustificherebbe un trattamento più blando rispetto a quanto previsto dal GDPR. Molte imprese dotate di controllo accessi cercano di aggirare l'ostacolo correndo ai ripari. Ad esempio – pur esercitando tutti i controlli logici, spaziali e temporali sugli accessi – il sistema viene configurato in modo da non registrare gli eventi relativi ai transiti dei dipendenti (dove è presente l'identificativo personale) ma soltanto quelli anonimi (anomalie, allerte, allarmi). Altre limitano al minimo indispensabile il tempo di conservazione dei dati. Difficilmente un furto di beni o di informazioni oppure un sabotaggio, infatti, vengono alla luce dopo molti mesi dall'evento (e da qui la necessità di andare ad analizzare nel dettaglio i movimenti compiuti in un determinato luogo e periodo di tempo). In altre, ancora, l'accesso all'archivio degli eventi è subordinato alla digitazione contemporanea di due password di cui una riservata al datore di lavoro e un'altra al rappresentante dei lavoratori.