“Insider attack”: americanata o problema reale?

Luca Salgarelli, Presidente e Amministratore Delegato TSEC

La progettazione dei sistemi anti-intrusione o, più correttamente, di un allarme antifurto prevede sempre una definizione di rischio basata sulla divisione dello spazio in zone d’azione. Ad alto livello, tali zone sono l’area da proteggere (zona interna), e la zona a essa complementare, ovvero quella esterna, con un perimetro a fungere da confine tra le due.
Nei casi più semplici, per esempio negli impianti residenziali medio/piccoli, questo tipo di architettura è già sufficiente per definire la struttura dell’impianto, con dispositivi funzionali alla protezione perimetrale (barriere, contatti magnetici, sensori inerziali, etc.), spesso coadiuvati, almeno negli impianti più importanti, da dispositivi complementari che proteggono la zona interna (sensori volumetrici, etc.).
L’architettura degli impianti più complessi, come quelli dedicati alla protezione dei centri commerciali, delle residenze prestigiose o degli edifici bancari, è certamente più articolata, e spesso prevede ulteriori suddivisioni degli spazi in sottoinsiemi omogenei per funzione, livello di accesso e rischio. Rimane comunque valida almeno ad alto livello, anche in questi impianti complessi, la nozione di divisione dello spazio in due macro zone: quella interna al perimetro protetto e quella esterna.

Allo stesso modo possiamo raggruppare le persone che operano all'interno o nelle vicinanze di un'area protetta da un allarme antifurto nelle seguenti tre categorie:

- categoria A: gli occupanti legittimi dell'edificio. Nel caso residenziale si tratta naturalmente di chi dimora nell'edificio, comprese le persone che hanno titolo per soggiornarvi (amici, parenti, etc.). Negli altri casi del personale di un'azienda, di una banca, etc.
- categoria B: i visitatori, ovvero tutte quelle persone che possono essere presenti nelle aree protette, ma soltanto in particolari condizioni, come i clienti di un supermercato negli orari di apertura, i correntisti di una banca, etc.
- categoria C: gli attaccanti, quindi tutte le figure che hanno l'intenzione di violare l'area protetta, di solito per commettere un furto o un crimine di altra natura.

In tutti i casi, dal più semplice al più complesso, la definizione di zone dell'impianto e, in maniera complementare, del perimetro che le divide ha la primaria funzione di separare le persone che interagiscono con l'impianto stesso in almeno due gruppi: gli insider, ovvero gli occupanti legittimi (categoria A), e gli outsider, ovvero gli attaccanti (categoria C).

I visitatori, la categoria B, trovano collocazione tra gli insider e gli outsider a seconda dello stato del sistema: per esempio, in un sistema di allarme a protezione di un supermercato, un cliente durante le ore di apertura sarà necessariamente un insider, dato che occupa durante gli acquisti una zona interna del sistema che verrà allarmata alla chiusura del negozio.
Questa separazione tra insider e outsider è alla base della filosofia costruttiva degli impianti di allarme antifurto: scopo primario del sistema, almeno ad alto livello, è segnalare con un allarme la presenza di un outsider in una zona interna dell'area protetta.
La divisione così netta degli attori di un sistema trova un fondamento particolarmente rilevante negli impianti residenziali, dove nella stragrande maggioranza dei casi i visitatori (categoria B) sono assimilabili agli occupanti legittimi (categoria A), e sono quindi da ritenersi benigni. Il sistema d'allarme in questo caso si trova a operare in condizioni ideali: può espletare la sua funzione di separatore tra insider e outsider nel migliore dei modi, dato che tutti gli insider si trovano nella zona interna (all'interno del perimetro protetto) e sono benigni, mentre gli outsider, potenziali attaccanti, si trovano nella zona esterna. In questo caso il rischio principale dal quale l'impianto di sicurezza è chiamato a proteggerci è l'outsider attack.
Il problema diventa però presto complesso se si analizzano le situazioni tipiche degli impianti dedicati alla protezione di edifici non residenziali. Qui concorrono due fattori di primaria importanza nel modificare radicalmente il rischio. Il primo è che i membri della categoria B, i visitatori, possono spesso mascherare un membro della categoria C: si pensi, per esempio, al caso di un ladro che inizi la perlustrazione di un esercizio commerciale durante le ore di apertura al pubblico, per poi sferrare il suo attacco nottetempo. Il secondo fattore è dovuto alla natura umana: in questo scenario anche i membri della categoria A possono infatti nascondere o coadiuvare qualcuno che rientra in categoria C. Per esempio, un dipendente che si sentisse maltrattato potrebbe decidere di aiutare un ladro nell'esecuzione di un furto, predisponendo dall'interno una qualche forma di sabotaggio dell'impianto. Questi due fattori, già importanti se considerati singolarmente, insieme formano una miscela esplosiva per l'innalzamento del livello di rischio. In questi casi infatti il rischio principale può arrivare dall'interno del perimetro protetto: il vettore primario del rischio diviene l'insider attack.
È altrettanto chiaro che un insider attack porta l'attaccante ad aver accesso alle parti vitali del sistema di sicurezza, facendo quindi in modo che le sue azioni possano avere una efficacia molto superiore al caso dell'outsider attack. Nel caso di un insider attack, il sistema non può più operare nelle condizioni ottimali che abbiamo descritto sopra nel caso

residenziale semplice, ovvero di divisione tra insider e outsider: in questo caso, l'insider cessa di essere benigno, e il sistema di sicurezza dovrebbe reagire di conseguenza.
La normativa statunitense negli scorsi anni è stata rivista in maniera estremamente significativa proprio dopo la scoperta di ripetuti furti in edifici appartenenti al dipartimento di stato: l'analisi forense dopo questi episodi rivelava vettori primari di insider attack, come per esempio il mascheramento preventivo dei sensori volumetrici, o quello magnetico dei contatti (rilevatori di apertura varco), anche per modelli ad alta sicurezza, grazie ai quali i sistemi anti-intrusione erano stati violati con sforzi relativamente contenuti. L'insider attack è passato in breve tempo da leggenda metropolitana a uno scottante problema per tutte le zone ad alta sicurezza. La questione ha provocato una revisione profonda delle norme e, di conseguenza, della tecnologia e del modus operandi dei professionisti. In particolare, nel 2009 è stato introdotto un nuovo livello di sicurezza nella norma statunitense UL 634, il Livello 2, specificatamente pensato per le aree a rischio di insider attack. Negli Stati Uniti, i dispositivi e i sistemi di sicurezza, per essere certificabili al Livello 2 (il più alto possibile), devono oggi contenere tecnologie esplicitamente progettate per renderli resistenti all'insider attack.
Purtroppo la normativa Europea, quindi quella in vigore anche nel nostro paese, ovvero il compendio di norme EN 50131, seppur recentemente rivisto, non contempla nemmeno questo tipo di problemi. La EN 50131 specifica quattro gradi di sicurezza, dal Grado 1 (il più basso), al 4 (il più alto), basandosi esclusivamente sulla raffinatezza tecnica dell'attaccante come parametro per la definizione del grado di sicurezza. In altre parole, un impianto di Grado 1 è pensato per i casi nei quali si prevede che l'attaccante abbia «una conoscenza bassa» del sistema anti-intrusione, e che disponga «di una limitata gamma di attrezzi facilmente reperibili». All'altro capo dello spettro, un impianto di Grado 4 è idoneo, sempre secondo la EN 50131, quando si ha a che fare con attaccanti che «abbiano la capacità o le risorse per pianificare in dettaglio un'intrusione o una rapina e che dispongano di una gamma completa di attrezzature, compresi i mezzi di sostituzione dei componenti di un impianto di sicurezza».
Nella normativa europea la distinzione tra attacchi che provengono dall'esterno del perimetro protetto e quelli che invece provengono dall'interno non è nemmeno considerata come parametro essenziale per l'assegnazione di un grado di sicurezza a un impianto. È quindi chiaro che i progettisti, i costruttori di apparati e gli installatori, pur rispettando la normativa, si trovano a dover combattere una battaglia impari. Da un lato i rapinatori, ben consci della potenza che un insider attack può avere nei loro piani di crimine, stanno sempre di più affinando questi vettori d'attacco, e recenti, molteplici casi eclatanti avvenuti anche nel nostro paese ne sono la prova. Dall'altro lato i professionisti del nostro settore si trovano loro malgrado a dover combattere questa guerra con un'arma tecnologicamente spuntata, perché non in grado, a partire dalle principali normative di riferimento, di rispondere in maniera opportuna a un vettore d'attacco così dirompente.
È auspicabile che, partendo dalle associazioni di categoria per arrivare ai comitati tecnici, venga intrapresa una strada di revisione delle norme in modo da recepire quanto di utile ci possa essere nelle norme statunitensi su questo tema. Questa sembra a chi scrive un'azione dovuta, quantomeno per permettere alla catena del valore europea nel settore dei sistemi di sicurezza di poter competere ad armi pari con quella che proviene da oltre oceano. E, non meno importante, per permettere a chi usufruisce di un sistema anti-intrusione di potersi difendere al meglio, almeno in futuro.