

## **La sicurezza antintrusione e la domotica: convergenza o contrasto?**

Trattare un argomento, come la relazione tra domotica e sicurezza, creerà di sicuro qualche interrogativo: chi tra i puristi arriccerà il naso, chi penserà che si sta parlando di due cose ben distinte che trovano solo alcuni punti di contatto, chi si chiederà che cosa ci sia di diverso tra una gestione domotica dell'edificio e l'integrazione nel suo ambito di funzionalità di sicurezza.

Proviamo a identificare intanto le due cose: "domotica" è un termine assolutamente vago e onnicomprensivo che, ancor prima che il suo reale mercato trovi maturità, già viene ampiamente abusato, a sproposito.

Nell'immaginario collettivo "domotica" infatti è la gestione integrata e automatica di un vasto edificio, e domotica, parimenti, per arrivare subito a livello infimo, è una lampada che si accende con un piccolo telecomando e che si acquista in un centro commerciale per pochi euro.

Ho voluto esemplificare i due estremi dell'ambito etimologico comprensivi del termine di domotica.

Ritengo, senza passare per distinzioni tra "domotique" e "immotique" francese o tra "home automation" e "building management", che per "domotica" s'intenda il rendere automatiche e gestite da sistemi elettronici più o meno integrati una serie, anche vasta e importante, di funzionalità dell'edificio ai fini del comfort ambientale, del risparmio energetico, dell'entertainment: in una parola dello star bene derivante dall'efficienza dell'edificio affidata al sistema di gestione.

Va da sé che la sicurezza, intesa come security, è naturalmente parte importante, anzi vitale, di questo concetto di "star bene".

La sicurezza quindi, come concetto e come soluzione, non potrà, in un'ottica temporale abbastanza breve, rimanere ancora a lungo disgiunta, separata, da una gestione "confortevole" dell'edificio.

## **L'evoluzione dei sistemi in atto**

Anche nel comparto specifico della sicurezza si avverte sempre più la necessità di relazionare impianti e strutture tra loro, di integrare funzionalità e servizi e di comunicare con il mondo esterno.

E' da molto tempo che le funzioni tradizionali del concetto di sicurezza sono largamente superate sia dalle opportunità tecnologiche sia dalle nuove esigenze dell'utenza.

Troviamo ancora larghi strati di mercato che sono tenacemente legati al concetto di impianto di base a basso rischio, che deriva dalla disinformazione, su un comparto così specifico, di vaste percentuali di operatori come di gran parte dell'utenza media.

E' comunque questa una percentuale, che se pur ancora significativa, sta progressivamente e rapidamente diminuendo.

La tecnologia dei sistemi attuali permette di andare, anche nel residenziale, molto al di là del semplice “impiantino” dove si ritengono sufficienti una “centralina, un paio di sensori ed una sirenetta.....”.

Quest'ultima tipologia di sistemi è, infatti, più funzionale al risvolto psicologico del “sentirsi” protetti che al fatto di “esserlo” effettivamente, salvo sorprese amare che si scoprono nel momento del bisogno.

### **Prima cosa: l'analisi del rischio**

E' pur vero che nella grande maggioranza di questi casi ci sono operatori improvvisati che pensano semplicemente che “saper fare” anche in questo caso come in altri apparentemente simili significhi essere in grado di gestire tecnicamente un apparato.

Nessun approccio alla sicurezza è più sbagliato di questo.

Nei piccoli come nei grandi siti, a parità di “cubatura” e struttura, si possono avere problematiche di sicurezza radicalmente diverse.

La sicurezza è un concetto organico prima che un mestiere.

Il ragionamento corretto di approccio non è “che apparecchiatura devo programmare” bensì “quali sono le fonti e il livello di rischio del mio cliente”.

E' prevalente il rischio furto, il rischio rapina, il rischio rapimento?

Quali sono i beni e il valore globale da proteggere?

La località è isolata, accessibile, difendibile?

Quali forme di rilevazione, difesa e comunicazione verso l'esterno è possibile mettere in atto?

Ad una segnalazione di evento grave in quanto tempo può essere espletato l'intervento esterno?

In poche parole, per fornire ragionevole sicurezza e non semplicisticamente “vendere un impianto” è necessario preventivamente effettuare una “analisi del rischio” specifica per ogni sito.

### **La definizione del sistema**

Dopo una corretta analisi del rischio si può procedere a prevedere l'insieme dei mezzi di rilevazione, segnalazione, difesa.

A volte sarà sufficiente un sistema abbastanza semplice, a volte si dovranno integrare funzioni particolari, a volte si prevederanno rilevazioni concentriche e blocchi di aree che

costituiscono barriera, spesso sarà necessario integrare rilevazione elettronica con difesa fisica passiva.

Vitale comunque sarà la segnalazione dell'evento specifico su vettori di trasmissione, possibilmente multipli verso il mondo esterno, volta a segnalare il problema, identificandolo e sottolineandone il livello di gravità. Questo per permettere a chi deve effettuare l'intervento dall'esterno di essere informato con grande tempestività e con i maggiori dettagli possibili.

Non è concepibile, se un sistema di sicurezza è strutturato correttamente, leggere sui giornali di famiglie sequestrate in casa per tante ore senza che all'esterno se ne sappia nulla.

Sicuramente in questi casi chi ha effettuato l'analisi del rischio era un dilettante, oppure l'utenza non si è attenuta alle procedure di sicurezza suggerite per la propria serenità.

Quel che si deve ben tener presente è che nessun sottosistema è efficace se non sia previsto intervento, che è conseguente a tempestiva e completa comunicazione.

La rilevazione e la comunicazione elettronica sono funzionali a prevenire, rivelando con tempestività il tentativo di crimine mentre le difese passive servono a rallentare l'intrusione o l'attacco. L'edificio o le persone sotto attacco godranno di un tempo relativamente adeguato per essere allertati, predisporre difese ed avere sufficiente tempo per esercitare attività deterrenti in attesa di intervento repressivo.

Quindi nessun sistema si può definire completo ed efficace se è poco efficace la comunicazione dell'evento al mondo esterno.

E questo, va da sé, non può essere demandato al suono ridicolo di una sirena.

Per questa ragione le apparecchiature che gestiscono la sicurezza sono macchine complesse che hanno la possibilità di essere strutturate e programmate a dare soluzione al rischio specifico individuale.

Per questa ragione le metodiche di gestione della sicurezza, a partire dall'analisi del rischio, non possono essere considerate a livello dell'accensione di di lampade alogene.

### **La domotica**

Finora abbiamo parlato di sicurezza, ma oggi il mercato offre apparecchiature unità di controllo che possono gestire ben altro che la sicurezza, per quanto avanzata e complessa sia.

Esistono, infatti, dispositivi di tipo polifunzionale che permettono sia la gestione della sicurezza, in accordo alle normative specifiche, sia funzionalità di automazione dell'edificio la cui esemplificazione, anche se non esaustiva può essere amplissima: la gestione della climatizzazione e relative fasce orarie, di situazioni di allagamento, gas, incendio, accensione e spegnimento luci, start e stop motori, azionamenti di chiusure come serrande, avvolgibili, tende, gestione cicli irrigazione.

Si potrebbe continuare per molto, e le applicazioni sono limitate solo dalla fantasia e dall'abilità degli integratori di sistema (installatori e programmatori dei sistemi, dai più semplici ai più complessi).

Ecco dove la domotica e la sicurezza si incontrano: nella ottimizzazione economica e funzionale degli apparati.

### **Le norme**

Quando parliamo di efficacia non è possibile disgiungere l'aspetto di rispondenza alle normative in vigore.

Se per la domotica ci si rifà, in generale, alle norme che riguardano l'impiantistica elettrica ed elettronica, ai fini della rispondenza ai requisiti della Legge 46/90 e seguenti e al DPR 380/2001 il concetto di regola d'arte trova rispondenza per quanto riguarda la sicurezza intesa come "security" nelle norme CEI 79-2 per gli apparati, CEI 79-3 per i criteri di analisi ed installazione e nelle normative a queste due collegate.

E' vero quindi che, se a livello funzionale si possono conseguire risultati di operatività che "apparentemente" sono relativi alla sicurezza utilizzando apparecchiature di derivazione esclusivamente "domotica", è altrettanto vero che chi le propone, vende, installa a questo fine, assume su di sé l'intera responsabilità di non rispondenza alle norme, dunque di falsa dichiarazione di conformità laddove rilasciata e, comunque, di responsabilità oggettiva.

Non si possono, dunque, utilizzare in installazioni di tipo polifunzionale apparati che non rispondano completamente a tutte le norme "ad hoc" delle specifiche funzionalità proposte.

E' doveroso tenere ben presenti questi principi del buon operare nell'utilizzo residenziale, industriale, commerciale, laddove integrazioni volte a conseguire economia e polifunzionalità sono richieste all'ordine del giorno e a ritmi crescenti da parte di un'utenza sempre più informata ed esigente.

Prima di essere sottoposti agli esami specifici per la sicurezza in senso stretto, gli apparati relativi alla sicurezza, rispondenti alle norme CEI 79-2 e collegate, devono preliminarmente essere conformi alle normative di tipo elettrico ed elettronico per l'impiantistica elettrica ed elettronica per gli edifici.

Ma non è vero il contrario. Quindi se si vogliono far coesistere domotica e sicurezza utilizzando solo apparecchiature di tipo "domotico" si dovrà ricorrere ad un interfacciamento della struttura domotica con una sezione speciale, normata sicurezza CEI, venendo così a perdere buona parte dei benefici inerenti l'integrazione piena, e mi riferisco esplicitamente ai mezzi di

comunicazione, comando e controllo attraverso i vettori di comunicazione, con aumento dei costi di setup, gestione e manutenzione del sistema.

Laddove comunque si scelga, per ragioni funzionali, specificità, design o per qualsiasi altro motivo valido, di utilizzare una struttura di sistema specificatamente “domotica”, si tenga sempre ben presente che la sicurezza potrà colloquiare col sistema, ma dovrà, indispensabilmente, in ogni sua parte essere conforme alle norme CEI79-2 ed essere installata secondo i criteri delle CEI 79-3.

### **I mezzi di comunicazione**

Quando si parla di domotica e di sicurezza, non si può prescindere dalla comunicazione e gestione a distanza.

Si potrà disporre del migliore sistema di gestione d’edificio possibile, ma se questo non opererà in ambiente integrato, non potrà colloquiare con il mondo esterno, non potrà essere interrogato, comandato, gestito a distanza dall’utente presenterà una carenza gestionale fondamentale nel mondo odierno dove comunicazione e disponibilità d’informazione sono onnipresenti.

I mezzi di comunicazione, oggi largamente utilizzati nella sicurezza sono il telefono (messaggi vocali, messaggi con protocolli di sicurezza standard, multifrequenza o in formato dati), il telefonino (formato vocale, dati, SMS), il ponte radio (tipico degli Istituti di Vigilanza) o, recentemente su vasta scala, la rete dati.

Ognuno di questi mezzi ha i suoi pregi e i suoi difetti: è per questo che occorre parlare di comunicazione su vettori multipli. Limitare la comunicazione ad uno solo di questi metodi presta il fianco a possibili azioni di blocco preventive da parte degli aggressori.

In realtà si deve dire che, dall’esperienza pluridecennale di metodiche usate nel settore bancario, il sistema di trasmissione dati in protocollo Ethernet-TCP/IP è quello che dà maggiori garanzie di completezza di dato e di supervisione costante del supporto di comunicazione “vivo” tra controllo e periferia.

Questo sistema, dati i costi sia degli apparati sia della comunicazione stessa, è stato fino a qualche anno fa prerogativa di siti ad altissimo rischio. Oggi i ridotti costi di comunicazione e degli apparati rende quasi universalmente disponibile questo vettore. Senza nulla togliere alla validità degli altri supporti, che sono sempre alla base di una comunicazione “normale” (messaggio telefonico vocale all’utente, o SMS sul telefonino) è bene che gli operatori si orientino ad acquisire esperienza sulle comunicazioni su reti e a valutare le nuove opportunità che ne derivano.

Stiamo ovviamente parlando degli apparati per la sicurezza, costruiti a norme CEI 79-2, che comunicano direttamente su rete Ethernet senza necessità per il loro funzionamento di collegamento

a PC locale, salvaguardando sicurezza, economia, efficienza e alimentazione secondaria a backup di mancanze di alimentazione primaria per decine di ore o addirittura per giorni.

Poiché queste tipologie di macchine hanno al loro interno ogni possibilità di comunicazione efficace ai fini della sicurezza, va da sé che i medesimi supporti consentono analogo gestione delle funzionalità di automazione dell'edificio.

Ciò costituisce connotazione comune, tra sicurezza e domotica, in quanto sia gli apparati per la sicurezza che quelli destinati alla domotica sono provvisti di affidabili mezzi di comunicazione spot o costante verso il mondo esterno su vettori multipli.

### **La gestione in rete LAN o WAN**

I dati, che nella sicurezza sono opportunamente criptati, vengono accettati e gestiti da uno o più centri di ricezione e gestione che possono essere locali (LAN) o in rete geografica (WAN), meglio se su VPN.

Qualsiasi architettura di rete supporta agevolmente questi apparati, che per la gestione del tutto inviano sulla rete pacchetti minimi, generalmente inferiori ai 500byte, ininfluenti quindi sulla massa del traffico dati, anche in ambienti industriali stretti o dove l'amministratore di rete poco concede ad apparati esterni. Il protocollo, sviluppato su scheda di rete con firmware generalmente proprietario ed encrypting dinamico non essendo legato ad alcun sistema operativo, rende gli apparati inattaccabili a intrusioni esterne, garantendo alta sicurezza del trasporto dati e la non ingerenza nei sistemi operativi connessi alla medesima rete dati.

Gli apparati sono collegati attraverso la rete al software di gestione remota o locale il quale può, a seconda delle configurazioni, gestire anche centinaia di controlli, senza alcuna rilevanza per le distanze.

Una gestione a mappe grafiche a livelli rende all'utente buona visualizzazione, contestualità e user friendly di una serie di informazioni e comandi disponibili su un supporto visivo che può essere il disegno in pianta dell'edificio o fotografie dell'ambiente stesso.

E' possibile, anche sullo stesso supporto grafico, l'integrazione di immagini video "live" provenienti da apparati dedicati connessi in rete. Sulle immagini video e sulla loro trasmissione si deve fare un'ulteriore analisi circa il peso dei pacchetti trasmessi che in questo caso diventano rilevanti e non trascurabili rispetto a quelli degli apparati "non video", e questo è un aspetto comune sia agli apparati di sicurezza che agli apparati domotici.

Una struttura di comunicazione di questo genere (soprattutto per quanto riguarda l'encrypting) può apparire ridondante per la gestione domotica, e probabilmente in effetti lo è, ma avendola già disponibile per la sicurezza, con una aggiunta di costo minima, pari al tempo di

programmazione del sistema, permette di integrare anche funzionalità di supervisione, controllo e comando relativi alla domotica.

### **Il risultato**

Resta evidente, quindi, che la gestione integrata di sicurezza e domotica in modo armonico e fruibile dall'utente su mappe grafiche, connessa in rete e, quindi, disponibile e gestibile in modo non limitato dalla posizione geografica degli apparati è sicuramente possibile a qualsiasi livello di edificio, residenziale incluso, e offre spunti di proposta da parte degli integratori di sistema che incontrano e spesso superano le aspettative del proprio cliente.

Esistono validissimi sistemi domotici come esistono validissimi sistemi per la sicurezza.

Quello che è certo, e mi auguro di aver offerto spunti di riflessione, è che la convergenza e l'ottimizzazione economico-funzionale unita a sicura comunicazione costituiscono una prospettiva alle porte.

La considerazione che segue è che, oltre all'aspetto tecnico, spesso propiziato da entusiasmo squisitamente ingegneristico secondo il quale tutto è possibile, è necessario sempre tener presente che esistono normative, esistono responsabilità oggettive ma soprattutto rendersi conto dell'ottimizzazione del prodotto che si fornisce all'utenza, soprattutto quando si parla di concetti di sicurezza, dove non si accendono luci e o si stabilisce il clima interno, ma si "gioca" con la vita e la serenità delle persone.

Ho scritto "gioca" a proposito, perché occorre riflettere che con la sicurezza, sotto il profilo della responsabilità penale, civile ed etica è assolutamente proibito "giocare" o, peggio, "barare".

Patrizio Bosello

Consigliere Direttivo Centro Studi Itasforum ([www.itasforum.it](http://www.itasforum.it))

Amministratore delegato Axel srl, azienda italiana produttrice di sistemi elettronici per la sicurezza e la domotica ([www.axelweb.com](http://www.axelweb.com))