essecome security&safety 02

Periodico di informazione su persone, tecnologie e applicazioni della sicurezza

2016 · ANNO XXXIX · ISSN 2384-9282

CST. Gli unici sensori passivi al mondo, brevettati e codificati quadruplo bilanciamento

Le problematiche sempre più attuali legate al controllo dei varchi, impongono un innalzamento del livello di efficienza nella rilevazione dei tentativi di elusione dei componenti passivi degli impianti di allarme.

Dal laboratorio **TSEC** nasce la prima piattaforma al mondo per la realizzazione di sensori magnetici su misura con tecnologia Magnasphere®.

CST è l'acronimo di **Coded Sensor Technolog**y, esclusivo brevetto di TSEC SpA che permette di realizzare coppie di sensori e magneti codificate.

Il sensore passivo è in grado di riconoscere il proprio magnete.

Sulla base di un cuore tecnologico comune, si possono personalizzare le funzionalità dei sensori in modo da soddisfare le più severe esigenze di alta sicurezza.

TSEC ha introdotto un nuovo concetto di modularità e, quindi, di personalizzazione del contatto magnetico passivo verso un corretto e davvero efficace utilizzo nella protezione dei varchi.

Grazie alla piattaforma **CST** oggi è possibile offrire un livello di sicurezza impensabile fino a pochi anni fa, in quella che è molto spesso la prima barriera di allarme.

La piattaforma **CST** è una validissima soluzione contro l'Insider attack.

Molto spesso, infatti, gli attacchi alle aree protette avvengono dall'interno del perimetro protetto, sia da parte di personale che di visitatori, soprattutto quando i sistemi di sicurezza devono supervisionare varchi temporizzati (bussole, uffici cassa, ecc.) o uscite di sicurezza. Con la piattaforma **CST** di TSEC questi problemi possono essere risolti con una tecnologia completamente passiva.

Attualmente, la gamma **CST** è composta dai modelli **CST-15**, **CST-16V** con sensore inerziale integrato e dal nuovissimo **CST-03** ad alta tolleranza.

Sono sensori garantiti 10 anni, prodotti interamente in Italia.

Sommario

ADV_03.2016

SORRIDI SEI IN ULTRA SMART

Immagini in HD, conveniente ed intelligente, funzioni semplici ed immediate migliorano la sicurezza

- Elevata sensibilità 0.002Lux/F1.2 (colore)
- Ultra WDR fino a 140dB
- Zoom ottico 30X
- Analisi Video
- Max 50/60fps @ 1080P

4K FULLHD · ICR D/N · IP67 · PoE · IK10

>> IPC-HF8231E >> IPC-HFW8331E-Z >> IPC-HDBW83331E-Z >> IPC-HUM8101

La tecnologia Ultra Smart non dispone solo di una qualità di immagine in HD ma anche di un sistema di videosorveglianza più professionale, conveniente ed intelligente, guidato da un aggiornamento comprensibile con funzioni semplici ed immediate che possono migliorare la sicurezza e proteggere le tue proprietà con spensieratezza.

GARANZIA 24 MESI

Videotrend offre 24 mesi di garanzia su tutti i prodotti Dahua

VIDEOTREND ITALIA | ESPAÑA *Chiedilo a noi!*

Distributore esclusivo Dahua in Italia

VIDEOTREND S.r.l. Tel. +39 0362 1791300 info@videotrend.net - www.videotrend.net

Se la sicurezza non è di qualità, non è sicurezza

Di questi tempi, la sicurezza è diventata una sorta di "commodity" universale, che serve praticamente dappertutto: dalla produzione di un alimento all'organizzazione di un concerto, dall'arredo di casa al progetto di un viaggio, dall'investimento dei risparmi alla scelta di una terapia, eccetera. Venendo toccato di volta in volta ciò che interessa di più alle persone (salute, soldi, relazioni o la vita stessa), tutti percepiscono che ciò che serve per "fare sicurezza" – strumenti, tecnologie, servizi, procedure – deve funzionare bene al momento del bisogno, altrimenti non serve. In altre parole, gli utilizzatori richiedono "qualità" che, secondo Wikipedia, "*esprime le caratteristiche o le proprietà di una entità - una persona, un prodotto, un processo, un progetto - in confronto a quanto ci si attende da tale entità, per un determinato impiego*".

Il moschettone che sostiene il rocciatore è, in quel momento, fondamentale per la sua sicurezza. Dovrà essere della migliore qualità possibile in relazione al suo impiego, senza compromessi: o il moschettone regge o il rocciatore precipita. Quest'ultimo, pertanto, sceglierà con molta attenzione il moschettone con le caratteristiche più adatte a proteggere la sua vita, ovvero cercherà quello di qualità migliore e non quello che costa di meno. Questo esempio si ripropone nella vita reale in un'infinità di casi. Si troveranno molti emuli di quel rocciatore, che scelgono con attenzione la soluzione che offre la migliore qualità (= la sicurezza maggiore) per lo specifico impiego di cui si stanno occupando. Se se si arrivasse alla prova dei fatti, il loro "moschettone" reggerebbe allo sforzo con buone probabilità di successo.

In molti altri casi, si troveranno invece persone più attente ai costi che alla qualità, con il risultato che, arrivando eventualmente alla prova dei fatti, il "moschettone" potrebbe non reggere.

Nella rapina al museo di Castelvecchio a Verona del 19 novembre scorso, quando furono razziati 17 capolavori del valore stimato di 20 milioni, il "moschettone" che ha ceduto non è stata la guardia complice della banda di rapinatori, ma l'inadeguatezza delle tecnologie e delle procedure che non hanno retto alla prova dell'infedeltà interna, facendo emergere una potenziale colpa in *eligendo* e in *vigilando* da parte dei responsabili della sicurezza del museo. La strage del tribunale di Milano dell'aprile 2015 è stata resa possibile dalla clamorosa mancanza di qualità dell'intero sistema di sicurezza (tecnologie, procedure, qualifica e formazione degli addetti), forse per motivi economici ma non solo: la sciatteria burocratica può vanificare anche investimenti ingenti come, probabilmente, è avvenuto a Verona.

Fatti esemplari che si spera possano servire come utili casi di studio ed evitare che si ripetano. Ma la qualità del "moschettone" è importante anche per il piccolo impianto di allarme della signora Maria, che deve essere realizzato con componenti adeguati, installazione a regola d'arte, manutenzione regolare. Se non funziona quando arrivano i ladri, la padrona di casa non sarà contenta, anche se ha speso poco.

Pyronix®
www.pyronix.it

Il primo rivelatore esterno volumetrico
con radio bidirezionale

XDH10TT-WE

Installazione in 4 passi

Passo 1: Memorizza il rivelatore ad una zona della centrale
Passo 2: Programma la tipologia della zona
Passo 3: Verifica la portata wireless prima di fissare il rivelatore alla parete
Passo 4: Installa il rivelatore

Compatibile con Enforcer, PCX, e UR2-WE.

Registrati qui per ricevere più informazioni

marketing@pyronix.it | www.pyronix.it | @PyronixItalia | assistenza.tecnica@pyronix.it

WiseNet HD+

Una nuova prospettiva

WiseNet HD+: un nuovo livello di qualità video Full HD su cavo coassiale.

Nella nuova gamma WiseNet HD+ ci sono tutti i nostri 39 anni di esperienza nel video e nell'ingegneria di precisione che ci permettono di fornire soluzioni di VideoSorveglianza Professionale con immagini caratterizzate da fedeltà dei colori, nitidezza e dettagli senza paragoni.

Wisenet HD+, la VideoSorveglianza FullHD su coassiale a prova di futuro.

samsung-security.eu

SAMSUNG

Una città non è smart se non è protetta e sicura. Verso una normativa europea

a colloquio con Enzo Peduzzi, presidente Euralarm
a cura di Raffaello Juvara

Il concetto di “smart city” è entrato da tempo nell’uso e nell’immaginario collettivo, anche se la definizione dei modelli di riferimento e i criteri per misurare oggettivamente il “QI” di una città siano ancora in fase di assestamento. A questo si è affiancato in tempi più recenti l’altro concetto di “safe city”, creando non poca confusione anche tra gli addetti ai lavori.
In realtà, “smart city” e “safe city” sono concetti che focalizzano aspetti diversi (**leggi articolo**) ma che dovranno venire sviluppati in parallelo per dare risposte adeguate alle esigenze delle città di oggi e, soprattutto, di domani. I presupposti di partenza, condivisi in linea di massima dalle diverse fonti, sono:

- l’intelligenza di una città viene espressa dalla capacità di rispondere in modo ottimale al fabbisogno degli abitanti in materia di energia, servizi, infrastrutture e salubrità ambientale, risparmiando le risorse non rinnovabili e garantendo la maggiore resilienza possibile agli eventi catastrofici di ogni natura con adeguati piani di continuità operativa;
- la sicurezza di una città si manifesta nella tutela delle persone e delle strutture urbane dalle minacce, attraverso la predisposizione di adeguati elementi di controllo del territorio e di intervento, di procedure e di sistemi gestionali per la raccolta e l’elaborazione delle informazioni da condividere in modo coordinato tra i soggetti preposti (forze dell’ordine, vigili del fuoco, assistenza sanitaria, protezione civile ecc).

Ma qual’è lo stato dell’arte dell’applicazione in concreto di questi concetti, nel mondo e in Italia? Esiste una normativa condivisa a livello internazionale che possa guidare in modo univoco la realizzazione di città resilienti e sicure? Quale sarà il coinvolgimento dell’industria della sicurezza nei prossimi anni?
Questi saranno i temi centrali del seminario **Le Eccellenze per la Sicurezza 2016**, che si terrà a Roma nel prossimo mese di ottobre, che anticiperemo con articoli e interviste pubblicati da **essecome/securindex.com**.
Il seminario sarà rivolto ai responsabili della sicurezza dei grandi utilizzatori pubblici e privati per la condivisione delle conoscenze con esperti internazionali, progettisti, produttori e system integrators sulla sicurezza delle città, delle persone e delle organizzazioni, nell’era del terrorismo globale.
Iniziamo con **Enzo Peduzzi**, presidente di **Euralarm**, l’associazione europea che rappresenta i produttori di tecnologie e servizi per la sicurezza e l’antincendio. Nell’intervista che segue viene anticipata la visione complessiva di Euralarm sull’argomento e l’azione che sta conducendo per creare uno standard europeo ispirato alla norma **ISO 37120**, attualmente utilizzata come riferimento da alcune città pilota in tutto il mondo, in una fase sperimentale coordinata dall’Università di Toronto.

L’Europa sta attraversando una fase molto difficile, nella quale i temi della sicurezza delle città e delle persone, della tutela dell’ambiente e del risparmio energetico sono diventati primari a seguito di fattori globali, come i terrorismi, i flussi migratori, i cambiamenti climatici. “Smart City” e “Safe City” sono termini usati con sempre maggiore frequenza ma non sempre in modo univoco. In realtà, in cosa si differenziano questi due concetti?
Entrambi i concetti sono complementari e dipendenti l’uno dall’altro. Con la crescita delle città, il concetto di “Smart City” deve affrontare l’aumento dei problemi delle megalopoli del futuro in relazione ai trasporti, all’intasamento delle strade, all’affollamento dei mezzi pubblici, ai consumi di energia fossile ed elettrica. Se non saremo in grado di gestire questi fattori, le megalopoli collasseranno. In ogni caso, è necessario che la crescita delle aree urbane sia accompagnata da una crescita contemporanea di security e safety. Più le persone vivono in ambiti ristretti, più questi attraggono criminali e terroristi, come è purtroppo avvenuto nel recente passato.
“Smart” e “Safe” sono concetti che devono crescere insieme ed in parallelo. Più la città è “intelligente”, più deve rispondere alle maggiori necessità di protezione e sicurezza espresse dai suoi abitanti. Le smart cities tendono ad essere più “impersonali” rispetto a quelle tradizionali ma gli abitanti cercano sicurezza ed è un dovere delle amministrazioni assicurarla ai propri cittadini. “Una città non è smart se non è protetta e sicura”.

Quali sono i modelli di riferimento per Smart e Safe City e quali le rispettive realizzazioni in ambito europeo da prendere come esempio e benchmark per l’analisi dei costi e dei benefici?
In questo momento molti progetti sono in cantiere con la denominazione “smart cities”, ma è ancora troppo presto per poter parlare di vantaggi o per individuare uno o l’altro come modello di riferimento. Prima di tutto, i progetti sono troppo “giovani” per poter produrre risultati consolidati; d’altra parte, i progetti stessi non sono realmente paragonabili tra di loro. Dobbiamo renderci conto che tra la definizione di un progetto e quando questo comincia a produrre risultati ci vogliono anni, se non decenni. Cambiare il funzionamento di una città è un processo che impegnerà almeno una generazione.
Per essere in grado di confrontare tra di loro le città, abbiamo bisogno di avere modelli coerenti con cui le amministrazioni cittadine possano valutare i propri risultati e confrontarli con le altre comunità. In ogni caso, questi schemi sono relativamente nuovi e non c’è ancora molta esperienza. In passato, c’è stata anche resistenza da parte delle amministrazioni cittadine a “essere misurate ”. Temevano forse troppo lavoro ma anche di ritrovarsi esposte impropriamente a valutazioni di ordine politico. Oggi, invece, le amministrazioni iniziano a rendersi conto che le città sono già in competizione per gli investimenti privati, con aziende che creano posti di lavoro, lavori qualificati e buoni contribuenti. Quindi iniziano ad aprirsi ad indicatori chiave delle performance e a valutare i propri risultati non tanto per la concorrenza all’esterno ma per migliorare all’interno.

Quali sono le norme (ISO, EN) a cui fare riferimento per gli amministratori pubblici, progettisti integratori che intendano sviluppare un progetto organico? Quali sono i soggetti abilitati – e da chi – a rilasciare le certificazioni di conformità per le soluzioni realizzate?
Ci sono molti metodi per valutare quanto sia

"intelligente" una città. Alcuni di questi si basano su iniziative private, più finalizzate alla pubblicazione di classifiche in giornali e riviste commerciali e politiche. In generale, questi indici hanno lo svantaggio di non essere trasparenti e, spesso, sono rivolti solamente verso alcune funzioni della città. Il metodo migliore e più completo è senza dubbio la Norma ISO 37120, che comprende un insieme di 100 indicatori per valutare i servizi della città e la qualità della vita, dei quali 11 riguardano espressamente la safety e la security. Nel complesso, questi indicatori sono rivolti alla security, alla sicurezza antincendio e alla gestione delle crisi, nonché all'acqua, all'energia e ai trasporti. Questo rende l'ISO 37120 l'unica norma con KPIs specifici per misurare il livello di security e safety nelle città su base comparativa. Approssimativamente, 250 città in 80 paesi stanno partecipando all'introduzione di questa norma, comprese Londra, Shanghai, Toronto e Rotterdam. La valutazione dei risultati viene fatta dall'Università di Toronto, non tanto per uno spirito competitivo, quanto per scambiare le migliori pratiche e imparare gli uni dagli altri. A livello europeo, manca un simile standard, ma la ISO può venire ugualmente usata. Euralarm ha tuttavia avviato in CEN T391 un nuovo progetto di norma: "Criteri per la qualità dei servizi della sicurezza sociale e della safety". Questo NWI (*New Working Item – ndr*) potrà creare concreti indicatori di valutazione che potrebbero racchiudere soluzioni tecniche di alto livello. Ciò potrebbe aiutare le amministrazioni cittadine a individuare i giusti criteri per migliorare la safety e la security nella propria municipalità.

La complessità di un progetto di Smart o di Safe City, la molteplicità delle componenti tecnologiche, procedurali e di servizio che necessariamente vengono coinvolte e, soprattutto, l'interazione con il territorio – che potrebbe anche superare l'ambito di una singola nazione – indurrebbero a pensare a una visione europea, con authority e osservatori transnazionali. Qual è la visione di Euralarm in merito? Ritiene che un coinvolgimento della EU sia possibile e/o utile in questo particolare momento o che ci possano essere percorsi diversi per coordinare il processo di implementazione a livello europeo?

La complessità del progetto potrà essere gestita quando tutti i partecipanti saranno inclusi nello sviluppo della soluzione e la soluzione sarà basata sul riconoscimento di norme internazionali, come accennato. Questo processo richiede una chiara individuazione delle responsabilità e degli incentivi per la sua realizzazione. Non dobbiamo dimenticare che, in particolare nel campo della safety e della security, l'industria specializzata ha già avuto dei risultati e noi non possiamo reinventare la ruota! La nuova sfida è probabilmente l'integrazione intelligente, o "smart", dei vari sistemi dentro piattaforme centralizzate per sostenere le forze di intervento. In questa prospettiva, l'UE potrebbe giocare un importante ruolo di supporto alle città, e convocare i partecipanti in ambiti neutrali per scambiare informazioni e buone pratiche supportate da ricerche accademiche. Ci può essere anche la possibilità per la UE di sostenere il cosiddetto "Lighthouse-Project", nel quale i partecipanti possono mettere alla prova la fattibilità di concetti e progetti.
In Eurolarm pensiamo che questa potrebbe essere un'eccellente opportunità per riunire insieme tutti i partecipanti e testare i concetti in un contesto reale (concreto). Allo stesso tempo, non dobbiamo perdere di vista il fatto che la resilienza di una città tende ad essere molto sopravvalutata e che alla fine, la tecnologia non è la soluzione per tutto. I cittadini che partecipano in modo attivo ed efficienti forze di intervento sono e saranno cruciali per la security e la safety di una città.

Videosorveglianza: l'affidabilità del fornitore, un fattore critico per la sicurezza del sistema

a cura della Redazione

La videosorveglianza ha assunto da tempo un ruolo determinante e irrinunciabile per qualsiasi applicazione di sicurezza in ogni parte del mondo, sotto tutti i regimi politici, in ambito pubblico e privato. L'evoluzione tecnologica ha trasformato le telecamere da "raccoglitori di immagini" a "sensori di scenario", in grado di raccogliere e interpretare le immagini e di inviare i dati a sistemi centrali di elaborazione e stoccaggio per gli utilizzi richiesti dall'utente.
L'ampliamento delle prestazioni ha prodotto un esponenziale aumento delle possibilità di impiego, superando i già ampi confini della security. Solo per fare qualche esempio: indagini forensi, riconoscimento facciale, loss prevention, business intelligence, telemedicina, prevenzione degli incendi, controllo dei processi di produzione eccetera. La connessione in rete ha reso possibile l'interoperabilità con altri sistemi, il controllo da remoto, l'uso del cloud.
Ma è recentissima la notizia che **Google ha disattivato i dispositivi domotici di Revolv**, una control room rilevata nel 2014, lasciando in mano ai clienti pezzi di ferro inutilizzabili. Girano voci ricorrenti di immagini ricoverate in cloud non più ritrovate dai clienti o ricevute da telecamere diverse dalle proprie. Ma la grande paura viene dagli attacchi informatici, la vera mina che dovrà venire disinnescata per tranquillizzare gli utenti di qualsiasi tecnologia in rete, con la videosorveglianza in prima fila.
Tutto ciò rende ancora più importante l'affidabilità complessiva dell'intera filiera di fornitura dei sistemi, dai produttori dei componenti agli integratori, per "mettere in sicurezza" a priori il sistema stesso rispetto a questi nuovi pericoli. Un'esigenza avvertita a livello globale, amplificata dall'avanzata di prodotti asiatici a basso prezzo, che non offrono le necessarie garanzie di qualità e di affidabilità richieste per gli impieghi critici di videosorveglianza.
Una delle tavole rotonde organizzate nell'ambito del **MIPS 2016** (Milestone Integration Platform Symposium - Scottsdale, Arizona, dal 23 al 25 febbraio) è stata dedicata proprio a quest'ultimo tema, che abbiamo ripreso consultando i rappresentanti per il mercato italiano di quattro leader della videosorveglianza che della qualità dei prodotti, della capacità organizzativa e dell'affidabilità societaria hanno fatto una ragione e una missione: **Axis, Bosch, Hanwha Techwin** e **Milestone**. **Pietro Tonussi, Stefano Riboli, Fabio Andreoni, Alberto Bruschi** hanno accettato il nostro invito a partecipare alla tavola rotonda virtuale, rispondendo in contemporanea a due nostre domande sui requisiti di affidabilità che i produttori di sistemi di videosorveglianza devono garantire ai propri clienti intermedi e finali.

L'evoluzione tecnologica della videosorveglianza ha trasformato le telecamere da "raccoglitori di immagini" a "sensori di scenario", con funzioni sempre più determinanti per la sicurezza pubblica e privata. L'affidabilità dei prodotti, le certificazioni, la qualità del servizio post-vendita, la garanzia sono quindi diventati fattori critici, che possono venire assicurati solamente da produttori qualificati. Qual è la vostra visione?

Axis (Pietro Tonussi)

E' indubbio che il mondo stia evolvendo e che allo stesso modo evolvano le richieste dei clienti, che sempre più chiedono una soluzione e non un singolo prodotto. In tal senso, l'affidabilità della soluzione dev'essere una prerogativa tra le più importanti. L'affidabilità di una soluzione si raggiunge prima di tutto sottoponendo i prodotti stessi ad una serie di test normati (cito fra le tante norme: EN62262 – robustezza, IEC 60068-2-2 vibrazioni, IEC/EN 60529 – resistenza acqua e polvere) in modo da garantire che il prodotto che stiamo proponendo sia in linea con le richieste specifiche dei clienti e delle loro necessità applicative. Il concetto di affidabilità non si ferma ai singoli prodotti che compongono la soluzione, ma si estende a tutto ciò che generalmente non si vede (o che diamo per scontato). Mi riferisco alla garanzia (fino a 5 anni) e a tutti quei servizi tanto importanti come l'Advanced replacement in caso di guasto, agli aggiornamenti software, il supporto in lingua locale e infine il supporto H24, anche attraverso chat.
Affidabilità vuol dire anche garantire al cliente una trasparenza di continuità di prodotto nel tempo e di tools (SDK) che permettano a coloro che sviluppano piattaforme di video management system, analitiche e PSIM di poter contare su una serie di supporti che ne permettano una facile integrazione per sfruttare poi al meglio le caratteristiche salienti della soluzione.

Bosch (Stefano Riboli)

La ricerca di maggior sicurezza nel pubblico e nel privato spinge il mercato ad un aumento esponenziale dei dispositivi IP interconnessi. La videosorveglianza rappresenta chiaramente questo fenomeno, con un incremento costante del 20% del numero di telecamere IP presenti sul mercato, della loro risoluzione e della maggior intelligenza a bordo camera. Questo impatta anche sulla rete in termini di infrastruttura, di sicurezza e di gestione dei dati, comportando anche ad un aumento ancora superiore delle unità di archiviazione. Bosch opera in questa direzione, cioè alla continua ricerca di tecnologie che permettano una maggior efficienza di trasmissione (iDNR) ed archiviazione (Dynamic Transcoding) così da compensare l'aumento della risoluzione. Le telecamere IP diventano sempre più intelligenti, anche tramite l'impiego di algoritmi di analisi a bordo camera (IVA). Infine, garantire la sicurezza dei dati anche nei dispositivi di videosorveglianza sarà l'aspetto chiave per assicurare una reale protezione del sistema: "Data Security".
Crediamo che ognuno debba vivere in un ambiente sicuro, e il nostro "focus" è il continuo impegno in termini di qualità ed innovazione, per lo sviluppo di soluzioni che migliorino realmente lo stile di vita. In breve "Invented for Life".

Hanwha Techwin (Fabio Andreoni)

Lo sviluppo tecnologico ci ha ormai abituato, nel quotidiano, ad immagini con risoluzione sempre crescente. Per le applicazioni di VideoSorveglianza, peró, non sempre questo parametro porta ad una maggiore efficienza ed efficacia della soluzione.
Oggi, gli utenti di Soluzioni di Videosorveglianza guardano sempre piú ad aspetti legati al ritorno sugli investimenti, misurato sul miglioramento dell'efficienza e delle procedure di sicurezza, sulla riduzione dei rischi e, in alcuni contesti, sulla riduzione di furti e mancanze.
Diventa quindi fondamentale affiancare alla qualitá intrinseca delle immagini altri aspetti, come la rispondenza agli standard, per garantire la continuitá dell'investimento e l'interoperabilitá con altre soluzioni open nonché la professionalitá del canale distributivo, che deve essere garantita da un percorso di selezione, qualifica e formazione da parte del vendor.

Milestone (Alberto Bruschi)

La tecnologia di acquisizione, l'incremento di banda e la riduzione dei costi sta trasformando il mercato della videosorveglianza. La possibilità di utilizzare sensori sempre più sensibili con risoluzioni sempre più elevate, rende possibile la gestione delle immagini e dei dati che se ne ricavano in ambienti, mercati e realtà fino a pochi anni fa non prevedibili. L'abbinamento di queste tecnologie con una piattaforma stabile e aperta assicura all'utilizzatore di avere un sistema in grado di evolvere, soddisfacendo i cambiamenti dettati dalle necessità maturate nel tempo grazie anche alle combinazioni offerte dai nostri partner tecnologici. L'affidabilità di prodotti e soluzioni, la professionalità delle aziende che le implementano e le manutengono sono alla base del successo di questo processo, che altrimenti fallirebbe. L'affidabilità è, purtroppo, un parametro non determinabile se non con il passare del tempo e, in molti casi, cede il passo al prezzo che invece è tangibile subito. Milestone crede molto nella certificazione dei propri partner a sostegno di quanto prima descritto, e il nuovo programma dei corsi ne è una prova.

Uno degli effetti dell'evoluzione in atto è la possibilità di offrire soluzioni avanzate per ottenere risultati specifici nel contesto sempre più ampio della sicurezza: business intelligence, lettura targhe, riconoscimento volti sono solo gli esempi più noti. Un percorso che enfatizza l'interazione del vendor con i partner (sviluppatori, distributori, systems integrator) nella relazione con il cliente, con una conseguente maggiore responsabilità sull'efficienza dei sistemi realizzati. Come affrontate questo tema qualitativo che, secondo gli analisti, sarà un fattore differenziante sul mercato, in contrapposizione ai prezzi sempre più bassi dei componenti?

Axis (Pietro Tonussi)

Già da qualche tempo gli utenti finali non cercano più un semplice prodotto, ma una "Soluzione", che possa risolvere le loro specifiche problematiche. Soluzioni come la lettura targhe, il riconoscimento volti o la Business Intelligence nel senso più ampio della definizione, prevedono un insieme di diversi prodotti per ogni singola applicazione e per ogni singola richiesta. Parti singole di un unico insieme, che si devono incastrare perfettamente tra loro per garantire l'affidabilità e la qualità della soluzione stessa. E' proprio in questo senso che le partnership devono funzionare e incastrarsi come i pezzi di un puzzle. Partnership che dividerei in due tipologie: le prime con gli "Sviluppatori" e le seconde con gli "Integratori", patrimonio del nostro canale. Con i primi le relazioni non devono essere solo commerciali o semplicemente di "go to market", ma tecniche, con interscambi di informazioni, con aggiornamenti continui (di prodotto e di firmware) e test sul campo per arrivare a garantire la soddisfazione del cliente. I secondi, gli integratori, sono coloro che veicolano le soluzioni, le installano e le configurano, garantendo il loro funzionamento. Proprio per questi motivi devono essere ben supportati e formati, con seminari di aggiornamento costanti nel tempo.

Bosch (Stefano Riboli)

La videosorveglianza ricade all'interno di contesti sempre più ampi, come in applicazioni di business intelligence, o in applicazioni che non sono propriamente del mondo security come ad esempio il marketing intelligence. Bosch Security Systems spinge al massimo l'intelligenza a bordo camera per ridurre i carichi e i costi dell'infrastruttura, cioè il Total Cost of Ownership (TCO) e tramite un programma di canale destinato agli integratori software permette di trovare la miglior soluzione per le necessità del cliente.
L'Integration Partner Program (IPP) è un programma di canale che consente di identificare il partner più idoneo, sia nell'ambito Safety, cioè rilevazione incendio e audio evacuazione, che nell'ambito Security, cioè antintrusione e videosorveglianza. Tramite una soluzione completa e partner specializzati nel mondo del software, possiamo offrire la possibilità di scegliere la soluzione integrata più idonea alle esigenze ed aspettative del cliente.
In contrapposizione ad un mercato che vede la battaglia del prezzo sul prodotto, come Bosch cerchiamo come prima cosa di offrire una soluzione, mettendo particolare attenzione al Total Cost of Ownership, cioè a tutte le voci che compongono il costo totale di gestione dell'impianto, senza rinunciare alla qualità del prodotto.

Hanwha Techwin (Fabio Andreoni)

Questo scenario pone gli operatori del mercato, dai costruttori ai system integrator ai security manager delle aziende, di fronte ad una scelta strategica: operare con soluzioni e standard proprietari o scegliere piattaforme open, rispondenti agli standard internazionali e, per conseguenza naturale, preparate per il futuro?
La nostra scelta, e non da ora, é quella di operare all'interno degli standard piú diffusi e consolidati, ed offrire, nel contempo, una piattaforma aperta per consentire a terze parti di sviluppare soluzioni e applicazioni che possano rispondere in modo diretto ad esigenze di mercati verticali specifici.
Riteniamo che, in uno scenario sempre piú aperto ed interconnesso, chiudersi all'interno di una soluzione proprietaria di un solo costruttore, possa lasciar intravvedere vantaggi nel breve, ma non garantisca l'apertura reale alle nuove opportunitá che un approccio Open Platform puó portare.

Milestone (Alberto Bruschi)

Milestone ha introdotto il concetto di open platform community, proprio per poter rafforzare il legame tra vendor in grado di sviluppare soluzioni specifiche atte a portare benefici all'utilizzatore. Sistemi di analisi video avanzata, riconoscimento volti, targhe, mappe calde e statistiche marketing basate su varie fonti sono alcune delle particolari soluzioni sviluppate da nostri partner. Milestone coinvolge e viene coinvolta in progetti nei quali l'unione di eccellenze tecnologiche permette di offrire soluzioni altrimenti non realizzabili, né per tipologia né per standard di qualità. La community è una grande opportunità per tutti per poter differenziare l'offerta, creando proposte sartoriali e molto efficaci. Grazie a questo, l'utilizzatore ha un beneficio anche dal punto di vista economico legato al ritorno di investimento e ad un costo di gestione notevolmente ridotto. Valutando il costo totale di esercizio, e non il solo puro costo di acquisto, il sistema risulta quindi economicamente vantaggioso.
Il coinvolgimento di partner specializzati è parte del DNA di Milestone.

Le responsabilità degli installatori, queste sconosciute

a cura di Alessandra de Juvenich

Ai sensi dell'art. 2043 Codice Civile "*Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.*" Da questa previsione di legge di carattere generale discendono le "responsabilità del fornitore" (e, quindi, dell'installatore di sistemi di sicurezza), che potranno essere civili se i danni sono causati da un'azione involontaria (fatto colposo), o penali in caso di azione volontaria (fatto doloso), configurando un'ipotesi di reato. Per estrema semplicità, diremo che, mentre le prime si possono risolvere con il risarcimento del danno causato all'altra parte dal responsabile, le seconde devono venire invece risolte solamente in sede giudiziaria, con pene più o meno gravi in capo all'autore del reato.

Dato che il risarcimento del danno è fondamentalmente di natura economica, è possibile assicurarsi sottoscrivendo apposite polizze assicurative, specifiche in relazione all'attività svolta e al tipo di rischio da prevedere. In alcuni casi, questa copertura assicurativa è obbligatoria per legge, ad esempio: RCA (rischio civile automobilistico) per i veicoli circolanti; RC (rischio civile) per i professionisti di ogni categoria (medici, avvocati, notai, commercialisti, ecc) così come per svariate tipologie di produttori di beni e servizi, fra i quali gli istituti di vigilanza.

Una prima osservazione, del tutto intuitiva, è che per l'installatore (ditta individuale o società con dipendenti) il rischio di provocare danni al proprio cliente o a terzi, è presente sia durante le fasi di installazione (tipicamente, il muro forato con danni nell'appartamento vicino), che successivamente se, per esempio, l'impianto non funzionasse correttamente e il cliente subisse un furto.

A partire da questo numero, **essecome/securindex.com** dedicherà a questo tema di fondamentale importanza per gli installatori di sicurezza una serie di approfondimenti con il contributo di esperti delle diverse materie e di rappresentanti della categoria – associazioni e operatori – per consentire a tutti gli interessati di condividere le informazioni ed individuare le soluzioni migliori per mettere in sicurezza se stessi.

Abbiamo affrontato con i presidenti di ANIE Sicurezza, **Rosario Romano**, di AIPS, **Aldo Coronati** e il contributo di un operatore, **Andrea Berti** di SI service, uno degli aspetti correlati di maggiore delicatezza: il profilo penale dell'installatore, ovvero dei dipendenti della società di installazione.

Un aspetto finora sottovalutato che, tuttavia, è potenziale portatore di conseguenze anche gravi per il datore di lavoro/installatore. Al di là del certificato penale, che potrebbe venire richiesto dal datore di lavoro all'atto dell'assunzione solamente se fosse previsto da una normativa specifica, come ad esempio, l'albo degli installatori auspicato dai nostri interlocutori sul piano della responsabilità contrattuale ciò che rileva è il comportamento del dipendente durante il rapporto di lavoro. In altre parole, se il cliente subisce un furto causato direttamente o indirettamente dalla complicità dell'installatore, sarà il datore di lavoro a dover rispondere dei danni provocati dal dipendente infedele.

Quanto questo argomento sia rilevante per tutte le categorie di operatori della sicurezza è attestato dall'attenzione degli istituti di vigilanza che, nelle proprie polizze RC prevedono il rischio "infedeltà" dei propri dipendenti.

Il profilo penale dell'installatore - 1

risponde Rosario Romano, presidente ANIE Sicurezza

L'elevato tasso di continua innovazione tecnologica richiede un innalzamento di know how specifico per guidare gli operatori professionali del settore impiantistico di sicurezza. E' obbligatorio un continuo aggiornamento e formazione professionale degli addetti. Il system integrator (l'azienda quindi che si occupa di progettazione, installazione, manutenzione, integrazione del network e dei software) nel corso degli ultimi anni ha percorso una profonda evoluzione, innalzando le proprie competenze tecniche. I riconoscimenti dei requisiti professionali, per poter operare nel settore, attualmente in vigore, sono banali ed accessibili, praticamente, a chiunque. Questo comporta una notevole disparità tra gli operatori che affrontano il mercato in maniera professionale e competente e coloro che, da perfetti improvvisati, operano in maniera approssimativa e senza specifiche competenze. Rimane altrettanto importante che l'Azienda, nel selezionare i propri collaboratori, valuti aspetti estremamente delicati come quelli relativi al profilo penale di operatori che devono realizzare sistemi e misure di sicurezza per i Clienti. La legge italiana non prevede alcuna regolamentazione in materia dei controlli dei precedenti penali, lasciando al singolo imprenditore l'onere e la responsabilità della scelta dei propri collaboratori che trattando una materia così delicata non possono che essere di provata e specchiata moralità. E' indispensabile che l'operatore professionale della sicurezza abbia un percorso formativo certificabile e riconosciuto. In questo percorso di formazione ben si inserisce la necessità di una verifica anche delle caratteristiche morali degli operatori della sicurezza. E, come per altre professioni, appare evidente che una persona con condanne specifiche non possa essere inserito in un contesto nel quale ha dimostrato di non essere affidabile. Ricordo che due anni fa, con D.Lgs. 4 marzo 2014, n. 39, lo Stato Italiano ha inteso dare attuazione alla Direttiva europea 2011/93/EU, in materia di lotta all'abuso e allo sfruttamento dei minori.

Il menzionato decreto legislativo, in particolare, inserisce un nuovo articolo, il 25-bis, al D.P.R. 14 novembre 2002, n. 313 (il testo che regolamenta il casellario giudiziale e l'anagrafe delle sanzioni amministrative dipendenti da reato), introducendo uno specifico obbligo per i datori di lavoro che intendano assumere personale per lo svolgimento di attività che comportino contatti diretti e regolari con minori.

Il nuovo articolo, in via sintetica, impone al datore di lavoro '*che intenda impiegare al lavoro una persona per lo svolgimento di attività professionali o attività volontarie organizzate che comportino contatti diretti e regolari con minori*' l'obbligo di richiedere 'il certificato penale del casellario giudiziale […] al fine di verificare l'esistenza di condanne' per i reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, iniziative turistiche volte allo sfruttamento della prostituzione minorile e adescamento di minorenni. Il datore di lavoro che non ottemperi alla nuova previsione è soggetto ad una sanzione amministrativa pecuniaria compresa tra 10.000 e 15.000 euro) Pur non volendo mettere sullo stesso piano argomenti così profondamente differenti, la domanda che il mondo degli operatori della sicurezza si pone è se non sarebbe il caso che, anche la sicurezza di beni e persone, fosse garantita da personale con caratteristiche morali ineccepibili.

Il profilo penale dell'installatore - 2

risponde Aldo Coronati, presidente AIPS

Caro Direttore,
Ti ringrazio per la richiesta di considerazioni in relazione al tema "profilo penale installatori".
Premesso che per trattare in modo approfondito la questione occorrerebbero moltissime pagine, cercherò di condensare nei punti più importanti le motivazioni che dovrebbero portare ad una regolamentazione di quelle attività che interessano a vario titolo la sicurezza delle persone e delle cose: guardie giurate, investigatori, portieri, installatori di sistemi di sicurezza.
Naturalmente per competenza mi riferisco principalmente a questi ultimi.
Già alla fine degli anni novanta la nostra associazione aveva cercato di evidenziare la necessità di regolamentare l'attività degli installatori di sistemi di sicurezza coinvolgendo i diversi attori che, ciascuno per la propria funzione, operano in stretto contatto con la nostra: le associazioni dei produttori e rivenditori di prodotti per la sicurezza, degli istituti di vigilanza, dei professionisti e progettisti di impianti di sicurezza.
Dagli incontri e scambio di idee, nonché dal confronto con le realtà esistenti negli Stati europei, si era concretizzata l'idea di formulare una proposta di legge sulla cosiddetta "sicurezza sussidiaria" che ci portò fino alla I Commissione Affari costituzionali il 28 ottobre 2003.
In quella occasione riuscii a far comprendere l'importanza e la delicatezza del nostro compito con un semplice ma chiaro concetto: per rispondere al meglio alle esigenze del committente, sia esso un privato, un ente pubblico, un'azienda commerciale o industriale, è necessario che ci vengano fornite tutte quelle informazioni di carattere strutturale (planimetrie, contenuti, ecc.) che personali (modalità operative, abitudini, ecc.) per cui concludevo dicendo "...quindi noi di Voi sappiamo tutto; ma Voi di noi cosa sapete?!".
L'impressione fu che avessero recepito positivamente il messaggio.
Poi cambiano i Governi, e le proposte vanno nel dimenticatoio.
Da allora le cose non sono cambiate: infatti continuano a proliferare improvvisati installatori senza alcuna esperienza e formazione, oltre ai sempre presenti venditori porta a porta che offrono "meravigliosi" sistemi di sicurezza, che di "meraviglioso" lasciano solo l'illusione.
Per concludere quindi risulta sempre più evidente la necessità di rendere fruibile da parte dell'utilizzatore finale un albo o un registro a cui possano iscriversi quelle aziende che hanno i requisiti essenziali di professionalità, capacità tecnico – organizzativa e, ciò che più conta, affidabilità e serietà, condizioni queste che debbono essere opportunamente verificate e vagliate, anche sotto il profilo penale.

Perché serve un patentino per montare un condizionatore ma non per installare un impianto di sicurezza?

di Andrea Berti, CEO di SIService s.r.l. - Security and communication systems for retail and industry

Buongiorno Direttore,
prendo spunto dagli articoli sul profilo penale di portieri e installatori scritti da **Luigi Alfieri**, **Alessandro Cascio** e **Aldo Coronati** e da quanto affrontato nel corso del **Security for Retail Forum** a cui ho partecipato lo scorso 23 febbraio, per dare il mio contributo all'argomento installatori, categoria di cui la mia azienda fa parte.

Da oltre 20 anni mi occupo dell'installazione di sistemi di sicurezza e videosorveglianza (e solo di questo) per i clienti retail, mediante un'organizzazione strutturata sul territorio italiano che può soddisfare le specifiche e complesse richieste di questo particolare settore di mercato.
Vorrei portare in questo articolo il punto di vista dell'installatore sulle responsabilità civili e penali che si assume e che porta al committente al momento dell'installazione di un impianto di sicurezza - di cui non sempre si è propriamente consapevoli.
In fase di scelta e implementazione di un sistema di sicurezza, l'imprenditore o il security manager si trova a dover prendere in considerazione queste diverse aree che celano delle responsabilità civili e penali:
- le reali necessità dell'azienda per cui si decide di attivare un sistema di sicurezza e da qui la compatibilità con le normative (pensiamo ad esempio alla questione inerente la videosorveglianza nei luoghi di lavoro e l'impossibilità di utilizzare tale strumento per il controllo a distanza dei lavoratori);
- la scelta tecnica degli apparati, che è un tema sempre dibattuto perchè la forte presenza di operatori esteri sul mercato porta la possibilità di acquisto di prodotti facilmente reperibili di basso costo ma non a norma per il mercato aziendale italiano, non per il malfunzionamento o la pericolosità di tali oggetti, ma per la soluzione tecnica che si scontra con le normative in vigore (ad esempio il sempre crescente mercato di telecamere e antifurti gestibili dagli smartphone);
- l'accesso e la gestione dei dati che è il punto più scottante in tal senso: l'attività dell'installatore esperto e attento non termina con il posizionamento e l'attivazione del sistema di sicurezza, ma continua fornendo all'azienda procedure e modalità per effettuare correttamente l'accesso ai dati (chi? come? quando?) e la gestione di questi - aspetto che è particolarmente rilevante in riferimento alla norma in materia di privacy e sicurezza dei dati. Per questo solitamente le collaborazioni proseguono nel tempo.

A questo punto ci si rende facilmente conto di quali siano le responsabilità concrete dell'installatore che, di fatto, introduce nella realtà aziendale le responsabilità civili e penali inerenti l'impianto di sicurezza: un errore grossolano può portare risvolti giudiziari significativi per l'azienda cliente e in questi anni mi sono trovato più volte ad affrontare situazioni complesse e multidisciplinari - motivo per cui la nostra azienda ha una stretta collaborazione con un avvocato e un consulente privacy. Devo altresì ammettere che in questi anni mi sono imbattuto in un numero così significativo di impianti non a norma o non correttamente gestiti da superare il 50% del totale!!!
L'ultimo, ma non meno importante, spunto di riflessione è il seguente: gli obblighi connessi al ruolo dell'installatore sono individuati dall'art. 6 del D.M. 37/08, in base al quale l'installatore ha l'obbligo di realizzare l'impianto "secondo la regola dell'arte, in conformità alla normativa vigente ed è responsabile della corretta esecuzione dello stesso".
Ma cosa intendiamo noi per regola d'arte?
La nostra azienda, consapevole delle responsabilità attribuite alla nostra professione, si è autoregolamentata, creando un sistema dove il committente (ad esempio l'ufficio tecnico del cliente) è a conoscenza dello stato dei suoi impianti, giornalmente e in modo automatico. Questo è uno strumento di controllo fondamentale per garantire al committente che il suo impianto sia veramente efficiente e che, in caso di intrusione, i suoi beni siano veramente protetti. Questo per noi è fare un impianto a regola d'arte!
Troppo spesso mi è capitato di prendere in gestione impianti con almeno il 60% dei rilevatori esclusi, dove il cliente, ignaro del problema, era convinto di avere un impianto efficiente...
Cosa è invece la regola d'arte?
L'art. 5 del D.M. 37/08 stabilisce che "i progetti degli impianti sono elaborati secondo la regola dell'arte. I progetti elaborati in conformità alla vigente normativa e alle indicazioni delle guide e alle norme dell'UNI, del CEI (...), si considerano redatti secondo la regola dell'arte."
Nel nostro settore esistono tutti gli elementi per effettuare in modo corretto un'attività di progettazione, ma dall'esperienza quotidiana mi risulta che solo un numero ridotto di operatori effettuino tale attività, per cui è necessaria tanto la competenza tecnica quanto quella normativa - e peraltro generalmente non valorizzata. Tale progettazione è però la base per un'installazione a regola d'arte.
Resta aperto un interrogativo importante: per quasi tutte le attività in cui siano richieste progettazione e installazione a regola d'arte è previsto un percorso di riconoscimento della competenza oltre ad eventuale formazione. E' possibile che serva un patentino per installare un condizionatore ma non per installare un impianto di videosorveglianza?

Da casamiamiasicura network le risposte alle necessità dell'installatore di sicurezza

a cura della Redazione

Il mercato della sicurezza sta cambiando profondamente per effetto di molteplici fattori, tra i quali:

• la divulgazione delle conoscenze - anche grazie a internet - ha reso i clienti sempre più informati ed esigenti;

• l'evoluzione tecnologica di tutti i componenti, dalle telecamere ai sensori perimetrali, sta cambiando le modalità di installazione ma anche quelle di progettazione e di manutenzione;

• l'interoperabilità e l'integrabilità dei sistemi avvicina sempre più alla sicurezza operatori provenienti da altri settori (IT, TLC, domotica, impiantistica civile ecc) aumentando la concorrenza.

A tutto questo si aggiunge un altro problema per l'**installatore di sicurezza**: la possibilità di richieste di risarcimento dei danni in caso di malfunzionamento del sistema venduto, con conseguenze patrimoniali potenzialmente molto pesanti per il fornitore. Su questo aspetto, la Cassazione ha assunto da tempo un orientamento di tutela sempre maggiore del consumatore, con il fornitore chiamato a dimostrare la propria correttezza in caso di contenzioso.

Dalla parte opposta, l'aumento della insicurezza percepita da tutti i cittadini, anche per effetto della situazione internazionale, sta facendo crescere la richiesta di sicurezza, con una crescita del mercato in tutto il mondo.

Per l'installatore di sicurezza ci sono dunque molti problemi ma anche notevoli opportunità.

Come può cogliere le seconde e ridurre i primi? Come si può tutelare l'installatore dai rischi contrattuali?

Come può fare sistema con i suoi partner di canale (vendor e distributori)? Come può innalzare il proprio livello professionale? Come può avvicinare nuovi clienti sul suo territorio?

Per dare risposte puntuali e concrete a queste domande, **SWL** (Security Web Lab), la società che gestisce il motore di ricerca B2C **www.casamiasicura.it**, ha sviluppato in collaborazione con **essecome/securindex.com** la piattaforma di servizi ***casamiasicura network*** dedicata agli operatori della sicurezza fisica, installatori e system integrator, per:

• facilitare il contatto con i clienti finali principalmente dei segmenti residenziale, soho e small business;

• sviluppare le competenze tecniche e giuridiche attraverso corsi di formazione specialistica;

• mettere a disposizione soluzioni assicurative specifiche e servizi di assistenza tecnica e legale.

Gli obiettivi principali di ***casamiasicura network*** sono la tutela del ruolo dell'installatore, la promozione del suo lavoro presso i clienti finali e il rafforzamento della credibilità dell'intera categoria.

Le attività di ***casamiasicura network*** vengono proposte agli installatori in partnership con i vendor e i distributori, con la possibilità di sviluppare progetti in partnership (roadshow, presentazioni, eventi, webinar ecc).

Qui di seguito le interviste all'**avv. Laura Lenchi** e a **Roberto Dalla Torre**, che collaborano con ***casamiasicura network*** per la realizzazione dei corsi formazione.

Per maggiori informazioni:
marketing@casamiasicura.it | www.casamiasicura.it

CASAMIASICURA.it
Dove trovi la sicurezza che cerchi

Responsabilità dell'installatore, un pericolo dal quale ci si può difendere - 1
La parola al legale

a colloquio con l'avv. Laura Lenchi - Studio Legale Lenchi

Qual è l'attuale orientamento della giurisprudenza in materia di responsabilità contrattuale dei fornitori?
Doverose alcune premesse. Con il termine responsabilità si intende l'accadimento di danni considerati giuridicamente rilevanti. Si ha responsabilità contrattuale ogni qual volta sussista un rapporto tra debitore e creditore, nel quale la prestazione rimanga inattuata. Perché dall'inadempimento possano derivare conseguenze giuridiche è necessario che lo stesso sia imputabile al debitore.
Secondo i principi generali, applicabili ad ogni tipo di obbligazione contrattuale, il debitore che non esegue esattamente la prestazione è tenuto al risarcimento del danno, se non prova che l'inadempimento o il ritardo è stato determinato da impossibilità della prestazione, derivante da causa a lui non imputabile.
In un rapporto contrattuale, oltre ad agire per il risarcimento del danno, una parte è legittimata a rifiutarsi di adempiere la sua obbligazione se l'altra parte non adempie o non offre di adempiere contemporaneamente la propria.
Andando ad applicare questi principi ai contratti di fornitura o di fornitura con posa in opera, significa che il fornitore, al termine della propria prestazione, può vedersi negare il versamento del corrispettivo pattuito per non avere adempiuto correttamente quanto richiesto. In altri casi, il rapporto contrattuale può intendersi concluso, ma il fornitore può vedersi richiedere dei danni come conseguenza della non

corretta esecuzione della fornitura o delle opere.
In entrambi i casi l'onere di provare, in un eventuale giudizio, il corretto adempimento grava sul fornitore. Nel primo caso, infatti, dal 2001, ossia dall'ormai nota sentenza n. 13533 della Cassazione a Sezioni Unite, l'orientamento della giurisprudenza è radicato nel ritenere che, di fronte ad un'eccezione di inadempimento, spetti – in caso di contratto di fornitura - al fornitore dimostrare il proprio adempimento oppure la non ancora intervenuta scadenza dell'obbligazione. Ciò significa che, qualora il fornitore sia costretto ad agire in giudizio per ottenere il saldo di quanto a lui dovuto per l'attività svolta, ed il debitore, nel costituirsi in giudizio, eccepisca di non aver avuto la corretta informazione oppure che il progetto non sia stato regolarmente eseguito, graverà sul fornitore l'onere di dimostrare l'avvenuto esatto adempimento. Il non fornire la richiesta prova comporta la conseguenza di vedere respinta la domanda di versamento del corrispettivo. Anche nel caso di azione diretta ad ottenere il risarcimento dei danni, secondo il consolidato orientamento giurisprudenziale, al danneggiato compete solo fornire la prova del contratto, del danno e del relativo nesso di causalità con l'azione o l'omissione del fornitore, mentre resta a carico di quest'ultimo dimostrare che la prestazione sia stata eseguita in modo diligente e che l'evento dannoso sia stato determinato da un evento imprevisto e imprevedibile.
Bisogna, pertanto, individuare quali obbligazioni derivino da un contratto di fornitura per poter essere pronti a dimostrare la corretta esecuzione del contratto.
Secondo la Cassazione compete all'esercente l'attività professionale, apprezzare il rischio del servizio domandatogli, informarne il committente ed eseguire la prestazione che questi comunque richieda, con l'adozione delle cautele necessarie, la cui adeguatezza va valutata alla stregua del criterio della diligenza. E la diligenza andrà valutata sulla base delle specifiche competenze che la natura dell'attività esercitata richiede.
La giurisprudenza ha, inoltre, elaborato una serie di doveri, c.d. "doveri di protezione", come obblighi insiti in ogni rapporto obbligatorio a tutela della parte debole. Mi riferisco, ad esempio, al dovere di informazione, al dovere di redigere progetti che assecondino le specifiche richieste del committente e le finalità perseguite, senza eccessivi oneri e sacrifici, secondo un principio di correttezza e buona fede.

Quali sono gli aspetti più a rischio per un installatore di sistemi di sicurezza e antincendio, che potrebbero esporlo maggiormente a richieste risarcitorie da parte dei clienti?

"*Se non si ritenesse che un allarme specifico possa in qualche misura essere utile per evitare l'evento furto o incendio o per attenuarne le conseguenze, allora non vi sarebbe alcuna ragione per installarlo*". Questa, in estrema sintesi, la conclusione cui è giunta di recente la Cassazione nel decidere in merito al risarcimento dei danni richiesti da un gioielliere che aveva subito un furto, alla società che aveva installato l'impianto di allarme. L'installatore di sistemi di sicurezza interviene per la protezione di beni che spesso sono di ingente valore, quali immobili, preziosi, opere d'arte.

La verificazione dell'evento che si mira a scongiurare, mette sotto la lente d'ingrandimento il suo operato ed in corso di causa si dovrà fornire la prova che non vi è un nesso causale tra l'evento e l'impianto. E non mi riferisco solo al funzionamento dell'impianto, ma anche alla sua progettazione, dalla quale potrebbe dipendere la non completa copertura di tutte le zone da proteggere; o alla colpevole divulgazione di dati, magari utilizzati dai dipendenti dell'impresa installatrice per la realizzazione dell'atto criminoso.

In che modo si può tutelare l'installatore?

Innanzitutto consiglio sempre di usare la massima attenzione nella stipula del contratto. Molte volte si è più concentrati sull'aspetto tecnico e sul voler assecondare le esigenze del cliente, e si dimentica di prevenire, grazie a dettagliati accordi contrattuali, eventuali contestazioni o eventi che potrebbero vanificare il lavoro svolto.

Mi riporto a quanto sopra precisato: l'installatore deve provare di avere adempiuto con la "diligenza qualificata". Per questo motivo è importante concordare per iscritto con il cliente le specifiche esigenze dallo stesso richieste o prevedere eventuali esclusioni. Quello che viene accettato dal committente oralmente, difforme da quanto previsto nel contratto, in caso di evento patologico del rapporto contrattuale, non può essere provato.

In un eventuale giudizio, la verifica sulla corretta esecuzione, a regola d'arte, è demandata ad esperti nel settore che dovranno espletare una attenta valutazione di tutto il processo di realizzazione, dalla fase progettuale alla concreta esecuzione, al tipo di materiali utilizzati: il tutto in conformità alla normativa. Ricordo, peraltro, l' esistenza di norme tecniche di riferimento.

Bisogna usare competenza in ogni aspetto, cercando di prevedere, innanzitutto in fase progettuale, ogni evento. Ed essere pronti a poter provare tale scrupoloso lavoro con dettagliata documentazione.

L'installatore, inoltre, è chiamato anche a controllare la correttezza di un progetto, quando da lui non predisposto, e la bontà delle istruzioni impartite dal committente, segnalandone gli eventuali errori. Solo in questo caso, qualora il committente, reso edotto, insistesse, comunque, per la realizzazione dell'opera, l'installatore andrebbe esente da responsabilità.

Dal suo punto di vista come interagisce la normativa sulla tutela dei dati raccolti dai sistemi di videosorveglianza – peraltro in fase di revisione complessiva a livello europeo - sul piano della responsabilità civile degli installatori verso il committente e verso terzi?

All'installatore di sistemi di sorveglianza è ormai richiesto di conoscere la normativa sulla privacy e di essere un esperto consulente per il cliente circa il corretto utilizzo degli strumenti tecnologici.

Non si può parlare di corretta esecuzione se l'installatore non ha fornito i dovuti chiarimenti tecnici su come debba essere posizionato il sistema di sorveglianza, sulla durata della conservazione delle immagini, sul tipo di informativa da predisporre, sul monitoraggio da effettuare in merito al funzionamento delle telecamere.

In particolare, l'art. 25 all. B Codice Privacy prevede che l'installatore debba rilasciare al committente una descrizione scritta dell'intervento effettuato che ne attesti la conformità alle disposizioni del disciplinare tecnico in materia di misure minime di sicurezza.

In questo caso l'installatore potrà andare esente da responsabilità, potendo dimostrare che i compiti attribuiti sono stati adempiuti in conformità alla normativa.

Responsabilità dell'installatore, un pericolo dal quale ci si può difendere - 2. La parola all'esperto di certificazioni

a colloquio con Roberto Dalla Torre – esperto di certificazioni

Il mondo della sicurezza sta cambiando rapidamente, sotto la spinta congiunta della digitalizzazione dei sistemi e di una domanda sempre più consapevole da parte degli utilizzatori finali, siano essi privati o professionali. In che modo le figure che progettano, installano e manutengono gli impianti di sicurezza si stanno adeguando a questo cambiamento?

Per comprendere l'importanza dell'evoluzione tecnologica nel mondo della sicurezza, bisogna soffermarsi un attimo e definire il significato di sicurezza. La sicurezza (dal latino "sine cura": senza preoccupazione) può essere definita come la "conoscenza che l'evoluzione di un sistema non produrrà stati indesiderati". In termini più semplici è: sapere che quello che faremo non provocherà dei danni. Il presupposto della conoscenza è fondamentale da un punto di vista epistemologico poiché un sistema può evolversi senza dar luogo a stati indesiderati, ma non per questo esso può essere ritenuto sicuro. Solo una conoscenza di tipo scientifico, basata quindi su osservazioni ripetibili, può garantire una valutazione sensata della sicurezza. La sicurezza totale si ha in assenza di pericoli. In senso assoluto, si tratta di un concetto difficilmente traducibile nella vita reale, anche se l'applicazione delle norme di sicurezza rende più difficile il verificarsi di eventi dannosi e di incidenti e si traduce sempre in una migliore qualità della vita.

Nel termine italiano "sicurezza" collassano due distinti concetti che in altre lingue sono espressi da parole differenti. Il termine inglese "security" corrisponde alla sicurezza intesa come protezione da atti intenzionali che potrebbero ledere cose o persone, mentre il termine "safety" riguarda la sicurezza delle persone, intesa come loro incolumità. La sicurezza anticrimine, quindi security, ha attinto a piene mani nell'evoluzione tecnologica per dare una risposta adeguata alla necessità di sentirsi protetti, utilizzando fin dai primi sistemi la possibilità di trasformare fenomeni fisici in segnali elettrici e affinando sempre più le tecniche di elaborazione/gestione di questi segnali. Quindi, sono stati studiati e realizzati dispositivi (rivelatori) quali ad esempio infrarossi passivi capaci di "sentire variazioni di calore" o rivelatori a microonde capaci di "vedere" un corpo che si muove (effetto Doppler) e altri numerosi tipi di rivelatori capaci di tradurre numerosi fenomeni fisici (rilevati come tentativi di intrusione) in segnali elettrici (avviso di allarme). I primi sistemi di sicurezza erano poco più che scatole piene di relè, il cui scopo principale era quello di azionare una sirena la più potente possibile. Lo studio per realizzare un sistema non richiedeva molto tempo, ma la rapida evoluzione dell'elettronica, passata dai transistor ai microprocessori, ha portato ai sofisticati sistemi di sicurezza odierni. Oggi tutto può viaggiare in rete, oggi tutto è disponibile con un click: quindi, la parte tecnologica dei sistemi ha fatto passi da gigante, l'utilizzatore può avere a disposizione una vasta gamma di soluzioni alle sue necessità. E' evidente che a fronte di un'evoluzione così spinta dei sistemi si deve essere verificata una altrettanto evoluzione delle conoscenze e della preparazione di chi progetta, installa e fornisce assistenza ai sistemi di sicurezza. Il mondo della sicurezza si è dato delle regole tecniche (NORME) per la realizzazione delle apparecchiature e altrettante per la realizzazione degli impianti, questi sono gli strumenti che i professionisti del settore devono conoscere ed applicare. Essendo un mondo in continua evoluzione risulta quindi indispensabile che i vari protagonisti (progettisti, installatori, manutentori) debbano accedere ad una formazione adeguata e continua.

Questo deve essere di stimolo al mondo della formazione, che deve preparare e rendere disponibili momenti formativi all'altezza del momento. D'altra parte i progettisti e gli installatori, se non vogliono essere superati dall'innovazione ma vogliono farne un loro un punto di forza, devono investire parte del loro tempo nella formazione.

Un altro effetto di questa evoluzione è l'arrivo nel mercato della sicurezza di operatori provenienti da altri settori, da una parte i systems integrator IT, dall'altra gli impiantisti elettrici e i general contractor dell'edilizia. In entrambi i casi, alle competenze tecniche sulle tecnologie da usare potrebbero non essere in grado di affiancare conoscenze specifiche in materia di sicurezza. Quali sono i percorsi da proporre a queste figure?

Il settore della sicurezza in Italia è per così dire "affollato", risultano infatti iscritti alle CCIAA più 40.000 soggetti che hanno nel proprio oggetto "… realizzazione di impianti e sistemi di sicurezza.". Ad un numero così elevato di soggetti si contrappone la loro dimensione, che è estremamente ridotta (per moltissime realtà risulta essere di un solo addetto). Di per sé, la "piccola dimensione" non vuol dire mancanza di qualità o di competenza, però evidenzia un mercato particolarmente frammentato.

In questo momento particolare si vedono entrare nel mercato della sicurezza operatori (costruttori e systems integrator) provenienti da altri settori con un'offerta di sistemi chiusi (sistemi di sicurezza, domotica, automazione), che non sempre hanno una conoscenza specifica in materia di sicurezza.

Viene quindi a manifestarsi sempre di più l'esigenza di formare le figure che dovranno progettare, realizzare e fornire servizi di sicurezza.

Sarebbe quindi auspicabile che i distributori, che sono tra i principali attori del settore, organizzino incontri formativi sul territorio, preparando un programma che preveda la trattazione di vari argomenti, dalla evoluzione tecnologica dei prodotti, alle normative prodotti/impianti, alla progettazione dei sistemi fino alla preparazione di pacchetti ad hoc di assistenza/manutenzione degli impianti. Incontri quindi che uniscono aspetti tecnici e normativi e che forniscono importanti momenti di confronto tra gli operatori e gli esperti del settore. Una particolare attenzione dovrà essere rivolta alla presentazione di questi prodotti/servizi al cliente finale: dovranno essere quindi preparati corsi ad hoc che preparino l'erogatore di servizi, sia esso installatore o altro, a curare con maggior attenzione l'aspetto comunicativo. Il cliente dovrà avere di fronte un partner della sicurezza dal quale avere soluzioni a 360 gradi.

Quali sono gli argomenti che lei, con la sua esperienza maturata in un ente di certificazione come IMQ, propone nelle sue lezioni frontali?

La mia esperienza in IMQ mi ha consentito di confrontarmi da una parte con i costruttori di sistemi di sicurezza, dall'altra con gli installatori e, infine, con gli utilizzatori finali (clienti). Questo mi ha dato l'opportunità di selezionare vari argomenti che sviluppo durante gli incontri formativi e che spaziano dalla tecnologia di costruzione, alla descrizione delle prove che devono superare i prodotti per essere conformi alle norme europee della serie EN 50131, all'analisi dei rischi che deve essere messa in atto prima di procedere al progetto di un sistema di sicurezza, alla preparazione di un progetto secondo la norma CEI 79-3:2012 fino all'analisi di quale deve essere la documentazione che deve essere fornita al cliente finale.

Al termine degli incontri formativi a cui partecipo propongo sempre di effettuare un test attraverso un questionario di una quindicina di domande che spaziano dalle soluzione tecnologiche alle normative CEI 79-3:2012 alle problematiche e/o soluzioni installative, questo consente di verificare la penetrazione e l'interesse degli argomenti proposti e di aggiornare e migliorare il pacchetto formativo.

La responsabilità contrattuale dell'installatore è un tema di sempre maggiore attualità. In che modo gli installatori possono prevenire possibili richieste di risarcimento?

E' necessario fare una precisazione prima di addentrarsi nell'argomento proposto e cioè che il D.M. n. 37 del 22/01/2008 (Norme per la sicurezza degli impianti) - Art. 5 "Progettazione degli impianti" recita quanto segue: "*.....omissis..... 3. I progetti degli impianti sono elaborati secondo la regola dell'arte. I progetti elaborati in conformità alla vigente normativa e alle indicazioni delle guide e alle norme dell'UNI, del CEI o di altri Enti di normalizzazione appartenenti agli Stati membri dell'Unione europea o che sono parti contraenti dell'accordo sullo spazio economico europeo, si considerano redatti secondo la regola dell'arte*".

La Norma CEI 79-3:2012 relativa agli impianti antintrusione ed antirapina recita quanto segue:

6 Progettazione dell'impianto.

6.1 Generalità - La progettazione dell'impianto di Allarme Intrusione e Rapina deve avere come obiettivo: la definizione delle aree da proteggere, il livello di prestazione, la scelta dei componenti secondo criteri di funzionalità e prestazioni coerenti con il livello di prestazione definito e la classe ambientale appropriati sulla base dell'analisi del rischio.

Quindi la strada migliore da seguire per realizzare un impianto di sicurezza antintrusione è quella di applicare la norma CEI 79-3:2012 che propone tutte le fasi che devono essere rispettate al fine di avere un impianto sicuramente a norme e quindi costruito secondo la Regola d'arte.

Ricordo che un impianto che non risulti almeno di 1 (primo livello) non può considerarsi a norma CEI e quindi non gode della presunzione della Regola d'arte.

Il progettista deve comunque, dopo aver effettuato un'accurata analisi del rischio ed individuato la tipologia impiantistica, proporre al proprio cliente un impianto del livello adeguato e comunque non inferiore al 1 (primo).

Nella Dichiarazione di Conformità dovrà quindi essere riportata la norma CEI 79-3:2012, la definizione della tipologia impiantistica di riferimento ed il livello raggiunto dall'impianto.

Dove stanno andando le tecnologie di sicurezza in Italia?

a colloquio con Andrea Hruby, Amministratore Delegato HESA S.p.A.
a cura della Redazione

L'evoluzione tecnologica della videosorveglianza sta trasformando la telecamera da "raccoglitore di immagini" in un "sensore di scenario", che rileva dati elaborati successivamente da software di analisi che gestiscono eventi, riconoscono target, alimentano business intelligence. Come valuta HESA questo processo evolutivo, dal suo osservatorio in prima fila del mercato italiano?
Negli ultimi anni, la videosorveglianza ha subìto un accelerazione così importante da diventare il settore in più rapida evoluzione nell'ambito della sicurezza, con soluzioni sempre più complete e affidabili che non sono più prerogativa degli impianti di fascia alta ma che diventano progressivamente accessibili a varie categorie di utenti. In questo scenario, l'evoluzione che sta avvenendo nell'ambito dei software analitici ha creato le premesse per un nuovo concetto di videosorveglianza, che potremmo definire "a monitor spento". Uno schema nel quale i monitor di visualizzazione sono normalmente spenti e si accendono soltanto quando i sistemi di videoanalisi individuano situazioni anomale, determina infatti una reazione immediata da parte del personale addetto e delle Forze dell'Ordine. Pensiamo alla potenza e all'affidabilità raggiunta dalle telecamere termiche: grazie alla capacità di offrire immagini assolutamente nitide anche in completa assenza di illuminazione e nelle condizioni climatiche più avverse, abbinate ai sistemi di video analisi consentono di trasformare il sistema di videosorveglianza in un potente strumento antintrusione, eliminando il problema dei falsi allarmi. Oggi sono disponibili termocamere in grado di coniugare costi contenuti e prestazioni eccellenti, ideali per gli utenti la cui applicazione primaria è la sicurezza a medio raggio. L'abbinamento di questi prodotti con la video analisi fa sì che si cominci a diffondere una tendenza all' utilizzo di questi strumenti anche in sostituzione al tradizionale sistema di sicurezza. La videoanalisi rende dunque possibile effettuare valutazioni molto approfondite su aree di interesse, con funzioni che possono anche travalicare i confini della sicurezza. Pensiamo soltanto alle possibilità che si sono aperte nell'ambito del marketing, dal momento che un sistema di videosorveglianza può dirci quali sono le aree in cui i clienti si soffermano maggiormente all'interno di un supermercato o di uno showroom. In generale, grazie alle nuove tecnologie, possiamo ottenere un'elevata affidabilità dei sistemi, unita ad una sempre maggiore semplicità di funzionamento e a costi accessibili. Come risultato finale, l'utilizzo delle più avanzate tecnologie di videosorveglianza consente di ottenere una sensibile riduzione dei costi, unita alla semplicità di gestione dei sistemi stessi, capaci di garantire una "multi funzionalità" che permette di spaziare in altri utilizzi fino ad una reale "business Intelligence". Vediamo che applicazioni di questo tipo cominciano ad essere utilizzate soprattutto nell'ambito del commercio, delle infrastrutture critiche e della pubblica amministrazione. Questo è un passaggio molto importante, che rappresenta il futuro, già iniziato, della videosorveglianza: il nostro ruolo è quello di guidare l'installatore verso questi nuovi trend, indirizzarlo alle soluzioni più adatte rispetto al contesto in cui opera e fargli superare anche quelle che possono essere le diffidenze iniziali verso i nuovi prodotti. Il settore della sicurezza è infatti abbastanza conservatore e se da un lato disponiamo di prodotti ad alto contenuto tecnologico, dall'altro permane talvolta la tendenza a installare apparecchiature anche datate perché conosciute e già rodate.

Il cambiamento in atto richiede competenze diverse nell'intero canale - progettisti, installatori ma anche gli utenti finali – e stimola l'ingresso nel mercato della sicurezza di nuovi operatori, provenienti in particolare dal mondo IT. Quali sono le vostre indicazioni?
Il cambiamento molto rapido a cui stiamo assistendo richiede un impegno importante da parte di tutti gli operatori del settore, dai produttori ai distributori, agli installatori. Soprattutto, si tratta di gestire i flussi di questo cambiamento e saperlo governare. Per l'installatore di sicurezza professionale, è importante sapersi adattarsi ai nuovi scenari e mettere in pratica delle azioni concrete per essere competitivo sul mercato. Il ruolo di HESA, in questo delicato passaggio, non è quello di un mero distributore di prodotti ma di un alleato strategico che accompagna la fornitura delle tecnologie con la più completa gamma di servizi esclusivi. Tecnologie e servizi che l'installatore deve imparare a sfruttare al meglio, per valorizzare la propria professionalità.

Quali sono le marche distribuite attualmente da HESA e in cosa si differenziano le diverse proposte tecnologiche e commerciali?
Dall'antintrusione alla videosorveglianza, dal controllo accessi alla rilevazione incendio, ai prodotti per l'integrazione di sistemi, la gamma di HESA è un catalogo eccellente dei migliori prodotti oggi disponibili sul mercato, tutti caratterizzati da alta qualità e tecnologia avanzata. I marchi distribuiti sono di altissimo livello: OPTEX, di cui HESA è distributore esclusivo per l'Italia da oltre trent'anni, UTC, DSC, JABLOTRON, TEXECOM, XTRALIS, per citarne solo alcuni nel settore antintrusione. Passando alla videosorveglianza, la gamma distribuita da HESA comprende tutti i prodotti SAMSUNG, DAHUA, CANON e la linea HESAVision, recentemente rinnovata con una serie davvero interessante di telecamere Over IP e AHD ad elevate prestazioni. La nostra proposta comprende inoltre la linea completa delle termocamere FLIR, tutta la gamma VIDEOTEC, i sistemi con analisi video e registrazione a bordo VideoIQ di AVIGILON, gli obiettivi TAMRON e le soluzioni più evolute per l'integrazione dei sistemi, rappresentate dai marchi MILESTONE, ARTECO e TECHNOAWARE. Con una proposta così completa e diversificata, capace di coniugare elevato livello tecnologico, attenzione al design e un ottimo rapporto prezzo-prestazioni, siamo in grado di fornire di volta in volta ai nostri clienti la soluzione più efficace per ogni contesto da proteggere.

Iniziative come il recente Digital Imaging Tour, organizzato assieme a Canon e Milestone, come vengono accolte dai vostri clienti?
Iniziative come il Digital Imaging Tour, che si è svolto nelle sedi HESA di Milano, Firenze e Roma nella seconda metà di febbraio con un'importante

partecipazione di pubblico, fanno parte di quel valore aggiunto che offriamo ai nostri clienti e che rappresenta, forse, l'elemento più distintivo della nostra realtà. In queste occasioni gli installatori hanno modo di conoscere nel dettaglio le più recenti novità tecnologiche introdotte nel catalogo HESA, comprendere come avviene l'integrazione tra specifici prodotti, assistere a prove di programmazione sulle apparecchiature e confrontarsi con altri operatori del settore. Sia questo road show organizzato con CANON e MILESTONE, sia gli altri che realizziamo di volta in volta nel corso dell'anno insieme ai vari partner tecnologici, riscuotono un grande interesse da parte degli installatori. Lo percepiamo sia dalla partecipazione in sala, sia dalle risposte nei questionari compilati al termine dei lavori.

La nuova gamma HESAVision

Pochi mesi fa, in occasione di SICUREZZA 2015, HESA ha presentato una linea completamente rinnovata di telecamere Over IP di HESAVision, un marchio che è sinonimo di affidabilità e innovazione nell'ambito della videosorveglianza. La nuova gamma di telecamere si compone di una serie di modelli da 2 Megapixel 1080p e di due telecamere 2K da 4 Megapixel, disponibili nei classici formati Bullet e Mini-Dome da esterno, oltre a una Speed-Dome con ottica zoom 30x con illuminatori IR integrati e portata fino a 100 metri.
Tutte le telecamere della nuova serie HESAVision sono compatibili con lo standard ONVIF Profilo S, grazie al quale si possono selezionare diverse tipologie di terminali di registrazione. A questa gamma di telecamere si aggiunge una linea di NVR compatti e da rack. Tra questi si segnalano gli NVR Serie WN con porte PoE per alimentare le telecamere, disponibili da 4 fino a 32 canali per le applicazioni più importanti dove è necessario l'utilizzo del software dedicato HV Central. Questa gamma assolutamente completa dispone inoltre di una serie di accessori di montaggio in grado di soddisfare qualsiasi esigenza di installazione.

CONTATTI: HESA SPA
Tel. +39 02 380361
info@hesa.com
www.hesa.com

SAMSUNG TECHWIN diventa HANWHA TECHWIN: un cambiamento che porta a una nuova prospettiva

a cura della Redazione

Si é compiuto lo scorso 1 Aprile un passo importante nella strategia di crescita globale del Gruppo Hanwha, con il cambio di nome di **Samsung Techwin Europe Limited** in **Hanwha Techwin Europe Limited**.
Il processo, iniziato nel dicembre 2014, ha visto in questi mesi il passaggio di tutti gli asset aziendali, delle strutture produttive e dei reparti di R&D all'interno del Gruppo Hanwha.
Fondato nel 1952, il **Gruppo Hanwha** si caratterizza per la soliditá organizzativa e finanziaria. E' una delle dieci maggiori imprese della Corea del Sud ed è inserito nella classifica "FORTUNE Global 500", con 52 societá affiliate e 146 partner in tutto il mondo, attivi in più settori: manifatturiero e costruzioni, finanza, servizi e tempo libero.
Forti investimenti in R&D ed un piano industriale rivolto alla crescita hanno portato il Gruppo Hanwha a giocare un ruolo di leader mondiale nel mercato dei pannelli fotovoltaici. La rete finanziaria, che comprende servizi bancari, assicurativi, gestione di asset e titoli, rappresenta il secondo maggior gruppo finanziario non bancario della Corea del Sud.

UNA NUOVA PROSPETTIVA
Con l'acquisizione di Samsung Techwin, inizia una nuova sfida per il Gruppo Hanwha, che intende ora supportare il processo di consolidamento del business della VideoSorveglianza e della Sicurezza Professionale. Il Gruppo Hanwha ha un programma di importanti investimenti stimolati dalle potenzialitá di crescita di questo mercato e dalla affidabilitá e dalle capacitá tecniche, commerciali e di relazione con il mercato che Samsung Techwin, e tutta la sua organizzazione nel mondo, ha portato in dote
. Il processo é iniziato, e prevede un piano di investimenti e di crescita organica per i prossimi anni.
Alcuni risultati sono giá visibili nell'immediato.
Nel corso di questi mesi, verranno lanciati piú di 50 nuovi prodotti per la VideoSorveglianza Professionale, con novitá in nuovi settori di mercato per **Hanwha Techwin** che porteranno, quindi, un aumento delle opportunitá di business per i partner sul territorio.
Sono gia disponibili dal mese di aprile due nuove gamme di prodotti.
La nuova gamma **WiseNetHD+**, che vede l'azienda

entrare nell'arena della Videosorveglianza FullHD su coassiale con un range di prodotti che sfruttano tutta l'esperienza nella gestione del video dei reparti di R&D per garantire immagini di elevata qualitá, come da tradizione di Samsung Techwin.
Anche la gamma IP si é ampliata ulteriormente con un nuovo range di telecamere PTZ con risoluzione Full HD e HD, caratterizzate da un livello di rapporto prezzo/prestazioni particolarmente interessante.
Ma non sono le uniche novitá.
Altri nuovi prodotti, piú incentrati su soluzioni ad altissima risoluzione (UHD e oltre) , e applicazioni di Video Analitics avanzate, basate sull' Open Platform disponibile sulle telecamere **Samsung WiseNetIII**, studiate per specifici mercati verticali come retail, banking e controllo traffico, verranno introdotti nel corso del 2016, affiancandosi a quelle giá disponibili per lettura targhe e time-lapse.

NOVITÁ ANCHE PER L'ITALIA

Anche sul mercato locale gli investimenti in marketing e risorse sono giá iniziati.

Il team italiano, recentemente ha visto due nuovi ingressi con **Gaia Chignola**, in qualitá di Sales and Marketing Assistant, e **Davide Castello** in qualitá di Technical Manager: un allargamento del team che porta ad essere sempre piú vicini ai nostri partner, non solo con prodotti e condizioni adeguate.
Tra Maggio e Luglio, inoltre, verra organizzato un roadshow in tutto il territorio nazionale, il **WiseNet HD Tour 2016**, per incontrare aziende, system integrator, progettisti e security manager, e presentare tutte le importanti novitá per il 2016 e la vision per il futuro.
Molto importante sará anche la presenza di **Hanwha Techwin** a **IFSEC 2016**, dove verranno presentate tutte i nuovoi prodotti e le nuove soluzioni per i mercati verticali.

"Una nuova prospettiva" é lo slogan che caratterizza questa campagna per presentare le novitá del 2016.
Il viaggio é appena iniziato, e, con la nuova veste, **Hanwha Techwin** é pronta ad affrontare le opportunitá del mercato con l'esperienza, la professionalitá, la solidità e l'entusiasmo di sempre.

WiseNet HD Tour 2016: la Nuova Prospettiva per la Sicurezza Professionale

Un viaggio entusiasmante per scoprire tutte le novitá Samsung per la VideoSorveglianza Professionale

Mantenendo un appuntamento ormai tradizionale per i Professionisti della Sicurezza, anche quest'anno il team di **Hanwha Techwin** sará impegnato in un roadshow per presentare tutte le novitá a marchio Samsung per la VideoSorveglianza Professionale, in collaborazione con i Distributori Certificati su tutto il territorio nazionale.
Con lo slogan **Una Nuova Prospettiva**, il tour nell'edizione 2016 si arricchisce di contenuti di formazione dedicati ad installatori e system integrator sulle normative che regolano le responsabilitá legali nella realizzazione di impianti di Sicurezza e VideoSorveglianza
Si parlerá inoltre delle nuove serie **Wisenet HD+**, per soluzioni FullHD su cavo coassiale, e di tutte le novitá per il mondo IP, con soluzioni complete in altissima risoluzione (UHD e 4K), con una attenzione particolare alle tecniche esclusive di compressione dei segnali, incluse nelle nuove telecamere Samsung.
Quando si parla di 4K e 12 MegaPixel, la risoluzione rappresenta solo una faccia della medaglia.
Senza un adeguato processo di compressione, gestione e ottimizzazione dei flussi, la reale implementazione di soluzioni ad altissima risoluzione, diventa complicata e il piú delle volte difficile da realizzare.
Le nuove telecamere ed i nuovi NVR Samsung, che verranno presentati nel corso del roadshow, implementano tutti lo standard H.265, oltre all'esclusivo algoritmo di compressione **WiseStream**, che riduce al 25%, rispetto a telecamere H.264, l'utilizzo di risorse di rete e di storage, senza inficiare sulla qualita delle immagini.
Si parlerá anche delle nuove soluzioni Open Platform, per analisi video, per nuove applicazioni e per nuove opportunitá di business, per il mondo retail, banking e controllo traffico.
L'esordio sará il **10 maggio a Verona**, e sono giá state fissate altre date in tutta Italia tra maggio e giugno.
Per ricevere il calendario completo e prenotare la partecipazione ad una delle date, é sufficiente mandare una mail a hte.italy@hanwha.com

Hanwha Techwin Europe

CONTATTI: HANWHA TECHWIN EUROPE LTD
Tel. +39 02 38608228
www.samsung-security.eu

Intelligenza Artificiale e sicurezza, l'inevitabile incontro

a colloquio con Frediano Di Carlo, consulente per la Sicurezza e le Tecnologia
a cura della Redazione

Uno dei grandi temi che in questo periodo interessano l'opinione pubblica è l'Intelligenza Artificiale (AI), descrivibile in estrema sintesi come la capacità dei calcolatori di effettuare "scelte", una proprietà tipica della mente umana. Scenari fantascientifici a parte, gli ambiti applicativi di questa disciplina (o tecnologia?) sono intuitivamente infiniti ma la sicurezza è uno dei campi di prova più diretti e immediati.

Per capire cosa sia in realtà la AI e cosa l'industria della sicurezza possa ragionevolmente aspettarsi dalle sue applicazioni, abbiamo chiesto a un "tecnologo" come Frediano Di Carlo di fare il punto della situazione.

La sua articolata risposta è un articolo dal quale abbiamo ricavato un **e-book** che suggeriamo di scaricare e consultare dopo aver letto l'intervista a Di Carlo che parte dal collegamento della AI con i metadata, l'altro grande tema che avevamo affrontato con Di Carlo (Cosa sono i Metadata).

Quali sono i collegamenti tra metadata e Intelligenza artificiale (AI)?

Come vedremo nell'articolo, alla base della AI ci sono le seguenti attività:

- far apprendere alle macchine informazioni di base; in altri termini 'dotare le macchine di esperienze specifiche';
- implementare algoritmi che, in base a tali informazioni, permettano loro di prevedere un risultato; come dire 'dotarle di ragionamento'.

Per attuare il primo punto abbiamo bisogno di dati da fornire alle macchine, in diversi casi in quantità non trascurabili; viene spontaneo pensare che una di queste fonti possa essere un DB di Metadati, che dopo un determinato periodo di tempo avrà certamente accumulato le quantità sufficienti.

Il secondo punto richiede studi e aggiornamenti costanti, data la continua evoluzione delle tecniche di settore, tipiche attività da enti di ricerca, istituzioni universitarie, ecc.

Quali sono le possibilità di applicazione immediate della AI nel campo della sicurezza, come si deduce dall'esempio citato nell'articolo della lettura targhe? Quali sono le applicazioni per il riconoscimento facciale in chiave anti terrorismo?

Per non trascurare le mie origini professionali, mi sento di affermare che nel campo della sicurezza fisica assisteremo, anche a breve, a ricadute interessanti di queste tecniche, anche in alcuni settori che hanno raggiunto una decisa maturità.

Un esempio significativo è rappresentato dai diversi studi applicati alla protezione perimetrale, in sperimentazione in diversi aeroporti degli USA; questi si sono concentrati in due distinte direzioni:

il processamento dei segnali dei sensori di rilevamento; per fare in modo che le analisi siano sempre più accurate e, soprattutto, per eliminare tutti quei fenomeni che generano allarmi impropri

lo studio del contesto legato all'uomo in procinto di violare il perimetro; es. presenza di mezzi di ausilio allo scavalcamento, comportamenti tipici, ecc., ciò ovviamente al fine di prevenire l'evento

Questo comunque è nulla in confronto alla quantità di studi, e investimenti, nel campo contro il terrorismo.

Negli USA sono state sviluppate diverse piattaforme SW dedicate, definite Intelligent Software Solution, tra cui la più famosa si chiama Dfuze, tanto da coniare l'appellativo, per le FF.OO. che ne fanno uso, di 'Polizia Predittiva', che richiama molto la Precog di Minority Report, salvo che nel film le precognizioni le avevano tre individui queste invece sono delle macchine.

Quali sono gli interlocutori italiani che possono utilizzare queste nozioni per sviluppare loro soluzioni/applicazioni nel settore sicurezza?

Abbiamo detto che gli ambienti più adatti sono quelli legati al mondo della ricerca, ma lo stesso vale nel il campo della Video Analytics per sviluppare algoritmi sempre più elaborati e precisi, potremmo dire *sempre più intelligenti*.

In Italia abbiamo diverse realtà del genere che operano in questo secondo campo, due esempi per tutti (non me ne vogliano gli altri) A.I. Tech di Salerno e Technoaware di Genova; la prima è uno spinoff universitario, la seconda ha una convenzione permanente, e un laboratorio congiunto, con il Dipartimento di Ingegneria Biofisica ed Elettronica dell'Università di Genova (DIBE); chi meglio di loro potrebbero implementare tecniche di AI? Disporrebbero *alla fonte* dei Metadata prodotti dai loro algoritmi e potrebbero facilmente migliorare parte di essi, o implementarne di nuovi.

Microsoft, investire sulla sicurezza per un futuro always-on

a colloquio con Carlo Mauceli, National Technology Officer di Microsoft Italia
a cura di Raffaello Juvara

La diffusione di dispositivi in rete per realizzare sistemi di sicurezza fisica – in particolare di videosorveglianza – ha comportato anche un avvicinamento tra IT e physical security, con l'esigenza di proteggere l'utilizzatore finale da "attacchi combinati". Banche, data center, retailer, pubbliche amministrazioni sono gli obiettivi più interessati da queste minacce. In che modo Microsoft ha affrontato questo tema e quali soluzioni offre per ridurre i rischi?

L'avvicinamento tra IT e sicurezza fisica non è una questione nuova, ma un tema sempre attuale che esiste da tempo. Anzi, il pensiero comune è quello di dovere alzare, soprattutto, le difese perimetrali piuttosto che operare a 360° coprendo le infrastrutture logiche, siano esse server, pc, tablet, smartphone piuttosto che apparati di ogni genere. Il fattore cruciale per lo sviluppo di un programma di protezione efficace è la creazione di una cultura che riconosca il valore prioritario della sicurezza. Questo va al di là di qualsiasi considerazione relativa alla sicurezza fisica piuttosto che a quella logica. Microsoft è consapevole del fatto che una simile cultura deve essere introdotta e supportata dalla dirigenza aziendale. Noi, come azienda, ci siamo impegnati a lungo per effettuare gli investimenti e fornire gli incentivi appropriati al fine di promuovere un comportamento orientato alla sicurezza. Guardando al panorama nazionale e non solo, traspare che questo livello di organizzazione e di consapevolezza è poco diffuso e questo comporta che le infrastrutture on premise non vengano aggiornate, gestite e segregate secondo i più classici dettami derivanti dalle best practice che pubblichiamo con regolarità. Di fronte a uno scenario simile in cui i produttori di applicazioni spesso sono i responsabili di questa situazione perché creano lock in, una possibile via d'uscita è il cloud. Viviamo nella società più digitale di sempre. Lo diceva già Al Gore proprio con il concetto di Information Society e Digital Life. Una società alla cui base sta, appunto, l'informazione; una società con keyword chiare quali global, always-on, broadband, mobile, digital inclusion, E-government, infrastrutture critiche, sicurezza, resilience. In questo scenario, Microsoft comprende perfettamente che il successo nel settore in rapida evoluzione degli Online Services dipende da sicurezza e privacy dei dati dei clienti e da disponibilità e flessibilità dei servizi offerti. L'azienda pertanto progetta e testa diligentemente applicazioni e infrastruttura sulla base di standard riconosciuti a livello internazionale per dimostrare di poter offrire tali caratteristiche unitamente alla conformità alle leggi vigenti e alle politiche interne per la sicurezza e la privacy. Come risultato, i clienti di Microsoft beneficiano di test e monitoraggio più accurati, invio automatico delle patch, economie di scala volte alla riduzione dei costi e continui miglioramenti sul piano della protezione.

I produttori di sistemi di sicurezza fisica stanno proponendo sempre più intensamente soluzioni su cloud, sia per lo storage dei dati di videosorveglianza che per la gestione dei sistemi stessi, in particolare per il mercato residenziale. Come vengono protetti i dati su cloud da Microsoft?

Microsoft classifica le risorse in modo tale da determinare la portata dei controlli di sicurezza da applicare. Le categorie tengono conto del potenziale relativo ai danni alla reputazione e finanziari, nel caso in cui la risorsa venga coinvolta in un incidente correlato alla sicurezza. Una volta classificata la risorsa, viene adottato un approccio approfondito alla protezione per determinare quali misure sono necessarie. Ad esempio, le risorse dati che rientrano nella categoria degli impatti moderati sono soggette ai requisiti di crittografia quando risiedono su supporti rimovibili o quando sono coinvolte in trasferimenti su reti esterne. Oltre a tali requisiti, i dati a impatto elevato sono soggetti anche ai requisiti di crittografia per l'archiviazione e i trasferimenti su reti e sistemi interni. I prodotti Microsoft devono rispettare le norme di crittografia SDL, che elencano gli algoritmi di crittografia accettabili e non accettabili. Ad esempio, per la crittografia simmetrica sono necessarie chiavi lunghe più di 128 bit. Quando si utilizzano algoritmi asimmetrici, sono necessarie chiavi lunghe almeno 2.048 bit.

Il concetto di business continuity nasce in ambito IT, ma si sta divulgando nelle organizzazioni complesse, pubbliche e private, finalizzato alla gestione delle emergenze fisiche di ogni natura. Quali sono le proposte di Microsoft?

Microsoft non sviluppa soluzioni di Disaster Recovery e Business Continuity per le infrastrutture fisiche, salvo fatto per i propri Datacenter. Noi crediamo che la vera innovazione stia nella possibilità di separare ciò che è soluzione logica (software) da ciò che è fisico, utilizzando solo il network come elemento indispensabile. In un contesto simile, il cloud ibrido può essere una soluzione vincente perché da un lato garantisce gli investimenti fatti dalle singole aziende e dall'altro mette a disposizione le piattaforme di cloud pubblico (Microsoft Azure) per la ridondanza e la continuità dei servizi.

Qual è la visione globale di Microsoft nel breve/medio termine sul tema dell'integrazione tra IT e physical security?

Riflettendo sugli scenari futuri, si andrà sempre di più verso l'integrazione, la virtualizzazione, la centralizzazione, l'always on: tutto in rete, tutto connesso, tutto disponibile in qualsiasi istante, da qualsiasi dove e su qualsiasi dispositivo. Chiaramente, tutto ciò comporta sempre il fatto che il livello di sicurezza sia adeguato, ma sempre più le aziende tendono a dotarsi di sistemi as a service. Pertanto, ci saranno sempre più servizi esperti, legati a persone e mezzi che avranno la necessità di essere geolocalizzati in modo tale che, in funzione delle differenti condizioni, saranno in grado di utilizzare i servizi di sicurezza più appropriati. Presumibilmente, tutto questo avverrà sfruttando connessioni e tecnologie di tipo wireless nonché soluzioni di knowledge managment in grado di gestire correlazioni di tipo cross tra sicurezza fisica, logica e in mobilità e ciò comporterà sempre più la necessità di utilizzare piattaforme di analisi dei dati che solo il cloud, attraverso l'utilizzo di soluzioni basate su machine learning, può offrire. Alla base di tutto resta sempre e comunque la cultura della sicurezza. Se l'Italia non cambia radicalmente il proprio approccio, nulla di tutto ciò avrà senso.

CONTATTI: MICROSOFT
www.microsoft.it

HESA Professional Tour, alla ricerca dei migliori professionisti della sicurezza

a cura della Redazione

Quali sono gli spazi per gli installatori professionali di sicurezza e qual è il ruolo del distributore a valore aggiunto nel mercato di oggi? Questi i due temi molto concreti che **Carlo Hruby**, amministratore delegato di **HESA spa**, ha posto al centro dell'incontro del 16 marzo nella tappa dell'**HESA Professional Tour** a Bologna con i professionisti interessati a entrare nella community di Installatori Autorizzati e Concessionari dello storico distributore milanese.

Partendo da una panoramica dei dati di mercato che confermano la crescita del settore sotto la spinta inarrestabile dell'aumento dei furti nelle abitazioni e nelle attività commerciali, Carlo Hruby ha sottolineato l'importanza dell'evoluzione culturale di chi propone le soluzioni di sicurezza ai clienti finali.

Un'evoluzione che parte dalla consapevolezza del cambiamento che sta attraversando il settore, determinato da più cause. L'ingresso di operatori provenienti da altri settori, in particolare dal mondo elettrico e dall'IT, l'aumento delle conoscenze degli utilizzatori, l'evoluzione tecnologica dei sistemi da una parte e la pervasività di internet dall'altra, sono solo alcuni dei fattori che interagiscono sia con la figura dell'installatore, che entra a diretto contatto con gli acquirenti finali, che con quella del distributore, impegnato sempre più a sostenere i propri clienti con azioni che aggiungono valore al rapporto di collaborazione.

Un impegno che HESA ha fatto proprio operando fin dall'inizio del suo percorso, per creare un gruppo consolidato di professionisti qualificati ai quali fornisce servizi esclusivi: l'organizzazione della distribuzione, l'assistenza tecnica, la garanzia, il supporto finanziario, la formazione. Un capitolo di estrema importanza nella realtà di HESA è rappresentato dalla **Fondazione Enzo Hruby**, un'iniziativa unica in Europa e forse al mondo, per intervenire concretamente a tutela del patrimonio artistico italiano proteggendo siti museali e singole opere con la realizzazione di sistemi di sicurezza.

Oltre a questa motivazione istituzionale diretta, le valenze delle Fondazione sono molteplici, dalla crescita dell'immagine del settore alla divulgazione della cultura della sicurezza al di fuori dell'ambito degli addetti dei lavori, passando per la creazione di opportunità per i propri partner. La centralità di questi ultimi nell'attività della Fondazione è testimoniata dal **Premio H d'Oro**, che ha celebrato nel 2015 la decima edizione con una straordinaria festa a Venezia lo scorso 23 ottobre. Il Premio rappresenta perfettamente l'attenzione della Fondazione (e dell'azienda HESA che la sostiene) per chi lavora nella sicurezza. E' un concorso aperto alle migliori realizzazioni, indipendentemente dai sistemi utilizzati, diventato anno dopo anno il momento di confronto e incontro più seguito e ambito dagli installatori di ogni dimensione e specializzazione.

"HESA investe nella filiera dedicando ogni sforzo per avere come clienti professionisti competenti, seri e competitivi, che basano la propria strategia sulla qualità. Avendo HESA come fornitore di riferimento, i nostri partner si distinguono sul mercato e sono in grado di proporre soluzioni su misura per i propri clienti - ha spiegato Carlo Hruby nel corso della sua esposizione a Bologna – sapendo che la nostra azienda li sostiene con prodotti e servizi eccellenti ed esclusivi. In una parola, offre loro la convenienza, ovvero una proposta che non si basa solo sul prezzo ma che è in grado di coniugare al meglio, con una serie di iniziative di alto livello, qualità, formazione, assistenza e anche risparmio".

CONTATTI: HESA SPA
Tel. +39 02 380361
www.hesa.com

Nasce il Laboratorio per la Sicurezza, luogo d'incontro virtuale per i security manager del retail

a cura della Redazione

Presentato a Security for Retail Forum 2016 da **Jerome Bertrume** (Guess), **Giuseppe Mastromattei** (H&M) e **Federico Saini** (Adidas), il progetto del **Laboratorio per la Sicurezza** è entrato nella fase operativa. Il gruppo dei promotori ha aperto un gruppo su Linkedin al quale possono aderire i security manager dei gruppi della distribuzione in attività interessati al progetto, per venire aggiornati sulle fasi del suo sviluppo.

E' previsto un primo incontro generale prima dell'estate 2016 per definire il regolamento e nominare il comitato etico-scientifico che indirizzerà le attività del Laboratorio, rivolte principalmente allo scambio delle conoscenze tra i security manager, alla formazione (mentoring) dei giovani che entrano nel settore, agli approfondimenti culturali sui temi di maggiore interesse di natura tecnica e giuridica e agli incontri con i fornitori di tecnologie e servizi specializzati.

"Noi security manager del retail avvertivamo da tempo l'esigenza di poterci conoscere, incontrare e scambiare informazioni in modo riservato – ha spiegato **Giuseppe Mastromattei** – *senza i vincoli dell'associazionismo tradizionale. La formazione continua di chi opera in questo settore è fondamentale, perché dobbiamo affrontare cambiamenti rapidissimi negli scenari socio-economici in cui operiamo, nelle strategie delle nostre aziende e, di conseguenza, nelle soluzioni da adottare per tutelare il patrimonio aziendale. Il Laboratorio sarà una struttura molto leggera, aperta a tutti i security manager in attività che desiderano ricevere e dare informazioni".*

"Ci siamo ispirati a un'iniziativa nata in Germania qualche anno fa, che raggruppa i responsabili della sicurezza dei maggiori retailer di ogni categoria merceologica. – sottolinea

Federico Saini – *Vengono organizzati due incontri all'anno presso le sedi a rotazione delle diverse aziende, per darci la possibilità di scambiare informazioni anche riservate. Per questo motivo, ogni partecipante ha sottoscritto un NDA (Not Disclosure Agreement – ndr) a tutela delle propria azienda. Questo gruppo favorisce anche l'incontro con gli stake-holders, per conoscere le reciproche posizioni e condividere le ricerca di soluzioni concrete".*

Precisa infine **Jerome Bertrume** *"Questa iniziativa può essere molto utile soprattutto per gli operatori internazionali che si affacciano al mercato italiano, che ha leggi e comportamenti diversi dagli altri paesi anche vicini in Europa. Poter chiedere indicazioni ai colleghi che operano già in Italia è molto importante, così come per i colleghi italiani è utile avere informazioni sugli altri paesi dove devono operare. Questo scambio dovrà avvenire soprattutto online, perché i nostri impegni in tanti paesi ci impediscono di avere incontri frequenti. Spero che questa iniziativa possa avere uno sviluppo anche fuori dall'Italia, sarebbe molto interessante avere anche un livello europeo".*

Per richiedere maggiori informazioni scrivere a: **eventi@securindex.com**

Grazie, sto solo guardando!

di Pietro Tonussi, Business Developer Manager Southern Europe at Axis Communications

Questa è la risposta che spesso il cliente dà al negoziante o al commesso che vuole occuparsi di lui. Di certo, ciò che "guarda" sempre sono le telecamere di videosorveglianza del negozio. Ci siamo abituati a considerare il sistema di videosorveglianza dei negozi come una loro parte intrinseca, allo stesso modo degli antifurti e degli altri dispositivi tipici per la sicurezza e la prevenzione delle perdite.

Vedere delle telecamere in un punto vendita non fa più nessun effetto, ormai fanno parte della nostra vita così come i cellulari, estensioni del nostro corpo da cui non possiamo più separarci. Quante volte ci è capitato di sentirci spersi senza il nostro smartphone, per poi accorgerci di averlo messo nelle solita tasca interna della giacca, con un gesto ormai automatico e per questo quasi scontato?

Quando pensiamo alle telecamere di un punto vendita dobbiamo però fare alcune riflessioni in più: quel sistema di videosorveglianza è davvero efficace per il controllo e la riduzione delle perdite? Tutti i sistemi hanno lo stesso effetto? Sono uguali per qualsiasi tipo di negozio? L'innovazione tecnologica comporta una differenza sostanziale dal sistema che un negozio sta utilizzando?

Queste e molte altre domande sono prese in considerazione e messe in discussione ogni giorno dai responsabili della sicurezza. Oggi, l'utilizzo di telecamere di videosorveglianza negli esercizi commerciali è una pratica abituale, accettata dai clienti anche in materia di Privacy, e il loro effetto dissuasorio sui possibili ladri conferma un buon ritorno degli investimenti. Nonostante ciò, anche in locali con telecamere di videosorveglianza continuano a essere commessi furti, frodi e altri atti criminosi. La sola dissuasione, quindi, non può essere sufficiente e l'uso proattivo del sistema video consente di fare un'analisi più dettagliata dell'investimento da realizzare.

In primo luogo, è importante stabilire se l'uso delle telecamere sarà puramente "forense" (analisi delle registrazioni in seguito all'evento), per la verifica di allarmi (tramite videosorveglianza remota), o in tempo reale (con l'intervento del centro di vigilanza o video controllo remoto) e/o integrato o connesso con altri sistemi (ad esempio barriere anti taccheggio e sistemi di anti intrusione). In funzione di questi usi, le telecamere, la loro tipologia, le caratteristiche del sistema di registrazione e visualizzazione devono assolutamente variare per essere adattate all'esercizio in cui verranno installate.

Considerando che, per avere un centro di controllo remoto in tempo reale, i costi sono sostenibili solo dalle grandi realtà come ipermercati e/o centri commerciali, la maggior dei punti vendita utilizza le telecamere come elemento di deterrenza e per registrare le immagini con cui poter comprovare incidenti in caso di necessità. Senza dubbio però, l'80% delle immagini che vengono consegnate alle forze dell'ordine per investigazioni è di scarsa qualità e non può essere utilizzato per lo scopo, specialmente per l'identificazione di persone sospette. (Fonte: Swedish Police Central Imaging Group White Paper on Image Usability).

Si aggiunga il fatto che l'attività marketing prevista nell'esercizio commerciale rende talvolta difficile la videosorveglianza, in quanto l'utilizzo di cartellonistica pubblicitaria e l'illuminazione artificiale possono ostruire la visione, e molto spesso la dislocazione degli espositori stessi per le promozioni in corso lascia alle telecamere una posizione inadeguata, causando un angolo di visione inefficiente o addirittura compromesso.

I contributi delle nuove tecnologie

Le nuove tecnologie video possono contribuire a minimizzare questi problemi: la possibilità di avere telecamere con risoluzione in HD garantisce, infatti, livelli di dettaglio sufficienti per identificare persone sospette e coprire angoli di visione maggiori. La matematica è semplice: basta dividere i pixel totali per i metri quadrati catturati dall'immagine. Di fatto, una buona pratica sarebbe quella di stabilire da subito quelle che sono le richieste di densità di pixel per metro. La maggior copertura (angolo di visione della telecamera) si riflette in un minor numero di telecamere e, quindi, nella riduzione dei costi di materiale, installazione e manutenzione. L'utilizzo di telecamere con visione panoramica o a 360° ha, inoltre, portato a un'evoluzione significativa, in quanto ha ridotto il numero di telecamere necessario per coprire aree di vendita di grande superficie.

Un esempio molto interessante delle nuove tecnologie è fornito dal cosiddetto **Axis Corridor Format**, che permette di ottenere dalla telecamera un flusso video con orientamento "verticale". Il video risulta adattato perfettamente all'area controllata, aumentando la qualità dell'immagine ed eliminando gli sprechi di larghezza di banda e spazio di archiviazione. Una funzionalità ancora più utile nelle telecamere di rete HDTV che producono immagini 16:9, poiché l'immagine risultante avrà un rapporto 9:16, il più adatto a rappresentare corridoi stretti, ingressi o passaggi. Questa opzione riduce drasticamente il numero di telecamere necessario e permette una copertura totale del corridoio stesso riducendo l'angolo cieco sotto la telecamera.

Quando le condizioni di luce non sono ottimali, una pratica abbastanza utilizzata è quella di installare telecamere con illuminatore IR (infrarosso). Lo scopo è quello di assicurare immagini buone anche nelle ore notturne con illuminazione scarsa o con luce molto bassa. Anche se il beneficio è evidente, ci sono senza dubbio alcuni aspetti tecnici da tenere in considerazione: molte di queste telecamere, specialmente quelle di bassa qualità, forniscono spesso colori alterati e immagini inutilizzabili. Anche durante la notte, queste

telecamere tendono ad abbagliarsi per effetto della propria luce riflessa dalle superfici chiare come, ad esempio, gli arredamenti dei negozi o le showcase di cristallo, restituendo anche in questo caso immagini inutilizzabili. L'alternativa a questi problemi è utilizzare telecamere con regolazione automatica dell'illuminazione infrarossa (che adattano la potenza della luce in funzione della distanza del soggetto) e filtro infrarosso rimovibile (funzione Day & Night meccanica) per un rendimento ottimale durante le ore diurne.

Come comportarsi, invece, con i "professionisti" del cappello con visiera? Chi entra in un negozio e vuole commettere un furto, spesso conosce dove sono state installate le telecamere e sa quali sono le aree scoperte. Il fatto che si tratti di sistemi utilizzati abitualmente, fa sì che i delinquenti siano consapevoli e conoscano bene i limiti di questi apparati e, di conseguenza, cerchino spazi senza copertura video sapendo che, ad una certa distanza, il loro volto non è riconoscibile, e utilizzino inoltre cappelli con visiera per complicare il riconoscimento.

Quando si installano le telecamere a soffitto, l'angolo di visione sarà ampio per evitare il problema della visiera. Se, però, pretendiamo che la telecamera catturi il volto a una distanza maggiore, dobbiamo ridurre l'angolo di visione verticale, la densità di pixel sarà molto minore e non si otterrà un'immagine con i dettagli necessari per il riconoscimento. La soluzione migliore in questi casi è collocare le telecamere in maniera tale che le immagini possano essere utilizzare a fini investigativi, posizionandole ad esempio vicino all'uscita del negozio ad altezza viso. Il problema con questo tipo di posizionamento è che devono necessariamente essere protette da possibili vandalismi e bisogna assicurarsi che il potenziale ladro, conoscendo la loro ubicazione, non faccia in modo di nascondere il suo volto. Per evitare tutto ciò, si utilizzano telecamere "discrete" tipo pin-hole che possono essere installate facilmente ma che nello stesso tempo garantiscono un'immagine del volto di qualità elevata e possibilmente in alta definizione, così da poterla utilizzare in caso si necessiti una identificazione.

Videosorveglianza per per la tutela del patrimonio aziendale

La nuova formulazione della norma sul controllo a distanza dei lavoratori del Jobs Act sta introducendo in questo senso delle novità significative, che dovrebbero consentire al datore di lavoro di utilizzare le telecamere anche per la tutela del patrimonio aziendale, ma non per controllare la qualità della prestazione e i ritmi di lavoro dei dipendenti. Occorrerà prestare molta attenzione non solo al fatto che si potranno installare queste telecamere, ma che tutto il processo decisionale di implementazione di un sistema di videosorveglianza si potrà realizzare in maniera più rapida purché il datore di lavoro informi i propri dipendenti di questa installazione, sulle modalità di utilizzo di tali strumenti e sui controlli che si riserva di effettuare, senza dover affrontare delle contrattazioni sindacali.

Lo proporrei con una formula più 'possibilista' e meno 'certa:

La nuova formulazione della norma sul controllo a distanza dei lavoratori del Jobs Act sta introducendo in questo senso delle novità significative, che dovrebbero consentire al datore di lavoro di utilizzare le telecamere anche per la tutela del patrimonio aziendale, ma non per controllare la qualità della prestazione e i ritmi di lavoro dei dipendenti. Occorrerà prestare molta attenzione non solo al fatto che si potranno installare queste telecamere, ma che tutto il processo decisionale di implementazione di un sistema di videosorveglianza si potrà realizzare in maniera più rapida purché il datore di lavoro informi i propri dipendenti di questa installazione, sulle modalità di utilizzo di tali strumenti e sui controlli che si riserva di effettuare, senza dover affrontare delle contrattazioni sindacali.

Integrazione Sicurezza e Marketing

Un altro aspetto di fondamentale importanza per far si che il sistema di videosorveglianza sia davvero utile è l'integrazione tra il Responsabile IT e lo Store Manager. È indubbio che il settore Retail si stia muovendo per unire la necessità di sicurezza e di loss prevention alle esigenze del Marketing. La telecamera di rete deve essere considerata come un sensore intelligente che può dare un aiuto molto importante per il negozio su strada nei confronti del suo concorrente più agguerrito: il negozio online. Quest'ultimo, infatti, ha un numero di informazioni nettamente superiore sui propri clienti. Nel negozio su strada, a guardare bene, ci sono due soggetti che "osservano" il cliente: i commessi/venditori e le telecamere. Ma solo queste ultime possono dare un grande contributo allo Store Manager: funzionalità come people counting, dwell time (tempo di permanenza di fronte a una certa zona), out of the stock on the shelf (mancanza del prodotto sull'espositore), queue control (controllo della coda alle casse) sono tutti elementi che possono aiutare il retailer nel soddisfare il cliente e migliorare il servizio complessivo. Le telecamere di rete, grazie all'intelligenza a bordo camera e ad applicazioni come heat mapping, tracking, people profiling (algoritmo molto più simile a quello dei negozi online quando un utente lascia volontariamente i suoi dati) consentono al punto vendita di profilare i clienti analizzando genere, età, ecc. conoscere chi entra in una certa fascia oraria, come e dove si muove all'interno dello store e quali sono le aree più "calde" per i prodotti più venduti. Informazioni che tutti i negozi online hanno, perché sono i clienti stessi a lasciargliele con le loro ricerche e i relativi acquisti.

In definitiva, la videosorveglianza degli esercizi commerciali è e sarà un sistema efficace per la prevenzione delle perdite, per le frodi, per la sicurezza del locale e per un aiuto alle operazioni di marketing. Senza dubbio, così come succede per altri tipi di tecnologia utilizzati, l'effetto dissuasorio della telecamera perderà la sua efficacia man mano che il delinquente conoscerà i limiti e i difetti del sistema di videosorveglianza. Le nuove tecnologie permettono di rimediare ad alcune di queste limitazioni, aumentando il livello di difficoltà per i delinquenti, elevando l'efficienza del sistema stesso e migliorando il ritorno degli investimenti. Le tendenze derivanti dall'uso di nuove tecnologie indicano l'impiego di un minor numero di elementi (minori costi di acquisto, installazione e manutenzione), il miglioramento della qualità di registrazione del video e un miglior adattamento estetico e funzionale delle telecamere, nonché una gestione più semplificata dell'intero sistema. Coperte tutte le necessità di prevenzione delle perdite e di sicurezza, i sistemi di videosorveglianza ora possono dare il loro contributo anche nella gestione aziendale, fornendo operazioni su dati di marketing e merchandising attraverso l'analisi del comportamento dei clienti. Questa è la nuova frontiera del video nello scenario della vendita al dettaglio in cui le telecamere, catturando i dati in modo sistematico, possano dire allo stesso modo del cliente con il commesso: " grazie, stiamo solo guardando!".

AXIS COMMUNICATIONS

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 0118198817
www.axis.com

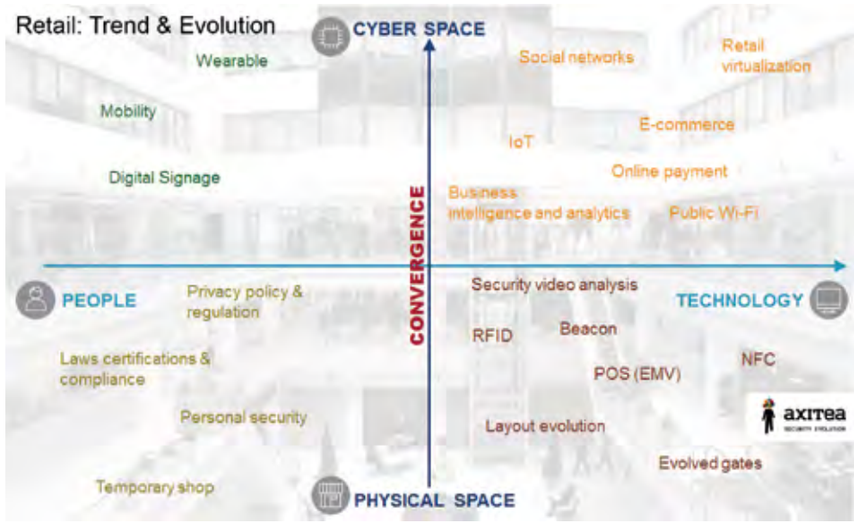
Attacchi combinati, la nuova minaccia per i retailer. Le soluzioni di un Global Security Provider

a colloquio con Maurizio Tondi, VP Strategy & Operations Axitea
a cura della Redazione

L'evoluzione del sistema distributivo al dettaglio sta determinando nuovi paradigmi per la sicurezza. Il tema dell'attacco combinato (IT + Phy) interessa i retailer tanto quanto la sottrazione di dati. Può farci un quadro della situazione a livello globale?

Da un lato il settore del Retail a livello globale è attraversato – per quanto riguarda la Sicurezza – da eventi e vulnerabilità assolutamente non dissimili da altri contesti industriali; ma dall'altro, proprio per alcune specificità operative, rappresenta un incrocio particolarmente previlegiato, una sorta di "melting pot" nella quale si fondono e risultato più evidenti gli effetti della convergenza tra fisico e cyber e tra uomo e tecnologia. Mi spiego meglio: da tempo parliamo di integrazione ma mai come ora e forse mai come nell'articolato sistema di distribuzione (dalla grande distribuzione organizzata, al dettaglio, ai punti vendita) minacce, attacchi, furti ed atti criminosi in genere stanno interessando tutto il "place", a tutti i livelli della filiera da un alto e tutti gli stakeholder dall'altro. Questo sostanzialmente perché il percorso di forte trasformazione del settore interessa aspetti giuridico-normativi, di compliance, di comportamento e di "awareness" e di attiguità tecnologica (IT, TLC, IoT, Mobility).

Il furto, la rapina, la sottrazione di merce e di denaro, la frode, l'atto predatorio e le differenze inventariali si intrecciano con sottrazione di dati sensibili, "data breaches", furti di identità, credenziali, carte di credito, database di clienti, profili di acquisto e proprietà intellettuali.. Non solo emergono, quindi, le evidenze più tipiche dell'attività predatoria tradizionale, ma quelle di attacchi e sottrazione di dati legati al cyber crime, basti ricordare i casi eclatanti di Target (70 milioni di clienti), Home Depot (56 milioni di carte di credito), Sally Beauty, etc. Ma la dimensione non conta. Il mix tra limitata informazione, consapevolezza e fragilità tecnologiche intrinseche o di configurazione, rende potenzialmente attaccabili e violabili aziende di ogni dimensione. Spesso le piccole, le meno protette, diventano il punto di vulnerabilità per attaccare poi le grandi organizzazioni. E spesso, sempre più, l'uomo è



l'elemento più debole di questa catena. In Italia, inoltre, la mancanza di obbligatorietà nel denunciare il furto informatico, falsa le dimensioni e la portata del fenomeno dal punto di vista della gestione del rischio e del danno. La superficie target degli attacchi Cyber è aumentata sensibilmente e ci sono infatti più utenti connessi, più dispositivi utilizzati e più dati digitali a disposizione. Se è vero che nel segmento del Retail ed in particolare nella gestione fisica del punto vendita, si sono ultimamente introdotti pattern di acquisto, propensioni e criteri tipici di market place ed e-commerce, è emersa anche pericolosamente una diversa postura di Sicurezza e di esposizione al rischio, tipica dell'interazione on line; è certamente evidente che vulnerabilità e debolezze legate alla posizione geografica ed all'architettura del punto vendita, al layout, alla disposizione dei varchi e degli accessi, agli impianti tecnologici, all'ergonomia dei punti di pagamento, ai magazzini e al comportamento dei dipendenti e dei fornitori, rappresentano oggi potenziali punti di attacco ai sistemi ed all'infrastruttura informatica e di comunicazione. Gli attacchi Informatici, inoltre, sono diventati sofisticati e di difficile rilevamento con i tradizionali sistemi di difesa, gli strumenti di attacco sono facilmente disponibili a poco prezzo e non richiedono particolari competenze.

Quali sono gli schemi difensivi per un retailer che da un cyber-attack può avere i maggiori danni per la sua reputazione?

Il primo livello di protezione è definitivamente la conoscenza e l'informazione. La consapevolezza del rischio, sia esso fisico o cyber, è certamente il principale elemento per costruire un adeguato sistema di difesa. La conoscenza di pratiche di successo – che si sono rivelate vincenti nel contrastare con efficacia la recrudescenza della minaccia – realizzata attraverso il confronto con operatori specializzati che abbiano nel proprio bagaglio professionale queste esperienze a livello nazionale ed internazionale, è sicuramente un asset da considerare come schema difensivo di massima. Attacchi come lo spear phishing, il watering hole ed attacchi di social engineering hanno tutti poi come obiettivo proprio le "persone". Ed i danni non solo materiali ma anche reputazionali e di immagine rappresentano un elemento di massima attenzione. La continuità operativa, ed a volte la sopravvivenza stessa di un'organizzazione, può essere messa fortemente a rischio. Immaginiamo nell'ambito fashion l'impatto della sottrazione dei nuovi modelli di una collezione, piuttosto che l'utilizzo abusivo di immagini o del brand da qualche parte nel mondo, su qualche sito web. Quindi il tema del comportamento e della cultura è centrale per proteggersi da furti e frodi ma anche dalla

sottrazione di dati molto sensibili. Poi certamente la tecnologia: è vero che tanti nuovi dispositivi non sono stati progettati per essere nativamente sicuri (dispositivi mobili, dispositivi specializzati e device IoT) e tanti di questi rappresentano proprio gli elementi di trasformazione ed innovazione applicata al Retail per amplificare la superficie di vendita, avvicinare sempre più i consumatori ed aumentare definitivamente le vendite, ma tecnologie innovative di intelligence e di prevenzione, l'ottimizzazione dei sistemi di protezione esistenti e di monitoraggio rappresentano strumenti e contromisure efficaci. Un'architettura integrata di servizi, procedure e strumenti che segua l'intero life cycle della sicurezza e che sia a disposizione dei Security Manager, rappresenta la barriera più rilevante anche alle trasformazioni morfologiche degli attacchi.

E' possibile individuare un modello di "sicurezza olistica" per un retailer, che coordini sotto un'unica regia le azioni per la difesa del patrimonio aziendale nei confronti delle diverse minacce a cui può essere esposto?

Un approccio di tipo olistico è definitivamente la risposta più attuale e più efficace alle mutate condizioni di attacco, di minaccia e di gestione integrata del rischio soprattutto nel settore del Retail in cui si radicalizza la convergenza tra fisico ed informatico ed in cui sono molteplici i potenziali punti di vulnerabilità: varchi, ingressi, accessi, mezzi di trasporto, parcheggi, personale, fornitori, partner, consulenti, sistemi informativi aziendali, sistemi tecnologici, dispositivi fissi e mobili. Ed in cui – come in altri settori – soprattutto nelle grandi organizzazioni emerge anche una debolezza strutturale anche in termini di Ownership. Spesso le Aziende sono per natura guidate dal Profit&Loss e da una predisposizione mentale nella gestione del rischio orientata pericolosamente all'accettazione della "forza maggiore" e della "conformità normativa" e di fatto meccanismi di protezione istantanea non sono applicati. Peraltro, tutti gli attacchi del passato conosciuti si sono dimostrati "trasversali" coinvolgendo elementi informatici, fisici, umani ed organizzativi ed evidenziando definitivamente la necessità di un approccio olistico ed integrato, per essere efficaci nella riduzione dei rischi. L'approccio a "silos" per la sicurezza fisica, informatica e per la protezione del capitale umano si è rivelato assolutamente insufficiente ed inadeguato.

Qual è la visione operativa di Axitea, che si propone come Global Security Provider focalizzato sul mercato verticale del Retail?

Axitea si inserisce in questo contesto ed opera attraverso differenti esperienze operative ed una singola, unificata ed integrata proposizione dedicata al presidio ed alla difesa dello spazio fisico-cyber del Cliente, indirizzando così il fabbisogno complessivo di sicurezza delle aziende impegnate oggi nella ricerca di livelli di protezione professionale e di elevata qualità.

Axitea valorizza da un lato l'esperienza, le specificità e le prerogative di un Istituto di Vigilanza che ha sempre operato nel settore del microbusiness e della protezione di negozi, esercizi commerciali, punti vendita e catene di distribuzione, perfezionando la formazione delle proprie Guardie Giurate, la disponibilità delle proprie Centrali Operative e la "cultura" della gestione degli allarmi e degli interventi. Di contro, attraverso centri di competenza – recentemente rinnovati in termini di tecnologie innovative e professionalità – per la realizzazione e gestione di soluzioni di video sorveglianza, video analisi, protezione perimetrale, monitoraggio e messa in sicurezza di punti sensibili dell'infrastruttura informatica del Cliente, con tecniche, metodologie e strumenti di intelligence, management e remediation. La system integration rappresenta per Axitea l'asset operativo più rilevante, nella realizzazione delle soluzioni innovative per il mercato Retail. Ad esempio l'utilizzo dell'infrastruttura di videosorveglianza anche per realizzare analisi video finalizzate al marketing analytics, coniuga le necessità di produttività di punti vendita, centri commerciali e supermercati con l'efficientemento e la riduzione dei costi, migliorando ingaggio, capture rate e valore delle vendite attraverso funzionalità di heat mapping, hot zone, visual merchandising, controllo della coda, controllo scaffali, controllo cestelli e carrelli, articoli abbandonati. Inoltre nell'integrazione della gestione del punto vendita, è centrale la proposizione di Axitea per la protezione personale dei dipendenti realizzata attraverso portable e wearable device dedicati all'anti-rapina e anti-aggressione. Le soluzioni satellitari sviluppate specificatamente per il retail, rappresentano il punto di incontro tra sicurezza e logistica per ridurre i rischi legati al furto del mezzo e della merce trasportata, fornire assistenza in caso di emergenza dalla Centrale Operativa, gestire la localizzazione, il posizionamento, i controlli gestionali sui consumi dell'intera flotta. Le applicazioni dedicate inoltre alla gestione della "catena del freddo" progettate da Axitea consentono di monitorare in tempo reale la temperatura negli appositi vani di carico, attraverso un controllo ed un supporto continuativo da remoto, oltre a fornire report analitici, report grafici, avvisi di superamento soglie e l'integrazione con sensori di IoT. Visione, scouting tecnologico, integrazione dei sistemi, conoscenza approfondita delle best practice di settore e servizi sono i contributi cruciali che Axitea mette a disposizione del mercato.

Axitea è la società leader in Italia nel settore della sicurezza, specializzata nello sviluppo di soluzioni integrate e personalizzate. Con oltre 1.500 dipendenti, Axitea offre servizi per la sicurezza di aziende, attività commerciali, istituzioni, residenze private, mezzi e beni mobili. L'offerta prevede l'integrazione di tecnologie innovative personalizzabili, la capacità di progettazione, di gestione delle infrastrutture e sistemi e un portfolio completo di servizi di sicurezza e di vigilanza. L'azienda è presente su tutto il territorio nazionale, grazie alle proprie filiali, alle Centrali Operative e alla rete degli Axitea Partner, società affidabili, accuratamente selezionate e certificate. Circa 32.000 clienti in tutta Italia hanno già scelto Axitea per la loro sicurezza.

CONTATTI - AXITEA SPA
marketing@axitea.it
www.axitea.it

Conforti, l'importanza di un progetto di sicurezza

di Luigi Rubinelli, CEO di Conforti spa

La Conforti spa, negli oltre 100 anni di attività, ha progettato decine di migliaia di sistemi di sicurezza, cavalcando l'evoluzione tecnologica dei materiali, dell'elettronica e dell'informatica. Negli archivi tecnici e nella professionalità degli addetti si ritrovano le esperienze risolutive di tante situazioni, ambienti e attività differenti che, nel tempo, hanno modificato le proprie necessità di salvaguardia come istituti di credito e di vigilanza, siti militari e industriali, autostrade, ministeri e ambasciate, supermercati, magazzini, negozi, gioiellerie, abitazioni private, chiese, ecc. Vogliamo condividere con i lettori di **essecome** la nostra filosofia nell' approccio alla progettazione e alla realizzazione di un sistema di sicurezza.

Nel tempo cambiano le distribuzioni dei valori, le tipologie di attacco, le attenzioni della malavita e, in oltre un secolo di esperienze, osserviamo che considerare le memorie dei fatti accaduti è di fondamentale importanza per sviluppare nuovi progetti. Per la Conforti, anche la richiesta di una "semplice" cassaforte diventa la richiesta di un sistema di sicurezza, in quanto necessita di un'analisi del rischio per poterne definire il grado di resistenza, il tipo di serrature, la sua allocazione, il tipo di ancoraggio, se è o meno protetta da un sistema di allarme, ecc.

Affrontiamo il progetto in modo sistematico, interagendo con il cliente, mettendo sul tavolo le sue necessità presupposte e quelle che derivano dalla nostra esperienza, i valori in gioco, i limiti tecnici e ambientali, le capacità procedurali e, certamente, anche il budget disponibile. Nelle varie iterazioni che si susseguono nell'affinamento del progetto, normalmente, emergono considerazioni che inducono al ridimensionamento di alcuni aspetti piuttosto che altri, fino ad arrivare ad un compromesso plausibile per il rischio che il cliente, a questo punto, intende coscientemente assumersi.

Lo potrà fare perché avrà avuto modo di considerare le necessità, le abitudini, i modi di operare e perché potrà confrontare le diverse soluzioni prospettate di protezione fisica, elettronica, organizzativa con i diversi livelli di sinergia e integrazione. Il cliente è accompagnato nella valutazione di uno o più scenari determinabili attraverso l'analisi del rischio, presupposto che varia in funzione delle condizioni di progetto e delle soluzioni che si assumono.

Tutto questo altro non è che il flusso logico nella strutturazione di un qualsiasi Progetto che va elaborato in successive revisioni fino al punto di convergenza ritenuto congruente con le ipotesi di partenza e i limiti di contorno.

Se pensiamo che la sicurezza di un ambiente non possa essere improvvisata ma debba essere progettata, semplice o complessa che sia, l'approccio e il modo di affrontare il progetto è sempre lo stesso, metodico con la visione più completa possibile degli scenari che si possono realizzare o che si vuole si realizzino. E in questo, l'esperienza diffusa in molti settori applicativi contribuisce enormemente nel dimensionamento corretto del progetto.

Sembrano discorsi scontati, ma quello che vediamo in giro ci dimostra il contrario.

Insistiamo su questo, perché un Progetto di sicurezza non può prescindere dalla sinergia (influenza reciproca) dei tre aspetti fondamentali e imprescindibili, ma spesso lasciati slegati nell'applicazione: le protezioni strutturali; i controlli elettronici; l'utilizzo, le procedure e i modi di gestire la sicurezza (inclusa la manutenzione e le prove periodiche di affidabilità).

La protezione dei valori deve avere una struttura che li contenga che dovrà resistere per un tempo sufficiente finché, in caso di tentativo di sottrazione, qualcuno possa intervenire. Già in queste poche parole, abbiamo messo in gioco l'affidabilità di un contenitore (es. cassaforte) che dovrà avere una resistenza in funzione del tempo nel quale qualcuno dovrà intervenire, se e quando avvertito da un sistema che dovrà, a sua volta, essere affidabile e adeguato all'insieme ambiente-percorsi-utilizzo. La scelta delle soluzioni tecniche non può prescindere dall'analisi del contesto particolare.

• Una cassaforte deve essere affidabile, come le persone che la usano e che la mantengono in efficienza: per questo serve un sistema che ne controlli gli accessi

e gli stati funzionali, li verifichi e comunichi le anomalie procedurali e/o tecniche in modo da informare chi le provoca o intervenire con manutenzioni preventive. E' chiaro che, per una cassaforte ad uso di un singolo utente, le cose si semplificano, ma dove ci sono più utenti che operano, o addirittura terze parti, si rende indispensabile definire puntualmente "chi-fa-cosa-quando e come". Il controllo va fatto in tempo reale, la risposta anche. Oggi la cassaforte non è più un oggetto passivo: è "intelligente", "ascolta", "pensa" e "parla". La sua manutenzione è affidata ad un servizio di tecnici professionisti. Il luogo di posizionamento della cassaforte è un altro aspetto molto importante che va progettato in funzione dell'ambiente e dei flussi operativi. Cambia radicalmente l'approccio progettuale se la cassaforte viene posizionata in ambiente chiuso dedicato, piuttosto che in spazio aperto. La predisposizione per un ancoraggio adeguato va progettata, non può essere in un posto qualunque, su una pavimentazione eseguita per uso civile. La norma En1143-1 prescrive che, ai fini assicurativi, le casseforti di peso inferiore ai 1.000 Kg debbano essere ancorate, ma prescrive solo la resistenza alla trazione alla quale deve resistere l'ancoraggio dal lato cassaforte. E' implicito che il pavimento dovrà offrire una resistenza maggiore o uguale a questo valore ed è un argomento da non sottovalutare.

• Un impianto di allarme (e TVCC) ricalca gli stessi concetti, deve essere affidabile per gli obiettivi per cui è stato pensato. Deve essere fruibile, ovvero facilmente utilizzabile, essenziale per lo scopo (meno sensori = meno guasti o falsi allarmi), possibilmente deve dialogare con la cassaforte perché i due sistemi si possano controllare a vicenda. In certi situazioni, si sceglie di mettere la centrale di allarme all'interno della cassaforte stessa, una soluzione ottimale per evitare i danni agli apparecchi in caso di intrusione e le manomissioni. Deve essere controllabile da remoto per verificarne l'efficienza e deve avere i canali di allarme ridondanti e reciprocamente controllati. Non è difficile, con la tecnologia oggi disponibile.

• Le procedure, ovvero l'organizzazione delle prassi, sono parte integrante del progetto e anch'esse devono essere affidabili. Perché le procedure siano affidabili è necessario siano praticabili e verificabili. In funzione di esse, il progetto può assumere aspetti molto differenti. Inutile pensare ad un sistema sofisticato, se poi risulta complesso da utilizzare e si devono inserire delle deroghe: sono la morte della sicurezza! Certamente il fattore umano gioca un ruolo centrale nel progetto sicurezza: questo elemento rimane il più spinoso da considerare. Lo si deve valutare da entrambe le parti, quella dei "buoni" e quella dei "cattivi" e dalla parte dei "buoni" non dobbiamo trascurare la possibilità di avere maldestri, superficiali e "furbetti". A tal fine, i sistemi andrebbero pensati, in funzione della loro complessità, con la capacità di rilevare e segnalare le anomalie nelle prassi e di segnalarle evidenziandole, così da correggere gli operatori e avvertirli che il sistema è vigile. Lo stesso per le condizioni funzionali dei componenti del sistema. Il centro tecnologico Conforti di monitoraggio riceve quotidianamente, dai sistemi connessi in rete, centinaia di segnalazioni di anomalie, che vengono rigirate automaticamente ai clienti che utilizzano il servizio. Se di fronte ad un'anomalia, nata per difficoltà dell'operatore, piuttosto che per problemi tecnici o per "prove di infedeltà", esiste l'opportunità di esserne informati e di chiedere agli interessati il perché di tali anomalie, è un'impagabile attività preventiva che produce dissuasione. L'operatore può essere corretto se maldestro, avvertito se malpensante. Se l'anomalia nasce da fattori tecnici, la si può correggere prima che si abbiano fermi del sistema. Infine il progetto di sicurezza, che contempla l'organizzazione delle prassi, include anche la manutenzione tecnica qualificata e le verifiche funzionali e operative, argomenti di importanza tutt'altro che trascurabile.

White Paper: PSIM, i criteri per la progettazione del sistema informatico dipartimentale

a cura di Nils Fredrik Fazzini, General Manager di Citel spa

1 - IL PSIM COME PROGETTO PERMANENTE

Tutti i sistemi informatici, corporate o dipartimentali (come in questo caso) tendono ad essere progetti permanenti con una vita attesa indefinita, senza limiti o scadenze ma alimentati da un adeguamento evolutivo continuo. Il processo di scelta del fornitore per ottenere un simile obbiettivo richiede valutazioni complessive che pesano aspetti diversi, anche antitetici, alla ricerca del punto di equilibrio tra specializzazione e dimensioni, tra longevità e spinta innovativa, tra dimensioni e flessibilità.

Questo White Paper non pretende di essere una guida alle valutazioni di un PSIM, essendo Citel parte interessata, ma può essere utile per ricordare quali sono i valori oggettivi e mettere in rilievo le criticità potenziali. Con lo scopo di contribuire alla professionalizzazione dei processi di valutazione facendoli emergere da una storia di settore dove il PSIM è stato concepito in anticipo sui mercati internazionali – soprattutto con una qualità unica: quella dell'architettura aperta multifornitore e multifunzionale.

L'abbinamento dell'architettura aperta con il concetto di progetto permanente in chiave evolutiva ha dato luogo a una sorta di *killer application* nel settore della sicurezza fisica informatizzata, a partire dal settore bancario (a cui si devono quasi tutti gli input progettuali per i grandi sistemi centralizzati) e postale per poi passare all'Oil&Gas e infine scendere verso fasce di mercato dove le dimensioni e i budget sono più contenuti, fino ad essere disponibile as a service da parte delle società di security più innovative. Si tratta del **Centrax-PSIM** di **Citel**, la società che si è trovata a raggiungere una parte maggioritaria dell'utenza PSIM in Italia apportando esperienze informatiche di telegestione e controllo di processo nel settore bancario proprio nel momento del cambio di passo tra la sistemistica chiusa del passato e l'apertura postulata dalla diffusione delle reti dati condivise.

2 - IL PSIM COME PROGETTO DI UN SISTEMA INFORMATICO DIPARTIMENTALE

In un ambito immateriale come quello della sicurezza, le esperienze di successo con utenti innovativi sono fondamentali per sistematizzare la materia in forma di utili principi e requisiti specifici. **La sistematizzazione è lo scopo di questo documento**, basato su un percorso positivo che ha portato nel tempo a maturare e consolidare in seno all'Ecosistema di Citel l'idea che la sicurezza fisica richiedesse un sistema informatico dipartimentale (il **PSIM – Physical Security In-formation Management**). Un Ecosistema, lo ricordiamo, che comprende buona parte del sistema bancario italiano, le grandi compagnie dell'Oil & Gas e un numero crescente di utenti di medie dimensioni nel manifatturiero, nel retail, e tra le società di security più innovative.

A rafforzare l'esigenza di un sistema informatico dipartimentale sono intervenuti gli adempimenti per la **compliance alle norme sulla business continuity**, sulla safety dei lavoratori, sul contenimento dei consumi; applicazioni in cui la gestione con un sistema informatico in tempo reale aiuta nel generare vincoli, rilevare eventi specifici, attivare interventi tempestivi, tracciare situazioni e adempimenti.

Peraltro, il concetto di *sistema informatico* è così ampio e generico che può essere attribuito sia a una semplice appli-cazione software che ad un ERP per la gestione di una multinazionale. **Se poi si tratta di sicurezza, dove sono immateriali sia l'esigenza che il prodotto finale, il rischio di confusione è particolarmente alto** ed è quindi indispensabile adottare un procedimento professionale che è peraltro raccomandabile in ogni settore applicativo.

Oltretutto, nel campo dei **sistemi** (da contrapporre ai semplici **prodotti**), l'utente non può pensare di poter rimediare a una scelta iniziale inadeguata, se non sbagliata, smontando quanto installato una volta ammesso l'errore di valutazione (come avviene nel caso di un semplice prodotto): quasi sempre in questi casi **l'utente non potrà fare altro che rassegnarsi a un ridimensionamento dei propri obiettivi**, visto che l'errore di valutazione emergerà in molti casi solo quando sarà troppo tardi per smantellare il progetto.

3 - I VALORI, I REQUISITI E I VINCOLI PER UN PROGETTO PROFESSIONALE DEL PSIM

É evidente, in base alle considerazioni appena fatte, che occorre procedere secondo criteri collaudati per la sistemistica informatizzata con i seguenti passaggi:
- individuare a priori i **"valori generali"** che si vogliono perseguire con il sistema di gestione della sicurezza fisica, associandovi i **processi** pertinenti agli obiettivi voluti, considerando anche le peculiarità del contesto aziendale;
- determinare i **requisiti generali e specifici per il buon fine** del progetto con processi efficienti in tempi prevedibili;
- individuare i **vincoli** che è consigliabile imporre al fornitore per il rispetto dei requisiti generali e specifici prefissati.

Le esperienze di Citel e il titolo per trattare in generale su questi argomenti nascono dal progetto Centrax, che ha avuto l'opportunità unica di nascere ed evolvere in contesti bancari informatizzati dove la tecnologia era padroneggiata, i valori generali ben presenti, così come i requisiti. Da quei progetti di successo è nato il paradigma PSIM, seguito negli anni dal perfezionamento progressivo dei requisiti e infine l'individuazione di vincoli oggettivi rilevanti per il buon fine del progetto.

Con la necessità di alcune precisazioni ai fini dell'impostazione corretta e prudente delle specifiche di progetto e delle scelte iniziali:
- il PSIM è in sostanza un **progetto permanente** come accade per tutti sistemi informatici;
- un progetto PSIM deve poter **tendere verso la multifunzionalità**, perché la storia dimostra che è quasi sempre opportuno (se non ovvio) sfruttare sinergicamente i processi di telecontrollo e telegestione della sicurezza fisica, anche al servizio dell'asset management, della compliance alla normativa sui consumi energetici, sull'inquinamento e sulla salute dei lavoratori, generando pertanto economie di scopo e interoperabilità a valore aggiunto;
- il PSIM coinvolge anche fornitori di servizi di integrazione, di installazione e manutenzione e quindi deve prevedere facilità di implementazione e supporto formativo e informativo mirato alle terze parti, oltre alla possibilità di terziarizzare alcuni.

Il procedimento logico preliminare alle valutazioni per l'adozione di un PSIM si basa su una sequenza del tutto ovvia che prevede di definire in successione:
A. *i* ***valori generali*** *irrinunciabili e i processi coinvolti, che coinvolgono anche*
B. *il* ***profilo del costruttore***
C. *i* ***requisiti di progetto*** *imposti dai valori e dai processi*
D. *i* ***vincoli*** *necessari per imporre il rispetto dei requisiti a chi progetta il sistema ed a chi lo realizza*

A - I VALORI GENERALI

I valori generali che qualificano obbiettivi, soluzioni e processi della Security aziendale, si traducono in pratica nell'allineamento della gestione della sicurezza fisica alle buone pratiche di una qualsiasi funzione dipartimentale dell'azienda: basata quindi su un insieme di processi informatizzati ai fini di una gestione operativa pertinente, efficiente, tracciata, auditabile. Ma anche **predisposti e supportati per una lunga vita utile del sistema**, accompagnata negli anni da un contesto di fornitori complementari e di utenza propositiva, anche ai fini della compliance alla normativa direttamente o indirettamente coinvolta.

D'altra parte, come tutti i sistemi informatici, un vero PSIM è un **progetto permanente** supportato da una società spe-cializzata e dedicata che opera in un Ecosistema costituito da tutti gli stakeholders attivi: gli utenti, innanzitutto, con le loro istanze evolutive, i produttori complementari integrati, le terze parti di servizio all'utente.

Se si punta consapevolmente alla sicurezza fisica gestita da un sistema informatizzato professionale, occorre preoccuparsi al momento della scelta del rispetto dei criteri professionali di valutazione e selezione che riguardano anche la parte visibile ma – nella fattispecie della sicurezza – soprattutto **la parte meno visibile e peculiare, quella funzionale e quella strutturale**.

Le peculiarità della gestione della sicurezza fisica richiedono **un sistema informatico, che combina funzioni particolari sia *gestionali* che di *controllo di processo***; pertanto il sistema non può che essere progettato da una struttura specializzata per affrontare non solo gli sviluppi di informatica gestionale ma anche quelli della telegestione combinata con processi in campo. Utilizzando oltretutto modalità realizzative e di supporto tali da assicurarne dinamicamente l'adeguatezza negli anni secondo requisiti fondamentali e buone pratiche così riassumibili:
1. in quanto **PSIM** (Physical Security Information Management) in architettura modulare e multifornitore, la conformità ai 7 requisiti di IMS/IHS, argomentati più avanti; mantenendo a **livelli professionali** le qualità sistemistiche, i processi gestionali, il reporting;
2. un'affidabilità particolare, considerate le potenziali conseguenze dirette e i riflessi indiretti sulla compliance alla business continuity e alla safety; con una esigenza specifica di **resilienza dell'infrastruttura** che deve assicurare l'interazione dei vari moduli del PSIM: dal sistema di governo fino all'ultimo componente in campo lungo la filiera, perché ogni misura resterebbe sterile o sarebbe dannosa in una catena di interazione interrotta;
3. in quanto calato nell'ambito dell'informatica moderna e al suo dinamismo, l'associazione ad una **politica di inte-grazione continua e spontanea, dei nuovi processi funzionali, delle tecnologie e dei prodotti** nell'ambito dello specifico ecosistema
4. la garanzia del fornitore, in caso di necessità particolari e non necessariamente generalizzabili, della **disponibilità di un servizio strutturato per sviluppi di processi particolari** su richiesta del committente.

B - DAI VALORI GENERALI DEL PSIM AL PROFILO COERENTE DEL COSTRUTTORE

Le peculiarità tecniche e di servizio elencate sono riscontrabili solo presso un produttore che disponga di una struttura interna da ***software farm*** a tutti gli effetti, con la capacità di intercettare e sviluppare in anticipo con proprie risorse le innovazioni di piattaforma e di processo, dalla compliance alla normativa sulla continuità operativa, all'informatica in-dossabile nel filone IOT fino a quelle nel campo del *big data* e dell'operatività su basi predittive.

Ma non basta; occorre che sia una *software farm* innestata in una struttura da ***System House***, perché un PSIM ha un cuore software ma richiede spesso una infrastruttura di sistema non meno articolata di un sistema informatico gestionale, che passa da reti di vario tipo, che interagisce con un campo eterogeneo, ma anche con altri sistemi informatizzati, non solo nella categoria dei tecnologici ma anche degli ERP. E non è affatto detto che una software farm capace di sviluppare programmi applicativi abbia la capacità di gestire la progettazione, la gestione e il problem solving di infrastrutture di sistema qualsiasi.

Il profilo di un costruttore PSIM dovrebbe in definitiva essere quello di una struttura con una forte specializzazione, attrezzata per coprire tutto il ciclo che va dal concepimento della soluzione, in chiave di sistema e prodotto informatico, al suo sviluppo, all'implementazione in campo, alla personalizzazione, alla manutenzione evolutiva, al problem solving H24. E uno specifico e dimostrabile orientamento verso la gestione del ciclo di vita *life-cycle* del sistema presso l'utente.

Tutto questo in pratica si traduce in un'impresa con una esperienza consolidata sul campo nella specifica specializzazione e risorse interne maturate nel contesto. Per un utente, la certezza di un successo progettuale e di un decorso fisiologico del ciclo di vita del PSIM è senza possibilità di smentita dal coinvolgimento di un fornitore caratterizzato come segue:

1. un **laboratorio interno** per sviluppi di sistema e di piattaforma strutturato per affrontare nuovi progetti per coprire l'architettura di sistema dalla base al vertice, con un assortimento di professionalità che devono necessariamente andare dai sistemi operativi alle applicazioni, dalle comunicazioni su ogni tipo di vettore all'hardware informatico, alla microelettronica hardware e firmware

2. risorse specializzate per ogni tipo di **integrazione con prodotti di terze parti**, in mancanza delle quali l'apertura architetturale di sistema è passiva o di pura facciata

3. una struttura di **assistenza H24** basato su tecnici specializzati e non limitato a operatori privi di capacità risolutive;

4. una **politica di evoluzione interna della sistemistica**, delle funzionalità e delle integrazioni per un adeguamento della tecnologia e dei processi aziendali, anticipando i tempi del mercato.

In definitiva dal rispetto dei *valori generali* deriva un profilo da **System House** *sui generis*, decisamente specializzata nella **tecnologia informatica di tipo dipartimentale** basata sulla condivisione della rete aziendale, funzionale all'interazione verso ambiti da monitorare e/o proteggere, dove gli eventi (e non solo semplici segnali) sono generati da dispositivi connessi e possibilmente correlati da un'intelligenza locale. Una struttura che deve essere necessariamente flessibile, espandibile, predisposta per la crescita applicativa e con prestazioni tecniche al passo con i tempi per un ciclo di vita indefinito.

Un **PSIM** deve infatti poter essere un **progetto permanente** e allo stesso tempo un **progetto sostenibile** in quanto basato su un catalogo noto del costruttore, senza personalizzazioni e sviluppi ad-hoc a spese dell'utente, salvo casi particolari; con la capacità di redistribuire i costi di nuovi sviluppi all'interno di una numerosa comunità di utenti ottenendo economie di scala e di scopo.

C - dai VALORI GENERALI ai REQUISITI INDISPENSABILI:

Se si condividono i valori generali applicabili ai sistemi professionali in categoria PSIM, il passaggio successivo, è la de-finizione di **requisiti** di dettaglio coerenti con quelli di una soluzione professionale indirizzata alla realizzazione di un sistema informatico dipartimentale per la gestione della sicurezza fisica, che vada al di là della semplicistica adesione ai requisiti del PSIM espressi in forma sintetica nella pubblicistica di settore.

I requisiti PSIM di IMS Research e le estensioni basate sui progetti professionali

Per arrivare a un indirizzo neutro alla scelta appropriata di un sistema informatizzato della sicurezza fisica sono stati decisivi i requisiti rilevati nel mercato da parte di IMS Research (ora IHS), prontamente adottati dalla comunità internazionale.

Sul piano del metodo, il contributo del tutto asettico che Citel può fornire è riportato nel prospetto più sotto, con i **requisiti PSIM e con la loro estensione a vincoli e precisazioni**, aggiunta da Citel per superare la schematicità di un paradigma che è stato condiviso prontamente dalla comunità internazionale ma codificato ad un livello di sintesi tale da prestarsi facilmente a interpretazioni strumentali.
Nel ruolo di fornitore della maggior parte dell'utenza italiana di PSIM, Citel ha pertanto aggiunto al prospetto dei requisiti la colonna ***"vincoli e buone pratiche per il buon fine del progetto PSIM"***. Si tratta di contenuti oggettivi perché **generati e condivisi dalla comunità dell'utenza PSIM nazionale in numerosi progetti di successo**, particolarmente quelli che hanno portato alla migrazione dalle architetture chiuse monofornitore a quelle aperte multifornitore.

Va evidenziato che il PSIM in architettura aperta è un valore aggiunto del mercato italiano, quello che per primo ha enunciato il concetto PSIM ma anche l'unico ad avere un protocollo pubblico – il CEI 79/5-6-11 di comunicazione e in-terazione per PSIM multifornitore. Un valore aggiunto che non consiste soltanto nel fatto che l'utente si rappropria della libertà di scelta nel corso della vita utile del sistema rispetto al fornitore e al suo sistema di interessi, ma anche nella **possibilità di adottare le buone pratiche innescate, favorite e diffuse da un ecosistema di utenti evoluti e di partner indipendenti, enunciate di seguito**:

a) i requisiti per la valutazione di un PSIM, non possono limitarsi all'enunciazione sintetica ma vanno **completati con requisiti complementari per il buon fine del progetto** PSIM scaturiti dalle esperienze esemplari di successo o fallimento negli anni recenti nel mercato italiano; pertanto non ci si può limitare a utilizzare il concetto sintetico del requisito, ma occorre che ad esso vengano abbinati **specifiche e vincoli ben precisi**, per capitolati professionali e valutazioni rigorose e a priori;
b) l'applicazione rigorosa del paradigma della **telegestione non proprietaria ad elevata resilienza** è vincolante nella gestione centralizzata di un edificio, di un comprensorio, di una pluralità di siti remoti diversificati per esigenze e dimensioni;
c) la **referenziazione di progetti a buon fine è fondamentale** ai fini della prova che le valenze tecniche dichiarate sono verificate e accompagnate da capacità realizzative e di project management del produttore del PSIM; mentre la sua stabilità nel lungo periodo e la continuità della spinta innovativa vanno pesate in funzione dell'estensione della comunità degli utenti del PSIM e delle spinte sinergiche verso l'innovazione di processo e non solo tecnologica.

I SETTE REQUISITI DEL PSIM E I VINCOLI PER IL BUON FINE DEL PROGETTO

n	**REQUISITI** *per la conformità concettuale al paradigma PSIM*	***VINCOLI e buone pratiche*** *per il buon fine del progetto PSIM in base all'esperienza in campo*
1	**Connettività e integrazione:** ricezione di dati da un numero qualsiasi di apparati o sistemi di sicurezza; capacità di integrazione sia nell'ambito della sicurezza fisica che rispetto ad altri sistemi di gestione dell'azienda, sia nei siti periferici che nell'interazione tra essi e il sistema centrale *(il requisito 1 e 2 vengono abbinati ai fini dell'associazione a requisiti e vincoli della colonna a lato in quanto condividono molti degli aspetti realizzativi)*	Nessuna limitazione a priori degli apparati gestibili nel sistema, che equivale a dire scalabilità, modularità, multi-funzionalità senza limitazioni tecniche. Ai fini della capacità di integrazione di altri sistemi non è sufficiente che il produttore sia *disponibile* a integrare: deve anche essere *in grado di realizzare direttamente interfacce hardware e software con apparati, sottosistemi e sistemi diversi per tecnologie, funzionalità, tipologie di connessione, costruttore.* In altri termini deve essere in grado di gestire in proprio tempi, costi, qualità e affidabilità dei processi di comuni-cazione, di gestione e di interoperabilità. La coerenza con i due requisiti comporta che il protocollo di trasmissione centro – periferia sia pubblico, bidirezionale, in grado di garantire la protezione dei dati a livello professionale, eseguire il monitoraggio continuo del fun-zionamento degli apparati periferici, della connessione in rete; e in grado di gestire la commutazione automatica della connessione su un vettore alternativo in caso di in-terruzione della connessione primaria.
2	**Gestione Real Time e configurazione con-trollata:** possibilità di configurare e modificare da centro procedure e parametri a bordo dei vari sistemi e dispositivi in ogni livello dell'infrastruttura (antintrusione, controllo accessi, videosorveglianza, ecc.)	
3	**Correlazioni e Verifiche:** connessione auto-matica centro-periferia e correlazioni multiple tra diversi apparati per la sicurezza; verifiche real-time e gestione flessibile delle interazioni correlate.	Funzioni configurabili di correlazione in grado: - di trattare segnali elementari provenienti indifferentemente da sensori, apparati, sistemi informatici, sia nel campo d'azione locale che di provenienza remota; - di generare eventi qualificandone l'attendibilità (allarmi certi, inattendibili, falsi positivi, ecc.) corredati dalla precisa descrizione e localizzazione: - per rendere immediata per un operatore qualsiasi la consapevolezza di ciò che ha generato l'evento (event awareness) - per tenere aggiornato in tempo reale l'operatore sull'evoluzione della situazione (situation management) - per supportare l'escalation del trattamento dell'evento in relazione alla dinamica della situazione. Con la possibilità di generare correlazioni sia a bordo di un dispositivo/ nodo locale presso il sistema centrale e anche presso il software centrale di supervisione
4	**Visualizzazione:** in caso di evento il PSIM deve essere in grado di visualizzare grafica-mente informazioni sulla situazione in modo da dare a chi deve gestire l'evento un'idea anche complessiva della natura dell'evento, del contesto locale e dell'ampiezza della mi-naccia.	Cruscotti per operatori unificati rispetto agli apparati che originano gli eventi. Suite di cruscotti per la libertà di scegliere tra diversi tipi di gestione operatore: con la grafica animata, con la video-ispezione correlata, con la video-sorveglianza interattiva e multimediale
5	**Processi di gestione eventi basati su proce-dure guidate:** avvio immediato dell'operatore su un percorso guidato passo-passo, basato su procedure mirate al contenimento o al contrasto della minaccia, monitorizzando progressivamente l'esito delle attività svolte sul posto	Funzioni da cruscotto operatore per la gestione per fasi proceduralizzate lungo un percorso guidato e obbligato, con la presentazione contestualizzata delle informazioni necessarie all'accertamento degli eventi, alla gestione degli interventi e all'acquisizione dei feed-back
6	**Affidabilità e Resilienza:** caratteristiche di robustezza e ripristino della piattaforma di sistema per ogni modulo ed a tutti i livelli, per assicurare la continuità del servizio e il ritorno alla normalità della gestione sia in caso di guasto parziale che di disastro totale.	Struttura di sistema e componentistica progettati e con-figurati per ottenere il requisito prioritario di una continuità di servizio superiore al 99,5%. Pertanto: - processi distribuiti ai vari livelli della sistemistica, - moduli di riserva in stand-by e servizio di teleassistenza specializzata H24 del fornitore per ripristini guidati - possibilità di configurare ridondanze remotizzate e solu-zioni di disaster recovery center
7	**Reportistica e Riesame post-evento:** tracciabilità e verbalizzazione do-cumentata della gestione dell'evento anche ai fini della ricostruzione criminologica dell'accaduto e della sua gestione	Tracciamento di ogni singola attività operativa. Funzioni di generazione guidata e facilitata di report nel corso della gestione dell'evento, con possibilità di allegare al report snap-shot, video-clip e book-mark. Riesame di video pertinenti a partire dallo storico eventi e non dall'archivio video.

Da Mirasys prodotti e servizi di qualità per un VMS sulla misura dell'utilizzatore

a colloquio con Elio Argenti, General Manager Mirasys Italia
a cura della Redazione

Il mercato della videosorveglianza è entrato in una fase di grandi cambiamenti, con una forte crescita di attenzione per i software gestionali e di analisi. Quali sono le proposte di Mirasys?

Mirasys sta intensificando la propria produzione di funzionalità base, in modo da rispondere sempre più alle esigenze del mercato VMS. Contemporaneamente, sta potenziando le proprie offerte per i mercati verticali, con una particolare attenzione alla gestione del traffico, alle integrazioni con applicazioni di marketing, Business Intelligence, controllo accessi, sistemi di allarme, e soluzioni di analisi video fornite da produttori esterni.
L'attenzione alle soluzioni ed alle integrazioni è diventato il motivo principale di sviluppo. Ci si rivolge sempre più al mercato di System Integrator a valore aggiunto, in modo da poter soddisfare e rispondere alla domanda di soluzioni che vengono richieste dal mercato.
Il tutto in funzione dell'uscita della nuova release 8.0, che verrà presentata nei primi mesi del prossimo anno che aggiungerà ulteriori possibilità di interfacciamento con sistemi esterni e di gestione completa del VMS e delle eventuali integrazioni tramite la GUI Mirasys.
L'attuale versione del software è stata implementata ponendo attenzione soprattutto all'usabilità della GUI, in modo da rendere l'attività del personale di sorveglianza e controllo più facile e pratica, con maggiori possibilità di prendere in carico tempestivamente gli allarmi. Ad esempio, nella GUI le mappe grafiche possono reagire agli allarmi cambiando automaticamente la mappa visualizzata; oppure le griglie dove disporre le telecamere possono essere dimensionate a piacere, consentendo la disposizione di telecamere di qualsiasi formato. Le stesse griglie personalizzate possono ora contenere anche moduli di plug-in, come il web browser, le mappe, il modulo di lettura targhe, i moduli custom di integrazione, eccetera, in modo da costruire un ambiente di visualizzazione e controllo eccezionalmente personalizzato, in modo semplice ed intuitivo. Tutti i layout così creati possono essere poi facilmente memorizzati, ed anche condivisi con altri utenti. All'occorrenza, un layout salvato può essere richiamato automaticamente in base a determinate condizioni.
Quindi, già oggi il client Mirasys, denominato Spotter, permette una visualizzazione immediata di molteplici funzionalità, oltre ad avere la possibilità di usare

eventuali integrazioni come plug-in, gestendole direttamente dallo schermo come parte integrante del prodotto.
Lavorando in collaborazione con i propri Partner, aumenta direttamente il numero di integrazioni possibili ed aumenta parallelamente anche il numero delle funzionalità di Analisi Video che possono essere gestite dal VMS Mirasys, integrando le già potenti funzioni VCA Mirasys con prodotti specifici di terze parti. Il prodotto Mirasys, vista la sua semplicità di integrazione, può essere diretto gestore di una soluzione che va ben oltre le funzioni di VMS, oppure può essere parte integrante di una soluzione di ancora più ampie dimensioni. Questo vale a dire, quindi, che può essere integrato in sistemi di supervisione che gestiscono un insieme di allarmi e sistemi, presentando un'unica interfaccia all'utilizzatore. Ritornando alle funzionalità dirette di supporto al Marketing, alla Business Intelligence ed all'analisi video, possiamo citare, per il supporto alla Business Intelligence, la possibilità di generare report, sia di dati di audit del sistema, che di qualsiasi altro tipo di dati (es. i metadati degli allarmi, della VCA, della lettura targhe, dei POS, etc...) tramite il modulo addizionale Carbon Reporting.
Inoltre, tramite i moduli di Mirasys Activity Map (MAP) disponiamo di un ottimo strumento per fornire importanti informazioni di marketing, grazie ai dati ricevuti dall'infrastruttura di sorveglianza. MAP è un insieme di strumenti atti a visualizzare la densità di movimento sulla base di dati pertinenti a diversi luoghi. Vengono mostrati sia i flussi di traffico, così come le persone o i veicoli che hanno sostato in un determinato punto per quello che potrebbe sembrare un periodo significativo. MAP è in grado di visualizzare il traffico nel tempo, oppure in tempo reale, al fine di fornire informazioni di marketing essenziali per campagne di vendita, o sul comportamento dei consumatori in determinati luoghi commerciali, nonché indicazioni generali sul traffico stradale, o segnalazioni nel caso di particolari congestioni.

Più in dettaglio, quali sono i vantaggi delle vostre soluzioni rispetto agli altri player?
Le nostre soluzioni sono basate su cardini fondamentali, molti dei quali sono visibili "sotto il cofano motore", come le tecniche per garantire l'affidabilità e la robustezza del sistema. Una delle caratteristiche proprietarie di Mirasys VMS è, infatti, il sistema per valutare l'effettiva potenza dell'hardware disponibile, sistema che garantisce sempre un controllo sulle prestazioni, prevenendo in tal modo i blocchi per sovraccarico dell'hardware. Un'altra caratteristica proprietaria di Mirasys VMS è la registrazione sicura su dischi multipli (SDD, Secure Data Distribution), che evita perdite nelle registrazioni dovute a guasti HW, anche in mancanza di costose controller RAID. Un'altra caratteristica utilissima, sia per i System Integrator che per il cliente finale, è la possibilità di salvare la configurazione completa di un sistema, anche multi-server, e di poterla ripristinare in tempo reale anche su un sistema installato ex-novo. Questa funzionalità è presente in Mirasys VMS praticamente da sempre e consente, quindi, di ricostruire, in pochi minuti ed in modo completo, un'installazione compromessa da guasti hardware irrimediabili. Sulle macchine complete fornite da Mirasys, inoltre, questa possibilità è potenziata dal cosiddetto sistema ABUR, cioè la possibilità di ripartire da una Flash Memory interna al sistema, e ricostruire in tempi brevissimi un sistema completo, compreso il sistema operativo Windows.
Partendo da questa solida struttura di base, ritengo che la flessibilità, la facilità d'uso, la facilità di integrazione con altri software facciano parte delle caratteristiche del sistema Mirasys VMS.
Un'ulteriore e fondamentale differenza, a mio modo di vedere, è data dal supporto pre e post vendita, che aiuta ad identificare le reali necessità del cliente, ad identificare il corretto dimensionamento di tutto l'hardware coinvolto, e ad effettuare un corretto dimensionamento della rete, al fine di consentire sempre un'installazione esente da difetti e, a posteriori, un efficace supporto della soluzione. Risulta, infatti, sempre essenziale il poter usufruire di un supporto diretto ed immediato a fronte di eventuali problematiche che si dovessero verificare su una installazione, soprattutto se complessa. Mirasys lavora a stretto contatto con i Partner e i System Integrator, in modo da poter fornire, attraverso supporto diretto e training mirati, una sempre maggiore conoscenza del prodotto che permetta di gestire in modo completo qualsiasi tipo di problematica legata all'utilizzo "sul campo". La presenza di Mirasys in Italia, con vendita e supporto, permette anche di avere un interfacciamento costante e veloce con la casa madre, a fronte di richieste commerciali particolari e di specifiche soluzioni tecniche legate ad un particolare progetto.

Dal vostro punto di osservazione, i clienti sono pronti a scegliere in base a criteri qualitativi dei prodotti e di affidabilità complessiva dei partner o prevale ancora il criterio del prezzo più basso?
Dipende molto dal punto di partenza, che risponde a questa domanda: quali sono le esigenze del cliente? Ogni cliente ha il proprio tipo di esigenza. Oggi esistono prodotti che rispondono a quasi tutte le esigenze, dalle più semplici alle più complesse. Lo dico da sempre: se un cliente risolve le sue esigenze con un prodotto che costa poco, è inutile che vada a cercare un prodotto più robusto o con più funzionalità che, per le proprie esigenze, non userà mai. È molto meglio che acquisti il prodotto che a basso prezzo risolva le sue necessità. Altro discorso se un cliente ha necessità più complesse. Sono, ovviamente, tipologie di mercato che necessitano di risposte diverse in termini di prodotto.
Qui si entra ancora nella risposta data al punto precedente in termine di considerazioni da fare. Io credo che, al di là di una ricerca economica la più conveniente possibile, anche i clienti si rendano conto di cosa chiedono e, di conseguenza, anche dei costi che bisogna sostenere per soddisfare le proprie esigenze. Una volta appurato che il prodotto risponde alle esigenze tecniche, il prezzo non è il problema principale.

I partner di canale di Mirasys sono i systems integrator. Come vi rapportate con i clienti finali?
Mirasys non vende ai clienti finali, ma ai System Integrator, attraverso alcuni Partner selezionati. Fino ad oggi Mirasys non ha utilizzato il Distributore classico perché il prodotto deve avere un minimo di conoscenza da parte del System Integrator che lo va ad installare dal cliente finale. Attualmente noi distribuiamo il nostro software attraverso System Integrator a valore aggiunto che supportano a loro volta i vari System Integrator che si rivolgono a loro per l'acquisto. Questo approccio ha riscontrato un buon risultato, in quanto tutta la catena coinvolta, Partner/System Integrator/End User, riceve un costante supporto, in dipendenza dal livello di complessità della richiesta.
I training fanno da complemento a questo scenario, in quanto chi va ad installare Mirasys da un cliente finale ha sempre un supporto efficace. L'utente finale si trova in questo modo ad avere a disposizione, in termini di supporto, una vera e propria organizzazione multilivello, con il vantaggio di avere contemporaneamente, quando necessario, sia il supporto diretto dei System Integrator, sia dei Partner di canale, fino ad arrivare al vertice, cioè alla casa madre, tramite il supporto ufficiale italiano.

MIRASYS

CONTATTI: MIRASYS LTD
Tel. +39 02 36723101
+ 39 345 1089102
www.mirasys.com

Seicento varchi in tre anni negli Aeroporti di Parigi. Un nuovo successo per Kaba

a cura della Redazione

Kaba, leader indiscusso nel mercato delle soluzioni aeroportuali, si è aggiudicata la vittoria della gara indetta dagli Aeroporti di Parigi per la fornitura, installazione e manutenzione di varchi per il controllo dei passeggeri e cancelli di imbarco automatico.
I varchi installati negli aeroporti parigini saranno seicento in tre anni. La gara prevedeva un periodo di test in cui **Kaba** e società competitors sul mercato sono state chiamate per fornire dei "varchi di prova". Attraverso la fase di test, sono state verificate le funzionalità e l'affidabilità delle macchine, considerando anche eventuali situazione critiche (es. accodamenti, biglietti non validi, ecc.).
Kaba è risultata aggiudicataria della gara con il miglior rapporto prezzo-prestazioni/progetto.

Le soluzioni Kaba per il mercato aeroportuale
Con più di 2000 installazioni nei principali aeroporti internazionali, **Kaba** è oggi fornitore leader di varchi automatici e soluzioni per il controllo dei flussi negli ambienti aeroportuali, dall'ingresso all'area sicura fino all'uscita doganale.

• Sistemi di controllo automatico delle carte d'imbarco
Questi sistemi aiutano il passeggero e il personale dell'aeroporto in quanto riducono le code e quindi i tempi di attesa all'ingresso dell'area di partenza, permettendo la lettura automatica del biglietto e il conseguente passaggio all'area sicura.

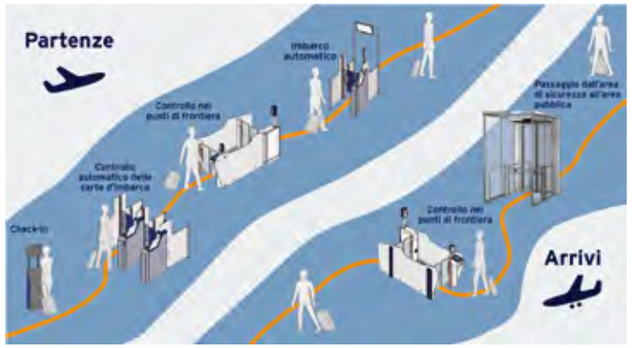
• Sistemi di controllo automatico nei punti di frontiera
I sistemi di controllo automatico alle frontiere migliorano l'efficienza aeroportuale e alleggeriscono anche il lavoro del personale. Il sistema consente di verificare congiuntamente la validità dei documenti e l'identità' dei loro possessori, prevenendo così l'utilizzo fraudolento di passaporti o carte d'identità.

• Cancelli d'imbarco automatico (Self Boarding Gate)
Kaba è stata tra le prime aziende a fornire soluzioni per l'imbarco automatico. Migliaia, infatti, sono i cancelli installati in tutto il mondo grazie anche a collaborazioni e partnership importanti nel settore. La soluzione è stata adottata sia nei grandi aeroporti che in quelli più piccoli, in questo caso per gestire il flusso dei passeggeri in orari di alto traffico.

• Sistemi per il controllo del passaggio dall'area interna sicura all'area pubblica
I corridoi a senso unico prodotti da Kaba, garantiscono la sicurezza negli aeroporti separando la zona pubblica (lato terra) dalla zona di sicurezza (lato aria).

I regolamenti di sicurezza prevedono infatti che le persone non autorizzate non abbiamo accesso al lato aria e che i passeggeri in arrivo non possano ritornare a bordo.

Alcune referenze: Italia (Aeroporti di Roma, Venezia, Bergamo, Torino, Bologna, Pisa), Germania (Aeroporto Internazionale di Francoforte, Aeroporto Willy Brandt di Berlino-Brandeburgo, Monaco), Regno Unito (Aeroporto Internazionale di Londra Heathrow, Aeroporto di Londra-Gatwick, Birmingham), Irlanda (Aeroporto di Dublino), Olanda (Aeroporto di Amsterdam), Svezia (Aeroporto di Malmö), Danimarca (Aeroporto di Copenaghen Kastrup), Francia (Aeroporto di Parigi Orly, Aeroporto di Parigi Charles de Gaulle), Svizzera (Aeroporto di Zurigo), Ungheria (Aeroporto di Budapest), Turchia (Aeroporto di Istanbul), Emirati arabi (Aeroporto di Abu Dhabi), Cina (Aeroporto di Hong Kong), Malesia (Aeroporto di Kuala Lumpur), Aeroporto di Singapore e molti altri.



BIGBAT, il marchio di affidabilità e durata nelle batterie al piombo e al litio

a cura della Redazione

Da anni, aziende e centri di ricerca lavorano per rendere le batterie comunemente in uso sempre più sicure e autonome. Tra le tipologie maggiormente utilizzate nell'industria e, in particolar modo, nel settore della sicurezza, ci sono le batterie primarie al piombo e al litio.
La **ELAN** di Camerano distribuisce da anni, con il famoso marchio BIGBAT, batterie al **piombo ricaricabili (VRLA)** per installatori e rivenditori del settore. I principali tipi di batterie al piombo commercializzati dalla ELAN sono essenzialmente due: le **BIGBAT Standard** e le **BIGBAT Long Life**.
Queste batterie trovano il principale campo di applicazione nel settore della sicurezza. Nello specifico, possono essere utilizzate per illuminazione di emergenza, UPS (gruppi di continuità), pannelli d'allarme, generatori back-up per sistemi di telecomunicazione, attrezzi da giardino, motori d'avviamento e accumulo di energia.
Questi prodotti utilizzano piastre di piombo e calcio separate da una fibra di vetro (AGM) assorbente, che trattiene l'elettrolita a contatto con le celle. Il materiale AGM è altamente poroso, essendo costituito da un tappetino di micro fibra di vetro con fibre polimeriche imbevute di elettrolito, per fare in modo che una sua fuoriuscita sia altamente improbabile.
Le BIGBAT al piombo rispettano i più importanti standard internazionali, su tutti lo **IEC60896-21/22** e il **BS6290-4** per la serie Long Life. Queste batterie possono venire montate in ogni posizione, hanno una bassa autoscarica e non richiedono alcun tipo di manutenzione.

Dal novembre scorso, a fianco delle tradizionale BIGBAT al piombo, gli istallatori e i rivenditori possono contare sulle **batterie al litio non ricaricabili da 3V e 3,6V**.
La caratteristica principale delle BIGBAT al litio si trova nella facilità di utilizzo e nella bassissima autoscarica, oltre alla comprovata qualità dovuta ad un marchio già testato e riconosciuto sul mercato.
I principali campi di applicazione di queste batterie sono i sistemi di sicurezza, i sensori, i telecomandi, i calcolatori, le telecamere e fotocamere, gli elettrodomestici a bassa potenza senza fili, gli orologi elettronici sia digitali che analogici, la memoria di back up su tutti i tipi di terminali, la luce segnale di emergenza, le serrature elettriche e le apparecchiature di misura elettronica.
Le batterie al litio da **3V** utilizzano metallo al polo negativo e biossido di manganese al polo positivo. La somma elettronegativa tra litio e biossido di manganese produce la tensione di 3 Volt. I modelli a disposizione sono la **CR14250 ½AA** e la **CR17335 123AA**.

Sempre con una tensione da 3V, BIGBAT propone anche due modelli **a bottone**, la **CR2025** e la **CR2032**. Nonostante la chimica utilizzata sia la stessa delle batterie cilindriche (litio metallico e biossido di manganese), le batterie a bottone sono più larghe e sottili rispetto alle alcaline.
Le batterie da **3,6V** sono invece composte da celle primarie al litio-cloruro di tionile, il quale può essere visto come un'anidride mista di acido solforoso e acido cloridrico. I modelli commercializzati dall'azienda in questo caso sono: **ER14250 ½AA**, **ER14505 AA**, **ER17505 A**, **ER26500 C**, **ER34615 D**.
Le batterie al litio primarie hanno una forma chimica stabile, nessun rischio "autoimmune" come le batterie alcaline, e hanno una scadenza che va dai dieci ai quindici anni dalla data di produzione. In particolare, i test hanno dimostrato che lo stoccaggio per 10 anni delle batterie al litio BIGBAT ad una temperatura ambiente, porta ad una dispersione di capacità inferiore all'1% l'anno.
La tecnologia del litio, difatti, garantisce l'immagazzinamento e la concentrazione di una grande quantità di energia in un volume particolarmente ridotto. Questo aspetto mette in guardia dai possibili rischi di esplosioni dovuti, soprattutto, all'utilizzo non appropriato di batterie con diverso livello di carica. Quando si utilizzano batterie in serie, infatti, a tutte viene chiesto di dare la stessa quantità di energia. Spremere una batteria più scarica rispetto alle altre

può, quindi, aumentare il rischio di eventuali guasti. Tali avvertenze sono comunque ridotte al minimo, in caso di utilizzo corretto di queste batterie.
Il marchio BIGBAT è, da anni, sinonimo di qualità sul mercato delle batterie, sia a livello nazionale che internazionale. Tutte le batterie al litio commercializzate da **ELAN** sono stabili e affidabili, in grado di operare a temperature comprese tra i -55°C e i +85°C.
Anche a causa delle stringenti normative riguardanti il commercio delle batterie al litio, ELAN è, di fatto, una delle poche realtà italiane in grado di garantirne il deposito, il trasporto e la **consegna in 24/48 ore** in totale sicurezza ed efficienza.
Tutte le batterie (sia al piombo che al litio) e le diverse tipologie di cavi sono, infatti, disponibili in magazzino e pronti ad essere consegnati agli installatori anche presso il cantiere nel quale stanno lavorando. La **puntualità** e la **disponibilità**, oltre alla comprovata **qualità**, sono il vero punto di forza di ELAN.

CONTATTI: ELAN SRL
Tel. +39 071 7304258
www.elan.an.it

OPTEX: una gamma completa ed eccellente per la sicurezza perimetrale

a cura della Redazione

Qualunque sia il contesto da proteggere, è necessario tener conto di un concetto fondamentale: la migliore risposta che si può ottenere da un sistema di sicurezza è la capacità di mantenere il più lontano possibile ogni eventuale minaccia dall'oggetto della protezione. Al fattore della distanza si aggiunge inoltre la velocità di reazione all'evento che ha causato l'allarme: quanto prima il personale di sicurezza o le Forze dell'Ordine sono avvisati di un'eventuale effrazione, tanto meglio possono infatti rispondere. E' quindi importante progettare un sistema di sicurezza strutturato con più "linee di difesa" che partono dal perimetro esterno della proprietà fino alle immediate vicinanze dell'edificio.
Nell'ambito della sicurezza degli spazi esterni, l'azienda giapponese OPTEX – di cui **HESA** è Distributore Esclusivo per l'Italia – rappresenta l'eccellenza, con una proposta completa in grado di offrire massima sicurezza, versatilità e assenza di falsi allarmi.
Per proteggere il perimetro esterno della proprietà, si rivela particolarmente efficace l'utilizzo delle **barriere a raggi infrarossi codificati Serie SmartLine**, i cui modelli sono disponibili sia in versione cablata, sia a basso assorbimento per impianti senza fili e offrono caratteristiche molto avanzate. Tra queste, la riduzione dei falsi allarmi grazie all'ampia separazione dei fasci e il controllo automatico della potenza trasmessa, che permette di ottimizzare automaticamente la potenza del fascio e ottenere prestazioni ottimali anche in presenza di condizioni atmosferiche critiche. I modelli della serie SmartLine sono progettati per semplificare l'installazione e realizzare alla perfezione l'operazione di allineamento della barriera, grazie ad un innovativo circuito di allineamento automatico del fascio.
Per realizzare la "seconda linea di difesa", ovvero

una protezione di prossimità che interessa l'area intermedia tra il perimetro e l'edificio, OPTEX offre una gamma eccellente di rivelatori volumetrici da esterno, da scegliere in base alle specifiche esigenze di sicurezza. In particolare, ricordiamo la **Serie VX Infinity**, che si caratterizza per la presenza, a fianco dei modelli più tradizionali, di sensori a doppia tecnologia con antimascheramento, sia cablati che senza fili. Disponibile in diversi modelli, è inoltre apprezzabile per le dimensioni contenute e il design moderno e lineare dei rivelatori, che si adattano a qualsiasi ambiente senza comprometterne l'estetica.
Da sempre molto stimati sono anche i rivelatori passivi d'infrarossi per esterno **Serie HX**, con portata fino a 24 metri, tecnologia a fasci multipli con 94 zone di rilevazione ad alta densità e una funzione che discrimina i movimenti della vegetazione. I modelli HX-40AM, HX-40RAM, HX-80NAM e HX-80NRAM dispongono inoltre di un'esclusiva tecnologia antimascheramento. La serie

HX è stata progettata per applicazioni in cui l'affidabilità e le prestazioni sono un requisito essenziale.
I modelli a basso assorbimento delle serie VX Infinity e HX sono inoltre disponibili già assemblati con i trasmettitori compatibili con tutte le centrali della gamma HESA.
Nell'ottica di una sicurezza su più livelli, OPTEX ha sviluppato anche delle soluzioni molto avanzate che offrono un'adeguata protezione alle vicinanze del luogo da proteggere, la "terza linea di difesa". Ricordiamo quindi il rivelatore **BX-80N**, disponibile sia in versione cablata sia a basso assorbimento, e il rivelatore **BX-100 plus**, che applicati al muro dell'edificio creano una protezione perimetrale di alto livello.
All'interno della gamma OPTEX vi sono inoltre prodotti "trasversali" che consentono di ottenere una valida soluzione nei differenti livelli di protezione.
Tra questi, il **rivelatore a scansione laser Redscan**, particolarmente adatto per applicazioni di massima sicurezza. Redscan è un dispositivo di soli 30 centimetri e di facile installazione, in grado di creare un vero e proprio "muro elettronico". Esegue una scansione incessante dell'area da controllare e, tramite un algoritmo particolarmente sofisticato, rileva distanza, dimensione, forma, velocità e direzione di un soggetto in movimento. Se montato in orizzontale, è in grado di controllare una superficie di ben 30 metri di raggio per 190° di ampiezza, corrispondente ad oltre 1.400 metri quadrati. Montato in verticale, crea invece un vero "muro elettronico" lungo ben 60 metri. Grazie al software **Redscan Manager**, è possibile delimitare con estrema precisione lo spazio da proteggere, che può anche avere una forma complessa, "ritagliando" situazioni come alberi, cancelli o altri oggetti che, muovendosi, potrebbero dar vita a falsi allarmi.
Di grande interesse sono anche i **rivelatori Redwall SIP**, dotati di doppio PIR, la soluzione ideale per proteggere aree esterne anche di dimensioni molto estese. Utilizzando un sofisticato algoritmo, sono in grado di rilevare vari dati, quali temperatura e luminosità provenienti dall'ambiente circostante e di regolare di conseguenza la sensibilità in maniera automatica. Sono totalmente protetti, in quanto integrano le funzioni di antimascheramento, antistrisciamento e anti-rotazione.
Tra i vari modelli si distingue il rivelatore SIP-100, che offre una protezione a lungo raggio (m 100 x 3) e ha 3 uscite indipendenti per le zone, utilizzabili anche per comandare telecamere brandeggiabili. Questa linea è disponibile anche in versione con interfaccia IP, offrendo la possibilità di collegare direttamente i sensori in rete IP con una vasta gamma di software di integrazione per sistemi antintrusione e di videosorveglianza.

CONTATTI: HESA SPA
Tel. +39 02 380361
info@hesa.com
www.hesa.com

PSIM case history, dalle parole ai fatti: ENEL e i nuovi paradigmi della sicurezza fisica

di Nils Fredrik Fazzini

Impiego innovativo delle infrastrutture informatiche combinate con Centrax-PSIM per un progetto di protezione dei lavoratori isolati nei negozi Punto ENEL.

Sintesi del progetto e highlights:

- ***130 negozi – 300 definitivi***
- ***Storage multimediale in Server Farm gestito da sistema ISILON di EMC2***
- ***PSIM multimediale Centrax di Citel in Control Room***
- ***connessione negozi – storage – Control Room su rete dati aziendale***
- ***nuove telecamere AXIS: ascolto ambientale da evento***
- ***connessione sensori in campo via telecamere***
- ***generazione di eventi aggressione / malore con connessione ERP - PSIM***

Tra le grandi società a partecipazione pubblica, **ENEL Spa** è tra quelle che mirano all'evoluzione dei processi gestionali interni che coinvolgono la sicurezza fisica in chiave decisamente PSIM – Physical Security Information Management, non solo in chiave teorica – come talvolta accade – bensì allo scopo di ottenere tutti i vantaggi dell'informatizzazione dei processi: efficienza strutturale, semplicità impiantistica, flessibilità di utilizzo e adattabilità all'evoluzione delle esigenze nel tempo.

Né, tantomeno, si tratta di uno dei casi in cui il PSIM viene inteso semplicisticamente, per cui se un prodotto per la sicurezza è un software di supervisione allarmi allora è un PSIM. Viceversa, in maniera del tutto indipendente dai fornitori, ENEL ha considerato il proprio PSIM su base Centrax come il contesto tecnico in cui innestare un nuovo progetto complementare e convergente per la compliance con la normativa sulla safety del lavoratore isolato e sulla business continuity. La spinta all'innovazione su piattaforme Citel si era già manifestata fin dal progetto originario, con l'uso della LAN nel cablaggio dei campi fotovoltaici e con la gestione da Centrax della geo-referenziazione del singolo pixel delle telecamere termiche per ottenere sui posti operatore mappe dinamiche con oggetti/figure in movimento in assenza totale di visibilità.

Ora l'innovazione si è estesa agli uffici di Enel aperti al pubblico, con formule particolari per ottenere soluzioni che saltano del tutto gli schemi abituali e dove verosimilmente si sta intravedendo cosa c'è dietro l'angolo nel percorso evolutivo della sicurezza fisica:

- gli input vengono generati a prescindere dalla sensoristica tradizionale
- le correlazioni avvengono a prescindere da una centrale di allarme
- lo storage è in una server farm
- le comunicazioni sono tutte digitali e anche in campo non c'è attività significativa di cablaggio

Con questo approccio sono stati attrezzati in tempi record circa 130 uffici di ENEL aperti al pubblico.

Le tecnologie chiave sono state selezionate dal team di progetto di ENEL:

- la gestione totalmente centralizzata e interattiva in ambito Centrax-PSIM di Citel, da anni presente in ENEL;
- la gestione centralizzata dei flussi video basata su Centrax Video Manager - il VMS di Citel – per la gestione di oltre 1.300 telecamere
- l'uso del networking di Gruppo e delle risorse della Server Farm con l'impiego di un sistema ISILON di EMC2 per il la gestione dei dati digitalizzati di video e fonia;
- Telecamere Axis di una nuova serie, dotate di I/O di campo gestibili in una catena con un capofila
- processi di generazione della situazione, in base all'analisi multimediale di contesto e la registrazione audio/video solo in caso di evento, nel rispetto della normativa applicabile
- la gestione della situazione attivata direttamente dall'applicazione gestionale dell'ufficio sul posto di lavoro del di-pendente mediante scambio dati da ERP a Centrax-PSIM
- l'attivazione e il governo dell'intervento, a seguito di video-analisi e video-verifica, secondo i casi affidata all'operatore in Control Room o ad avvisi da sistema multimediale
- l'emissione di reportistica automatica agli stakeholders dei processi di security e safety di ENEL.

Tempi rapidi, semplicità installativa, costi minimizzati, normativa rispettata, sia per i vincoli sulla privacy nei luoghi di lavoro, e sia per la compliance alle norme sulla tutela del lavoratore e quelle sulla business continuity. Tutto questo è stato possibile in tempi insolitamente ridotti rispetto alla novità di alcune integrazioni e di alcuni processi gestionali.

Il **PSIM Centrax di ENEL** gestisce la sicurezza dei siti di produzione di energia green raccogliendo segnali provenienti da fonti e tec-nologie diverse: dagli impianti avanzati nei campi fotovoltaici a soluzioni semplificate come ad esempio i PLC degli impianti di produzione connessi a SCADA impiegati negli impianti idroelettrici con protocollo IEC 60870-5-104. Nei campi fotovoltaici la gestione centralizzata da Control Room interagisce con piattaforme di correlazione di Citel che collegano telecamere termiche con geo-referenziazione del singolo pixel e analisi della scena, generando un cruscotto operatore multime-diale su mappe geo-referenziate che ha permesso di abbattere i costi dei servizi di vigilanza, il numero degli attacchi e i danni subì-ti.	**CITEL** è il è il fornitore di PSIM ai grandi gruppi dell'energia e dell'Oil & Gas nazionali, come ENI, SAIPEM e SNAM, che sono passati progressivamente da architetture chiuse basate su singoli impianti strettamente legati alla sicurezza fisica a una logica PSIM di palazzo o comprensorio in architettura aperta, multifunzione, e multifornitore, gestiti singolarmente o telegestiti da Control Room interne o esterne. Tra questi anche Poste Italiane e Finmeccanica, Mediaset, ma an-che banche di ogni dimensione, da Intesa Sanpaolo alle BCC, le principali Società di Security e i loro grandi utenti dell'industria, della GDO e della logistica. La resilienza delle infrastrutture di telegestione di **Citel** è ai vertici del settore, essendo compliant al massimo livello della normativa CEI 79/5-6, ma anche della 79/11, applicabile alle qualità sistemi-stiche.
EMC² ha avuto un ruolo primario nel progetto fornendo le risorse di storage centralizzate con sistemistica ISILON per l'erogazione dei necessari servizi di protezione dei dati, la continuità operativa e le prestazioni di ricezione e restituzione dei flussi video. Lo spirito con cui EMC Italia ha partecipato al progetto è stato quello di confermare il ruolo di innovatore nella digitalizzazione e dematerializzazione dei processi aziendali, in questo caso nell'ambito di un PSIM integralmente conforme non solo ai requisiti condivisi dal mercato ma alla loro applicazione rigorosa, come ci si deve aspettare dai processi informatizzati.	In quanto protagonista della rivoluzione del video over-IP, **AXIS** ha colto l'occasione di un progetto strutturalmente innovativo per portare un contributo di peso fornendo le nuove telecamere M1014 e M1054. Elevata qualità video ai fini degli analytics, ingressi/uscite digitali gestibili in una catena di telecamere con capofila, configurazione automatica one-click e, infine, un nuovo rapporto prez-zo/prestazioni per favorire la diffusione di nuovi paradigmi sistemistici come quello adottato da ENEL in un ambito PSIM di **Citel**.

Pyronix XDH10TT-WE Rivelatore volumetrico per esterni wireless bi-direzionale

a cura della Redazione

La consapevolezza degli utenti rispetto alla necessità di fermare l'intrusione già all'esterno dei locali ha dato impulso a una crescente domanda di protezione esterna. Nel 2012, **Pyronix** ha lanciato la serie di rivelatori per esterni cablati XD, subito molto apprezzati dagli installatori per prestazioni e affidabilità.
Fino ad ora, la maggioranza dei produttori non ha dato una risposta decisiva alla richiesta del mercato per una soluzione di protezione wireless per esterni. Più che una soluzione, la risposta è stata una combinazione improvvisata di rivelatori per esterni cablati a basso consumo (wireless ready), collegati a ricevitori wireless e alimentati da una batteria tipicamente non specificata. Questa soluzione si basa su una serie di compromessi tecnologici come:
1. Verifica dello stato della batteria disabilitato;
2. Inibizione dell'allarme per lunghi periodi;
3. Problemi legati alla portata wireless;
4. Inibizione della supervisione wireless compromettendo la sicurezza;
5. Inibizione della segnalazione dei LED d'allarme rendendo il test immediato impossibile.

Alla fine, questi compromessi minano l'affidabilità dei rivelatori, riducendo la sicurezza generale della protezione esterna. Inoltre, una soluzione di questo genere richiede molto tempo agli installatori che, spesso, devono gestire ripetitivamente i diversi componenti della soluzione prima e dopo l'installazione.
Il nuovo rivelatore per esterni wireless bi-direzionale **XDH10TT-WE** è il primo della gamma di rivelatori per esterni wireless completamente integrato ad essere lanciato da **Pyronix**. Questo prodotto segna l'evoluzione della popolare serie di rilevatori cablati XD. Conserva la tecnologia a triplo rilevamento, combinando 2 sensori

PIR (ad infrarossi passivi) con 1 sensore a microonde ed è inserito in un nuovo contenitore in plastica di policarbonato con grado di protezione ambientale **IP55** con numerosi miglioramenti per rendere montaggio e installazione ancora più veloci e semplici.

Installazione semplice
Il montaggio e l'installazione dell'XDH10TT-WE sono davvero molto semplici:
1. Memorizza il rivelatore sul sistema e programma la tipologia della zona.
2. Controlla la portata radio al punto di installazione su rivelatore.
3. Installa il rivelatore.
4. Esegui un walk test del rivelatore.

Altezza d'installazione e portata di rilevamento
Il sistema ottico dell'**XDH10TT-WE** è progettato per essere installato a 2,4 metri d'altezza. La lettera "H" nel nome del prodotto indica "high mount", l'installazione con posizionamento alto. L'XDH10TT-WE offre una copertura volumetrica a 90 gradi dell'aria protetta fino a una portata massima di 10 metri. Con 78 zone e 5 piani, il rivelatore offre una protezione incredibilmente densa per la massima affidabilità del rilevamento. Il rivelatore è anche immune agli animali con un peso fino a 10kg.
L'**XDH10TT-WE** viene fornito con 2 griglie di mascheramento delle lenti, una fissa e una flessibile, utilizzate per schermare i sensori ad infrarossi. La maschera fissa può essere usata per creare una protezione a tenda, mentre la maschera flessibile può essere usata per creare diversi modelli di rilevamento. In combinazione con i supporti e gli adattatori speciali studiati per XDH, è possibile gestire vari problemi di installazione: ad esempio creando una protezione volumetrica con la staffa di 45 gradi **XD-WALLBRACKET** e protezione a tenda lungo le pareti dell'edificio; con la staffa da parete **XD-WALLBRACKET** montata sull'adattatore **XD-45D-ADAPTER** per ottenere un orientamento a 90 gradi e le griglie di mascheramento fisse.
Nell'estate del 2016, la gamma wireless XD si amplierà con l'introduzione del rivelatore di protezione perimetrale wireless **XDL15TT-WE**. Il sistema ottico di questo membro della gamma è stato studiato per essere installato a 1,2 metri d'altezza. La lettera "L" nel nome del prodotto indica "low mount", l'installazione con posizionamento basso. L'**XDL15TT-W**E offrira' una copertura stretta a 14 gradi dell'area sorvegliata, fino a una portata massimo di 15 metri. Con 6 zone e 1 piano, il rivelatore è la soluzione ideale per la protezione perimetrale con un alto grado di immunità per animali fino a 35 kg.
L'**XDL15TT-WE** è usato in combinazione con le staffe e gli adattatori opzionali per creare una protezione lungo la parete, quali la staffa da parete **XD-WALLBRACKET** montata su l'adattatore XD45D-ADAPTER per ottenere un orientamento a 90 gradi, o la staffa fissa XD-FIXEDBRACKET.

Tecnologia
L'**XDH10TT-WE** sfrutta una serie di tecnologie avanzate che ne aumentano prestazioni e affidabilità. La logica di rilevamento a tre tecnologie individua la presenza dell`intruso grazie all'analisi avanzata della sequenza d'attivazione del sensore a microonde e dei due sensori ad infrarossi. Tutti e tre i sensori devono essere attivati nello stesso momento per generare una condizione di allarme. Questa tecnologia aumenta la stabilità dei rilevatori e la loro immunità agli agenti esterni di disturbo.
Le diverse bande di frequenza delle microonde permettono l'installazione di più rilevatori a poca distanza tra di loro. Grazie a quest'opzione, gli installatori hanno la sicurezza che i rilevatori non interferiscano tra di loro.
Pyronix ha messo a punto altre tecnologie appositamente studiate per garantire la stabilità dei rilevatori in ambienti difficili. La compensazione digitale della temperatura ne è un esempio: il rivelatore XD si autoregolerà per mantenere la portata di rilevamento in ambienti freddi, caldi o umidi, anche quando la temperatura ambientale si avvicina a quella del corpo umano.
La tecnologia di eliminazione dell'oscillazione della vegetazione ha lo scopo di mantenere la stabilità del rivelatore quando è installato vicino alle piante.
La tecnologia IFT delle soglie di allarme fluttuanti e indipendenti è un brevetto **Pyronix** che aumenta ulteriormente la stabilità di tutti i rilevatori prodotti. Grazie ad essa, il rivelatore può autoregolare le soglie dell'allarme, filtrando le interferenze causate da agenti di disturbo quali illuminazione, caduta di piccoli oggetti, insetti, pioggia, neve e simili.
I filtri ultravioletti proteggono il rivelatore da radiazioni ad altitudini elevate o a livello del mare che, altrimenti, potrebbero destabilizzare le lenti, riducendo le prestazioni ottiche nel lungo periodo.
L'ottica sigillata protegge i sensori ad infrarossi isolandone dagli agenti esterni di disturbo.

Tecnologia wireless bidirezionale
L'XDH10TT-WE sfrutta la premiata tecnologia wireless bi-direzionale **Enforcer** sviluppata da **Pyronix**. L'uso di questa tecnologia con i rivelatori per esterni wireless XD assicura alcuni vantaggi chiave.
Il rivelatore conosce lo stato del sistema in ogni momento e, dunque, si comporta di conseguenza. Se il sistema è inserito, il rivelatore si inserisce a sua volta, rimanendo sempre attivo e aumentando la protezione dell'area sorvegliata. Se il sistema è disinserito, anche il rivelatore si disinserisce risparmiando batteria, senza usare il classico metodo di risparmio della batteria applicato dai rivelatori cablati a basso consumo, ovvero l'inibizione dell'attività di rilevamento per 2 minuti o più, a scapito della sicurezza.
La modalità supervisione è sempre attiva nei rivelatori

wireless XD, assicurando la protezione in caso di manomissione. Le batterie del rivelatore, inoltre, sono monitorate costantemente per garantirne la funzionalità in ogni momento.
Un elemento importante per la riduzione dei tempi di installazione è l'indicatore del segnale di potenza wireless integrato nel rivelatore, che mostra in tempo reale la potenza del segnale wireless sul rivelatore nel punto di installazione.
Il protocollo wireless bidirezionale usato per i rivelatori XD permette un raggio d'azione fino a 1,6 km in spazi aperti, rispondendo alla maggior parte dei requisiti d'installazione. Usando un ricevitore particolarmente sensibile e la tecnologia antenna hopping, la gamma wireless è garantita nel lungo periodo.
Il tasto "one-push-to-learn" sui rilevatori XD è uno standard comune a tutti i dispositivi wireless bidirezionale Enforcer. Questa caratteristica semplifica il processo di memorizzazione del rivelatore. Basta premere il tasto per pochi secondi e il rivelatore è memorizzato.

Compatibilità
L'**XDH10TT-WE** ha il vantaggio di essere compatibile con le centrali **Enforcer**, **PCX** e ricevitore universale UR2-WE.
La centrale wireless bi-direzionale **Enforcer32-WE/APP** offre una soluzione wireless completa con diverse opzioni. Il sistema può essere connesso a **PyronixCloud** e all'app **HomeControl+** che permette il controllo del sistema via smartphone o tablet da qualsiasi luogo nel mondo.
Inoltre, l'**XDH10TT-WE** è compatibile con la centrale ibrida **PCX46-APP**, che offre i vantaggi delle opzioni conformi all'EN50131 grado 2 e grado 3. L'**XDH10TT-WE** si memorizza alla centrale **PCX46-APP** attraverso il modulo di espansione wireless RIX-32WE, dando agli installatori la possibilità di aggiungere al sistema fino a 32 zone wireless, 32 telecomandi e 2 sirene wireless. Infine, l'**XDH10TT-WE** può essere integrato con altri centrali cablati di qualsiasi marca tramite il ricevitore universale wireless bidirezionale UR2-WE. Una soluzione di questo tipo offre tutti i vantaggi del rilevamento affidabile firmato **Pyronix** e un protocollo wireless bidirezionale multipremiato.

Altre caratteristiche
La gamma di rivelatori per esterni wireless XD sfrutta due batterie al litio da 3v con 10A "extra power" assicurando una ottima performance di durata a lungo termine. Queste batterie sono provate alimentando la sirena esterna **Deltabell WE**, confermando la loro incredibile affidabilità.
L'**XDH10TT-WE** è dotato anche di un cicalino "walk test" per semplificare notevolmente la verifica della copertura durante i test. Il cicalino walk test si attiva automaticamente quando la centrale viene impostata in modalità walk test dall'utente master o dall'installatore.
È presente anche una morsettiera per collegare il tamper della staffa.
Con l'**XDH10TT-WE**, Pyronix porta avanti la sua trentennale storia di innovazione e miglioramento continuo attraverso il feedback del mercato. Il nuovo rivelatore XDH10TT-WE sintetizza il meglio della gamma XD, della gamma wireless bidirezionale Enforcer e gli ultimi sviluppi dell'innovazione, portando sul mercato un prodotto in grado di soddisfare le esigenze di installatori e utenti.

CONTATTI: PYRONIX
Tel. +44 (0) 1709 700100
www.pyronix.com

Telecamere Dahua Technology 4K Ultra HD serie DH-IPC-81200

a cura della Redazione

Dahua Technology, produttore leader a livello mondiale di prodotti di videosorveglianza, presenta la nuova serie di telecamere **DH-IPC-81200**.
Questa nuova serie di telecamere IP 4K Ultra-HD ha un sensore con risoluzione di 12 Megapixel (4K UHD), codec video 4K Ultra-HD e video analisi intelligente integrata.
Tutti i modelli delle telecamere **DH-IPC-81200** forniscono immagini e video ad una risoluzione di 3840 x 2160 pixel (8 Megapixel) fino a una frequenza di 30 frame al secondo, oppure 4000 x 3000 (12 Megapixel) a 15 frame al secondo, con una qualità di immagine spettacolare.
Questa serie utilizza un sensore a colori **CMOS Sony Exmor R da 1/1.7 pollici** con risoluzione effettiva di **12 Megapixel** e un **processore dual-core Ambarella Cortex-A9 da 1 GHz** che genera immagini nitide, con elevata sensibilità e con disturbi ridotti al minimo. Grazie alla ottima qualità video e alla sensibilità del sensore, le nuove telecamere IP della serie Dahua sono adatte per installazioni sia interne che esterne, e forniscono sempre immagini fedeli e dai colori brillanti. I due modelli più performanti, **HFW81200E-Z** (bullet camera) e **HDBW81200E-Z** (dome camera), sono dotate di zoom ottico fino a 4x con messa a fuoco automatica in soli 5 secondi. Il potente obiettivo garantisce un ampio angolo di visione (106° ~ 32°). La serie Ultra-HD 4K include la nuova funzione di **E-PTZ** con auto-tracking intelligente e automatico per seguire gli oggetti in movimento. L'hardware di fascia alta è completato da firmware e software di elevato livello che permettono funzioni evolute di analisi video tra cui rilevamento dei volti, conteggio di persone e heat map (rilevazione delle zone con maggiore movimento sull'intera immagine).
Oltre ad offrire una incredibile qualità d'immagine, le telecamere 4K Ultra-HD garantiscono una estrema semplicità di uso e di installazione: l'interfaccia di configurazione da browser segue gli standard di usabilità di tutti i prodotti IP Dahua. Come tutti i prodotti Dahua offrono massima sicurezza, efficienza operativa e compatibilità con gli NVR della serie 4K.

I prodotti Dahua Technology sono distribuiti in esclusiva da:

VIDEOTREND
ITALIA | ESPAÑA
Chiedilo a noi!
Distributore esclusivo Dhaua in Italia

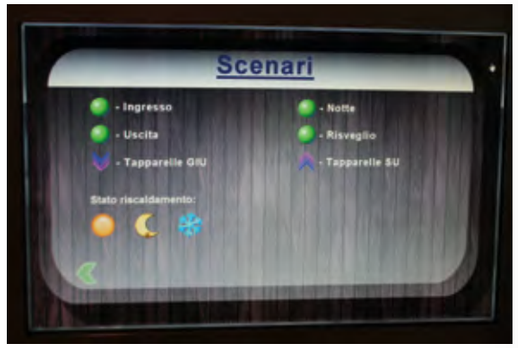
CONTATTI: VIDEOTREND SRL
Tel. +39 0362 1791300
info@videotrend.net
www.videotrend.net

Premio H d'oro 2015
Categoria Residenziale

a cura della Redazione

Categoria: **RESIDENZIALE**
Azienda installatrice: **VILLA IMPIANTI – Cislago (VA)**
Denominazione e località dell'impianto: **Abitazione privata in provincia di Varese**
Impianto realizzato: *Impianto domotico per abitazione di persona disabile*

Nella categoria Residenziale del Premio H d'oro 2015 è arrivata in finale la società Villa Impianti di Cislago (VA) per l'impianto domotico per l'abitazione di una famiglia con persona disabile.



Descrizione dell'impianto

Il progetto rappresenta l'occasione per sperimentare alcune novità nella gestione di un contesto residenziale. La prima grande novità è costituita dalla domotica. In prospettiva futura, è immaginabile uno scenario di risposte residenziali diversificate a seconda dei bisogni dell'utente che consenta, attraverso l'uso della tecnologia, un maggior grado di autonomia.
Committente del progetto è una famiglia con una persona affetta da sindrome di Down.
Gli obiettivi del progetto realizzato sono riassumibili nei seguenti punti:

- Sviluppare secondo il modello "action-research/ricerca-azione", contesto residenziale nel quale le persone con disabilità intellettiva possano acquisire le competenze necessarie per la gestione della vita domestica con il massimo grado di autonomia possibile;
- Integrare l'esperienza di autonomia dei disabili con il loro progetto di vita;
- Individuare delle risposte al problema del "dopo di noi" attraverso il coinvolgimento attivo delle famiglie.

Il progetto domotico è destinato ad un appartamento di circa 140 mq al primo piano di una palazzina, composto da ingresso, zona soggiorno, tre camere da letto, una cucina e due bagni. Gli ambienti sono suddivisi in interni ed esterni, ed è possibile creare un numero infinito di scenari. Per l'avvio degli scenari, si può impostare un timer personalizzato con i diversi eventi. L'utente, attraverso un monitor touchscreen, può comodamente effettuare diverse azioni, come abbassare/ alzare le tapparelle, impostare la temperatura del proprio impianto di riscaldamento e accendere/spegnere le luci in diverse zone della casa.
Il sistema permette di controllare l'impianto elettrico, la climatizzazione con controllo delle temperature in ogni ambiente, l'impianto antifurto con videosorveglianza interna ed esterna, l'automazione delle tapparelle, la rete dati in tutti i locali, i sensori di rilevamento delle fughe di gas e i sensori di allagamento.
Il sistema gestisce anche la memoria eventi: chi ha inoltrato una chiamata dal videocitofono, chi ha suonato al campanello, quando è stato attivato e disattivato l'antifurto e altre segnalazioni. Ad esempio, l'immagine scattata dalla telecamera di ingresso viene spedita ad un indirizzo mail. Si possono creare diversi scenari.

Materiali utilizzati

n. 1 videoregistratore digitale 4 CH-HDD; n. 1pagina grafica interattiva; n. 1 monitor TV 19"; n, 1 miniled 25W; n. 2 consolle LCD 020; n. 1 centrale con vocabolario; n. 10 contatti magnetici; n. 2 sensori incasso; n. 10 contatti a fune per tapparelle; n. 1 centrale domotica; n. 7 sensori temperatura; componentistica varia

Grado di difficoltà, problemi, soluzioni e caratteristiche particolari dell'opera

Il grado di difficoltà è stato medio. E' stato necessario ascoltare con attenzione le esigenze della famiglia per trovare le risposte migliori.

Caratteristiche particolari dell'opera

Il sistema consente la generazione di messaggi vocali per far sì che i genitori possano essere informati in merito alle esigenze del famigliare diversamente abile quando si trova in locali diversi dalla sua camera.

Staff e tempo impiegati per la realizzazione

Due tecnici per due mesi.

Premio H d'oro 2015
Categoria Soluzioni Speciali

a cura della Redazione

Categoria: **SOLUZIONI SPECIALI**
Azienda installatrice: **I.P.S. IMPIANTI – Corte Franca (BS)**
Denominazione e località dell'impianto: **Roccolo storico nei vigneti della Franciacorta (BS)**
Impianto realizzato: *Sistema di videosorveglianza IP*

Lo scorso 23 ottobre nel Cenacolo Palladiano della Fondazione Cini sull'Isola di San Giorgio Maggiore a Venezia si è svolta la cerimonia di premiazione dei vincitori e dei finalisti della decima edizione del **Premio H d'oro**.
Nella categoria Soluzioni Speciali ha vinto il Premio H d'oro 2015, la società **I.P.S. IIMPIANTI di Corte Franca (BS)** per il sistema di videosorveglianza IP di un roccolo storico nei vigneti della Franciacorta, destinato allo studio della fauna ornitologica locale.

Descrizione dell'impianto

Il sistema realizzato nasce dalla passione del committente, già produttore vinicolo della Franciacorta, per la natura. Il Roccolo Brogilus è infatti un presidio scientifico di particolare rilevanza per lo studio delle rotte degli uccelli migratori e dell'habitat agricolo della zona. Grazie ad un studio dedicato, al fine di approfondire le operazioni di raccolta dati, la cattura dei volatili con le reti è stata sostituita da un moderno sistema di videosorveglianza basato sulla tecnologia IP ad altissima definizione ed estremamente flessibile.
Il sistema è composto da telecamere fisse Day&Night con definizione da 5 MegaPixel ed ottica varifocale, inserite in apposite custodie per l'ambiente esterno. La gestione e la registrazione delle immagini riprese è affidata ad un PC WorkStation dedicato con apposito software ed un'adeguata capacità di storage per la conservazione dei dati. Il dispositivo consente la visione, la registrazione, l'esportazione e la trasmissione delle immagini in sicurezza anche attraverso dispositivi "Mobile".

Materiali utilizzati

n. 5 telecamere fisse IP 5Mp Day&Night; n. 5 custodie per esterno; n. 5 Licenze software vers. Core; n. 1 Switch PoE 8 ingressi; n. 1 NVR Workstation con Hard Disk 1TB.

Grado di difficoltà, problemi, soluzioni e caratteristiche particolari dell'opera

La principale difficoltà incontrata è stata quella di ottenere immagini precise e dettagliate dell'ambiente e dei volatili, naturalmente in rapido movimento, per incontrare le richieste espresse dagli studiosi.

Caratteristiche particolari dell'opera

Non è facile cogliere i dettagli di piccoli oggetti in campo aperto soprattutto quando questi sono in rapido movimento. Non essendoci soluzioni standardizzate per un confronto, il tempo dedicato al posizionamento delle telecamere, le regolazioni dei parametri delle stesse e l'estrapolazione di adeguate immagini hanno comportato un dispendio di tempo ed energia. Ottenere ciò che il cliente si attende, influenzato spesso da filmati televisivi dove i dettagli la fanno da padrone, è sicuramente il fattore che ha reso difficile la realizzazione del sistema.

Staff e tempo impiegati per la realizzazione

Sono stati impiegati 1 tecnico commerciale per l'analisi e lo sviluppo del progetto, 1 direttore tecnico per supervisionare le fasi di lavoro e personalizzare l'interfaccia col software di gestione e 2 tecnici specializzati per realizzare l'intera opera. Il tempo tecnico dedicato all'installazione è stato di circa 3 giornate lavorative.

Dichiarazione del committente sull'impianto

Il cliente è rimasto soddisfatto del lavoro realizzato, poiché come ha espresso successivamente, ha potuto apprezzare il servizio offerto dall'azienda, considerata anche la lunga fase di "progettazione e test in campo".

Da FAAC la soluzione per la protezione del perimetro di aree sensibili

a cura della Redazione

FAAC, la società italiana leader a livello mondiale nelle soluzioni di automazione per serramenti e di controllo degli accessi pedonali e veicolari, offre anche un'efficace soluzione per la protezione dagli attacchi perpetrati tramite autoveicoli. Si tratta del dissuasore a scomparsa **J355 M30-P1**, provvisto di certificazione M30-P1 in conformità alla norma AST M F 2656-07. In termini pratici, questo certificato garantisce che il dissuasore è in grado di arrestare un camion del peso di 6,8 tonnellate lanciato a 50 chilometri l'ora, limitando a un metro la penetrazione del veicolo all'interno dell'area perimetrata. Il video del 'crash test', più eloquente di qualunque certificato, può essere visualizzato all'indirizzo **https://vimeo.com/43389324**.

Il dissuasore a scomparsa FAAC J355 M30-P1 rappresenta una soluzione ideale per la protezione del perimetro di una grande varietà di obiettivi sensibili, come aeroporti, ambasciate, consolati, banche, porti, centrali di polizia, palazzi governativi ecc. Il sistema consente, infatti, al personale di vigilanza di gestire facilmente l'accesso dei veicoli autorizzati, senza rinunciare a una robusta difesa dei varchi. I dissuasori, inoltre, presentano diversi vantaggi rispetto a cancelli di pari robustezza: offrono infatti tempi di apertura e chiusura molto più brevi, una totale visibilità sui veicoli in avvicinamento e permettono il passaggio di pedoni e biciclette. La serie J355 M30-P1 comprende anche la versione EFO (Emergency Fast Operation) che consente sollevamenti molto rapidi, riducendo al minimo il tempo di reazione in caso di pericolo. La protezione è assicurata anche in caso di sabotaggio dell'impianto elettrico poiché, in assenza di alimentazione, l'azionamento oleodinamico garantisce il blocco del dissuasore in posizione alta.

Anche nel caso dei dissuasori per impieghi antiterrorismo, la tecnologia FAAC ha consentito la realizzazione di una soluzione particolarmente competitiva, che offre vantaggi agli utilizzatori finali, ai progettisti edili e agli installatori. Il mini-sito dedicato espressamente ai dissuasori FAAC (**www.dissuasorifaac.it**) contiene una ricca e completa documentazione tecnica di tutti i prodotti, comprendente i modelli 3D in vari formati e le descrizioni di capitolato, per facilitare la stesura dei progetti e la preparazione delle gare d'appalto.

"L'attuale turbolenza nel panorama socio-politico internazionale, insieme al riacutizzarsi della minaccia terroristica, contribuiscono a ridurre la sicurezza sociale percepita. Questo rende purtroppo più stringente la necessità di difendere obiettivi sensibili dal pericolo di attacchi condotti per mezzo di autoveicoli. I dissuasori a scomparsa FAAC J355 rappresentano una risposta efficace a questo bisogno e un contributo della tecnologia italiana alla sicurezza", ha affermato **Davide Querzè**, Product Manager di FAAC.

CONTATTI: FAAC SPA
Tel. +39 051 61724
info@faacgroup.com
www.faacgroup.com

Da Betafence soluzioni integrate su misura per la difesa degli obiettivi sensibili

a colloquio con Ruggero Carpentiere – Direttore Commerciale Betafence Italia
a cura della Redazione

Le attuali tensioni a livello internazionale nella sicurezza pubblica e privata stanno comportando una rinnovata attenzione per la "materialità" delle soluzioni. Recinzioni, barriere, sistemi di chiusura e di controllo degli accessi fisici hanno assunto un ruolo nei sistemi di difesa degli edifici e delle aree che sembrava superato dalla sicurezza attiva. Come valuta Betafence, uno dei leader internazionali del settore, questa situazione?

Purtroppo i recenti fatti di cronaca legati agli attentati all'aeroporto di Bruxelles, riportano in piena luce la questione della sicurezza fisica in tutte le infrastrutture nevralgiche. In Italia, lo scorso anno abbiamo avuto l'Expo 2015, l'evento più importante che Milano abbia mai conosciuto, ma anche il Giubileo: questi eventi di massima rilevanza hanno comportato tutta una serie di nuove necessità di rinforzare le misure sicurezza che non erano richieste da tempo. In tale senso, è stato elaborato un complesso e articolato piano di prevenzione e controllo del territorio, attraverso l'impiego di sistemi di sicurezza integrati: accanto all'intelligence dei servizi di sicurezza, soprattutto negli scali aeroportuali e nelle strutture sportive, si è reso opportuno predisporre per i controlli agli accessi pedonali e ai varchi, strumenti per lo *screening* radiogeno (X-RAY) e l'utilizzo dei metal detector etc... e la questione dell'integrazione tra sicurezza fisica e sicurezza elettronica è tornato ad essere un punto centrale nelle politiche di sicurezza di tutti gli enti preposti.

In che modo i sistemi passivi possono interagire con i sistemi attivi (sensori, telecamere) per applicazioni integrate e governate da sistemi informatici per la gestione degli eventi?

La nostra prospettiva volge allo sviluppo di soluzioni integrate e " chiavi in mano", risultato di sinergie tecnologiche importanti tra protezioni passive e protezioni attive, che comprendono anche i servizi di assistenza e manutenzione post-vendita. A livello internazionale, il Gruppo Betafence ha già sviluppato numerose e prestigiose esperienze di successo in questo senso, con committenti di primo livello, istituzioni governative, enti per l'alta sicurezza per cui la proposta commerciale si è ampliata in modo rilevante: oltre ai prodotti di recinzione tradizionali, si estende a soluzioni fortemente innovative di protezione perimetrale, comprendendo molteplici servizi: ingegneria, risk analysis, studi di fattibilità e consulenza specializzata nell'ambito dell'alta sicurezza. In chiave di offerta, ci avvaliamo inoltre di partnership tecnologiche con aziende specializzate del mercato, nonché di accordi quadro che abbiamo a livello di gruppo in ambito internazionale con i principali player del settore.

Basti pensare alle recenti operazioni statunitensi: dalla recente acquisizione di Secure USA, leader negli Stati Uniti nelle soluzioni perimetrali intelligenti, nata con l'obiettivo di far fronte a una crescente domanda di soluzioni di sicurezza complete per progetti ad alta criticità; oppure alla recente operazione conclusa con Gibraltar che - grazie all'acquisizione dei diritti di proprietà intellettuale delle barriere antisfondamento (anti-ram) prodotte da Gibraltar US - ha consentito di migliorare l'offerta sul mercato globale dell'alta sicurezza, nei settori di Oil & Gas, Difesa ed Energia. Ultimissima acquisizione quella di Hesco, leader nella progettazione e nella produzione di sistemi di barriera a schieramento rapido, con referenze importanti soprattutto nei settori della difesa, dell'energia e della pubblica sicurezza

Sempre parlando delle linee di prodotti di sicurezza, vi rivolgete al cliente finale tramite il vostro canale oppure attraverso general contractor/systems integrator? In che modo viene informato il cliente finale sulle caratteristiche delle protezioni fisiche passive?

In Italia ci rivolgiamo al mercato della sicurezza attraverso tutti i principali player operanti sul territorio, quindi certamente siamo in contatto diretto con i principali clienti finali per tutti gli importanti snodi nevralgici italiani: stazioni, aeroporti, stadi, energia e telecomunicazioni, infrastrutture di trasporto, enti ministeriali, etc... L'altissima sicurezza richiede infatti un approccio diretto, con soluzioni progettate direttamente con il proprio cliente. In questi casi, ci muoviamo a stretto contatto con il cliente finale fin dalle fasi inziali della concezione del sistema, la progettazione di massima, l'industrializzazione e la messa in opera. A titolo di esempio, in alcune importanti stazioni ferroviarie sono già stati installati i nostri sistemi innovativi di barriere e controllo accessi integrati,

proprio per aumentare la sicurezza all'interno della stazione nelle attività di prefiltraggio dei viaggiatori in avvicinamento ai binari, a stretto supporto del personale di sicurezza delle Ferrovie dello Stato. Al contempo, abbiamo collaborazioni in essere con i principali contractors e system integrator attivi nel mondo della sicurezza. Infine abbiamo sviluppato importanti partnership tecnologiche con produttori di tecnologia a tutti i livelli, per poter offrire sempre una proposta tecnica ai massimi livelli. La nostra attività di informazione verso il mercato passa attraverso una struttura diretta di ingegneri qualificati che seguono i clienti in tutte le fasi del processo decisionale: dalla scelta delle soluzioni tecniche all'assistenza progettuale per arrivare fino all'installazione e messa in opera del sistema.

Possiamo fare una rassegna dei vostri prodotti?

Oggi non possiamo più parlare di prodotti, e nemmeno di sistemi, ma di vere e proprie soluzioni, spesso studiate totalmente su misura rispetto all'esigenza del cliente. Anche la scelta dei materiali viene completamente fatta in funzione dell'esigenza dei clienti: nonostante la nostra azienda si caratterizzi da sempre per la lavorazione dell'acciaio, abbiamo sviluppato soluzioni completamente diverse, ad esempio con l'uso di nuovi materiali trasparenti, dal vetro al policarbonato; per integrare le esigenze di visibilità e basso impatto ambientale con quelle della sicurezza fisica e anti-balistica. La gamma, pertanto, comprende tutti i sistemi dei nostri cataloghi professionali, ma anche i sistemi disponibili in seguito alle recenti acquisizioni prima menzionate.

CONTATTI: BETAFENCE ITALIA SPA
Tel. +39 0861 7801
www.betafence.it

Ora Elettrica sceglie soluzioni Gunnebo per la nuova sede del CREA

a cura della Redazione

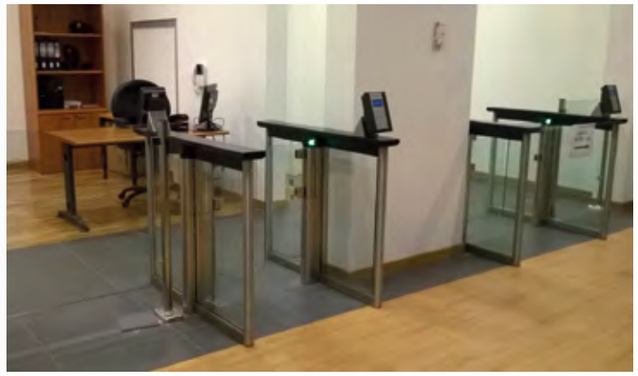
Il **CREA** - Consiglio per la Ricerca in Agricoltura e l'analisi dell'Economia Agraria - è il principale centro di ricerca italiano dedicato al settore agroalimentare; questo importante ente pubblico affronta con la competenza e professionalità, apportate da centinaia di ricercatori e tecnici altamente qualificati, aspetti fondamentali come la sostenibilità e l'efficienza della produzione alimentare, occupandosi del settore agrario, forestale e ittico.

Recentemente il CREA ha cambiato sede, trasferendosi in via Po a Roma, a pochi passi dai giardini di Villa Borghese. Nella nuova sede sono stati installati varchi per la rilevazione delle presenze: l'importanza delle ricerche e del lavoro svolto dall'ente rende opportuno che agli uffici possano accedere solo le persone autorizzate, e un sistema che comprende barriere per il controllo degli accessi è fondamentale in tal senso. Di questo importante aspetto si è occupata **Ora Elettrica** (info@ora-elettrica.com, www.ora-elettrica.com), dinamica società con sede alle porte di Milano che, da quasi un secolo, è attiva nel settore dell'orologeria industriale. L'azienda fornisce sistemi di controllo accessi e di rilevazione orari e presenze che contribuiscono con discrezione al corretto funzionamento e all'efficiente organizzazione del lavoro di numerose imprese e enti in tutta Italia.

Per la nuova sede del CREA, Ora Elettrica ha valutato le numerose soluzioni presenti sul mercato, con l'obiettivo di identificare un sistema che garantisse la sicurezza richiesta senza, per questo, disturbare

l'estetica degli accessi agli uffici con barriere dall'aspetto respingente. Dopo un'accurata ricerca l'azienda ha scelto le barriere **SpeedStile FLs** prodotte da **Gunnebo**.

I varchi SpeedStile FLs, quasi minimalisti nella loro essenzialità, riescono a concentrare in strutture prevalentemente trasparenti e per nulla ingombranti il meglio della produzione della multinazionale svedese. Design all'avanguardia e tecnologia, trasparenza e luminosità, robustezza e sicurezza, elevato flusso di transito e ingombro ridotto: queste caratteristiche si ritrovano tutte nello SpeedStile FLs, in una combinazione innovativa e vincente. I pannelli in cristallo conservano la naturale luminosità dell'ambiente; essendo a battente, scompaiono agevolmente nei cassonetti che devono contenerne lo



spessore, non la larghezza, e hanno quindi un minimo ingombro. Sottile e slanciato nelle forme, SpeedStile FLs offre molteplici possibilità di personalizzazione. La leggerezza della forma non deve trarre in inganno: nella sostanza SpeedStile FLs è molto solido, in grado di bloccare in modo efficace eventuali tentativi di accesso non autorizzato.

Deterrente efficace per gli ingressi fraudolenti, SpeedStile FLs è invece sicuro per le persone autorizzate ad utilizzarlo: il posizionamento dei pannelli in apertura e chiusura è regolato con la massima precisione, evitando che una loro posizione scorretta causi urti accidentali. Sistemi di emergenza consentono l'apertura in caso di sospensione dell'alimentazione elettrica.

Nel progettare SpeedStile FLs, sono state prese in considerazione le esigenze delle persone con ridotte capacità motorie: idealmente, tutti devono poter utilizzare varchi per quanto possibile simili, in modo da evitare percorsi o accessi alternativi che potrebbero essere percepiti come discriminatori. Per questo SpeedStile FLs è disponibile anche nella versione con varco largo 900 mm, che permette alle persone con disabilità motorie di utilizzare un accesso con le stesse caratteristiche estetiche dei varchi standard ed è collocabile nello stesso ambiente.

Come Ora Eletrica ha potuto verificare, SpeedStile FLs è compatibile con tutti i sistemi di rilevazione delle presenze, ed è stato quindi semplice per l'azienda integrare le barriere con i propri innovativi software.

Oltre all'eleganza, all'affidabilità e alla robustezza del prodotto, Ora Elettrica ha potuto apprezzare anche l'efficiente servizio di assistenza tecnica e commerciale pre e post vendita, che costituisce da sempre uno dei principali punti di forza dell'offerta Gunnebo.

Con questa installazione, Ora Elettrica e CREA si aggiugnono alla lunga lista di aziende e enti che hanno accordato fiducia a Gunnebo, rimanendo del tutto soddisfatti della scelta compita.

GUNNEBO®
For a safer world

CONTATTI: GUNNEBO ITALIA SPA
Tel. +39 02 267101
info.it@gunnebo.com
www.gunnebo.it

Vigilanza al bivio, servizi regolamentati o diversamente regolamentati?

a cura di Raffaello Juvara

Questa domanda se la stanno ponendo da parecchio tempo sia gli 800 imprenditori del settore che le 40.000 guardie giurate che lavorano alle loro dipendenze. Una domanda imposta dallo sviluppo della “altra vigilanza”, i portieri diventati “operatori fiduciari”, che ha conquistato prima i servizi di presidio, che rappresentavano la maggioranza dei posti di lavoro per guardia giurata; poi si è lanciata verso altre attività (antitaccheggio, facility management, assistenza, scorte personali, eccetera) inaccessibili agli istituti di vigilanza non solo per motivi economici.

La rigidezza dell’impianto normativo e, soprattutto, della contrattualistica del lavoro, esasperata in molti casi da prese di posizione dei sindacati difficilmente comprensibili, ha infatti impedito che la vigilanza privata si adeguasse tempestivamente ai cambiamenti di scenario conseguenti alla sentenza di Strasburgo del 2007 e alla crisi economica globale iniziata nel 2008. Così, mentre si assottigliavano le richieste dei servizi di vigilanza regolamentati, sono cresciuti in modo clamoroso i servizi “diversamente regolamentati” che, secondo alcune stime, dovrebbero aver già doppiato gli altri, puntando ormai verso quota 100.000 posti di lavoro.

Le innovazioni introdotte dai DM 269/2010 e 115/2014 hanno recepito in buona parte le esigenze di adeguamento normativo del sistema, andando a stabilire sia i requisiti dei soggetti abilitati a svolgere i servizi di vigilanza sia ciò che identifica questi ultimi. In altre parole, il normatore ha cercato di mettere ordine definendo “chi può fare cosa”: da un lato le attività regolamentate dal TULPS, coincidenti in parte con quelle definite di sicurezza “sussidiaria” o “partecipata” (così definite perché configurano la collaborazione

dei privati con lo Stato per la sicurezza pubblica e la protezione degli obiettivi sensibili); dall’altro, le attività non regolamentate o soggette a normative diverse (custodia, raccolta di informazioni, steward, buttafuori ecc).

Trattandosi della ristrutturazione di un sistema che era stato rivisto per l’ultima volta 85 anni fa (nel 1931), è comprensibile che sia necessaria una corposa fase di assestamento, per consentire agli interessati di adeguarsi alle novità. Non è detto che tutti i bruchi riescano a diventare farfalle, come avevamo sottolineato già nel 2013 (**leggi articolo**) ma si cominciano a delineare i diversi orientamenti dei protagonisti, in relazione alle rispettive scelte d’impresa ma anche alle richieste di aggiustamento della riforma, elaborate responsabilmente per evitare che la riforma stessa abbia punti di caduta che potrebbero inficiare il risultato complessivo.

Abbiamo raccolto le dichiarazioni in merito dei rappresentanti delle principali associazioni di categoria e di alcuni operatori della vigilanza e dei servizi fiduciari. Anticipiamo con una sintesi i testi integrali, pubblicati nelle pagine successive.

Cosa dicono gli operatori in sintesi:

Dalle interviste e dalle dichiarazioni dirette e indirette raccolte da essecome/securindex.com tra marzo e aprile, si possono individuare quattro linee di pensiero, che rappresentano uno spaccato le diverse posizioni degli operatori dei servizi di sicurezza privata, nei due segmenti vigilanza e servizi fiduciari. Abbiamo aggiunto una quinta linea che sarà quella che con ogni probabilità dominerà il mercato nei prossimi anni.

A. I trasportatori di valori

Gli operatori del trasporto e del trattamento del denaro hanno già affrontato la selezione delle specie imposta da BCE e Bankitalia e ben sanno che questi servizi possono venire effettuati solamente da organizzazioni adeguate e di “fiducia”. Per Assovalori , quelli previsti del DM 269 sono solo i pre-requisiti d’ingresso. Con la diminuzione del numero degli operatori, viene auspicata anche la possibilità di adeguare i prezzi agli ingenti costi organizzativi.

B. I vigilantini puri

Eredi delle tradizione della vigilanza riservata agli aventi le caratteristiche di legge, da svolgere in modo professionale e giustamente retribuito, sostengono la riforma. Chiedono però l’urgente definizione dei servizi di sicurezza sussidiaria per smarcarsi dalla “altra vigilanza”, e la messa al bando del massimo ribasso per gli appalti pubblici. I portavoce sono ANIVP, ASSIV e, forse, anche Assicurezza che in passato si era fieramente opposta ai DM 269 e 115.

C. I vigilantini aperti

Pur nati nella stessa foresta di Tulpswood dei vigilantini puri, hanno cercato il modo per aprirsi alla “altra vigilanza”, ritenendo che di sola sicurezza sussidiaria sia difficile vivere, soprattutto se non vengono riconosciuti i costi organizzativi per farla sul serio. Federsicurezza e UNIV puntano alla revisione del CCNL per tenere insieme le anime laica e togata dei

servizi di sicurezza, senza aver però ancora trovato il consenso degli altri interlocutori. Almeno finora.

D. La vigilanza diversamente regolamentata

Erano i “paria” della sicurezza, oggi solo il doppio dei lavoratori della vigilanza, spinti da una domanda inarrestabile di servizi non solo low-cost, ma anche diversi da quelli offerti dalle guardie giurate. I problemi di qualificazione degli addetti e la mancanza di CCNL credibili e universalmente riconosciuti li rende ancora una “zona grigia”, con abusi e illegalità di vario tipo. Prima o poi si troverà la strada per regolamentare il settore, entrato ormai tra le abitudini del mercato.

E. Le grandi società di sicurezza

I maggiori operatori del settore si ispirano ai modelli internazionali di “general security provider”, dove la vigilanza regolamentata è una minima parte di un’offerta che spazia dalla tecnologia alla IT security, dall’intelligence ai portierati, al trasporto valori. La diversificazione strutturale li rende meno esposti ai problemi normativi e tariffari delle aziende “monoservizio”. Ancora lontani dall’essere compresi come evoluzione obbligata della specie dalle istituzioni di riferimento e dalle associazioni di categoria, anticipano in Italia il modello di sicurezza privata integrata, consolidato da tempo nel resto del mondo.

Assovalori, la selezione della specie necessaria per la sicurezza dei clienti

a colloquio con Antonio Staino, presidente Assovalori

Le imprese rappresentate da Assovalori sono istituti di vigilanza che effettuano anche il trasporto e il trattamento del denaro che, per loro natura, sono attività che richiedono un livello organizzativo diverso dagli altri servizi. Come valutate il percorso delle certificazioni previste dai DM 269/2010 e 115/2014 ai fini della vostra operatività?

Il possesso dei requisiti minimi previsti dal DM 269/10 per l'attività di trasporto valori ha portato alla diminuzione del numero di operatori e l'auspicato aumento della professionalità di chi continua a credere ed investire nel settore.

Assovalori ritiene che quanto oggi viene visto da molti un aumento di oneri dal punto di vista economico e burocratico debba essere considerato come opportunità; l'utilizzo dei sistemi c.d. "tecnologicamente avanzati" porterà a ridurre l'appetibilità di attacco dei C.I.T., con tutte le conseguenze che ne derivano.

La via tracciata deve essere percorsa fino in fondo, l'obbligo di certificazione richiesto non deve essere il punto d'arrivo, ma la base di partenza e chi è preposto al controllo dovrà provvedere in merito, evitando l'elusione delle regole da parte di chicchessia, fino alla revoca della licenza.

Uno dei problemi paventati è l'applicazione dei provvedimenti nei confronti degli operatori che non risultassero in possesso dei requisiti previsti dalle norme, con le possibili conseguenze sul piano della continuità operativa e dell'occupazione. Qual è la posizione in merito di Assovalori?

Assovalori non ritiene che questo possa considerarsi un problema nel modo in cui è stato posto. Il sistema necessita di CIT, sale conta e aree attrezzate per il deposito, ma nella stessa misura vuole serietà, sicurezza e qualità. Pertanto, dal punto di vista occupazionale, non crede che possano esserci riduzioni di addetti, piuttosto potrebbe verificarsi la chiusura di quelle aziende che avvelenano il comparto e discreditano gli operatori che hanno sempre voluto lavorare coscienziosamente.

Il trasporto valori è da tempo sottoposto a normative cogenti, con controlli effettuati non da organismi privati come gli enti di certificazione ma da istituzioni tutorie (Bankitalia, Ministero dell'Interno) con poteri sanzionatori diretti. Quali sono gli effetti sulla qualità dei servizi effettuati per conto dei clienti?

I controlli svolti da Banca d'Italia, hanno imposto un grande aumento di qualità soprattutto nell'attività di processamento del denaro, l'utilizzo di valorizzatrici, selezionatrici certificate BCE, contratti di assistenza e di manutenzione costantemente rinnovati ed adeguati. Senza trascurare tutto l'aspetto burocratico, contrattualistico e, non ultimo, di verifica delle giacenze nei caveaux.

Tutto quanto purtroppo ad oggi non si è ancora trasformato in un corretto riconoscimento economico e morale da parte della clientela: potremmo tranquillamente affermare che siamo passati dal vecchio treno locale con le carrozze di legno al Frecciarossa 1000, ma gli utenti sono sempre insoddisfatti e vorrebbero acquistare il biglietto sottocosto.

Quali sono le proposte di Assovalori per rendere più efficace il nuovo quadro normativo del settore?

Assovalori ritiene che maggiore efficacia potrà essere raggiunta quando anche all'utenza sarà imposto di scegliere fornitori che, prima della sottoscrizione del contratto, dimostrino anche documentando (e non attraverso lo strumento dell'autocertificazione) di avere almeno i requisiti minimi, fornendo: coperture e garanzie assicurative certe con primarie compagnie; attestato di regolarità con l'anagrafe tributaria; mezzi idonei all'attività da svolgere ed in numero adeguato; attrezzature di sala conta certificate; obbligo di erogare direttamente in quantità predominante i servizi senza ricorrere al subappalto, oppure l'utilizzo del sistema RTI (Raggruppamento Temporaneo d'Impresa).

CONTATTI: ASSOVALORI
www.assovalori.it

Le possibilità di sopravvivenza degli istituti di vigilanza passano per la loro qualificazione

a colloquio con Maria Cristina Urbano, vice presidente ASSIV

Alla fine di marzo 2016, gli istituti in possesso delle certificazioni previste dai DM 269/2010 e 115/2014 risultavano meno di un quarto del totale, con prospettive incerte tanto sui tempi necessari per certificare l'intero parco, quanto sui provvedimenti che verranno adottati nei confronti di quanti non avranno ottenuto le certificazioni. Incertezze che consentono di proseguire l'attività anche ad aziende non in possesso dei requisiti minimi fissati dal DM 269, perpetuando in tal modo le condizioni di disparità nel mercato che affliggono la categoria dal 2007. Quali sono le sue valutazioni in materia?

Siamo di fronte ad un cambiamento profondo nelle modalità di verifica dei requisiti minimi di qualità per la legittimità delle attività di vigilanza ex art. 134 TULPS. Il Ministero dell'Interno, pur rimanendo titolare assoluto di ogni controllo sulle nostre attività, ha deciso di avvalersi di Enti di Certificazione a loro volta accreditati presso ACCREDIA, e quindi di completa fiducia sia sotto il profilo della terzietà che della competenza, per svolgere le verifiche periodiche sugli IDV, ai fini del mantenimento/modifica dei titoli di polizia. Però, se il cambiamento esiste, e non solo nelle modalità di controllo, ma nell'essenza stessa delle norme che ci governano, che adesso sono dettagliate, trasparenti e oggettivamente verificabili nella loro declinazione, non stiamo parlando di qualche cosa di completamente estraneo alle aziende di vigilanza. E' passato molto tempo da quando il concetto di qualità e di verifica sulla qualità è stato introdotto nel nostro mondo, ed è un dato incontestabile che tutte le aziende di vigilanza conoscono cosa è un modello organizzativo e i meccanismi di audit per le finalità certificative. Siamo passati da certificazione di norme volontarie a certificazione di norme cogenti, attraverso meccanismi assolutamente conosciuti, e questo è emerso molto chiaramente nel corso del convegno del 23 marzo. Tutti i testimonial hanno parlato delle loro pregresse esperienze nel campo della certificazione, e delle problematiche incontrate nell'affrontare questo ulteriore modello. Non ho dubbi che il processo di certificazione obbligatoria andrà avanti, in maniera senz'altro più spedita di quanto non sia successo fino ad ora, e darà i frutti che dal sistema si attendono: il Ministero dell'Interno avrà, credo per la prima volta, una raccolta di dati completa ed omogenea rispetto agli indicatori prescelti per valutare il livello di compliance degli IDV, ed anche un significativo data base sui provvedimenti delle singole Prefetture sul territorio nazionale. Un bel cruscotto per prendere le decisioni strategiche di comparto! Mi pare chiaro che l'adeguamento dovrà essere al 100%. Come potrebbe essere diversamente? Stiamo parlando di norme cogenti e di livelli minimi.

E' possibile parlare di "mercato etico" e di "imprenditori etici" nella vigilanza privata, con riferimento al rispetto delle regole che determinano e definiscono il ruolo sussidiario dei privati nei confronti delle Forze dell'Ordine per garantire la sicurezza dei cittadini, in particolare nell'attuale contesto internazionale?

La domanda propone la vexata quaestio sulla natura morale del mercato. Da liberale, ritengo che il mercato non sia etico, anche se, per funzionare, si avvale di regole condivise che possono avere una matrice etica (penso al concetto di buona fede, alla cogenza degli accordi contrattuali, etc. etc.) che trascende il timore delle sanzioni ed è espressione di reale convincimento degli individui. Ma se il mercato non è (necessariamente) etico, gli imprenditori possono esserlo nei loro comportamenti e nel loro approccio al business. Anche nel nostro settore ci sono imprenditori che ritengono giuste e necessarie le regole date e sentono di doverle rispettare, a prescindere dalla leva costituita dal timore delle sanzioni, o, meglio, dal timore della probabilità, più o meno grande, di essere colpiti dalla sanzione. Inutile spaccare il capello in quattro per indagare se coloro che rispettano le regole lo facciano per seguire l'imperativo morale, o piuttosto perché lo ritengono utile, anzi indispensabile, al funzionamento del sistema, e quindi in definitiva alla loro sopravvivenza sul mercato.

Sia come sia, questi imprenditori stanno alle regole, dimostrano affidabilità e condivisione degli obiettivi pubblici – tutela dei beni e della sicurezza delle persone,- anche se la prospettiva ad un certo punto diverge, dato che si fa impresa per lucro. Questi imprenditori rappresentano la parte sana, che fa fatica a competere con chi non sta alle regole, e che non deve essere messa in condizione, non più, di competere con questi ultimi. Per venire all'ultima parte della domanda, ritengo che l'attuale contesto internazionale ed europeo, caratterizzato da questa ondata di terrorismo, che temo non si esaurirà a breve, richiederà al nostro Stato uno sforzo grandissimo per adempiere a quei compiti di sicurezza che solo l'apparato pubblico può e deve garantire, quindi lo Stato stesso si troverà maggiormente sollecitato a fare affidamento, per compiti di rilievo minore, sulla sicurezza sussidiaria, e avrà la necessità di affidarsi a imprese conformi agli standard di legge.

Luigi Gabriele, presidente di UNIV/Federsicurezza, intervenuto dopo di lei al convegno del 23 marzo, ha sostenuto il diritto a operare anche per imprese non in possesso dei requisiti minimi previsti dalla normativa vigente, in una visione portata all'estremo della libertà di mercato, affermando che "i costi della professionalizzazione della categoria sono un incentivo alla distruzione dei posti di lavoro" e che gli "aspiranti primi della classe non hanno affatto il futuro assicurato": cosa risponde Maria Cristina Urbano sia come rappresentante di un gruppo che della qualità ha fatto da sempre la propria bandiera, che di ASSIV/Confindustria che ha sostenuto fin dall'inizio l'impianto concettuale della certificazione della rispondenza a requisiti qualitativi minimi?

Tutte le opinioni sono da ascoltare e rispettare, e ho trovato molto interessante l'intervento dell'avvocato Gabriele, che oltre tutto dice cose vere, quando parla della grande depressione del mercato. Però ritengo che il tempo trascorso, ben otto anni dalla fatidica data della sentenza della Corte europea, rappresenti un periodo molto lungo e tale da consentire agli imprenditori del settore di capire dove sarebbe approdata la vigilanza, quali sarebbero stati i principi normativi di riforma del comparto, e, di conseguenza, per fare le scelte più opportune in riferimento al proprio tipo di business. Non credo proprio che i costi della professionalizzazione siano un incentivo alla distruzione dei posti di lavoro. Anzi, il contrario! Forse potremmo andare incontro ad una diversa segmentazione del mercato, ma questo fa parte dell'evoluzione dello stesso. Dopo di ché, mi sembra di poter serenamente dire che, oggi, nessuno ha un futuro assicurato, ma se c'è una possibilità di sopravvivenza, ed in special modo per gli IVP, questa sta nella loro qualificazione.

A cosa e a chi servono le certificazioni? Le risposte e le richieste di A.N.I.V.P.

a colloquio con Marco Stratta, Segretario Generale A.N.I.V.P.

Sono passati più di sei mesi dalla scadenza fissata dal DM 115/2014 per la certificazione degli istituti di vigilanza rilasciata da Organismi di Certificazione (OdC) autonomi, in merito al possesso dei requisiti determinati dal DM 269/2010. Qual'è il punto della situazione, in un processo dal quale dovrebbe derivare il nuovo corso del settore in Italia?
Sono 23 gli enti di certificazione che, a fine febbraio, risultavano accreditati al Ministero dell'Interno. Di questi, 7 sono autorizzati per tutte e tre le categorie di norme ricomprese dal DM 115/2014.
Questi, pertanto, sono i soggetti ad oggi deputati ad effettuare i controlli sulla regolarità degli istituti di vigilanza agli obblighi di settore, per rimetterli poi all'attenzione delle 103 Prefetture presenti in Italia, oltre ai Commissariati della Valle d'Aosta e del Trentino/Alto Adige.
Tutto il processo è presidiato dal Ministero dell'Interno, tramite l'occhio vigile del Coordinatore dell'Unità Organizzativa per la vigilanza privata del Dipartimento della Pubblica Sicurezza.
Un sistema articolato, che rappresenta sicuramente un "momento di innovazione" nella sinergia tra pubblico e privato, in quanto la struttura si basa per la prima volta su un gioco di forze che unisce regole di mercato e potestà statali.

Ma, secondo l'idea che vi siete fatti, chi sarebbe l'utilizzatore finale di questo "momento di innovazione"?
Le Prefetture. Formalmente sono loro che dovrebbero confermare, sospendere o ritirare licenze nel caso venissero rilevate delle "non conformità" da parte degli organi di certificazione. Ma oggi percepiamo la presenza sempre più forte del Ministero dell'Interno. Come dicevo prima, il sistema si è articolato molto e gli uffici preposti di Prefetture e Questure non sempre riescono ad avere la sensibilità, o le risorse, per seguire tutto attentamente, per cui si appoggiano sempre più spesso a chi oggi coordina il sistema. Questo per certi aspetti è un bene, nell'auspicio ovviamente che ci sia sempre di più una regia politica discendente dai vertici: quella che viene definita normalmente "governance"; in caso contrario, la gestione delle regole sarebbe demandata alla sola sensibilità di singole persone.

Senza risorse però le cose non funzionano, chi finanzia il tutto?
Chi è il soggetto che finanzia questo sistema? Ma, ovviamente, è l'oggetto del controllo, cioè le società di vigilanza! Tutto l'impianto normativo oggi di riferimento per il mondo della vigilanza privata, trova le sue risorse dal comparto stesso.
Però mi hanno insegnato che, quando un'azienda investe, vuole un risultato. Ad oggi invece sinceramente non saprei dire quali risultati tutte queste articolazioni normative abbiano prodotto. Ci domandiamo, pertanto, cui prodest (a chi giova) tutto l'impianto della riforma? Questa sarà una delle risposte che speriamo emerga il 23 marzo a Roma al convegno "Certificatori, Certificati, Certificandi".

Secondo lei, può esserci qualche ipotesi di risposta alla domanda "cui prodest"?
Mi limito a una breve panoramica delle risposte finora spese nei canali ufficiali.
La prima risposta è quella che è stata data per "sponsorizzare" il DM 269/2010 e tutta la riforma normativa: ne beneficiano tutte le aziende sane, perché quelle non sane verranno allontanate dal mercato.
Sinceramente, su questo punto abbiamo già avuto modo di provare che, in questi sei anni, non pare assolutamente essere successo questo. Circa 800 erano le licenze nel 2010 e oggi, malgrado fusioni, incorporazioni ecc, sono lo stesso numero, se non addirittura di più. Inoltre, in molte zone del Paese abbiamo ancora licenze datate anteriormente il 2012, quindi prive dei nuovi controlli di qualità.
Ne dovrebbe giovare quindi, ed ecco la seconda risposta, la qualità dei servizi. Spiace doverlo dire, ma il sentire comune verso il nostro settore è sempre lo stesso (come comparto manchiamo di appeal ma, soprattutto, di una buona politica di marketing culturale) e i fatti e le notizie di cronaca sicuramente non dimostrano il contrario.
Terza risposta: ne gioveranno le aziende di grandi dimensioni che, avendo maggiori possibilità economiche, possono assicurare una migliore qualità dei servizi.
Anche qui abbiamo dei dubbi e, per i conoscitori del nostro settore, le risposte sono già tutte contenute nelle prime due.

Quindi, quali sono le vostre conclusioni e le vostre aspettative?
Caricando su terzi, le società di certificazione per intenderci, il lavoro di screening per identificare le aziende che, prima come adesso, non hanno nulla a che fare con un corretto assetto imprenditoriale, probabilmente si otterrà qualcosa; ma questo "qualcosa" sono convinto che cambierà di pochissimo le sorti economiche del settore.
Tutto ha una storia, e le riforme nel nostro comparto partono dalla sentenza della Corte di Giustizia Europea del 2007. Le associazioni di categoria avevano allora appoggiato appieno l'inevitabile riformulazione delle regole, nell'aspettativa di ricevere almeno delle garanzie sulla specificità dei servizi di vigilanza. Oggi, pertanto, vorremmo che venisse garantito l'affidamento agli istituti di vigilanza dei servizi che, per legge, dovrebbero essere già di loro esclusiva pertinenza, anche da parte degli enti pubblici; vorremmo che fossero seriamente sanzionate quelle società che, senza licenza, erogano servizi di vigilanza semplicemente definendoli in modo diverso; vorremmo che non venissero più emessi decreti da parte del Ministero senza preventivo confronto con tutte le rappresentanze di comparto. In ultimo, perché no, che si potessero recuperare parte dei molti costi sostenuti per garantire l'erogazione dei servizi di vigilanza secondo le regole in essere.
A fronte di queste garanzie, si possono anche lasciare ai portieri la custodia dei cantieri in orario notturno, assieme a tutte le altre attività che non competono per legge alle guardie giurate.
Crediamo che tutto ciò possa davvero giovare economicamente agli istituti di vigilanza che comunque, in tal modo, potrebbero almeno trovare una ragione degli investimenti imposti dal nuovo sistema.
Diversamente, dovremmo schierarci con coloro che il problema neanche se lo pongono e stanno già preparando il terreno al "superportiere" che, senza o con molte meno regole, svolgerà di fatto le stesse mansioni delle guardie giurate, con buona pace delle società di certificazione.

CONTATTI: A.N.I.V.P - ASSOCAIZIONE NAZIONALE ISTITUTI VIGILANZA PRIVATA
info@anivp.it
www.anivp.it

Intervento di Luigi Gabriele al convegno “Certificatori, Certificati e Certificandi” Roma – 23 marzo 2016

intervento di Luigi Gabriele, Presidente FederSicurezza

Non mi sono preparato una citazione al pari degli altri relatori, ma mi viene in mente il “rinnovarsi o perire” di D’Annunzio. Perché “rinnovarsi o perire?” Indubbiamente stiamo scontando in otto anni quello che non abbiamo scontato in settanta: prima settant’anni di stasi normativa, poi otto anni di accelerazione furibonda che ci hanno scaraventati sul mercato in un regime protezionistico, impossibilitati ad adeguarci con tanta velocità. Personalmente, al contrario della Dott.ssa Urbano, temo l’accelerazione dei processi, preferirei piuttosto un’andatura un po’ più “calma e riflessiva”…il problema, in ogni caso, è che l’interlocutore muto, che arresta qualsiasi risultato positivo che si tenta di raggiungere, è la domanda, che in questo momento non ci permette di competere né di reggere il confronto.

Ho un grande problema dal punto di vista di chi rappresento. Cosa devo fare? Supponiamo che un’associazione, o una federazione di associazioni, sia una classe scolastica: su cinquanta alunni di media, non tutti sono a livelli ottimali.

C’è quello che segue bene e quello che segue meno bene: in ogni classe c’è una tipologia molto variegata di alunni. La domanda che mi pongo è questa: in associazione seguiamo la “politica della razza”, e quindi espelliamo coloro i quali non ce la fanno, o cerchiamo di portare gli ultimi ad essere anch’essi

aspiranti primi? Se così deve essere, è chiaro che non possiamo andar di fretta più di tanto.

In aggiunta a questo, pur apprezzando moltissimo quanto la Dott.ssa Urbano abbia elevato il tono della discussione, il concetto dell’etica dell’imprenditore o dell’etica del mercato lo prenderei un po’ “con le molle”, dal momento che temo non siamo più in epoca di Adriano Olivetti o simili, né credo che il sistema moderno sia in grado di ricreare le condizioni che, nel tempo, hanno partorito gli Adriano Olivetti.

Perché ho esordito dicendo “rinnovarsi o perire”? Perché ben venga la certificazione, attenzione, nessuno accusi me di non volere un processo di qualità e nessuno accusi il nostro sistema di rappresentanza di non volere un processo di perfezionamento e di innalzamento del livello di capacità professionale, ci mancherebbe altro. Ma ritengo che il servizio di vigilanza armato, quello “forte”, debba prendere coscienza che non ha più davanti a sé gli spazi, in termini di quantità, che ha avuto fino all’altro ieri.

Perché il mercato non vuole più riconoscere i costi, sia pur “slabbrati”, o meglio, gli “slabbrati” valori del nostro servizio. E non c’è nessuno, neanche tra coloro i quali ci stanno “acculturando”, a calci negli stinchi, che poi però sia in condizioni di metterci delle ginocchiere per evitare che si cada e ci si faccia male quando ci costringono a uscire a 12,75 euro l’ora. Perché è pur vero che chi esce a 12,75 euro probabilmente ha l’animo del raider o del borderline, ma è altrettanto vero che molte committenze, non ultime quelle pubbliche o analoghe, non mettono certo in gara i servizi ai valori indicati dalla tabelle ministeriali sul costo del lavoro.

Allora delle due l’una: o ci si accultura, e poi ci si accompagna a difendere i risultati della nostra acculturazione, o ci si fanno buttare i soldi dalla finestra, e ci si impone di essere i borderline o i raider di mercato, evidentemente. Perché l’Italia è lunga e stretta e sfido chiunque a dire che chi opera a Trapani possa gestirsi come chi opera a Torino.

Allora, se vogliamo essere un veicolo alla disoccupazione, facciamo pure la jihad, non c’è nessun problema; ma se noi vogliamo accompagnare, non con etica da imprenditori a livello spirituale, ma con capacità di coscienza apprezzabilmente onesta con la quale andare ad affrontare il mercato e questo processo ineludibile di qualificazione, teniamo altresì presente che questa qualificazione farà sì che possa salvaguardare solo una parte di questo esistente, ma non credo tutto.

Spiego cosa voglio dire: sapete meglio di me che il sistema di vigilanza privata, o sicurezza privata, in qualunque forma si chiami – e personalmente sono più per il complementare che il sussidiario, che lessicalmente parlando mi pare un minus, perché siamo comunque parte integrante –, è diventato la famosa quarta gamba del tavolo, perché lo Stato non ha più i le risorse e i mezzi per sovraintendere a certi obiettivi.

Il percorso di cui discutiamo va fatto, è ineludibile: a monte del percorso c’era la nostra ignoranza, più o meno diffusa, così come la nostra impreparazione e il nostro non essere online, sempre in modo più o meno diffuso; a valle del percorso, invece, siamo tutti laureati: che facciamo, i laureati inseriti al giusto valore o i laureati disoccupati, i neet?

Per fare un paragone con l’Europa, sapete tutti perfettamente che le grandi concentrazioni di vigilanza privata e sicurezza a livello europeo hanno numeri – anche in un solo istituto – che bissano, dalle due alle tre volte, l’insieme italiano. E sapete altrettanto che fatto 100.000 l’indice di occupazione di questi istituti, 95.000 è “servizi diversi”, e 5.000 è vigilanza privata armata.

Perché? Perché è giocoforza che con questo mercato andremo alla riduzione delle quantità, e che nessuno vorrà pagare quello che dovrebbe veramente pagare per avere una guardia veramente professionale che abbia alle spalle un istituto veramente professionale, con un comandante e una centrale operativa veramente professionali e a norma.

Il mondo si è guardato intorno, si è diversificato, e se è vero – come è vero – che security and safety è una partizione che esiste, e che in Italia dobbiamo imparare a “digerire”, è evidente che se vogliamo salvare la security ci dobbiamo professionalizzare, ma i costi di questa professionalizzazione, se dobbiamo pagarli noi come li stiamo pagando, ci vuole qualcuno che ci accompagni a recuperarli, altrimenti è un incentivo ad una distruzione di mercato, ad un avvio a disoccupazione…danno e beffa, beffa e danno.

Perché ha ragione, chi ci sovraintende, a pretendere che siamo “a posto”, e che non bastano le uniformi in regola, perché per fare questo mestiere ci vogliono la testa e tutta la formazione richiesta. E va tutto bene, ma questi costi chi li riconosce?

Altrimenti diciamo ai nostri cari associati che chi

ha un “quoziente” da 0 a 50 è fuori, mentre chi è da 50 a 100 resta dentro in quanto aspirante “primo della classe”. Ma neanche gli aspiranti primi della classe hanno il futuro assicurato: è proprio questo il vero problema. Chi ha qualche anno in più si ricorda cosa abbiamo subito dalle banche, un tempo grandi postulanti di servizi di sicurezza, che ci hanno prima gonfiati “come ranocchie” per poi farci scoppiare quando non gli è convenuto più, e dalla grande distribuzione, dall’amministrazione pubblica, dagli enti locali e da quelli previdenziali. Forse stiamo recuperando qualcosa con gli aeroporti, ma solo perché hanno visto che non era cosa lucrativa costituirsi la società di servizi aeroportuali di sicurezza, come in molti hanno tentato di fare quando pensavano fosse un boom.

In sintesi estrema, va bene tutto quello che stiamo facendo, lo condividiamo in pieno, riteniamo però di affiancare tutti e non di ammarare quelli che non sanno nuotare. Non riteniamo che lo scopo di un’associazione di rappresentanza datoriale possa essere ammarare quelli che non sanno nuotare e portarsi dietro solo i campioni. Bisogna tendere la mano a tutti, ma l’amministrazione dello Stato deve far capire ad un’altra amministrazione dello Stato, e mi riferisco al Ministero del lavoro, che è inutile perdere pomeriggi con i nostri tecnici per lavorare al Dm sulle tabelle del costo del lavoro, se quel Dm vale zero. Il livello di quella norma non è cogente, è un indicatore qualificato che nessuno rispetta né rispetterà, perché non c’è sanzione per il suo mancato rispetto. I due Ministeri si mettano dunque in sinergia e comprendano che il nostro servizio, che sempre più l’amministrazione dello Stato ci richiede di gestire in sostituzione di ciò che lo stesso Stato, per motivi di bilancio, non può più fare, ci dev’essere riconosciuto per ciò che vale.

Noto con piacere che siamo passati dal “costo del lavoro” al “valore del servizio” (che suona un po’ meno dequalificante), ma sull’etica dell’imprenditore ci andrei molto cauto, perché poi ci vorrebbero anche un’etica di sistema e un’etica dello Stato, tutti valori concettuali fortissimi dei quali, in questo momento, siamo sufficientemente carenti...

Cosa fare? Continuiamo come stiamo facendo, perché qui, in questa platea, non ci sono non certificati: sono tutti certificati, o certificandi, o comunque intenzionati a farlo, e il fatto che la platea sia nutritissima dimostra che l’istanza di migliorarsi c’è...purché però non sia un’istanza che si coltiva solo perché è un obbligo. Se questo rasenta l’etica lo posso anche condividere, evidentemente. L’etica imposta invece non funziona, o la si ha o non la si ha, e non la conferisce una circolare ministeriale, né il rispetto o meno della stessa.

Per concludere, ci auguriamo che il Ministero dell’interno riesca a far capire anche al collega Ministero del lavoro, con il quale ci stiamo già confrontando, che o veniamo messi in condizione di farci ingaggiare per quello che valiamo o è inutile che ci certifichiamo.

Strage al Tribunale di Milano, chi è il vero colpevole?

di Luigi Alfieri, CEO di CSA Security

Un copione già visto, saturo di congetture e di precipitose conclusioni. Eppure dovremmo essere ormai abituati ai paradossi della comunicazione, che spostano l’attenzione su argomenti che distraggono l’opinione pubblica e allontanano il giudizio comune per un unico obiettivo: la colpa non è dei colpevoli!

Nel caso della strage nel tribunale di Milano, le indagini starebbero facendo emergere, dopo mesi, informazioni considerate “clamorose” ma che, per intenderci, le autorità di P.S. potevano ottenere, in tempo reale, collegandosi al sistema d’indagine interforze (c.d. S.D.I.).

Se la regola è quella di focalizzare l’attenzione solo sulla parte finale di un problema con un atteggiamento miope che declina ogni responsabilità del legislatore, che ha ingessato un sistema con decreti ministeriali che mescolano lo stesso “brodo” da anni, non dobbiamo poi lamentarci della mancanza di chiare “istruzioni d’uso”nel settore della sicurezza.

Il vero dilemma è se dobbiamo considerare colpevole un portiere, messo lì a lavorare da un sistema di norme sulla sicurezza che permettono la promiscuità, per non dire la surrogazione, di figure professionali opportunamente profilate; oppure se dobbiamo, più costruttivamente, guardare altrove e puntare il dito verso altri soggetti.

Gli addetti a lavori ricorderanno sicuramente che l’art. 62 del T.U.L.P.S (Testo unico Leggi Pubblica Sicurezza) recitava testualmente: *“I portieri di case di abitazione o di albergo, i custodi di magazzini, stabilimenti di qualsiasi specie, uffici e simili, **quando non rivestono la qualità di guardia particolare giurata**, devono ottenere l’iscrizione in apposito registro presso l’autorità locale di pubblica sicurezza*.”

Altresì, l’articolo 113 del Regolamento per l’esecuzione del T.U. (R.D: 6 maggio 1940, n. 635) recita: “*l’autorità di P.S., nel provvedere sulle domande per la iscrizione nel registro dei portieri, valuta, con criterio discrezionale, la idoneità morale e politica dell’aspirante e, in particolare, accerta se, per età, condizioni di salute, intelligenza, egli sia in grado di spiegare la necessaria vigilanza e di opporsi efficacemente alla consumazione di azioni delittuose. Il portiere è tenuto a corrispondere ad ogni richiesta della autorità di P.S. e a riferire ogni circostanza utile ai fini della prevenzione generale e della repressione dei reati*.”

Ci domandiamo, allora, che fine abbia fatto la “domanda per la iscrizione nel registro dei portieri” che permetteva alle autorità di P.S. di valutare l’idoneità della singola persona a prestare la specifica mansione. La risposta la

troviamo nell'art. 1, commi 1 e 3 dell'allegato B alla l. 24 novembre 2000, n. 340 riguardante le "*Disposizioni per la delegificazione di norme e per la semplificazione di procedimenti amministrativi – Legge di semplificazione 1999*".

Non deve allora scandalizzare l'affermazione che il vero responsabile morale del triplo omicidio consumatosi per mano di Claudio Giardiello il 09 aprile 2015 è lo Stato Italiano che, 16 anni fa, ha determinato il paradosso della eliminazione del solo procedimento d'iscrizione dei portieri, ma lasciando invariato ogni altro articolo riferibile agli stessi. Il colpo di grazia è arrivato con l'introduzione dell'art. 1 del D.P.R. 04 Agosto 2008, n. 153 lettera g, pubblicato sulla G.U. n. 234 del 06 Ottobre 2008 che introduce anche il 3° comma del 256bis "*Rientra altresì nei servizi di sicurezza complementare la* ***vigilanza presso tribunali*** *ed altri edifici pubblici, installazioni militari, centri direzionali, industriali o commerciali ed altre simili infrastrutture,* ***quando speciali esigenze di sicurezza impongono che i servizi medesimi siano svolti da guardie particolari giurate***."

Nel caso di specie, dobbiamo ricordare che proprio il T.A.R. Lombardia, con procedimento N. 00385/2011 REG.RIC del 30/12/2011 acconsentiva l'impiego dei portieri presso il Tribunale di Milano nonostante il ricorso di alcune associazioni di categoria che si erano opposte all'affidamento dello specifico servizio a soggetti non muniti di licenza.

Chiarito quindi il quadro normativo di riferimento e le ragioni che hanno permesso "legalmente" alla società di portierato di vincere la gara di appalto per l'erogazione di servizi di sicurezza presso il tribunale di Milano, possiamo parlare di "*Guardie Giurate vs Portieri*", partendo dal presupposto fondamentale che i servizi di sicurezza erogati da privati devono tenere conto dell'esigenza del'utente, e non di chi eroga il servizio stesso.

Tuttavia, mettendo a fuoco le caratteristiche essenziali di questi servizi, il primo "problema sociale" consiste nella indiscutibile necessità di non permettere a pregiudicati di poter lavorare in un settore delicato come quello della prevenzione dei reati, riferendomi in primo grado ai proprietari delle società di portierato, investigative e di vigilanza piuttosto che ai loro dipendenti.

Di fronte alla clamorosa decisione di lasciare liberi i portieri e, quindi, le società, di non essere sottoposte allo stesso preventivo controllo di P.S. previsto per investigatori e guardie giurate al monitoraggio della P.S. - vedi art. 259 del Regolamento (*), si è generato un trattamento impari che si riflette negativamente anche sull'equilibrio economico del settore stesso. I fruitori del servizio, ignari nella maggior parte delle volte delle complesse sfumature esistenti tra il portiere, l'investigatore e la guardia giurata, scelgono la soluzione meno onerosa, rappresentata dall'impiego di portieri, favorendo in tal modo società senza scrupoli che non solo utilizzano personale non in linea con i requisiti di buona condotta, ma anche ponendosi sul mercato con tariffe insostenibili, spesso sorrette da gestioni molto fantasiose delle buste paghe dei loro dipendenti.

In conclusione, a parere dello scrivente, la soluzione andrebbe ricercata in una evoluzione del settore stralciando tutte le attuali norme appartenenti ad un periodo lontano del nostro paese (1931), a favore di un nuovo ed integrale testo di legge da contestualizzare alle specifiche esigenze del settore che ha bisogno proprio di maggiore sicurezza!

(*) "*Salvo quanto dispone il Regio Decreto-Legge 12 novembre 1936, n. 2144, gli enti ed i privati di cui all'art. 133 della Legge, e chiunque esercita un istituto di vigilanza o di custodia o di ricerche ed investigazioni per conto di privati,* ***è tenuto a comunicare al Prefetto gli elenchi del personale dipendente e a dar notizia, appena si verifichi, di ogni variazione intervenuta****, restituendo i decreti di quelle guardie che avessero cessato dal servizio…*"

Sorveglianza Italiana, un marchio recente con una storia importante alle spalle

a colloquio con con Dario La Ferla, Direttore Generale di Sorveglianza Italiana
a cura della Redazione

Come nasce Sorveglianza italiana, un marchio recente con una storia importante alle spalle?

Nonostante Sorveglianza Italiana sembri un'azienda giovane, la sua tradizione risale dalla fusione per incorporazione tra le due società di vigilanza privata di riferimento locale e con storia quasi secolare: il Corpo Vigilanza Città di Bergamo S.r.l. (operativo dal 1920) e l'Istituto Sorveglianza Provinciale Bergamasco S.p.A. (operativo dal 1929).

Per questo motivo, il logo aziendale è il risultato dell'affiancamento dei due distintivi "storici" delle aziende, che abbiamo voluto così per mantenere viva la nostra storia, ricordando il passato mentre guardiamo al futuro.

Il gruppo è solidamente radicato a Bergamo ma il nome fa pensare a progetti ad ampio raggio. Ce ne può parlare?

Sorveglianza Italiana opera principalmente in Bergamo e provincia. Stiamo guadagnando quote di mercato anche nelle zone confinanti nelle provincie di Lecco e Brescia. L'ottimizzazione tecnologica assieme all'innovazione, la professionalizzazione dei dipendenti, la comunicazione trasparente convincono sempre più clienti ad affidare la propria sicurezza a noi. In questo periodo di contrazione, abbiamo imparato dai nostri concorrenti che la "guerra al ribasso" comporta solo una dequalificazione del livello di servizio. Noi siamo orgogliosi di presentare un'offerta di servizio che consente al nostro utente di apprezzare e misurare il reale valore aggiunto, che si concretizza affidandosi ad un'organizzazione come la nostra che non vende solo pacchetti standard e, soprattutto, non propone soluzioni inutili. Questo risultato è stato raggiunto attraverso la nostra azione commerciale, con collaboratori altamente qualificati e con un approccio che si differenzia di molto dalla tradizionale offerta.

Le altre società del gruppo operano in un mercato più vasto. L'azienda di installazione (Orobica Service S.r.l.) è operativa in tutto il nord Italia, mentre il nostro network di servizi (Securmatica Security Management) opera anche a livello internazionale. Da qualche anno, con un nostro impianto produttivo localizzato in Romania (DDR Proxy vision), produciamo anche DVR e telecamere che vengono esportate in oltre 30 paesi.

Qual è il modello organizzativo dell'istituto in città e provincia, i cui abitanti sono di frequente vittime di furti, rapine, vandalismi?

Il nostro modello organizzativo è diverso da quelli delle aziende nostre concorrenti, innanzitutto perchè il management è totalmente familiare: Non abbiamo manager di prima linea che non siano membri della

famiglia di riferimento e rispettiamo regole ben precise sulle modalità di ingresso di un familiare in azienda.
Qualche anno fa, durante un'attività di confronto con alcuni professionisti della qualità, abbiamo scoperto di applicare un sistema di "total quality control" già da parecchi anni. L'attenzione alla qualità è uno dei nostri tratti peculiari.
Solo nella provincia di Bergamo, durante la fascia notturna abbiamo a disposizione contemporaneamente oltre 40 guardie giurate che, con le autovetture aziendali, supervisionano la propria area di competenza. E' facilmente intuibile che una simile struttura consenta tempi di intervento a seguito di allarme molto ridotti, un dato molto apprezzato dai nostri clienti. Rivolgendo lo sguardo alla concorrenza, notiamo che il player più strutturato presente in provincia di Bergamo dispone per lo stesso territorio 15 guardie giurate.

I servizi di sicurezza vengono frequentemente assegnati anche da enti pubblici a "operatori fiduciari", privi di qualificazioni professionali specifiche e di controlli del profilo penale. Come valuta questa situazione e quali interventi normativi?
Tutti i giorni ci impegniamo per dimostrare che la sicurezza non sia solo un fatto di "costi". L'abuso di figure non regolamentate in questo settore non provoca solamente azioni di concorrenza anomala per le imprese di vigilanza autorizzate, ma mettono una pesante ipoteca a scapito dell'affidabilità e della sicurezza dei servizi erogati. Un servizio di vigilanza deve garantire quel valore aggiunto che, in termini di efficacia, corrisponde al proprio scopo.
Il minor costo tenta, ma una stazione appaltante dovrebbe essere in grado di capire (anche se, spesso, pare voglia ignorare) che un eccessivo ribasso potrebbe nascondere condizioni organizzative tali da favorire disservizi. L'esempio del Tribunale di Milano è calzante: se l'ente avesse scelto di utilizzare sistemi di automazione di controllo degli accessi con guardie giurate, come previsto dalla legge, invece di inserire portieri, avrebbe non solo evitato la perdita di vite umane, ma avrebbe anche risparmiato in termini economici.
Colpisce il fatto che stazioni appaltanti pubbliche sembra non si rendano conto che alcuni dei servizi appaltati sono gestiti da aziende che non li possono svolgere sul piano della legalità. Si dovrebbe segnalare che tale scelta comporta per la stazione appaltante anche l'impossibilità di pretendere un risarcimento, qualora le prestazioni dell'appaltatore non fossero conformi al capitolato. In poche parole, sono soldi (pubblici) spesi senza garanzia di servizio. A questo problema, si aggiunge la perversione dell'assegnazione al massimo ribasso, che consente ad aziende di vigilanza privata più spregiudicate di altre di offrire guardie particolari giurate sottocosto. Come fanno? Facile: imbrogliando sulle retribuzioni, i contributi previdenziali, gli oneri fiscali, la formazione, la sicurezza dei dipendenti…
Per contrastare il fenomeno della "altra vigilanza" sarebbe innanzitutto necessario che l'Autorità Nazionale Anticorruzione intervenisse per censurare i bandi che richiedono i servizi di competenza esclusiva del settore della vigilanza privata mascherati da servizi di facility management. In secondo luogo, sarebbe utile rimarcare la responsabilità civile e penale del responsabile di quel procedimento amministrativo (tale è una gara d'appalto) che comporta l'utilizzo di figure non autorizzate, a danno di una filiera autorizzata e certamente più affidabile. Sarebbe sufficiente applicare la norme e organizzare un sistema di controllo che non sia basato solo su autodichiarazioni ma su fatti inconfutabili.
Mi permetterei di suggerire agli organismi ispettivi delle autorità di controllo (Questure e Direzioni Territoriali del Lavoro) di intensificare i controlli soprattutto tra le 22 e le 7, l'arco temporale di maggior impiego del personale di sicurezza.

CONTATTI: SORVEGLIANZA ITALIANA SPA
Tel. +39 035 38888
www.sorveglianza.it

Axis presenta le nuove telecamere mini dome della serie AXIS M30 per una sorveglianza discreta in ambienti interni

AXIS COMMUNICATIONS
(+39) 011 8198817
www.axis.com

Le tre nuove telecamere mini dome della serie **AXIS M30: AXIS M3044-V, AXIS M3045-V e AXIS M3046-V**, dal design compatto e di facile installazione, sono ideali per la videosorveglianza discreta in ambienti interni di piccole e medie dimensioni che necessitano di molte telecamere per coprire l'intera area senza punti ciechi come hotel, ristoranti, punti vendita, uffici e scuole. Offrono una qualità d'immagine HDTV per captare ogni dettaglio, la tecnologia Wide Dynamic Range per adattarsi a condizioni di illuminazione variabili e la tecnologia **Axis' Zipstream** che riduce lo spazio di archiviazione e l'occupazione di banda senza sacrificare dettagli importanti. Permettono di visualizzare più flussi H.264 e Motion JPEG configurabili singolarmente e includono il rilevamento di movimento nel video, l'allarme antimanomissione e **l'Axis' Corridor Format** che sfrutta l'intero sensore trasmettendo flussi video orientati verticalmente. Supportano inoltre la tecnologia Power over Ethernet e sono dotate di slot per scheda di memoria MicroSD/microSDHC per applicazioni edge storage.

Rivelatori Serie NV35 di PARADOX

DIAS SRL
(+39) 02 38036901
www.dias.it

La serie di rivelatori passivi d'infrarossi a effetto tenda **NV35** di **PARADOX** distribuita da **DIAS** è ideale per protezione di porte e finestre. I rivelatori Serie NV35 sono progettati per essere installati sia all'esterno sia all'interno e offrono una rilevazione precisa, un'elevata immunità ai falsi allarmi e agli animali domestici e un'altissima affidabilità. Con la funzione antimascheramento, i rivelatori NV35 riconoscono oggetti posti in prossimità della lente, vernici trasparenti, fogli di alluminio e nastro adesivo trasparente. Rilevano inoltre il movimento a distanza ravvicinata dall'unità e il degrado delle lenti causato da sporcizia o da polvere. Questi nuovi rivelatori hanno anche l'importante funzione antistrisciamento, per estendere la protezione all'area sottostante il rivelatore.
- Funzione antimascheramento
- Doppio rilevatore controllato da Full Authority Digital Electronics Control (FADEC)
- Protezione antirimozione e antiapertura
- Funzione antistrisciamento
- Conforme EN 50131-2-2 Grado 2 (mod. NV35M, NV35MR) e Grado 3 (mod. NV35MX)

ELANFIRE: resistenza al fuoco e tecnologia del cavo

ELAN SRL
(+39) 071 7304258
www.elan.an.it

Per i cavi resistenti al fuoco vengono usate 3 tecnologie di produzione. In quella classica, il conduttore in rame è ricoperto da un nastro di mica e isolato con reticolato di poliolefina. I conduttori isolati con XLPE e PPE non rispondono alla normativa CEI 20/22. La seconda generazione di cavi è quella che usa il silicone per isolare i conduttori, ma spesso la sua qualità molto economica lascia dubbi sull'affidabilità in caso di incendio. ELAN ha sviluppato una terza tecnologia: **ELANFIRE (PH120)**, il cavo resistente al fuoco che utilizza la mica senza XLPE o PPE per l'isolamento dei conduttori. ELANFIRE usa conduttori isolati con una speciale mescola LSZH che rispetta tutte le regolamentazioni, garantendo zero emissione di gas e fumi tossici e un perfetta spelatura dei conduttori.
Tutti i cavi **ELAN** resistenti al fuoco e la gamma ELANFIRE sono efficaci e affidabili. La loro resistenza al fuoco e la capacità di mantenere i circuiti in funzione in caso di incendio rappresentano la soluzione ottimale per architetti, ingegneri e costruttori.

ekey net, lettori d'impronte ora anche in un residence di prestigio

EKEY BIOMETRIC SYSTEMS SRL
(+39) 0471 922712
www.ekey.net

ekey net è un sistema di controllo degli accessi collegabile in rete per un numero massimo di 80 lettori d'impronte digitali. Dalla porta d'ingresso all'ufficio fino alla sala server o al laboratorio: tutte le zone di un'azienda possono essere riunite e gestite a livello centrale tramite un PC. Con l'ausilio di un software di uso intuitivo, le persone vengono registrate e organizzate in gruppi di utenti liberamente definibili. ekey net supporta una serie di interfacce per il collegamento a sistemi esterni (p.es. gestione dell'edificio, rilevamento tempi, gestione delle stampanti, sistemi WIEGAND, ecc.).
Come nuovo progetto di referenza, ekey vanta il prestigioso complesso **HPA Lake Luxury Life** (www.hpagardalake.com), situato direttamente sul lago di Garda. La struttura dotata del comfort di un albergo a 5 stelle combina un sistema domotico, integrato con una gamma di raffinati servizi, e un sistema di controllo accessi ekey, con 60 lettori d'impronte. Il progetto è stato realizzato dal System Integrator **www.prestigeliving.it**.

ERMES presenta una tromba POE

ERMES ELETTRONICA SRL
(+39) 0438 308470
www.ermes-cctv.com

Semplicità, efficienza, adattabilità sono i termini che meglio descrivono la nuova tromba amplificata Over IP introdotta da **ERMES** per il suo sistema di diffusione sonora SoundLAN-E.
Questa tromba da 10W è alimentata in POE ed è dotata di un connettore IP66 che ne consente l'installazione senza la necessità di accedere al suo interno: fissare alla parete la staffa e collegare il cavo sul connettore per RJ45 fornito a corredo sono le sole operazioni necessarie per la sua installazione.
Le operazioni di settaggio e regolazione si effettuano su rete tramite browser e pertanto l'uso di questa tromba è il mezzo più semplice, rapido ed economico per dotare di diffusione sonora una qualsiasi area dove sia disponibile una rete IP.
Il funzionamento in modo reversibile (talk-back), la possibilità di memorizzare messaggi a bordo scheda, l'attivazione della loro riproduzione su comando da remoto o con pulsanti connessi agli ingressi ausiliari ne rendono facile l'utilizzo, oltre che per diffondere annunci, anche per effettuare l'ascolto ambientale o implementare un sistema di allarme.

HESA presenta le nuove centrali senza fili bidirezionali WP8010 e WP8030 di DSC

HESA SPA
(+39) 02 380361
www.hesa.com

Tra le più recenti novità presentate da **HESA** si segnalano le centrali senza fili bidirezionali **WP8010** da 30 zone e **WP8030** da 64 zone di DSC. Affidabili, flessibili e innovative, sono semplici da installare e da gestire e sono adatte per qualsiasi ambiente da proteggere, sia in ambito residenziale che commerciale. Queste nuove centrali permettono di creare 3 aree indipendenti con inserimento parziale e totale per area. Hanno un combinatore telefonico PSTN incorporato e GSM/GPRS (opzionale) per l'invio di eventi alla centrale di vigilanza, messaggi vocali e SMS fino a 4 numeri telefonici. La gestione avviene tramite telefono remoto, SMS e a breve sarà disponibile un' app per dispositivi Android e iOs per il controllo del sistema da smartphone e tablet. Per risolvere i problemi da interferenze radio, queste centrali offrono fino a 4 salti di frequenza sincronizzati 868MHz-869MHz. Tra i vari componenti del sistema, si distingue un innovativo rivelatore passivo d'infrarossi con telecamera integrata, disponibile anche nella versione Pet Immunity.

Intelligenza domotica e risparmio, con Inim Flex5/DAC

INIM ELECTRONICS SRL
(+39) 0735 705007
www.inim.biz

Flex5/DAC di **Inim Electronics** è l'espansione a tensione di rete per il controllo domotico intelligente. Consente di gestire in modo centralizzato i sistemi SmartLiving attraverso cinque uscite dimmer. Se si connette alla scheda una coppia fase/neutro di rete su un morsetto, si ottiene la misura della tensione prelevata. Ogni uscita comunica con la centrale via BUS permettendo di gestire scenari domotici e controllare l'intensità di grandi carichi di energia (elettrodomestici, luci e prese) monitorandone i consumi. È possibile verificare lo sfasamento tra corrente e tensione di ogni uscita, in modo da rilevare anomalie elettriche a favore del risparmio energetico. Ogni terminale può essere usato come relè, triac ON/OFF o dimmer. In combinazione con gli impianti SmartLiving, **Flex5/DAC** offre un ampio ventaglio di possibilità: apertura e chiusura di tapparelle, finestre, porte, cancelli, regolazione della luminosità di un ambiente e altro ancora.

XDH10TT-WE – Rivelatore volumetrico per esterni wireless bi-direzionale

PYRONIX
+44 (0) 1709 700100
www.pyronix.com

L'**XDH10TT-WE** sfrutta la tecnologia wireless bidirezionale **Enforcer** sviluppata da **Pyronix**, offrendo speciali vantaggi chiave:
• Il rilevatore riconosce quando il sistema è inserito/disinserito, rimanendo attivo se il sistema è inserito e andando in stand-by quando è disinserito. Il rilevatore non applica metodi di risparmio della batteria che compromettono la sicurezza.
• La modalità supervisione è sempre attiva, assicurando la protezione in caso di manomissione.
• Gli indicatori di potenza del segnale mostrano in tempo reale l'intensità del segnale wireless sul rilevatore presso il punto di installazione.
• Il protocollo wireless bidirezionale usato per i rilevatori XD permette un raggio d'azione fino a 1,6 km in spazi aperti
• Il pulsante "one-push-to-learn" sui rilevatori XD è uno standard comune a tutti i dispositivi con compatibilità wireless bidirezionale Enforcer. Questa caratteristica semplifica il processo di impostazione per i pannelli. Basta premere il pulsante per pochi secondi e il rilevatore è impostato.

Nuova centrale Laser Unit

SAET ITALIA SRL
(+39) 06 24402008
www.saetitalia.it

Laser Unit è interattiva, semplice e immediata, programmabile vocalmentr anche da remoto; da 6 a 24 zone con moduli espans. a 6 ingr/2 usc; possibili 48 zone con la funzionalità "zona doppia"; GSM integrato con antenna a base magnetica, alimentat. da 2.4 A e involucro metallo per batt. 18 AH.
In dettaglio:
Invio di info e ricezione di comandi via SMS e messaggi voc. – messaggi voc. impianto, area e zona - SMS allarme puntiformi, uso, tecnici – programmaz. speciali tramite SMS - programmabili > 30 uscite diverse – attivaz/disattivaz da chiave elettronica, codice, oraria, guida vocale, SMS, dispositivo ausiliario – memorizz. eventi per categoria, interrogabili da consolle e tramite SMS – esclus. da utente di zone da telefono – riconness. autom. se terminale GSM disconnesso da rete - firmware centrale e consolle aggiornabili nel tempo – gest. automatica credito residuo e scadenza SIM – movimentaz. uscite telecomando da remoto da guida vocale, SMS e squillo (identificativo del chiamante)
Info: www.saetitalia.it/prodotto/antifurto-cat-49/

AOD-200 Rilevatori da esterno evoluti anche WIRELESS

SATEL ITALIA SRL
(+39) 0735 588713
www.satel-italia.it

La novità di **Satel** per la protezione da esterno WIRELESS con un design minimalista ed una evoluta funzionalità. Garantisce un'ottima protezione perimetrale grazie alle tecnologie PIR e MW. La doppia tecnologia, combinata con l'algoritmo di rilevamento automatico e adattamento alle condizioni ambientali, garantisce un'alta immunità ai falsi allarmi.
Caratteristiche:
Sensore infrarossi passivo (PIR) e sensore a microonda; algoritmo digitale di rilevazione del movimento; compensazione digitale della temperatura. da -40°C a + 55°C; pet immunity fino a 20 Kg; filtro anti oscillazione; resistenza ai falsi allarmi; zona anti-strisciamento; sensore crepuscolare incluso; configurazione della sensibilità dei sensori; configurazione remota; tre LED di segnalazione nella modalità test; supervisione del segnale ricevuto dal sensore; controllo stato batteria; protezione anti-manomissione contro l'apertura dell'alloggiamento o la rimozione; contenitore protetto contro gli agenti atmosferici.

Da SAVV una app multifunzione per Android

SAVV SRL
(+39) 0383 371100
www.savv.it

Datix2App di S**AVV Srl** è un'app multifunzione per smartphone Android. Essa rappresenta la soluzione tecnologica vincente per innovare la gestione dei servizi di ronda, la rilevazione delle presenze della forza lavoro mobile e la protezione dei lavoratori isolati.
Combinando lettura NFC e localizzazione GPS con avanzate funzionalità tipiche di un sistema di allarme uomo a terra (allarmi SOS, perdita di verticalità e immobilità) Datix2App si presenta come soluzione intelligente e integrata per tracciabilità, sicurezza e protezione di beni e persone. Datix2App è compatibile sia con software presso datacenter delle Società di Vigilanza sia con Datix2Cloud, il nuovo servizio cloud di SAVV per la gestione di picchi di lavoro e commesse temporanee senza investimento in PC dedicati.
Datix2App è la soluzione per le Società di Vigilanza moderne per le quali la semplificazione delle procedure, la razionalizzazione delle risorse, la sicurezza degli Operatori e l'erogazione ai Clienti di servizi sempre più puntuali risultano fattori determinanti.

CLV-01 Sensori inerziali passivi senza vincolo di posizionamento

TSEC SPA
(+39) 030 5785302
www.tsec.it

I sensori inerziali **CLV** di **TSEC S.p.A.** sono i primi al mondo ad utilizzare la tecnologia magnetica Magnasphere® per il rilevamento delle vibrazioni.
Basati su un nuovo principio ibrido inerziale/magnetico, non sono soggetti a vincoli di posizionamento.
Ciò permette di installare il sensore nelle zone e nelle posizioni più probabilmente oggetto di eventuali azioni di scasso, permettendo un ulteriore innalzamento del grado di sicurezza dell'impianto.
In una porta blindata ad esempio, il sensore ad incasso **CLV-01** può essere installato con l'adattatore **CLV-BL** in senso orizzontale in prossimità della serratura e sarà in grado di rilevare le vibrazioni dovute ad un tentativo di manomissione della serratura stessa, prevenendo l'intrusione.
Il **CLV-01** è compatibile con le porte veloci delle più comuni centrali e con le più comuni schede di analisi contaimpulsi.
Sono garantiti 10 anni. Accoppiati alle schede di analisi VAS permettono la gestione puntuale di sensibilità molto elevate.

LightSYS™2 di RISCO, il sistema di sicurezza ibrido

RISCO GROUP
(+39) 02 66590054
www.riscogroup.it

Nel panorama dei sistemi di sicurezza, **LightSYS™2** è un'ottima soluzione per i vantaggi che offre tanto agli installatori quanto agli utenti finali: creata per soddisfare le esigenze del mercato residenziale e per attività commerciali di piccole dimensioni, con un numero di zone espandibili fino ad un massimo di 50, è un **sistema di sicurezza ibrido e comodamente gestibile via APP**.
E' la scelta ideale per installatori professionisti che ricercano un sistema flessibile, modulabile, facile da installare e con un ottimo rapporto qualità prezzo. Si può scegliere all'interno di un ampio ventaglio di possibilità tra accessori e rivelatori cablati, radio bidirezionali o via BUS RISCO, VUpoint per la videoverifica live in alta definizione.
Grazie al **Cloud RISCO**, con le applicazioni per web e Smartphone, gli utenti sono sempre connessi al proprio sistema, mentre gli installatori possono programmare la centrale, localmente o anche da remoto con il Software di Configurazione via Cloud, ottimizzando i costi e i tempi di Installazione e Diagnostica.

Guarda il video di LightSYS, scansionando il QRcode:

essecome security&safety

n. 02 marzo-aprile 2016 | ISSN: 2384-9282 | Anno XXXIX
Periodico fondato da Paolo Tura

DIRETTORE RESPONSABILE E COORDINAMENTO EDITORIALE
Raffaello Juvara
editor@securindex.com

HANNO COLLABORATO A QUESTO NUMERO
Luigi Alfieri, Andrea Berti, Nils Fredik Fazzini, Alessandra de Juvenich, Luigi Rubinelli, Pietro Tonussi

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Bozzini 3/A
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

ISCRIZIONE AL ROC
Secman srl è iscritta al ROC (Registro Operatori della Comunicazione)
al n. 22892 del 26/10/2012

REGISTRAZIONE
Tribunale di Verona n. 1971 R.S. del 21 dicembre 2012

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
contatto@lilastudio.it

STAMPA
Grafiche Porpora Srl
Via Buozzi, 12/14
20090 Segrate (MI)
Tel. 02 21871340
www.grafiche porpora.it

Partner essecome 2/2016

AXIS COMMUNICATIONS
www.axis.com
46-49, 103

AXITEA SPA
www.axitea.it
50-53

BETAFENCE ITALIA SPA
www.betafence.it
84-85

CITEL SPA
www.citel.it
57-62, 72-73

CONFORTI SPA
www.conforti.it
54-56

DAHUA TECHNOLOGY CO
www.dahuasecurity.com
2-3, 77

DIAS SRL
www.dias.it
45, 103

EKEY BIOMETRIC SYSTEMS SRL
www.ekey.net
104

ELAN SRL
www.elan.an.it
68-69, 103

ERMES ELETTRONICA SRL
www.ermes-cctv.com
25, 104

FAAC SPA
www.faacgroup.com
82-83

FLIR
www.flir.com
39

FONDAZIONE ENZO HRUBY
www.fondazionehruby.org
78-81

GUNNEBO ITALIA SPA
www.gunnebo.it
86-87

HANWHA TECHWIN EUROPE LTD
www.samsung-security.eu
I romana, 35-37

HESA SPA
www.hesa.it
32-34, 42-43, 70-71, 104

ICIM SPA
www.icim.it
17

IFSEC 2016
www.ifsec.co.uk
4

INIM ELECTRONICS SRL
www.inim.biz
31, 105

KABA SRL
www.kaba.it
66-67

MICROSOFT
www.microsoft.it
40-41

MIRASYS LTD
www.mirasys.com
63-65

PYRONIX
www.pyronix.com
II copertina, 74-76, 105

RISCO GROUP
www.riscogroup.it
23, 106

SAET ITALIA SPA
www.saetitalia.it
IV copertina, 106

SATEL ITALIA SRL
www.satel-italia.it
III copertina, 106

SAVV SRL
www.savv.it
106

SORVEGLIANZA ITALIANA SPA
www.sorveglianza.it
101-102

SWL
www.casamiasicura.it
22

T-SEC S.P.A.
www.tsec.it
copertina, 106

VANDERBILT INDUSTRIES
www.vanderbiltindustries.com
27

VIDEOTREND SRL
www.videotrend.net
2-3, 77

essecome 02
online su > **securindex.com**

Tutti i sistemi di sicurezza

un Brand tutto made in Italy

Entra anche tu nella grande rete delle concessionarie Saet!

ELENCO DEI CONCESSIONARI SAET IN ITALIA

BERGAMO: S.C. SECURITY CENTER	TEL.	035 244728
BOLOGNA: SAET BOLOGNA	TEL.	051 520701
BOLZANO: THEOREMA	TEL.	0471 811343
BRESCIA: LAIS	TEL.	030 3540419
CAGLIARI : ITALTEC	TEL.	070 912395
CHIETI: EASY TECH	TEL.	0871 561759
CREMONA: DISAITALIA SISTEMI	TEL.	0372 838720
CROTONE: DIELETTRA	TEL.	0962 902370
CUNEO: COBER	TEL.	0172 693867
FROSINONE: P.B. SYSTEM	TEL.	0775 270323
GENOVA: TECNOSICUREZZA	TEL.	010 5761513
MANTOVA: ALGOR ELETTRONICA	TEL.	0376 48246
MESSINA: MEGA SISTEM	TEL.	090 7381062
MILANO: SAET MILANO	TEL.	02 2440294
MILANO: TECNOESSE	TEL.	02 3491321
MODENA: MODENA ANTIFURTO	TEL.	059 222999
NAPOLI: CENTRO SECURITY NAPOLI	TEL.	081 5920372
NAPOLI: SECURITY ANTIFURTI	TEL.	081 0332812
PADOVA: SITEL SISTEMI	TEL.	049 8074945
PALERMO : SAET SICILIA	TEL.	091 6884191
PERUGIA: S.D.S.	TEL.	075 8989292
PESCARA: LOGIKEY	TEL.	085 4465582
POTENZA: GENOVESE	TEL.	0971 594358
REGGIO EMILIA: CENTRO ALLARMI	TEL.	0522 322304
RIETI: SECUTRON	TEL.	0746 689053
RIETI: BIO IMPIANTI	TEL.	0746 482877
RIMINI: 3 G ELETTRONICA	TEL.	0541 778605
ROMA: SAET S.p.A.	TEL.	06 24402002
SALERNO: SALERNO KONTROL	TEL.	089 772070
TORINO: G.P.M.	TEL.	011 3358127
TREVISO: SECURITY CENTER	TEL.	0422 305511
MATERA: DC ELETTRONICA	TEL.	083 5337452

SAET ITALIA • SISTEMI DI SICUREZZA E CONTROLLO
Sede legale: Via F.Paciotti, 30 • 00176 Roma - Sede operativa: Viale Filarete, 122/128 • 00176 Roma
Tel. 06.24.40.20.08 - Fax 06.24.40.69.99 - www.saetitalia.it - saetitalia@saetspa.it