essecome security&safety 03

Periodico di informazione su persone, tecnologie e applicazioni della sicurezza

2016 · ANNO XXXIX · ISSN 2384-9282

SAET da 40 anni al tuo fianco

SAET ITALIA S.p.A., distributrice in esclusiva dei prodotti a marchio SAET, rappresenta, con la sua rete di concessionari, l'unica iniziativa di questo genere in Italia e forse in Europa nel campo degli operatori della sicurezza: un punto di riferimento di un numero sempre crescente di concessionari situati su tutto il territorio nazionale, integrati nel tessuto locale e sintonizzati tra loro.

L'obiettivo di Saet Italia è di consentire ai concessionari di utilizzare la qualità dei prodotti e la professionalità degli operatori Saet per ottenere il miglior risultato possibile.

Saet Italia mette a disposizione un catalogo di prodotti vastissimo e completo per ogni categoria dell'impiantistica di sicurezza: dall'antifurto all'antincendio, dai sistemi tvcc a quelli di controllo accessi e gestione presenze, con innumerevoli accessori che completano l'offerta con per rappresentare il fornitore di riferimento per i concessionari. Si aggiunge a questo l'assistenza post-vendita con help-desk tecnico, al quale rivolgersi per avere aiuto in tempo reale o per richieste di informazioni e documentazione, disporre di continui corsi di aggiornamento e di formazione tecnica o commerciale.

Il concessionario SAET dispone quindi di un catalogo di apparecchiature completo e concorrenziale da un unico fornitore, potendo ottenere una concessione anche in esclusiva per la propria zona di competenza. Può contare su un magazzino fornito e veloce; su un gruppo di colleghi sparsi in tutta Italia; sulla partnership di aziende produttrici disponibili a soddisfare anche richieste specifiche; su un knowhow tecnico e professionale condiviso tra i colleghi concessionari. Può inoltre beneficiare di una campagna pubblicitaria su scala locale e nazionale.

Sommario Interattivo

CLICCA SULLA FRECCETTA ROSSA (@) PER SCARICARE L'ARTICOLO CHE TI INTERESSA

ADV_06.2016

StarLight

ORA ANCHE IN HDCVI

Immagini nitide a colori anche
in situazioni di scarsissima luce.

- Ottime prestazioni con bassa illuminazione 0.005Lux/F1.65 (colore)
- Ultra WDR fino a 120dB
- Ottica zoom fino a 30x
- Max 50/60Fps@1080P

La tecnologia STARLIGHT permette di godere di immagini nitide con colori brillanti anche in condizioni di luce estremamente scarsa, senza dover commutare in bianco e nero come avviene con le tecnologie tradizionali. Le immagini a colori forniscono informazioni utili per l'identificazione della scena.

0.005Lux COLOR · IP67 · PoE · IK10

24 MESI Garanzia

Videotrend offre
da Aprile 2016
24 mesi di garanzia
su tutti i prodotti Dahua

>> DH-SD59230I-HC

>> SD6AL230F-HNI

>> DH-SD6C230I-HC


>> HAC-HFW3231E-Z/ZH
>> IPC-HFW8331E-Z


>> HAC-HDBW3231E-Z/ZH
>> IPC-HDBW8331E-Z

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

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

TECHNOLOGY
www.dahuasecurity.com

Brexit, ha vinto l'Inghilterra anziana e conservatrice

La signora perbene che la mattina del 24 giugno si allontana da Westminster verso Blackfriars dopo aver assistito alle manifestazioni di giubilo dei sostenitori della Brexit potrebbe essere l'immagine di quanto era avvenuto il giorno prima: l'Inghilterra anziana e conservatrice ha sconfitto la Gran Bretagna giovane e progressista 52 a 48. Secondo gli analisti, il 75% dei giovani britannici voleva rimanere in Europa ma hanno vinto coloro che pensano che la vecchia battuta "nebbia sulla Manica, tagliato fuori il continente" valga ancora nell'era della globalità.

Ma quali saranno gli effetti per il mercato della sicurezza?

Il 23 giugno, giorno del referendum, si era tenuto a IFSEC un convegno sulle conseguenze della Brexit per il settore, durante il quale alcuni dei più influenti operatori della sicurezza, britannici e non, si erano confrontati sugli effetti in caso di vittoria del *Leave*. Favorevoli e contrari si equivalevano numericamente ma i favorevoli erano indiscutibilmente più convinti degli altri nel sostenere i vantaggi derivanti all'industria britannica del settore in caso di uscita dalla UE. La liberazione dai vincoli comunitari e la certezza nella forza dei brand isolani erano gli argomenti più usati, peraltro non troppo contrastati dai sostenitori del *Remain* con il tema del libero scambio in un mercato più ampio.

Ma c'era anche chi paventava che, in caso di uscita, i produttori americani e asiatici che si erano insediati in UK negli anni passati per guardare al mercato europeo, avrebbero poi spostato nel continente le loro filiali, facendo perdere posti di lavoro, competenze e investimenti.

In effetti, già a pochi giorni dal voto si è delineata una situazione forse non prevista dagli stessi britannici favorevoli al *Leave*, per la quale gli europei dovranno forse paradossalmente ringraziarli.

Le multinazionali globali di ogni settore stanno infatti valutando di trasferire le proprie filiali europee nel Continente, come è stato subito percepito dal mercato immobiliare e dalle agenzie di lavoro interinale. Si potrà capire più avanti quanto questo fenomeno interesserà anche l'industria della sicurezza, ma è prevedibile che le aziende d'oltremare che si erano posizionate in UK per la vivacità di un mercato locale appartenente oltretutto alla UE, stiano considerando ipotesi più adatte a seguire il baricentro del business che, nel frattempo, si è spostato proprio nel cuore di quell'Europa alla quale la Gran Bretagna ha voltato le spalle.

Al contrario, i produttori britannici saranno costretti a far leva sulla forza del "made in UK" per tentare di esportare in Europa i loro prodotti ma, oltre alle micro-onde in cui primeggiano tradizionalmente, non si vedono per ora molte tecnologie in grado di competere nel rapporto qualità/prezzo sul mercato globale con i produttori asiatici, americani e perfino europei, italiani compresi.

Inoltre, la scarica adrenalinica prodotta dalla Brexit non potrà non provocare reazioni tra i politici che hanno la responsabilità della UE. E' quindi possibile che, questa volta, vengano presi seriamente in considerazione gli innumerevoli segnali finora trascurati, per indirizzare l'Unione verso la realtà delle persone e delle aziende. Solamente in questo modo, i giovani potranno finalmente vivere in un'Europa autentica, non più afflitta dalle utopie onanistiche dei suoi burocrati rintanati a Bruxelles e Strasburgo.

Tutto questo, grazie agli anziani inglesi. Good shot!

ELAN
CAVI & BATTERIE

BIGBAT

CAVO ANTINCENDIO ELANFIRE

- Tecnologia Mica senza impiego di PE o PPE per l'isolamento dei conduttori.

- Resistenza alla fiamma per oltre 120'

- EN 50200 (PH120), CEI 20/22 III, CEI 20-36, CEI 20-37, CEI 36762 C-4 (U0=400V) - CE - "Date"

RoHS

PHTHALATEFREE

CAVI RESISTENTI AL FUOCO

Cavi antincendio ELANFIRE non propaganti e resistenti la fiamma (EN50200 - PH120'). Bassa emissione di fumi e gas alogenidrici tossici.
Cavi schermati, twistati, EVAC CEI 9795.

ELAN srl
Via Osimana, 70
60021 Camerano (AN)
Italy

Contatti
info@elan.an.it
www.elan.an.it
+39.071.7304258

Social

Manca qualcosa?

HOME LOCK

ANTIFURTO SENZA FILI

Home Lock è semplice da installare, ha un design elegante, ma soprattutto è sicuro. FAAC ha creato Home Lock per non farvi avere brutte sorprese. Chiedete al vostro installatore di fiducia la qualità di un grande marchio italiano ad un prezzo competitivo. Date il benvenuto alla sicurezza per la vostra casa con Home Lock, l'allarme senza fili!

FAAC
Simply automatic.

homelock.it

Entrato in vigore il nuovo Regolamento Europeo per la protezione dei dati personali

di Alessandra de Juvenich

Dal **25 maggio 2016** è ufficialmente in vigore in tutti gli Stati membri dell'Unione Europea, il **Regolamento UE 2016/679 (GDPR)** del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
Il testo è stato pubblicato in Gazzetta Ufficiale dell'Unione Europea (GUUF) in data 4 maggio 2016.
Il nuovo Regolamento, che abroga la Direttiva 95/46/CE (Regolamento sulla protezione dei dati generali), sarà definitivamente applicabile in via diretta dal **25 maggio 2018**.
In questi due anni, i cittadini e le imprese dovranno adeguarsi alle nuove disposizioni, se non vorranno essere soggette a sanzioni alla scadenza del biennio.
Il GDPR vuole garantire, da un lato, una maggior tutela dei dati a seguito delle nuove tecnologie digitali utilizzate per il loro trattamento e la loro conservazione; dall'altro, ottenere un'armonizzazione normativa all'interno dell'UE, in modo da evitare difformità nella gestione dei dati personali,rendendo il mercato più sicuro per gli utenti e competitivo per le aziende.
Queste sono alcune tra le principali novità introdotte dal GDPR per le imprese:

- le aziende pubbliche e private con un numero maggiore di **250 dipendenti** dovranno nominare al loro interno un *Data Protection Officer (DPO)*, un responsabile per la protezione dei dati con il compito di garantire il pieno rispetto della normativa
- sarà aumentato l'importo delle sanzioni per le aziende che violeranno le disposizioni del GDPR. Fatti salvi i minimi di legge, si potrà arrivare fino al **4% del fatturato annuo** dell'impresa
- in caso di violazioni dei dati personali (*data breach*) al proprio interno - per esempio accessi non autorizzati - l'azienda dovrà notificare il fatto all'Autorità e ai propri utenti entro un periodo prestabilito dal momento della scoperta della violazione
- le aziende dovranno rispondere al requisito del *privacy impact assessment*, effettuando una valutazione complessiva dell' impatto della normativa all'interno della propria impresa
- sarà applicato il principio generale del *privacy by design*, ossia la necessità di prevedere specifiche misure tecniche ed organizzative a protezione dei dati, dal momento della progettazione di un prodotto e di un servizio
- riconoscimento agli interessati del **diritto all'oblio**, cioè la possibilità di decidere quale informazioni personali far circolare (specialmente on-line), dopo un periodo di tempo, eccetto specifiche esigenze (es. obblighi di legge)
- riconoscimento agli interessati del diritto alla **portabilità del dato**, ossia la facoltà di trasferire i propri dati da un soggetto giuridico ad un altro

Per l'industria della sicurezza rileva in modo particolare quanto disposto dall'art. 32 del GDPR in merito all'obbligo del titolare dei dati a **"mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio**" comprendenti **"la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento"**.
I fornitori di dispositivi che trattano dati personali come, ad esempio, i sistemi di videosorveglianza e i lettori biometrici, dovranno dunque esplicitare al proprio cliente titolare del trattamento le caratteristiche dei dispositivi proposti, affinchè possa decidere consapevolmente quali soluzioni adottare.

Internet of Things e Sicurezza Fisica: il ruolo delle Norme per la sfida del futuro

di Per Björkdahl, Steering Committee Chair di ONVIF
traduzione a cura della Redazione

Le ricerche sul termine “Internet of Things” generano ogni giorno milioni di accessi su Google. Per rendere l’idea, quelle su Barak Obama e World’s Cup ne generano molte meno.
Internet of Thing (IoT) è un concetto di cui si sta parlando molto in tutto il mondo.
C’è un acceso dibattito su cosa sia in realtà “Internet of Things”. Le discussioni si soffermano spesso sui possibili effetti di Iot per il futuro delle tecnologie, lo sviluppo dei prodotti e la crescita delle vendite senza, però, definire esattamente cosa esso sia.
Alcuni azzardano che esista già un “Internet of Things”, rappresentato dall’integrazione tra mobile, rete e applicazioni su web, con il futuro Web 3.0 che promette di rendere possibili esperienze di utilizzo ancora più personalizzate di quanto sia possibile adesso.
Alcuni tecnologi ritengono, invece, che il termine IoT si riferisca semplicemente alla connessione di oggetti con altri oggetti, e hanno coniato il termine “Internet of Everything” per definire le reti intelligenti necessarie per connettere tutti questi oggetti tra di loro.
Ci sono anche serie preoccupazioni per la sicurezza delle informazioni che vengono scambiate connettendo tutti questi oggetti tra di loro, con la creazione di nuove porte di accesso che, di fatto, annullano le difese di una rete ben protetta e delimitata.
I primi dispositivi IoT vengono criticati per l’alta vulnerabilità dei loro scadenti livelli di difesa e le presunte capacità di raccogliere segretamente dati e di invadere la privacy delle persone, ma anche per la possibilità di perdere il controllo dei dispositivi stessi.
Diverse autorevoli figure, tra cui **Stephen Hawking, Bill Gates, Elon Musk**, hanno espresso preoccupazione

per la mescolanza tra IoT e Intelligenza Artificiale. Questi signori ritengono che possano esserci pericoli reali da macchine che prendono decisioni e controllano dispositivi.
Il dibattito su IoT all’interno della comunità della sicurezza fisica è leggermente diverso da quelli che avvengono in altri settori.
Il nostro mestiere è mettere in sicurezza cose, persone e informazioni e noi cerchiamo di realizzare soluzioni sicure usando la combinazione tra barriere fisiche e oggetti tecnologici. Pertanto, è naturale che il nostro approccio a IoT imponga maggiore attenzione e prudenza degli altri, perché sappiamo che le informazioni non sono solamente potere ma potrebbero anche diventare una seria minaccia per la sicurezza fisica, se finissero in mani sbagliate.
L’industria della sicurezza fisica deve, quindi, esercitare molta attenzione nello sviluppo di prodotti e capabilities per IoT.

E’ inevitabile che una maggiore condivisione dei dati faccia sì che la violazione della sicurezza di un singolo sistema o dispositivo possa compromettere quantità enormi di informazioni provenienti da innumerevoli altri sistemi e dispositivi. **HP** ha segnalato di recente che oltre il 70% dei dispositivi IoT utilizzati comunemente risultano vulnerabili agli attacchi informatici.
Un altro aspetto importante per l’industria della sicurezza è la possibilità che vengano sviluppate nuove leggi per proteggere la privacy degli utilizzatori finali, alle quali i produttori si dovranno ovviamente adeguare.
L’integrità della sicurezza che noi garantiamo in quanto operatori del settore non deve venire messa a repentaglio da IoT.
Le attività produttive, le amministrazioni pubbliche e le persone si rivolgono a noi per proteggere ciò che ritengono importante ed è nostro dovere continuare a mantenere gli elevati livelli di sicurezza che stiamo garantendo oggi.
Questo non vuol dire che gli operatori della sicurezza fisica debbano ignorare IoT. Piuttosto, dovranno essere molto attenti e determinati nel loro approccio a IoT, allo stesso modo con il quale sviluppano nuovi prodotti, software e sistemi.
E’ un fatto importante che molti operatori del nostro settore e dell’industria tecnologica in genere sostengano che le norme siano adesso e saranno in futuro l’asse portante per tenere insieme il sistema e fare dello IoT una realtà.
E’ previsto che si arrivi ad una norma globale per IoT già nel 2016. L’associazione professionale più grande al mondo dedicata alla tecnologia, lo **IEEE** (Institute of Electrical and Electronics Engineers), è da tempo al lavoro per sviluppare delle norme per IoT riferite a diversi settori tecnologici.
Si sono anche formate numerose alleanze per sviluppare protocolli di automazione e comunicazione per far fronte all’incremento delle comunicazioni machine-to-machne e allo sviluppo di IoT.
Queste alleanze, come **Zigbee, THREADGroup, ZWave e HomeKit**, hanno tra i loro membri sia costruttori che organizzazioni della sicurezza fisica. Alcune di esse hanno già sviluppato specifiche di certificazione riguardanti anche videosorveglianza, antintrusione e controllo accessi.
Le norme saranno fondamentali per lo sviluppo delle tecnologie IoT nel settore della sicurezza fisica, come del resto hanno previsto in molti.
Gli standard per l’interoperabilità di ONVIF sono stati creati originariamente per innalzare il livello di utilizzabilità, permettendo agli utenti finali di scegliere e utilizzare tecnologie di marche differenti, senza compromettere la funzionalità dei dispositivi.
Allo stesso modo, IoT richiederà ai costruttori e agli sviluppatori di lavorare insieme per stabilire le norme e le specifiche di base che, in futuro, permetteranno ai sistemi di sicurezza fisica di interagire non solo con altri dispositivi per la sicurezza fisica, ma anche con altre tipologie di dispositivi, oltre i confini del nostro settore.
Malgrado rimangano aperte molte domande, è chiaro che IoT si stia già sviluppando e crescendo nel più ampio mercato della tecnologia, dal momento che i consumatori acquistano sempre più prodotti connessi, con la previsione che questa tendenza aumenti nei prossimi anni. Verizon, nel suo **2015 State of the Market IoT report**, prevede che da qui a 10 anni le organizzazioni che useranno dispositivi IoT in modo massiccio potrebbero aumentare la redditività del 10%, con previsioni che parlano di una crescita del 204% del numero di dispositivi IoT connessi nel settore manifatturiero.
L’Internet of Things non può dunque essere ignorato, malgrado l’inquietante mix di potenziali vantaggi e di possibili punti deboli. Si è sviluppato da uno stato puramente concettuale a una realtà ancora embrionale, anche se qualcuno ritiene che IoT rappresenti la prossima fase della rivoluzione industriale.
In ogni caso, siamo assolutamente certi che IoT diventerà una realtà per il settore della sicurezza fisica, anche se non fosse pronto.
Se dell’Internet of Things per il settore della sicurezza fisica è dunque inevitabile, la domanda da porci non è “*IoT influenzerà il nostro mercato?*” ma, piuttosto “*come prepararci al meglio per affrontare IoT?*”
Naturalmente, la sfida sarà di fornire maggior operabilità e facilità d’uso agli utenti finali, senza perdere l’integrità della sicurezza che noi dobbiamo garantire come settore.
E’ nostro dovere comprendere come continuare al meglio la nostra missione di protezione dei beni di valore, mentre offriamo agli utenti finali la funzionalità, la facilità d’uso e l’interoperabilità che si aspettano, bilanciando, nel nostro percorso di sviluppo di prodotti e di norme, gli aspetti positivi e negativi di IoT.

ONVIF, l'evoluzione di un Ente di Normazione

di Per Björkdahl, ONVIF Steering Committee Chairman
traduzione a cura della Redazione

ONVIF è molto cresciuta dal momento della sua fondazione nel 2008. Oggi raggruppa circa 500 membri e sono più di 5.000 i prodotti sul mercato conformi agli standard ONVIF che, come molti altri enti normatori, è evoluto esponenzialmente. Altri enti come l'**International Electrotechnical Commission (IEC), l'Institute of Electrical and Electronic Engineers (IEEE)** e **Bluetooth** hanno fatto percorsi molto simili a quello di ONVIF.

Fondando un'Organizzazione

ONVIF è stato fondato da **AXIS, Sony** e **Bosc**h per creare una norma globale di interfaccia delle videocamere in rete e i sistemi dei gestione video (VMS). Questo permette una maggiore libertà di scelta per gli installatori e gli utilizzatori finali, che possono così selezionare prodotti di costruttori diversi. Stabilendo fin dall'inizio una norma di base per il video, i fondatori speravano anche di semplificare lo sviluppo dei prodotti per i costruttori. ONVIF ha subito compreso che si sarebbero dovuti fare degli aggiustamenti al loro approccio per realizzare una norma. Malgrado i membri fossero d'accordo sul come specificare le APIs (Application Programming Inteface) per il video, le strade che i produttori seguivano per sviluppare i prodotti erano diverse. Di conseguenza, ONVIF ha rimesso in discussione il concetto di profilo, partendo dall'idea che se i costruttori avessero sviluppato i prodotti secondo il profilo, questi avrebbero lavorato insieme indipendentemente dal produttore di VMS o di telecamere.

Bluetooth aveva sperimentato un percorso similare quando ha introdotto e aggiornato la specifica per le cuffie. Bluetooth ha introdotto il "Profilo per Cuffie" per far lavorare i dispositivi indipendentemente da quando fossero stati costruiti. Un nuovo profilo con un nuovo nome sarebbe stato creato solo quando i cambiamenti futuri l'avessero richiesto. ONVIF sta usando lo stesso approccio: se, per esempio, un prodotto è conforme al Profilo S, continuerà a esserlo sempre, a prescindere da quando è stato costruito.

Una prospettiva di ampliamento

Due anni dopo la fondazione, ONVIF ha esteso la propria attività ai sistemi di controllo accessi. Come prevede il modello costitutivo di ONVIF, l'attività dell'organizzazione può includere ogni disciplina riguardante l'industria della sicurezza fisica, non focalizzandosi solamente sulla parte video. Come ONVIF, altri enti normatori hanno allargato il proprio scopo nel tempo. Ciò che sono oggi IEEE e il suo corpus di norme è iniziato nel 1880 come organizzazione per gli ingegneri elettrici, la cui missione era la regolamentazione dell'elettricità. IEEE è cresciuta incorporando altri settori e oggi è considerata una delle maggiori e più influenti organizzazioni per le norme tecnologiche al mondo. Allo stesso modo, IEC ha cominciato l'opera di normazione nell'industria elettrica, riservandosi ovviamente di allargare la propria attività nel tempo.

IEC e ONVIF

Dal momento che la richiesta di interoperabilità tra i vari dispositivi sta crescendo, e il concetto di Internet of Things (IoT) sta diventando una realtà, i diversi gruppi di normazione lavorano insieme sempre di più. ONVIF e IEC stanno procedendo lungo questo percorso di collaborazione. Una specifica di ONVIF è stata inclusa nella nuova norma internazionale IEC 62676 per i sistemi di videosorveglianza, la prima norma internazionale su questo tema. Inoltre, la norma IEC 60839 di prossima pubblicazione ha incorporato anche la più recente specifica di ONVIF sul controllo accessi. Questa collaborazione tra organizzazioni per la normazione come ONVIF e IEC potrà proseguire positivamente per sviluppare i più alti livelli di interoperabilità di cui, in conclusione, beneficerà l'utente finale.

Esaminando l'evoluzione delle altre norme, possiamo vedere quanto siano fondamentali per i diversi comparti industriali, spesso partendo da obiettivi relativamente ridotti in uno specifico ambito, per espandersi successivamente in altri che l'accettano, facendo così allargare la platea di utilizzatori. I prossimi passi di ONVIF verranno decisi dagli associati e dalla community della sicurezza fisica che sono insieme alla sua guida, spingendo l'organizzazione dove le nuove tecnologie si sviluppano ed evolvono.

Caduta dei prezzi, attacchi fisici, minacce informatiche: videosorveglianza sotto tiro

a cura della Redazione

Dopo anni di dominio incontrastato della scena della sicurezza da parte della videosorveglianza, con tassi di crescita a due cifre costanti, innovazioni spettacolari presentate a getto continuo e una sempre più diffusa convinzione di onnipotenza del mezzo video per la sicurezza pubblica e privata, si stanno registrando alcuni segnali di "appannamento", che potrebbero preludere a scenari diversi da quelli finora previsti. Riassumiamo i più recenti e importanti:

Rallentamento della crescita: secondo IHS, il mercato globale dei componenti HD e SW dei sistemi di videosorveglianza sarebbe cresciuto solamente dell'1,9% contro il 14,2% dell'anno precedente. Jon Cropley, capo analista settoriale di IHS, ha commentato che la frenata sarebbe dovuta da un lato al forte calo dei prezzi medi dei componenti che, di fatto, ha annullato gli effetti della crescita quantitativa dei pezzi venduti; dall'altro, alla brusca contrazione del mercato interno cinese, che da solo vale il 40% di quello globale, che sarebbe aumentato nel 2015 solo 4,9%, contro il 26,7% nel 2014.

IHS ha subito rivisto al ribasso le stime di crescita del fatturato nei prossimi anni, con un CAGR non più a due cifre costanti come aveva indicato fino a pochi mesi fa, prevedendo inoltre che la filiera dei produttori, stretti tra l'erosione dei margini e la necessità di investimenti continui e crescenti in R&D, dovrà concentrarsi ulteriormente.

Efficacia della videosorveglianza: stanno cominciando a circolare dubbi sull'efficacia della videosorveglianza come "arma assoluta" contro le minacce fisiche.

I più recenti attacchi terroristici a Parigi, Bruxelles e, ultimamente, all'aeroporto di Istambul, confermano che la raccolta e l'elaborazione delle immagini sono indispensabili per l'attività investigativa a posteriori per ricostruire i fatti e individuare i responsabili, ma non sono in grado di impedire che quei fatti avvengano.

L'interdizione di un attacco terroristico con bombe e mitra, così come di una rapina con un taglierino o di un furto con grimaldello, non potrà mai prescindere da barriere in grado di resistere fisicamente a quel tipo di minaccia, anche quando le tecniche di analisi video saranno tanto affinate da riconoscere volti o interpretare gesti in mezzo alla folla. Non a caso stanno crescendo le barriere fisiche "intelligenti", le soluzioni di controllo accessi e i sistemi antintrusione integrabili con la videosorveglianza per la difesa complessiva degli obiettivi.

Minacce informatiche: la sicurezza dei sistemi video nei confronti delle minacce di attacchi informatici sta diventando un tema spinoso per quanto riguarda la tutela dei dati e le minacce combinate (Cyber + Physical). Un interrogativo che accompagna i sistemi di videosorveglianza IP fin dall'inizio del loro sviluppo e che, oggi, è al centro dell'attenzione dei Garanti europei della privacy. Il nuovo Regolamento sulla tutela dei dati (vedi articolo pag. 8) impone al titolare del trattamento dei dati personali di dotarsi di "soluzioni adeguate" per la loro protezione dagli attacchi informatici; di conseguenza, i fornitori dovranno esplicitare le caratteristiche delle soluzioni proposte, per consentire al cliente titolare del trattamento di scegliere consapevolmente la soluzione adeguata.

Iniziamo ad affrontare con **AXIS**, **BOSCH** e **Millestone** quest'ultimo argomento, sul quale si giocherà la reputazione dei produttori in un mercato che probabilmente sarà costretto dalle norme internazionali a guardare con maggiore attenzione alla qualità che al prezzo dei sistemi video.

Quali sono allo stato attuale le possibilità di proteggere le camere per videosorveglianza in rete dai rischi informatici che possano mettere a repentaglio la riservatezza dei dati raccolti sul campo?

Axis (Pietro Tonussi)
Prima di tutto va detto che la Cyber Security è un concetto, non un prodotto. La responsabilità di proteggere la rete, i suoi dispositivi e i servizi che supporta ricade su tutta la catena di approvvigionamento del fornitore, nonché sull'organizzazione dell'utente finale. Essa interessa persone, processi e tecnologie. Non è possibile creare un sistema sicuro al 100%. Almeno non un sistema utilizzabile. E' possibile solamente rendere il sistema più sicuro, riducendo le aree di esposizione e attenuando i rischi. Ci saranno sempre dei rischi che devono essere conosciuti e gestiti. Come ogni produttore di dispositivi in rete, Axis non può fornire garanzie sul fatto che i prodotti, le applicazioni o i servizi di rete non presentino vulnerabilità che possano venire sfruttate per attacchi dannosi, ma ci siamo impegnati a offrire suggerimenti su come ridurre ed eliminare i rischi.

Bosch (Stefano Riboli)
Rispondo facendo riferimento al Cyber Security Framework, introdotto nel febbraio 2014 dal National Institute of Standards and Technology (NIST), un Framework progettato specificamente per ridurre i rischi informatici alle infrastrutture critiche e alla loro rete di dispositivi e dati ad essa collegata. Questo permette di capire i rischi collegati alla sicurezza informatica esterni ed interni all'organizzazione di qualsiasi dimensione, classificandole dal Livello 1 al Livello 4.
Nello specifico, dell'ambito di videosorveglianza si possono indicare 14 punti per migliorare la sicurezza dei dispositivi:
1. Limitare l'accesso alla telecamera tramite la restrizione degli indirizzi IP. Questo può essere fatto tramite IPAM o indirizzamento IP in congiunzione con la subnet;
2. Limitare l'accesso a specifici MAC Address e specifiche porte;
3. Proteggere tramite password: lunghezza tra 8 e 12 caratteri, con maiuscole e minuscole, un carattere speciale e almeno un numero;
4. Assicurare l'accesso via software tramite protocolli minimi, cioè disabilitando quelli non utilizzati;
5. A seconda del livello di sicurezza richiesto dall'installazione, potrebbe essere necessario cambiare le porte HTTP o HTTPS per evitare di fornire informazioni sulle porte standard alle applicazioni di discovery;
6. Disabilitare se non necessario il protocollo Telnet;
7. Impiegare il Telnet tramite "web sockets", con connessione sicura HTTPS;
8. Disabilitare i servizi Cloud se non utilizzati;
9. Se necessario usare il protocollo RTSP per video ONVIF, incapsulandolo su una connessione tunnel HTTPS;
10. Disabilitare il discovery tramite UPnP;
11. Ridurre l'impostazione TTL (salti di rete) così da bloccare accessi da altre reti;
12. Filtrare gli indirizzi IPV4 autorizzati in rete;
13. Autenticazione tramite server RADIUS 802.1x;
14. Se su una rete pubblica, usare reti certificate dalla pubblica autorità per garantire le comunicazioni tra dispositivi autorizzati.

Milestone (Alberto Bruschi)
I sistemi video over IP fanno parte del mondo dell'IT e, come tali, le prime precauzioni sono quelle di realizzare una infrastruttura che segua le specifiche standard di protezione delle reti dati. Ogni prodotto dovrebbe poi avere protezioni specifiche per evitare di essere utilizzati come target o veicolo (malware).

Quale policy avete adottato per tutelare gli utilizzatori finali dai rischi informatici e gli integratori dalle possibili azioni di responsabilità nei loro confronti, qualora i prodotti installati non fossero ragionevolmente sicuri?

Axis (Pietro Tonussi)
Partendo dal concetto espresso prima, la missione di Axis in termini di Sicurezza Informatica è di aiutare le parti interessate a raggiungere un livello di sicurezza accettabile per i sistemi video e a ridurne i relativi costi per la protezione. oltre a fornire i prodotti, le applicazioni e i servizi più sicuri. La definizione di un livello di protezione accettabile dipende dalla situazione, dal livello di minaccia e dal costo di possibili violazioni (analisi di rischio del cliente).
Abbiamo creato una guida dedicata per i nostri clienti, siano essi partner o utenti finali, che intende fornire un supporto su come sfruttare al meglio le features che comunque sono già insite in tutti i prodotti Axis. Essa stabilisce una configurazione di base e una strategia di protezione avanzata per affrontare il panorama delle minacce in continua evoluzione. In tal modo si aumenta il valore delle soluzioni video di Axis per i propri clienti e partner commerciali.

Bosch (Stefano Riboli)
Quando si tratta di dispositivi video IP Bosch, la prima linea di protezione sono i dispositivi IP stessi. Gli encoder e le telecamere Bosch sono costruiti in un ambiente controllato e sicuro che viene continuamente sottoposto ad ispezioni. I dispositivi possono essere scritti solo tramite il firmware certificato Bosch che è costruito per una specifica serie hardware e chipset, non contraffabile. La maggior parte dei dispositivi video IP Bosch sono dotati di un chip di sicurezza integrato che fornisce funzionalità simili a crypto SmartCard e il cosiddetto "Trusted Platform Module" (TPM). Questo chip si comporta come una cassaforte per i dati critici, proteggendo i certificati, chiavi, licenze e l'accesso non autorizzato anche quando la telecamera è aperta fisicamente. I dispositivi video IP Bosch sono stati sottoposti a più di trentamila (30.000) test e della vulnerabilità e di penetrazione effettuati da società di sicurezza indipendenti. Finora, non ci sono stati casi di vulnerabilità in quanto i dispositivi sono adeguatamente protetti.
Inoltre, abbiamo prodotto una guida su come configurare i prodotti così da ridurre i rischi precedentemente indicati.

Milestone (Alberto Bruschi)
Da sempre Milestone implementa tutti i parametri di sicurezza necessari legati al sistema operativo utilizzato. Sistema operativo che deve comunque sempre essere aggiornato e curato da parte del manutentore o dal cliente finale in modo da evitare possibili minacce. Per affrontare ulteriormente questi problemi di sicurezza e dei rischi connessi, Milestone ha inoltre implementato diverse funzioni in aggiunta alle misure standard che possono essere utilizzate per aumentare l'inviolabilità del sistema video generale e delle sue registrazioni.
Milestone XProtect® Corporate e XProtect® Smart Client forniscono una serie di meccanismi di protezione che consentono agli utenti di mantenere la piena sicurezza e l'integrità dei dati video registrati. Crittografia del database, firma digitale e una funzione per impedire la riesportazione del materiale esportato sono alcune delle componenti fondamentali della soluzione di gestione video Milestone per garantire e proteggere l'integrità delle prove video.
Il team di sviluppo Milestone è sempre impegnato a mantenere alto il livello di guardia e, per quanto riguarda le nostre soluzioni, ad implementare le ultime tecnologie in fatto di gestione e protezione dei dati.

Cyber Physical Security, indispensabile l'approccio integrato contro le minacce con vettori multidimensionali

a colloquio con Claudio Ferioli, Intesa SanpaoloGroup Services
a cura di Raffaello Juvara

L'interazione tra sicurezza fisica e sicurezza informatica è diventata il tema dominante nel mondo della sicurezza professionale, stravolgendo i paradigmi in base ai quali erano state costruite le organizzazioni dedicate alla tutela dei beni aziendali. Da cosa deriva in realtà questo cambiamento?

Le competenze specialistiche verticali sono sempre più necessarie nei diversi ambiti della sicurezza, per affrontare rischi e utilizzare tecnologie con una complessità che cresce in modo esponenziale.

Tuttavia, sta emergendo con forza l'esigenza di affiancare alle specializzazioni verticali (sicurezza fisica, sicurezza ICT, ecc.) anche meccanismi di integrazione orizzontali.

Questo cambiamento è imposto dalla realtà: con sempre maggior frequenza, vengono realizzati attacchi con vettori multimensionali: attacchi fisici per infiltrare malware in sistemi informatici; attacchi comportamentali di social engineering per compromettere sistemi informatici e realizzare danni fisici, ecc. Si parla di "Cyber Physical Security" per identificare questa nuova realtà emergente. Possiamo quindi dire che gli *offender* hanno compreso come integrare le competenze fisiche, informatiche e di ingegneria sociale e stanno generando, dal loro punto di vista, forti sinergie tra le diverse componenti.

Il mondo della sicurezza professionale deve reagire conseguentemente, inventando meccanismi snelli di integrazione da affiancare alla crescente e necessaria specializzazione verticale.

Quali sono stati a suo avviso gli episodi più rilevanti a livello globale che hanno fatto comprendere che era avvenuto un cambiamento?

A mio avviso, dal punto di vista simbolico il cambiamento parte dal noto attacco alle centrali iraniane di arricchimento dell'uranio realizzato con stuxnet. Non si tratta del primo attacco condotto con vettori multidimensionali, ma di quello che ha avuto la maggior eco internazionale per gli effetti che ha causato.

Inoltre le modalità con cui è stato realizzato sono paradigmatiche: il sito attaccato, secondo i canoni usuali, era super protetto sia dal punto vista fisico, sia da quello informatico. Nonostante ciò, gli offender sono riusciti ad infettare i sistemi di controllo industriale delle centrifughe con stuxnet (violazione informatica), attraverso un pc o una pen drive – i dettagli non sono noti – di un fornitore (vettore organizzativo e di ingegneria sociale) e, in tal modo,

a distruggere gli impianti (obiettivo fisico).
Negli ultimi anni, la frequenza di attacchi di Cyber Physical Security con vettori multidimensionali è cresciuta rapidamente: nel report dell'ENISA sulle Cyber Threat 2015, pubblicato a gennaio 2016, il vettore Cyber Physical è incluso tra i tre più rilevanti e pericolosi - si tratta di una realtà attuale, non di una previsione.
Anche il settore bancario, cui appartengo, ha subito attacchi di Cyber Physical Security, sinora maggiormente a danno delle banche di altri paesi e meno delle banche italiane. Spesso gli obiettivi sono tradizionali (ad esempio il contante contenuto in un ATM, il caveau), altre volte sono nuovi (ad esempio l'accesso alle procedure della banca): in entrambi i casi vengono usati vettori d'attacco multidimensionali.

Quali sono gli effetti concreti sulle organizzazioni? In che modo devono evolvere per fare fronte a questo nuovo scenario?
L'effetto concreto è l'esigenza di soluzioni per integrare orizzontalmente competenze specialistiche verticali.
La sfida è intrigante: da un lato servono professionalità sempre più verticali, perché la complessità tecnologica cresce continuamente sia negli attacchi, sia nelle soluzioni di protezione; dall'altro, servono meccanismi per integrare e far parlare le diverse specializzazioni. Il "come" è in parte da inventare ed è diverso da organizzazione a organizzazione.
Si possono individuare alcuni step esemplificativi.
Il primo step è l'awareness: è fondamentale che l'esigenza dell'approccio multidimensionale della Cyber Physical Security sia compreso ai livelli decisionali adeguati e venga fatto proprio dagli specialisti della sicurezza. In altri termini, la Cyber Physical Security deve entrare nei "radar" della sicurezza in azienda.
Il secondo livello è quello dell'azione organizzativa: trovare i meccanismi più adeguati per integrare le competenze necessarie per rispondere ai rischi multidimensionali della Cyber Physical Security. La soluzione deve essere declinata in modo specifico in ogni realtà: non esiste l'one best way, la soluzione che va bene per tutti; al contrario ogni organizzazione deve individuare le risposte più adeguate in relazione

al contesto esterno in cui opera ed alle proprie contingenze interne.
Ad esempio, in alcuni casi è stata usata la leva progettuale, creando task force di progetto con competenze specialistiche differenti (sicurezza fisica, informatica, comportamentale, ecc.). Le task force hanno obiettivi concreti, ad esempio riprogettare in ottica di Cyber Physical Security la sicurezza di un asset rilevante.
In altri casi, viene utilizzata la leva della struttura organizzativa, creando un unico responsabile per le diverse specializzazioni verticali. In altri casi ancora, sono state percorse soluzioni differenti.
Infine la Cyber Physical Security deve entrare nel business as usual della sicurezza: per questo, le esperienze progettuali devono tradursi in policy, linee guida e metodologie che permettano, in un certo senso, di industrializzare l'approccio multidimensionale della Cyber Physical Security.

Come deve evolvere di conseguenza la figura del security manager, per poter gestire in modo efficiente/efficace le minacce combinate?
La risposta a questa domanda richiederebbe un intero libro. Mi limito ad evidenziare due aspetti.
Il primo è la collaborazione. Nella realtà, il security manager ha quasi sempre una competenza specialistica, in genere di sicurezza IT o di sicurezza fisica. La prevenzione delle minacce combinate impongono una forte capacità di collaborare, con tutto ciò che questo comporta: capire che si ha bisogno di altre competenze, saper ingaggiare i propri pari, ecc.
Il secondo è l'innovazione. Le minacce combinate richiedono spesso di inventare soluzioni nuove: oggi più che mai, serve capacità di innovare, di creare soluzioni nuove o ricercare soluzioni in ambiti tecnologici non usuali. L'esigenza dell'innovazione richiede, anche a chi fa sicurezza, di riuscire a pensare out of the box, cioè di guardare anche dove non si è mai guardato. Inoltre comporta la "frequentazione" della frontiera tecnologica: occorre intuire cosa si potrebbe fare non solo con i prodotti oggi esistenti nel proprio dominio tecnico, ma anche attingendo ad altri domini e comprendendo i trend di innovazione.

Come imposterebbe un modello divulgativo per i decisori dei Grandi Utilizzatori (banche, amministrazioni pubbliche, IC, grandi industrie) per informarli della necessità di adeguare le proprie organizzazioni ai nuovi scenari, superando le tradizionali separazioni interne tra IT e PhY Security?
Penso che la miglior alleata di un piano di sensibilizzazione sia la realtà. Il racconto dei casi, ormai numerosi in quasi tutti i settori, di attacchi realizzati in modo combinato è l'arma più efficace per far comprendere l'urgenza in cui ci troviamo.
Inoltre, ritengo sia utile la creazione di osservatori, che raccolgano in modo sistematico i casi di attacchi di Cyber Physical Security all'interno di un settore. Un esempio del passato: quando le rapine erano un problema serio per le banche, ABI creò il database dell'Osservatorio per la Sicurezza Fisica (OSSIF), con la raccolta di tutti gli eventi e la descrizione degli aspetti salienti nelle loro dinamiche. Questa base di conoscenza è stata fondamentale nel capire come prevenire le rapine, obiettivo che può dirsi raggiunto. Soprattutto, ha aiutato i security manager a sensibilizzare i vertici delle aziende e ad allocare correttamente le risorse. Penso che l'esperienza si possa ripetere, ovviamente con soluzioni in linea con le sfide attuali.

IFSEC International 2016, l'ultima volta in Europa

a cura della Redazione

Per quanto *understatement* si potesse disporre, è innegabile che il tema dominante di questa edizione siano state le previsioni del voto dei cittadini britannici sulla permanenza in Europa del 23 giugno, ultimo giorno di fiera, più che le novità tecnologiche presentate che, per la verità, non sono state particolarmente rilevanti. I sondaggi della vigilia, fino ai primi *exit poll* la sera del 23, davano in vantaggio il *"Remain"* e i commenti raccolti tra gli operatori erano relativamente sereni. L'esito del voto è stato diverso e IFSEC International 2016 è stata l'ultima edizione "europea" della fiera che per decenni ha rappresentato la vetrina dell'industria mondiale della sicurezza verso il mercato continentale. La nuova situazione geopolitica non potrà non avere effetti sul futuro di IFSEC, con una presumibile accelerazione della tendenza, già avviata da qualche anno, di progressiva "regionalizzazione" della fiera londinese, presumibilmente a vantaggio di Security Essen.

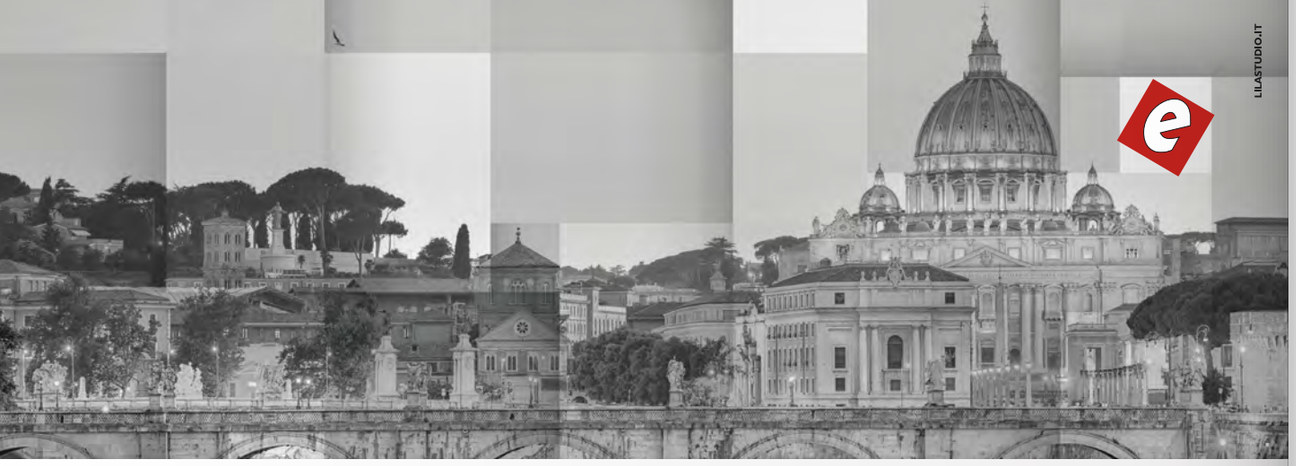
Tornando ai contenuti tecnologici, questa edizione di IFSEC International parrebbe aver riportato al centro dell'attenzione i sistemi antintrusione, le barriere fisiche e il controllo accessi per la protezione degli edifici e delle aree riservate, dopo anni di dominio incontrastato della scena del mercato della sicurezza da parte della videosorveglianza in ogni sua componente.

Molteplici le spiegazioni di questa nuova situazione, che trova conferma anche nell'accelerazione nel processo di integrazione tra produttori video, antintrusione e controllo accessi.

Da una parte, i più recenti episodi di terrorismo in Europa hanno evidenziato quanto sia importante la difesa fisica degli obiettivi sensibili; dall'altra, la stessa crescita delle prestazioni della videosorveglianza, in termini di definizione delle immagini e di capacità di interpretazione dei dati, suggerisce impieghi sempre più ampi nell'intelligence pre-post evento, piuttosto che di interdizione dello stesso.

Si aggiunge a questo il crollo dei prezzi nel 2015 dei componenti hardware e software dei sistemi video, come ha riportato **IHS (leggi)**, che potrebbe aver indotto i grandi produttori globali a spostare gli investimenti verso ambiti che, almeno per il momento, sembrano offrire maggiori opportunità di crescita e di fidelizzazione dei clienti.

Complessivamente soddisfatti gli espositori italiani presenti a IFSEC 2016, che hanno trovato notevole interesse per i prodotti presentati tra gli operatori del mercato britannico.



LE ECCELLENZE PER LA SICUREZZA 2016

13 Ottobre 2016 | Palazzo Rospigliosi Pallavicini, Roma

"UNA CITTÀ NON È SMART SE NON È PROTETTA E SICURA"
seminario a inviti

- **MODELLI, STANDARD E SOLUZIONI PER LA CITTÀ SICURA**
- **PUBBLICO E PRIVATO, LA VIRTUOSA COLLABORAZIONE PER LA SICUREZZA DEL CITTADINO**
- **LE ECCELLENZE PER LA SICUREZZA DEGLI OBIETTIVI SENSIBILI: INFRASTRUTTURE CRITICHE E CITTÀ SICURA – SECURITY FOR RETAIL**
- **REGOLAMENTO EUROPEO PER LA TUTELA DEI DATI: LE RESPONSABILITÀ DEL TITOLARE DEL TRATTAMENTO E DEI FORNITORI DI SISTEMI DI SICUREZZA**

L'appuntamento esclusivo 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

PER INFORMAZIONI SULLE MODALITÀ DI PARTECIPAZIONE: MARKETING@SECURINDEX.COM

Le Eccellenze per la Sicurezza 2016, le migliori soluzioni per i grandi mercati verticali

a cura della Redazione

Nel rispetto del concept sviluppato all'inizio del progetto, programma e partnership dell'edizione 2016 delle E**ccellenze per la Sicurezza** sono stati definiti con largo anticipo sulla data fissata del 13 ottobre, per poter invitare gli ospiti indicati dai partner e consentire ai relatori di preparare opportunamente gli interventi. Rispondendo al criterio di alternanza con Milano, dove si è tenuta l'edizione 2015, la scelta della sede di Roma nel prestigioso **Palazzo Rospigliosi Pallavicini** di fronte al Quirinale, favorisce la partecipazione delle istituzioni con sede nella Capitale come Autorità di riferimento degli argomenti che verranno trattati nel seminario. Sono stati invitati la Polizia di Stato, l'Associazione Nazionale Comuni d'Italia e l'Autorità Garante dei Dati Personali per trattare argomenti di primaria importanza per l'industria della sicurezza quali:

- I modelli di partecipazione tra pubblico e privato per la sicurezza delle città nell'era del terrorismo

- L'integrazione tra sicurezza fisica e sicurezza informatica per la tutela dei dati e le responsabilità dei fornitori di sistemi.

In parallelo, le soluzioni che i partner presenteranno in questa edizione saranno rivolte ai grandi utilizzatori pubblici e privati di sicurezza, potendo usufruire della possibilità di rapporti esclusivi con la partecipazione alle singole sessioni di lavoro di una sola azienda per ambito tematico. I partner sono stati invitati in base all'eccellenza tecnologica e organizzativa conquistata nel rispettivo ambito operativo, che potranno illustrare nella sessione del seminario più adatta.

L'agenda del seminario sarà suddivisa in tre sessioni distinte, ma legate da un filo conduttore unico: **la ricerca delle soluzioni migliori per sicurezza del cittadino.**

La sessione di apertura sarà intitolata **Modelli, standard e soluzioni per la Città Sicura** ed avrà come special guest **Enzo Peduzzi**, presidente di **Euralarm**, l'associazione europea dei costruttori di sistemi e fornitori di servizi per la sicurezza e l'antincendio impegnata nei rapporti con la UE per lo sviluppo di norme comunitarie per innalzare il livello di sicurezza dei cittadini europei. In questo ambito, Euralarm ha affrontato l'argomento dei modelli di riferimento di Smart City e Safe City, ponendosi l'obiettivo di sviluppare una norma europea per offrire alle amministrazioni cittadine un benchmark al quale riferirsi nel momento in cui dovranno implementare soluzioni specifiche.

Seguiranno interventi dei partner che illustreranno applicazioni tecnologiche e operative per concretizzare il modello di Città Sicura, favorendo l'integrazione tra pubblico e privato per garantire la sicurezza ai cittadini.

Dopo l'intervento del rappresentante della Polizia di Stato e una testimonianza eccellente di integrazione tra pubblico e privato per la tutela del patrimonio artistico nazionale, una tavola rotonda affronterà il tema della sicurezza delle Città dal punto di vista degli amministratori locali, per individuare le soluzioni più efficaci e sostenibili, con il contributo dei fornitori maggiormente focalizzati sull'argomento.

La seconda sessione all'inizio del pomeriggio, dedicata a **Le eccellenze per la sicurezza degli obiettivi sensibili**, sarà suddivisa in due parti. Nella prima, **Infrastrutture Critiche e Città Sicura**, verranno presentate soluzioni innovative di integrazione tra barriere fisiche, sensori intelligenti e videosorveglianza per la protezione di obiettivi sensibili come ambasciate, aree monumentali, musei, aeroporti, centri commerciali. Nella seconda, **Security for Retail**, verranno esaminate con la partecipazione di security manager di gruppi internazionali del retail soluzioni innovative ai fini di loss prevention, in particolare l'analisi video e i software predittivi.

La terza sessione conclusiva interesserà tutti gli operatori del settore, fornitori e utilizzatori di sistemi di sicurezza. Con l'intervento di un rappresentante del Garante, verranno illustrate le novità introdotte dal **Regolamento Europeo per la tutela dei dati**, pubblicato il 25 maggio scorso e che dovrà essere attuato entro due anni. Verrà esaminato in particolare, con la partecipazione di legali specializzati, l'art. 32 del Regolamento, che impone al titolare del trattamento dei dati personali di terzi di adottare "soluzioni idonee" alla tutela dei dati da attacchi esterni, con le conseguenti responsabilità dei fornitori di sistemi che acquisiscono, elaborano e conservano dati di terzi come, ad esempio, videosorveglianza e lettori biometrici.

Le Eccellenze per la sicurezza 2016 è un evento unico nel panorama degli eventi di settore per offrire ai decisori e ai responsabili della sicurezza della grande utenza pubblica e privata momenti di approfondimento sugli argomenti di maggiore attualità e importanza per le organizzazioni di cui sono responsabili, con l'intervento di rappresentanti delle istituzioni di riferimento e la partecipazione di esperti di valenza internazionale e di produttori di soluzioni e servizi di riconosciuta eccellenza nel rispettivo settore di appartenenza.

Per maggiori informazioni e richieste di invito scrivere a:
marketing@securindex.com
eventi@securindex.com

TSec, overview e risposte concrete alle esigenze di sicurezza integrata

a colloquio con Luca Salgarelli, presidente TSec
a cura di Raffaello Juvara

TSec e "Le Eccellenze per la Sicurezza", una collaborazione iniziata nella prima edizione del seminario nel 2015 dedicato ai decisori per la sicurezza dei Grandi Utilizzatori, che presuppone la condivisione della visione che ha ispirato il progetto: un momento esclusivo di incontro e di confronto tra chi progetta e sviluppa soluzioni di sicurezza ai massimi livelli e chi le utilizza, per individuare le linee guida del futuro del settore, anche dirompendo gli schemi consolidati. Quali provocazioni lancerà TSec nella prossima edizione del seminario?
Nessuna, perbacco! "Le Eccellenze per la Sicurezza" nasce come momento di incontro tra chi crea tecnologie per la sicurezza, i produttori, e chi queste tecnologie le usa per soddisfare un bisogno, ovvero i security manager, gli integratori e i decisori. In questo ambito, TSec nel passato come nel presente sta cercando di guardare a noi stessi ed al mercato della sicurezza con un occhio critico. Credo che la nostra giovane età (industrialmente parlando, s'intende) e la passione che ci guida ce lo permettano. Questo essere critici con noi stessi e con il nostro mercato, costruttivamente, ci porta qualche volta a fare analisi che possono sembrare provocazioni, ma non vogliono assolutamente esserlo. Gli spunti che ci guidano derivano da una visione della tecnologia per la sicurezza che crediamo debba necessariamente contaminarsi con la rapida evoluzione dei settori a noi vicini, innanzitutto quello dell'IoT, e cercare di investire il più rapidamente possibile in nuovi sistemi, nuove tecnologie e nuovi approcci alla sicurezza. Perché questo processo abbia successo, è però necessario slegarsi dall'approccio iper-frammentario e di contrapposizione tra concorrenti che il nostro settore (insieme ad altri) ha perseguito fino ad oggi. È invece utile guardare agli investimenti in nuove tecnologie attraverso la lente dell'open *innovation*,

unendo capitali, conoscenze e strategie per innovare insieme, a livello di sistema. Io non penso che questa sia una provocazione, ma una necessità pressante se il settore della sicurezza vuole tornare a contare sia sul piano nazionale che su quello internazionale, non crede?

Uno dei leitmotiv del momento è la "scoperta" della vulnerabilità dei devices per la sicurezza fisica rispetto alle minacce informatiche, conseguente in particolare alla diffusione delle tecnologie IoT. Qual è il vostro punto di vista in merito?
Purtroppo la diffusione sempre più capillare di dispositivi "*always on, always connected*" sta portando alla superficie un problema finora dormiente: la sicurezza nelle comunicazioni. Finché si trattava di gestire la sicurezza di computer, la tecnologia ci ha aiutato, almeno in qualche modo: a livello professionale con architetture di rete, sistemi di *firewalling* e di antivirus tutto sommato efficaci; a livello consumer un po' meno, ma, con gli anni, anche gli utenti meno professionali hanno imparato a cavarsela. Il processo in corso sta portando lo stesso livello di connettività IP fino a ieri riservato ai computer, anche alla miriade di dispositivi che rendono "intelligenti" gli edifici, gli spazi di lavoro e le città, dai termostati alle telecamere, dagli apriporta ai sistemi di condizionamento dell'aria fino ad arrivare ai semafori e ai sistemi di illuminazione cittadina. In virtù di questo processo, immediatamente si moltiplicano i vettori di possibile attacco, e contemporaneamente le ricompense per gli attaccanti diventano più allettanti: con un attacco di successo, diventa infatti possibile monitorare e condizionare in maniera capillare non più solo i nostri computer, ma la nostra vita quotidiana. Credo sia necessario pensare ad una infrastruttura di sicurezza informatica e delle telecomunicazioni nuova, progettata esplicitamente per il mondo IoT che sta arrivando. Ad ogni processore (CPU), sia esso in un termostato, in uno smartphone o in una centrale d'allarme, è necessario affiancare un processore dedicato alla sicurezza e, in particolare, alla comunicazione sicura. Sono dell'opinione che solo con una nuova architettura basata su sistemi hardware dedicati alla sicurezza si possa scongiurare quello che potrebbe essere un vero e proprio disastro informatico, e che altrimenti rischiamo di subire a causa dell'introduzione capillare di dispositivi connessi. Purtroppo, un disastro tecnologico di tale portata porterebbe con se' anche ricadute economiche molto significative, che non ci possiamo permettere, specialmente in questo momento storico.

Aumenta la richiesta a livello globale di "protezioni perimetrali intelligenti" dalle abitazioni private agli obiettivi sensibili, con soluzioni che integrano rilevamento, immagini, analisi dei dati, sistemi di risposta. Quali sono le proposte di TSec?
Nei prossimi mesi presenteremo due soluzioni perimetrali esterne basate su tecnologie che stiamo sviluppando da tempo: la prima si basa su concetti di *signal processing* evoluto, applicati all'analisi delle vibrazioni; la seconda su sistemi radar avanzati. In entrambi i casi, i sistemi permetteranno di rilevare con precisione luoghi e tipologie di effrazione perimetrale, minimizzando contemporaneamente i falsi allarmi. Entrambe le soluzioni sono state ingegnerizzate non per funzionare isolate da altri sistemi di protezione, in primo luogo la video sorveglianza e la video analisi, bensì per divenirne strumenti di supporto, in grado di coadiuvare la loro funzione e, allo stesso tempo, di moltiplicarne l'utilità. Anche qui, come in quello dell'open *innovation* citato sopra, crediamo che l'unione, in questo caso di sistemi tecnologici diversi anche provenienti da produttori diversi, faccia la forza.

Quali sono gli altri ambiti ai quali il vostro Gruppo si sta dedicando?
TSec non è un gruppo industriale propriamente definito, ed è focalizzata in maniera estremamente verticale sul mercato della sicurezza fisica, quindi non ci dedichiamo esplicitamente ad ambiti diversi da quello delle tecnologie per la sicurezza. È però vero che collaboriamo in maniera molto stretta con una serie di aziende, alcune delle quali nostre socie, che ci permettono da un lato di "contaminare" i nostri prodotti con esigenze, tecnologie e funzionalità che provengono da altri settori industriali, come quello dell'automazione; dall'altro, di lavorare insieme a nuove piattaforme tecnologiche come, ad esempio, quelle legate alla sicurezza delle telecomunicazioni, condividendo esperienze, costi, rischi e benefici. In questo senso, non ci stiamo dedicando ad altri ambiti, ma lavoriamo a stretto contatto con aziende, piccole e grandi, che lavorano in diversi settori tecnologici, dalla building automation, alla safety industriale, al medicale per finire con il mondo dei servizi informativi.

Come si articolano e si integrano, dal vostro punto di vista, i concetti di "Sicurezza" e di "Intelligenza" della Casa, dell'Edificio, della Città?
Credo che vedremo una rapida evoluzione di questi sistemi in due direzioni. Da un lato, ci sarà un processo di veloce integrazione dei sistemi di building/campus/city automation con quelli che ne gestiscono la sicurezza. Dall'altro, tutte le piattaforme tecnologiche per la sicurezza dovranno evolvere per orientarsi sempre più all'erogazione dei servizi. Queste due forze di cambiamento sono già in atto, parte di un processo di evoluzione che non solo è inarrestabile, ma si sta velocizzando sempre più. Stiamo vedendo l'alba di quella che molti definiscono come la prossima rivoluzione industriale: sulle fondamenta dell'ultima rivoluzione che abbiamo vissuto, quella di Internet, stiamo per costruire il prossimo strato tecnologico che guiderà il progresso nel prossimo decennio. L'integrazione di funzioni diverse su questo strato, nello specifico la sicurezza, l'intelligenza e l'automazione, aprono opportunità davvero strabilianti, sia per i produttori, che per gli utilizzatori di queste tecnologie. Sta a noi tutti fare in modo che le opportunità non si trasformino in problemi, e qui faccio riferimento al problema della sicurezza delle comunicazioni citata poco fa, e che gli attori del mercato si muovano a livello di sistema per guidare questo processo di integrazione, anziché subirlo.

Dove va il mercato globale della sicurezza? Intervista a Joe Grillo, CEO di Vanderbilt

a colloquio con Joe Grillo, CEO di Vanderbilt
a cura di Raffaello Juvara

Mr. Grillo, iniziamo l'intervista al leader della classifica annuale redatta da IFSEC sulle persone più influenti nel mercato globale della sicurezza, chiedendole di tracciare un bilancio operativo del primo anno del progetto Vanderbilt.

Nel corso di questo anno, il nostro obiettivo primario è stato la transizione del marchio da Siemens a Vanderbilt, e abbiamo investito una grande quantità di denaro per promuovere il nuovo marchio e analizzare gli indicatori nei mercati chiave in cui operiamo, per verificare il mantenimento con successo della nostra quota di mercato.

I risultati sono stati finora molto incoraggianti. Ad esempio, nel mercato tedesco, che pensavamo sarebbe stato il più colpito dall'allontanamento dal marchio Siemens, abbiamo invece registrato una crescita del business. Lo stesso vale per la Francia. Sono pertanto lieto che in due dei nostri principali mercati stiamo assistendo a un alto grado di accettazione del marchio Vanderbilt, e che la fedeltà dei nostri clienti sia rimasta immutata.

In sintesi, la nostra strategia si è basata sulla costruzione del marchio, sulla promozione dei prodotti, valutando come spingere i marchi per introdurre nuovi prodotti nel corso dei successivi 12 mesi, continuando nel frattempo a monitorare il mercato. Ma non dobbiamo abbassare la guardia. Una delle principali aree di investimento per quest'anno è la partecipazione a eventi di settore praticamente in ogni mercato in cui operiamo - Polonia, Spagna, Danimarca, Norvegia, Italia, Spagna, Regno Unito, Germania e Svezia - ed è sempre utile incontrare i clienti di persona.

Quali sono i programmi di Vanderbilt in termini di prodotti e strategie per i prossimi mesi?

Vanderbilt è radicata nel controllo accessi attraverso i suoi legami storici con Mercury negli Stati Uniti e Bewator in Europa (tramite l'acquisizione Siemens). Tuttavia il nostro portafoglio prodotti è ben più ampio - come abbiamo dimostrato a IFSEC a Londra, a giugno. Per quanto riguarda il controllo accessi, abbiamo offerto un'anteprima di **Aliro 2.0**, basato sul notevole successo di Aliro, lanciato 18 mesi fa in Europa. Questa nuova generazione sarà caratterizzata dall'integrazione con **Aperio** e da altre entusiasmanti innovazioni, e

affiancherà la nostra gamma di lettori di carte VR, che hanno già incontrato il favore del mercato. Il principio fondamentale che abbiamo adottato nel settore controllo accessi è garantire sempre ai clienti un percorso di migrazione che consenta loro di non dover ripartire da zero, restando sempre al fianco dei nostri integratori per assisterli in tutte le fasi.
La nostra strategia video è chiara. A IFSEC abbiamo presentato la gamma di prodotti **Eventys**, rilanciando un nome utilizzato dall'azienda in passato per presentare la nostra nuova gamma di telecamere e videoregistratori accessibili.
Per il settore intrusione abbiamo dimostrato il portale **SPC Connect**, un interessante sviluppo per i nostri clienti che possiedono già o prevedono di installare gruppi di centrali SPC dislocate in diverse postazioni. Il portale infatti facilita la gestione in cloud di più centrali. Ad esempio un installatore con 5000 centrali, dislocate presso svariati clienti, potrà gestirle e controllarle facilmente in un ambiente sicuro senza necessità di abilitare il port forwarding. Il risparmio di tempo e denaro che questo portale offre ai nostri clienti è enorme, perché consente loro di verificare in remoto lo stato di ogni singola centrale per meglio gestire le priorità degli interventi di assistenza.

Successivamente all'acquisizione di Siemens SP da parte di Vanderbilt, il mercato ha assistito a numerose altre fusioni e acquisizioni globali, a dimostrazione della tendenza verso l'integrazione tra videosorveglianza e rilevazione intrusioni (l'ultima, Hikvision e Pyronix) da un lato, e tra servizi e tecnologie (Johnson Controls e Tyco) dall'altro. Da player globale nel campo della sicurezza, Vanderbilt come valuta questo scenario? Vanderbilt sarà protagonista di altre fusioni e acquisizioni nel prossimo futuro?
Negli ultimi 12 mesi abbiamo assistito a un grande fermento nelle operazioni di fusione e acquisizione. A mio parere, disponendo di risorse sufficienti, chiunque può dominare qualsiasi mercato.
Tuttavia, il problema in questa strategia è che l'entità degli investimenti rende difficile raggiungere un solido rendimento finanziario. Esiste anche l'ulteriore rischio dell'abbattimento del prezzo di mercato, poiché se un'azienda sceglie di comprarsi il dominio sul mercato, il prodotto potrebbe venire irrimediabilmente svalutato! E questo fenomeno si sta già manifestando in alcuni settori, particolarmente in quello video.
Anche la confusione nei canali di mercato genera un problema. I produttori iniziano a fornire prodotti non solo ai propri integratori e distributori, ma anche direttamente all'utente finale, con un fortissimo rischio di conflitto tra canali, situazione difficile da gestire in modo efficace.
In una prospettiva più ampia, ritengo che, in particolare in Europa, il mercato sia ancora frammentato, e che nessuna azienda abbia il predominio su una specifica area di prodotto. In generale, i nostri principali concorrenti sono presenti in tutti i mercati internazionali, ma è improbabile che possano dominarne alcuno. Le aziende concorrenti internazionali specializzate in una singola area di prodotto si impegneranno in tutti i principali mercati, ma, ancora, anche per loro raggiungere il predominio sarà improbabile. Vi sono poi i concorrenti locali, che saranno presenti in uno o due mercati, ma anche in questo caso non li potranno dominare, pur raggiungendo solide quote di mercato.
Trovo che la fusione di Tyco/Johnson Controls sia particolarmente interessante, poiché sulla carta si tratta di una fusione di un'azienda di produzione con un fornitore di soluzioni - ma in realtà entrambe operano nel settore soluzioni. Vi è dunque un punto critico in cui è necessaria un'azione volta ad evitare lo spreco di denaro che deriva dalla concorrenza tra due aziende, e chiaramente Tyco/Johnson Controls hanno individuato sufficienti sinergie per giustificare la fusione dei due colossi. Tuttavia, chiunque abbia esperienza di fusione tra due aziende complesse, sa che il grado di turbativa può essere considerevole.
Sarà interessante osservare l'impatto che questo avrà sul settore, poiché la gestione di aziende di tali dimensioni presenta costi enormi e ciò impatterà la capacità di attirare e supportare i clienti.
Nel caso di Vanderbilt, è nostra intenzione consolidare il business in Europa e integrarlo con il nostro business globale, non escludendo in questo processo possibili acquisizioni, in particolare quelle in grado di aiutarci a raggiungere i nostri obiettivi di crescita.

La convergenza della sicurezza fisica e della sicurezza IT è l'argomento più importante nell'evoluzione tecnologica scaturita sull'onda di IoT, con la crescente attenzione verso la protezione dei dati personali raccolti dai dispositivi e dai sistemi di rete, in particolare per le soluzioni di storage in cloud. Cosa ne pensa di questo argomento, inclusa la sicurezza degli utenti intermedi e finali?
A mio avviso la forma più pura di IoT, basata su sistemi autonomi che operano con un intervento umano minimo, è ancora lontana nel tempo, e il concetto intrinseco di sicurezza richiede spesso l'intervento umano per una gestione efficace. Finora non abbiamo sicuramente visto un elevato livello di autonomia IoT nel mercato principale delle tecnologie di sicurezza. L'introduzione dell'IP nei prodotti di sicurezza ha avuto un forte impatto in tutti i portfolio del settore. Tuttavia, ritengo che dovremo ancora attendere l'introduzione di prodotti IoT commerciali nel settore sicurezza.
Detto questo, è questione di tempo - certamente per il controllo accessi e la rilevazione di intrusioni - e prevedo che l'analisi video avanzata possa contribuire in modo similare e fornire un grado di autonomia ai sistemi di monitoraggio video.
In Vanderbilt diamo grande importanza alla sicurezza dei dati - come dimostra il nostro SPC Connect. I dati richiesti per la manutenzione e la gestione delle centrali intrusione archiviati nel cloud di SPC Connect sono protetti secondo requisiti definiti per gli istituti finanziari, e gli algoritmi che utilizziamo sono progettati per soddisfare tali specifiche.
Siamo dunque fiduciosi - ma non seduti sugli allori - di poter fornire ai nostri clienti un livello di sicurezza adeguato al livello di dati che conserviamo per loro conto.

VANDERBILT

Premio H d'oro 2016: nascono gli H d'oro Point

a cura della Redazione

Prosegue la raccolta delle candidature per partecipare al Premio H d'oro 2016 e la Fondazione Enzo Hruby annuncia la prima novità di questa undicesima edizione: nascono gli H d'oro Point, ovvero spazi dedicati al Premio presso le sedi di diversi operatori della sicurezza. Qui gli installatori possono ricevere tutte le informazioni sul concorso e consegnare le proprie candidature.
La decisione di creare dei veri e propri spazi dedicati al Premio H d'oro è nata dopo il successo che ha avuto lo scorso anno il coinvolgimento di alcuni distributori locali, i quali si sono fatti promotori dell'iniziativa della Fondazione Hruby e hanno contribuito ulteriormente a diffonderne la conoscenza e il valore.
Ricordiamo agli installatori che la partecipazione al Premio H d'oro è totalmente gratuita e che per iscriversi basta compilare il modulo presente presso gli H d'oro Point o scaricabile dal sito **www.fondazionehruby.org**, che va riconsegnato entro il prossimo 31 luglio presso i punti di raccolta o all'indirizzo mail **candidature@accadoro.it**, o via fax allo 02.38036629. Tutti i professionisti della sicurezza sono invitati a cogliere questa straordinaria occasione per valorizzare la propria competenza e ottenere un riconoscimento ufficiale di grande prestigio.

Gli H d'oro Point sono attualmente presenti presso:

3P ELETTRONICA srl
Modugno (BA) - Tel. 080/5560600

ABES srl
Torino - Tel. 011/2290703

CIBF srl
Napoli - Tel. 081/7349175

CM INTERNATIONAL sas
Loc. Fontanelle (PO) - Tel. 0574/636861

DI.ERRE srl
Arese (MI) - Tel. 02/9382011

HESA S.p.A.
Milano, Firenze, Roma - Tel. 02/380361

LB SECURITY srl
Silvi (TE) - Tel. 0871/565448

MAC SYSTEM sas
Gruaro (PD) - Tel. 0421/74106

TROLESE srl
Padova - Tel. 049/8641940

Le aziende interessate a diventare anch'esse partner dell'undicesima edizione del Premio H d'oro possono mettersi in contatto con la Segreteria Organizzativa del concorso telefonando allo 02.38036625.

Illuminotronica 2016, le competenze professionali per un nuovo mercato in crescita

a cura della Redazione

Un progetto di formazione capace di fornire all'installatore le competenze professionali indispensabili per diventare un vero esperto di domotica, per potere così sfruttare concretamente le opportunità di un settore che cresce a ritmi molto elevati. È SmartPro, nato dal progetto BRICKS per il patentino europeo dell'installatore e dalla collaborazione tra Smart Hut ed Enea. A Illuminotronica (PadovaFiere, 6-8 ottobre) sarà possibile seguire i primi corsi per installatori e professionisti del settore.

Integrazione di sistemi, luce, domotica, sicurezza, spazi pubblici e privati. La natura pervasiva dell'elettronica giustifica il focus sulla convergenza digitale delle tecnologie per la **smart home**. Proprio la domotica nelle sue implicazioni sociali, economiche, tecnologiche e nei suoi percorsi integrati con la sicurezza, rappresenta oggi in Italia una delle maggiori sfide per i professionisti. Installatori, impiantisti, system integrator, architetti, ingegneri, sono tutte figure coinvolte, a vari livelli, in questa espansione delle soluzioni intelligenti, enorme potenziale di business per il mercato italiano, considerando le spinte alla riqualificazione degli edifici obsoleti, gli incentivi fiscali legati al loro efficientamento energetico (vedi Ecobonus 2016) e la crescente richiesta di sicurezza. Un potenziale che, per diventare concreto, passa attraverso un'adeguata formazione e la creazione di network a supporto di professionisti e aziende.

In questa prospettiva opera il progetto **Smart Hut**, che, dopo aver portato le tecnologie per l'home automation in tour per l'Italia, con i roadshow della domotica e le partnership con le principali associazioni di categoria, approda alla fiera **Illuminotronica** (Padova, 6-8 ottobre) con un percorso formativo efficace e qualificante.

Cambiano le tecnologie, cambiano le professioni

I progetti di home automation, soprattutto se inseriti in progetti per la riqualificazione degli edifici obsolescenti, appaiono come un puzzle in cui le tessere vanno perfettamente incastrate, partendo dalle esigenze e dai costi stimati del cliente, per trovare una soluzione condivisa alle varie aree dell'impianto e problematiche. Il quadro iniziale, composto da impianto domotico (scenari, luce, energia, sicurezza, clima, serramenti, calendario, impianti tecnologici); tecnologie per la sicurezza (IoT, allarme, telecamere, video citofonia, telefonia, audio/video) e dispositivi di interconnessione (comando vocale, NFC, Android, iOS, Pc/Mac ecc.), obbliga installatori e progettisti a prestare attenzione ai rischi e alle sorprese legate a questo puzzle da incastrare e fare funzionare correttamente. Il vero esperto di domotica non può più ragionare a compartimenti stagni: ogni elemento dell'impianto deve nascere pensando alla sua connessione e integrazione nel sistema-casa.

Da installatore a Smart Pro…

Questo cambio di mentalità deve necessariamente essere supportato da una adeguata preparazione dei professionisti, che devono fare proprie sia competenze tecniche sia normative e di marketing per moltiplicare le opportunità e per poter scegliere e installare i prodotti giusti al momento giusto, venendo incontro alle richieste sempre più consapevoli dei clienti finali. Su queste direttrici si muove il progetto **Smart Hut**, che, grazie alla partnership con **ENEA** e all'interno del **progetto BRICKS**, si impegna a promuovere e valorizzare le competenze dei professionisti della domotica attraverso la formazione e l'aggiornamento professionale, per far sì che vengano riconosciute le specifiche competenze "evolute". Il primo passo è quello di creare un network (registrazione gratuita su **pro.smarthut.it**) dove ogni installatore **Smart Pro** può essere trovato e contattato in modo efficace nel proprio territorio di appartenenza.

… con il patentino europeo

Il secondo step del progetto Smart Hut prevede, per i professionisti registrati al network, la fase formativa, con percorsi promossi dalle aziende partner e da

esperti di domotica, per il conseguimento di una **certificazione dal valore internazionale**. Questo percorso, dedicato agli oltre tre milioni di professionisti che a vario titolo e con varie competenze hanno a che vedere con il sistema-casa, partirà con i primi moduli già a **Illuminotronica** (PadovaFiere, 6-8 ottobre), dove Smart Hut sarà presente, nel **padiglione 5**, con una vera e propria Casa Domotica, sotto il coordinamento tecnico di **KNX** e in collaborazione con CasaClima, luogo dove toccare con mano e vivere la domotica, con aree demo, laboratori e corsi abilitanti al conseguimento della certificazione di Smart Pro.

Resta aggiornato su **www.illuminotronica.it** o chiedi maggiori informazioni alla segreteria scrivendo a **hut@assodel.it**

Un programma ricco di contenuti

Accanto a esposizione e iniziative speciali, Illuminotronica propone una serie di corsi, dibattiti e convegni focalizzati sul tema dello smart lighting e non solo… Inoltre, la sinergia con gli enti e le associazioni del territorio, abiliterà i partecipanti al conseguimento di crediti formativi professionali.

Tra gli appuntamenti in programma:

Giovedì 6 ottobre – ore 10.00

Smart Lighting tra luce, benessere e sicurezza

Tecnologie e architetture innovative per sistemi di illuminazione a LED più "intelligenti" e capaci di migliorare l'efficienza e stimolare l'integrazione di altri sistemi, in casa come in città

Giovedì 6 ottobre – ore 11.30

Smart home, smart city… smart opportunities. La riqualificazione come strategia per una crescita di sistema*

Idee e proposte per una riqualificazione intelligente e sostenibile dei centri storici

Giovedì 6 ottobre – ore 14.30

Il modello Smart city tra soluzioni di luce intelligente e nuovi servizi per il cittadino

Finanziamenti, opportunità e nuove tecnologie per le città del futuro

Venerdi 7 ottobre - ore 10.00

Parola d'ordine: integrare! La domotica del visibile tra luce, benessere e sicurezza*

Opportunità e soluzioni per l'integrazione delle tecnologie per la smart home

Venerdi 7 ottobre - ore 11.30

Illuminazione a LED: i Top Trend 2016

Le ultime tecnologie alla base dei sistemi a LED. CRI, CCT (temperatura colore), luminosità/efficienza, adattabilità della luce sono solo alcune delle tematiche affrontate

Venerdi 7 ottobre - Ore 14.30

Human Centric Lighting: sistemi di illuminazione intelligente possono migliorare la qualità della vita delle persone?

L'uomo è al centro della luce

Venerdi 7 ottobre - Ore 16.30

Premio Codega 2016: anticipazioni

Sabato 8 ottobre - Ore 10.00

Una nuova professione per un nuovo mercato: lo smart pro e le opportunità dell'integrazione*

Un progetto europeo per i nuovi professionisti della smart home

convegni che prevedono crediti per i periti industriali. Tutti gli aggiornamenti in merito su* ***www.illuminotronica.it*

Dab Centro Operativo, la soluzione di Vigilanza Tecnologica Avanzata

a colloquio con Guido Congiu, SM di DAB Centro Operativo
a cura della Redazione

Parliamo di DABco. Ci parli della storia e dell'offerta di DAB Centro Operativo.

DAB Centro Operativo (DABco) è l'Azienda del Gruppo DAB specializzata nei servizi di Monitoraggio e Vigilanza Tecnologica, Supervisione di Sistemi Integrati e Coordinamento delle Attività Operative di Security, Safety e Controllo Tecnologico. Gruppo DAB, con la propria expertise in tecnologia e soluzioni è stato il contesto di nascita e crescita ideale per il nuovo modello di Sicurezza che DABco, società autorizzata ai sensi dell'art.134 del TULPS, promuove per il nuovo approccio multifunzionale e interdisciplinare alla sicurezza.

Il Gruppo, presente su tutto il territorio nazionale, si è dotato di un Centro Operativo di Controllo, Supervisione e Coordinamento H24 composto da operatori abilitati e qualificati, che fornisce un insieme di servizi di security management attraverso una piattaforma di supervisione evoluta, aperta e scalabile che si pone come assoluta novità nel panorama dei servizi.

DABco si propone come un Security Center per i Clienti e Partner che devono completare la propria e personale soluzione di tutela del patrimonio e degli asset aziendali e privati con i sistemi più avanzati che un centro di Controllo evoluto possa avere.

Il Centro Operativo monitora e centralizza i sistemi di Sicurezza e Controllo Tecnologico installati presso

i Clienti, riceve e gestisce le segnalazioni secondo procedure operative personalizzate e condivise e coordina le attività di intervento presso i siti con la finalità di ottimizzare in termini di efficacia ed efficienza. Contribuisce costantemente alla verifica del corretto funzionamento degli impianti supervisionati, a tutela degli investimenti effettuati. E quando parliamo di impianti, ci riferiamo a una miriade infinita di possibilità. Dai più basilari sistemi antifurto fino alla complessità di sistemi SCADA passando per la puntuale verifica di sistemi antincendio in monitoraggio real time.

Mi piace parlare di una "Nuova fase della Vigilanza" ovvero un nuovo concetto di servizio di sicurezza che da tradizionale istituto di vigilanza si evolve in Centro di Controllo e Monitoraggio Avanzato.

Ci può descrivere più in dettaglio i Servizi offerti da DABco?

DABco ha una solida esperienza nelle diverse attività di Supervisione degli impianti di sicurezza; Vigilanza tecnologica; Monitoraggio dello stato di funzionamento degli impianti centralizzati; Organizzazione e coordinamento degli interventi sul territorio.

Coordinamento delle attività espletata sul campo, perché la tecnologia è uno strumento che assiste l'attività umana ma non la può prescindere totalmente.

La misura della performance è la chiave di ottimizzazione che il nostro metodo vuole garantire e certificare.

Organizziamo servizi a 360 gradi, a partire da Gestione da remoto di Sistemi di Sicurezza; Gestione da remoto di Sistemi di Telesorveglianza e Teleallarme; Pronto Intervento e Pattugliamento, Gestione e Custodia Chiavi, Piantonamento fisso di personale armato, localizzazione e gestione delle Emergenze.

Da sempre attenti alle norme di riferimento, offriamo un servizio di Security Management evoluto, forti di una piattaforma proprietaria con la quale interfacciamo qualsiasi sistema. **L'integrazione è la chiave di lettura vincente per fare incontrare domanda e offerta.**

Tutto questo sta sotto il nome di "**VIGILOGICA Vigilanza Tecnologica Avanzata"**.

Si tratta quindi di un approccio innovativo. Ci può parlare di VIGILOGICA?

VIGILOGICA è un insieme di servizi di security management forniti dal Centro di Controllo, Supervisione e Coordinamento H24 che, attraverso una piattaforma di supervisione evoluta ed esclusiva (PSIM), monitora, centralizza e gestisce sistemi di sicurezza e controllo tecnologico del sito da tutelare.

VIGILOGICA permette di adottare e garantire un efficace ed efficiente modello di *Business Continuity e Security Governance* per prevenire ed evitare danni economici determinati da furti, atti vandalici, rapine, interventi tecnici non risolutivi e tempestivi, utilizzo impropri dei sistemi, tempi di approvvigionamento elevati e ridimensionare gli ingenti costi di vigilanza fisica a presidio o vigilanza itinerante.

Quali sono i vantaggi offerti da VIGILOGICA?
Attraverso VIGILOGICA è possibile ottimizzare i costi di Security&Safety senza nessun vincolo nell'integrazione di tecnologie multi-brand esistenti garantendo la *Business Continuity*.
VIGILOGICA è una soluzione personalizzabile per i più molteplici settori applicativi come:

- Building
- Realtà multisito
- Fotovoltaico
- Piccola e media azienda
- Industrie e Utility
- Logistica
- Arte e Musei
- Residenziale
- Personal Monitoring

Quindi DABco si propone come un **"Centro Stella"**? DABco rappresenta un centro stella capace di coordinare le forze in campo, umane e tecnologiche, dai manutentori agli installatori di tecnologie, alle risorse dedicate alla prima risposta in caso di emergenza,

dagli agenti di sicurezza agli addetti alla sorveglianza antincendio.
Rappresentiamo un centro di supervisione ed erogazione di servizi interdisciplinare, con un doppio controllo tecnologico e umano.
La Sicurezza in senso lato e la Vigilanza sono cambiate e solo le mentalità ancorate al passato e a schemi prefissati lamentano il ritorno a vecchi approcci. **Il focus sul cliente e la ricerca di soluzioni sono la chiave di volta e sviluppo per un settore che può e deve ancora offrire molto.**

CONTATTI: DAB CENTRO OPERATIVO SRL
Tel. +39 06 41200713
info@dabco.it
www.dabco.it

Videoregistratore HDCVI 4 CH Dahua per mezzi mobili Modello MCVR5104

a cura della Redazione

Videotrend presenta una novità assoluta nelle applicazioni TVCC per mezzi mobili. Si tratta del primo videoregistratore **HDCVI** tribrido per applicazioni su mezzi di trasporto capace di 4 ingressi HD/SD su cavo coassiale o IP fino a risolu-zioni di 1080p. Dotato di HDD SATA e slot SD per memory card, è caratterizzato da connettori tipo *Aviation*, output video VGA/TV, 2 porte Ethernet RJ-45 (10/100Mbps) e tra le opzioni disponibili anche GPS e connettività 3G/4G/Wi-Fi. Interfacce ausiliarie 2xUSB 2.0, RS-232/485. Un concentrato di tecnologia, ottimo connubio tra prestazioni ed affidabi-lità. Perfettamente abbinato un line-up completo di telecamere anti-shocking tra le quali spicca l'ultima novità wedge-camera **Dahua modello HAC-HDBW2220F-M** che si propone come riferimento del mercato Mobile grazie alle specifi-che IP67 IK10 e Smart IR 20m.

Insieme ai dispositivi standard IP già lanciati nel corso degli ultimi tre anni, si conferma il catalogo più ricco e competi-tivo sul mercato nelle applicazioni verticali per mezzi mobili in abbinamento alla piattaforma **Dahua HW/SW DSS7016D-M** che consente il controllo e lo storage in tempo reale di ogni periferica associata anche attraverso visua-lizzazione su mappe grafiche.

Videotrend dispone di competenze tecniche ed unità dimostrative per offrire consulenza mirata allo sviluppo di pro-getti chiavi-in-mano.

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

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

ekey insieme a KNX: lettori d'impronte digitali ekey integrati nei sistemi domotici - NUOVO Convertitore ekey KNX

a cura della Redazione

ekey ha una tradizione di **leadership** nel settore dei lettori biometrici da oltre 16 anni. I prodotti ekey sono **classificati ad un altissimo livello tecnologico** e godono di un'immagine di massima **affidabilità** e **sicurezza**. Continui investimenti nella ricerca e sviluppo dei componenti nonché una scelta accurata dei materiali e delle tecnologie, costituiscono solo alcuni elementi distintivi di ekey. Con ekey l'autorizzazione è letteralmente nelle mani dei clienti! Chiavi, schede e codici possono essere persi, dimenticati o rubati, ma "le dita sono sempre disponibili!". ekey offre per tutti i suoi prodotti una **GARANZIA DI 5 ANNI** (3 + altri 2 anni dopo la registrazione del prodotto da parte del cliente).

ekey biometric systems ha messo a punto l'**ekey home CV KNX** allo scopo di collegare i lettori d'impronte digitali ekey alla tecnologia KNX per la domotica e l'automazione degli edifici (vedi anche foto e articolo a pag. 103). Il convertitore sarà disponibile sul mercato con l'inizio della produzione in serie prevista **durante l'estate.**

Allo scopo di massimizzare il comfort e la sicurezza della vita nel XXI secolo con un sistema d'accesso a impronte digitali ekey, ora KNX può rilevare **"chi" attiva un'operazione** consentendo quindi il controllo, la gestione o l'accesso all'immobile con riferimento a una persona specifica.

Progetto di referenza ekey: una moderna casa unifamiliare con lettori d'impronte digitali ekey integrati in un sistema KNX

La casa della famiglia Kaiser si trova a Kirchschlag, un paese austriaco nei pressi della città di Linz. Qui l'architettura moderna s'inserisce armoniosamente nel paesaggio di campagna offrendo a Reinhold Kaiser, alla moglie Martina e ai due figli Fabian (5 anni) ed Emilie (3 anni) lo spazio di vita che hanno sempre sognato. La famiglia si affida a prodotti collaudati per la propria abitazione. *"Articoli di poco valore che provengono dall'Asia per me sono fuori questione"*, rivela **Reinhold Kaiser** strizzando l'occhio. Per casa sua, punta a diverse varianti di lettori d'impronte ekey: i modelli da incasso e integra, combinati a una centralina di comando **ekey multi**, si prestano perfettamente alla villetta. Tre lettori d'impronte digitali in una casa non sono un record, ma dimostrano quanti accessi si possano comodamente proteggere nell'edilizia privata con lo strisciamento di un dito.

Requisiti del cliente:

• Il cliente voleva utilizzare la centralina di comando e i lettori d'impronte digitali ekey multi per controllare tre punti di accesso e il sistema d'allarme. L'idea era di attivare o disattivare il sistema d'allarme in un unico modo: dal lettore d'impronte digitali della porta principale della casa mediante un dito specifico.

• Martina e Reinhold devono avere accesso a tutte le aree, Fabian ed Emilie non hanno il permesso di aprire la porta del garage.

• La famiglia voleva avvalersi dei vantaggi decisivi offerti dal sistema KNX per il controllo personalizzato dell'edificio con dati biometrici, con configurazioni riferite a una persona specifica, quali per esempio:

- Sicurezza per i bambini: disabilitare i fornelli, abilitare la telecamera interna
- Comando delle impostazioni per luci e veneziane
- Simulazione della presenza durante periodi di assenza o ferie

ekey multi – Soluzioni per più accessi

ekey multi è un rivoluzionario sistema d'accesso che consente di gestire fino a 4 lettori d'impronte digitali connessi in una piccola rete. La particolarità è che la programmazione avviene senza PC direttamente su una centralina di comando assegnata. Ogni utente può effettuare diverse operazioni. I diritti d'accesso individuali (comprese le fasce orarie) possono essere assegnati con semplicità a utenti specifici (p.es. membri della famiglia e ospiti, collaboratori, personale delle pulizie) tramite la centralina di comando. ekey multi può memorizzare fino a 99 impronte digitali e permette la registrazione degli accessi da ogni lettore in un apposito archivio.

Per quanto riguarda i lettori d'impronte digitali, sono previsti vari modelli e versioni in base allo scopo e all'applicazione (montaggio a parete o ad incasso, integrazione in porte, impianti citofonici, cornici di interruttori di molti produttori,..). ekey offre molti **frontalini** per rinomati produttori di impianti citofonici (bticino, Elvox, Urmet, Comelit, GIRA, Siedle…). Esistono varie opzioni per il montaggio in diversi accessori progettati da ekey (p.es. tettoie, frontalini in vetro,..). Sono infine disponibili varianti speciali dei lettori d'impronte digitali ekey con supplementare lettura di schede RFID e/o funzionalità Bluetooth.
ekey ha realizzato circa **250.000 installazioni nel mondo intero**, in regioni dal clima umido (UK) e secco (Dubai) con temperature sia calde che fredde (da +70°C a -35°C). Molti modelli sono adatti per l'uso all'esterno (in questo caso è necessaria la categoria IP).

© ekey biometric systems

Nel presente progetto, i proprietari hanno scelto il lettore d'impronte ekey integra installato nel set di montaggio a parete in acciaio inox (esiste anche una variante con LED che segnalano lo stato del sistema d'allarme). Inoltre, il lettore d'impronte da incasso è stato integrato in un impianto citofonico di bticino (modello Sfera).
L'**integratore KNX** definisce il contenuto delle funzioni mediante il **tool** di configurazione **Software ETS5**. I dati del prodotto (dati di configurazione) sono forniti agli installatori da un database centrale dell'organizzazione KNX. Essendo disponibile nel database di prodotti KNX, il nuovo ekey CV KNX consente agli integratori di implementare le soluzioni ekey con la massima semplicità.
Una volta definiti nell'ETS5, le operazioni e gli scenari possono essere attivati dall'utente strisciando le dita sul lettore. A tale scopo si deve prima rendere operativa la funzione KNX nelle impostazioni dell'ekey multi centralina di comando, poi assegnare i vari eventi alle dita dell'utente.
Nel menu dell'**ekey multi centralina di comando** è possibile assegnare un nome (descrizione) a ogni ekey-Event.
Per quanto riguarda la funzione KNX, l'utente può attivare varie operazioni nel sistema KNX utilizzando dita diverse. Lo stesso dito può addirittura attivare operazioni diverse in base al lettore d'impronte digitali utilizzato.
Il numero di operazioni dipende dalla centralina di comando in uso (sistema ekey home o ekey multi). Il

sistema ekey multi consente di attivare 12 eventi (10 ekey-Event e 2 eventi correlati al “dito sconosciuto” o alla “manipolazione”). Il sistema ekey multi, che è impiegato nel progetto qui presentato, richiede una sola centralina di comando. ekey multi CO è un modello montato su guida DIN.
Strisciando un dito a cui è stato assegnato p.es. l’Event 2, si attiveranno le operazioni o gli eventi definiti nell’ETS5 come Event 2. L’evento 11 sarà attivato solo se un dito sconosciuto viene strisciato sul sensore, o se un dito autorizzato non viene riconosciuto.
Nella casa unifamiliare in questione, i seguenti ekey-Event personalizzati sono stati programmati e assegnati alle dita di un adulto.

ekey-Event 1	Sicurezza riferita ai bambini	Forno, TV e PC sono spenti, la telecamera interna è attivata
ekey-Event 2	Simulazione della presenza	Se la famiglia non è in casa (p.es. perché è in ferie), il sistema KNX inganna gli eventuali ladri trasmettendo l’impressione che qualcuno sia presente. La luce si accende e si spegne automaticamente a orari definiti. La chiusura automatica delle veneziane di notte impedisce la dispersione di calore dalle finestre.
ekey-Event 3	Uscita dalla casa	Tutte le finestre eventualmente rimaste aperte, gli interruttori e i dispositivi elettrici ancora accesi vengono spenti con un solo strisciamento del dito. La temperatura del riscaldamento viene abbassata nelle stanze secondarie.
ekey-Event 4	Comando delle veneziane	Quando si invia un valore -> si attiva l’abbassamento delle veneziane fino a una determinata percentuale (p.es. il 50%)
ekey-Event 5	Scenario “Rientro a casa”	Quando i genitori rientrano a casa, si accendono l’impianto audio, i lampadari e il PC

Oltre ai 5 eventi appena descritti, per la casa dei Kaiser sono disponibili anche gli **ekey-Event Sconosciuto e Sicurezza che**, nell’ekey multi centralina di comando, non necessitano di impostazioni specifiche.
La funzione “Dito sconosciuto” attiva l’evento definito a ogni presenza di un dito sconosciuto.
La funzione “Sicurezza” richiede invece la presenza di “Dita sconosciute” senza interruzioni.
La funzione non sarà attivata se, nel frattempo, viene strisciato un dito riconosciuto. In questo caso il conteggio è nuovamente azzerato. Il numero di tentativi di manipolazione può essere impostato da 5 a 50.
La finestra temporale in cui sono rilevabili le dita sconosciute può essere impostata da 1 a 10 minuti. Se questo periodo è superato, il conteggio delle dita sconosciute riparte da 0.
In questa casa unifamiliare, l’evento “Sconosciuto” programmato dall’integratore KNX comporta l’accensione della luce esterna e la memorizzazione in archivio di un’immagine ripresa dalla telecamera della porta.
La funzione “Sicurezza” comporta altre due operazioni: dopo lo strisciamento di 5 dita sconosciute sullo scanner, si attiverà un segnale d’allarme visivo e acustico e un messaggio SMS sarà inviato agli adulti.
Per ciascuno dei 12 eventi (ekey-Event da 1 a 10, “Dito sconosciuto” e “Sicurezza”) si possono effettuare le seguenti impostazioni:

- Commutazione: opzioni “On”, “Off” e “Toggle”
- Invio di un valore (%): un valore compreso tra 0 e 100 viene inviato al sistema
- Comando dello scenario: attiva uno scenario (a cui è assegnato un numero) configurato nel sistema KNX

È inoltre possibile attivare 2 o tutte le 3 funzioni contemporaneamente.


© ekey biometric systems

Integrando le soluzioni d’accesso ad impronta digitale ekey nel suo sistema KNX, la famiglia può vivere il maggiore comfort di un’abitazione pienamente personalizzata, con funzioni automatizzate intelligenti!
Solo la fantasia degli utenti pone un limite alla personalizzazione delle opzioni.
Il nuovo ekey convertitore KNX sarà disponibile a partire dall’estate. Essendo disponibile nel database di prodotti KNX, ekey pertanto è un “PARTNER KNX” certificato.
ekey, oltre a diversi convertitori (KNX, UDP, Wiegand), offre anche la possibilità di accoppiare direttamente i lettori d‘impronte digitali a sistemi esterni e di gestirli tramite un kit di sviluppo software.

Le informazioni tecniche (p.es. istruzioni per l’uso, schede tecniche, schemi di cablaggio) saranno approntate assieme alla produzione in serie durante l’estate. È possibile richiedere maggiori dettagli per e-mail a **italia@ekey.net** oppure consultare il depliant ekey sull’integrazione nei sistemi domotici da scaricare al link: **http://goo.gl/FWEIs0**

Prodotti ekey: la sicurezza della qualità.

ekey
IL TUO DITO. LA TUA CHIAVE.

PARTNER KNX

CONTATTI: INFO: EKEY BIOMETRIC SYSTEMS SRL
Tel. +39 0471 922712
www.ekey.net

I vantaggi dei lettori d'impronte digitali ekey combinati con i sistemi domotici sono evidenti.

L'identificazione univoca
è la condizione migliore per un ottimale Home Automation System che consente **al tuo edificio di sapere chi si trova in casa!**

Tecnologia innovativa
- Le moderne soluzioni d'accesso sono un elemento basilare degli edifici dotati di tecnologie avanzate
- Valorizzazione dell'immobile

Configurazione personalizzata, p. es.
- Bambini: disattivazione del forno, attivazione della telecamera in casa
- Gestione di scenari luminosi, climatizzazione e riscaldamento, oscuramento

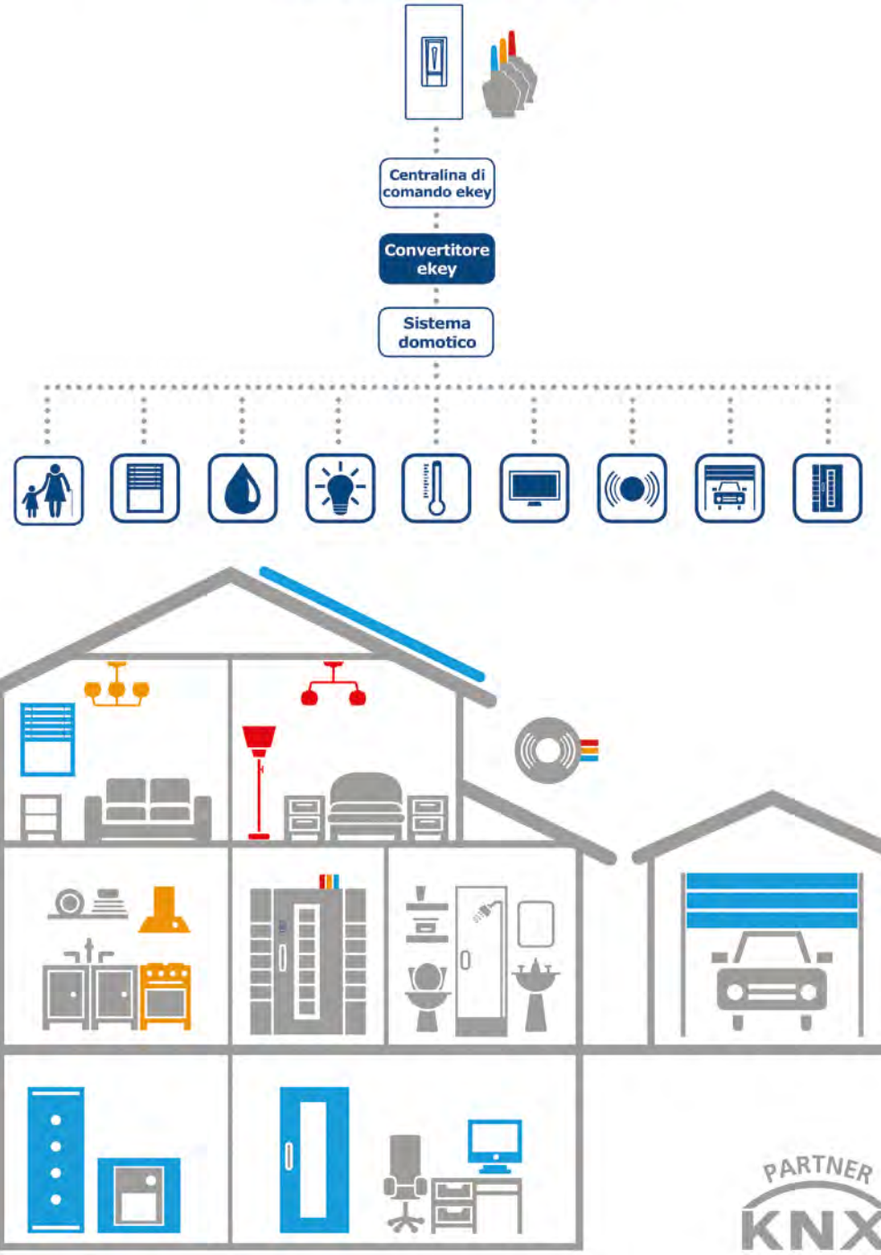
Controllo degli accessi
- La registrazione ci consente di sapere chi, quando e dove ha attivato una funzione!
- È possibile quindi anche l'uso per lo scopo del rilevamento tempi!
- Informazione sull'autorizzazione del dito passato sopra il lettore!
- Abilitazioni temporizzate, ad esempio per gli addetti alle pulizie (venerdì dalle ore 08.00 alle 12.00)

Diverse funzioni sono attivabili con dita differenti, ad esempio
- Attivazione/disattivazione dell'impianto d'allarme
- Registrazione e deregistrazione (nel sistema domotico)
- Apertura porta, portone, ecc.
- Attivazione di diverse centraline

Risparmio energetico
- ad esempio tramite la gestione di intere sezioni di edifici
- tramite impostazioni predefinite per luci, veneziane, riscaldamento, climatizzatore e ventilazione
- Funzione vacanze

Accessibilità, niente barriere
per giovani e anziani – spesso un criterio decisivo!
ad esempio attivazione del comando vocale con l'identificazione dell'impronta digitale

La tua casa può essere dotata di funzioni **automatizzate intelligenti** solo con un sistema d'accesso ad impronta digitale ekey.



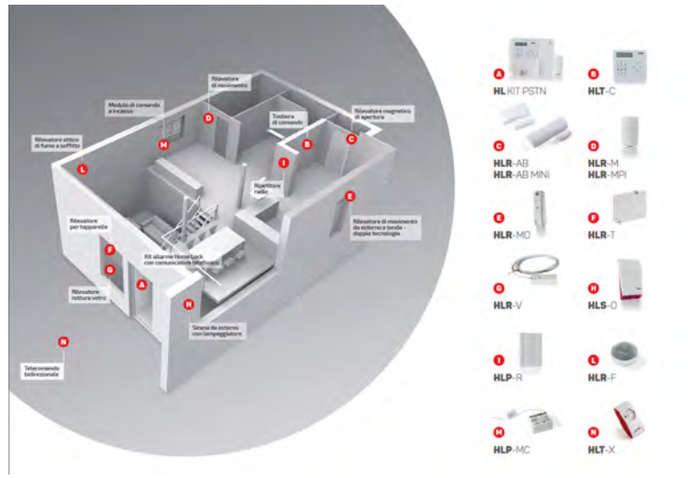
FAAC presenta il sistema d'allarme senza fili Home Lock

a cura della Redazione

Semplice da installare, dal design accurato, frutto delle più innovative tecnologie.
FAAC, la società italiana leader a livello mondiale nelle soluzioni di automazione per serramenti e di controllo degli accessi pedonali e veicolari, ha presentato **Home Lock**, un innovativo sistema d'allarme senza fili che unisce elevata efficacia antintrusione, grande semplicità di installazione e un aspetto estetico estremamente raffinato. Grazie all'impiego delle tecnologie più avanzate, il nuovo **Home Lock** di FAAC elimina il problema dei falsi allarmi, è protetto contro i tentativi di neutralizzazione elettronica e consente un completo controllo remoto tramite telefono (fisso o cellulare). Progettato espressamente per le applicazioni domestiche, il sistema **Home Lock** di FAAC offre un'ampia gamma di sensori e periferiche adatti ad ogni tipo di serramenti. Dotato di funzionalità generalmente disponibili solo nei prodotti più costosi, **Home Lock** di FAAC si caratterizza anche per un prezzo molto competitivo.
Il nuovo allarme FAAC si inserisce in modo ideale anche negli ambienti domestici più raffinati, grazie al piacevole aspetto estetico della centrale e degli accessori, veri e propri 'oggetti di design'. La scelta di utilizzare collegamenti wireless (senza fili) tra la centrale e i sensori, inoltre, consente una posa estremamente semplice e non invasiva, senza alcuna opera muraria.

Nel nuovo **Home Lock** l'attenzione agli aspetti estetici si concilia con un'elevata efficacia antintrusione, grazie a numerosi accorgimenti tecnici:
- le batterie che garantiscono il corretto funzionamento dell'impianto anche in caso di blackout o sbalzi di corrente;
- l'impiego di una tecnologia radio bidirezionale su tutte le periferiche e sul telecomando, per confermare costantemente l'assenza di guasti e l'avvenuta esecuzione dei comandi;
- la trasmissione con segnali radio criptati, inattaccabili dagli hacker;
- il comunicatore telefonico (per linea fissa o cellulare) che in caso di tentata intrusione chiama automaticamente i numeri memorizzati. Grande attenzione è stata dedicata anche all'eliminazione dei falsi allarmi, un problema che in altri prodotti può indurre gli utilizzatori a disattivare il sistema con conseguenti rischi.

Il sistema **Home Lock** è anche estremamente interattivo e flessibile. Il comunicatore telefonico permette la verifica dello stato o l'attivazione/disattivazione dell'allarme tramite SMS e offre la possibilità di ascolto ambientale; il menù di programmazione, estremamente ricco, consente molte diverse configurazioni d'uso. **Home Lock** è un kit composto da centrale con tastiera e sirena incorporate e batterie di backup incluse, telecomando bidirezionale, sensore volumetrico



e contatto magnetico per infissi, cioè gli elementi necessari per creare un impianto base. La modularità del sistema permette l'aggiunta - anche successiva all'installazione - di rilevatori, telecomandi e periferiche, per proteggere nuove parti della casa o attivare nuove funzionalità.
La gamma degli accessori comprende rilevatori di movimento da interno ed esterno (in versione 'pet immune' per evitare falsi allarmi dovuti agli animali domestici), rilevatori di apertura per tutti i tipi di infissi presenti su porte e finestre (a battente o tapparelle), rilevatori di rottura vetri, rilevatori di fumo, tastiere di comando, sirene da esterno ecc, tutti che comunicano via radio con la centrale. La protezione della casa è quindi totale.

Grazie alla tecnologia radio FAAC, **Home Lock** garantisce inoltre una completa integrazione domotica, permettendo di gestire automazioni e sistema di allarme grazie allo stesso telecomando.
"FAAC consolida la propria presenza nel mercato degli allarmi antintrusione domestici con il lancio di un prodotto molto competitivo", ha affermato **Davide Querzè, Product Manager di FAAC**. "Scegliendo FAAC anche per l'allarme di casa, oltre che per le automazioni dei serramenti, i consumatori otterranno un doppio vantaggio: un servizio completo da un singolo installatore e la protezione garantita da un allarme senza compromessi. Ciò si rifletterà positivamente anche sull'attività degli installatori".

Per essere sempre aggiornato sul mondo FAAC iscriviti su **www.homelock.it**

FAAC
Simply automatic.

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

Il nuovo cilindro meccatronico Kaba

a cura della Redazione

Con i nuovi cilindri meccatronici viene ampliata la linea di prodotti Kaba evolo, dispositivi con design pluripremiato e di alta qualità. I nuovi cilindri meccatronici uniscono l'elettronica intelligente ad una meccanica affidabile e si integrano perfettamente e con facilità negli impianti di chiusura esistenti.

Cilindro meccatronico Kaba, versione con elettronica separata

La meccanica collaudata incontra il cilindro meccatronico

Il nuovo cilindro meccatronico Kaba si integra in modo flessibile negli impianti di chiusura meccanici esistenti. L'autorizzazione all'accesso si basa sulla corrispondenza della fresatura meccanica con la validazione elettronica dei dati contenuti nella Kaba smart key. In questo modo il cilindro meccatronico garantisce una doppia sicurezza.

Un'elettronica che garantisce un accesso comodo e sicuro

L'elettronica integrata apre nuove possibilità agli utenti; le autorizzazioni di accesso possono essere regolate in base a profili spazio-temporali e le chiavi possono essere programmate in modo rapido e semplice. Le chiavi smarrite possono essere bloccate tempestivamente e con estrema comodità senza dovere procedere con la sostituzione del cilindro, vantaggio notevole in termini di costi. Con il cilindro meccatronico un impianto di chiusura può essere ampliato in modo flessibile in qualsiasi momento e la memoria degli eventi porta è sempre disponibile. Inoltre, la comunicazione tra cilindro e la Kaba smart key è crittografata, garanzia di una sicurezza ancora più elevata.

Assortimento completo: una soluzione per ogni tipo di porta

Il cilindro meccatronico sarà disponibile in 3 versioni: compatto (con o senza pomolo), con elettronica separata (nella variante mezzo cilindro, cilindro doppio con o senza pomolo) o integrata (nella variante doppio cilindro, con o senza pomolo). Il cilindro compatto, con elettronica nel pomolo interno, è stato adattato al nuovo design dei componenti Kaba evolo. I cilindri esistenti possono essere facilmente sostituiti con il cilindro meccatronico compatto. La versione con elettronica integrata rappresenta la soluzione perfetta per porte antincendio e vie di fuga. La versatile soluzione con elettronica separata offre invece prestazioni elevate e rappresenta la soluzione ideale per porte situate nelle aree di ingresso e nei punti principali di transito.

Funzione wireless

I cilindri meccatronici saranno disponibili anche nella versione wireless. Il cilindro viene collegato al sistema di controllo accessi e connesso in rete via wireless attraverso il dispositivo Kaba gateway. I diritti di accesso sono concessi in modo semplice e rapido senza più programmazione in loco e possono essere modificati in tempo reale comodamente dalla postazione PC. In qualsiasi momento è possibile avere informazioni sullo stato attuale della porta e tutti gli eventi collegati, e distribuire gli aggiornamenti del firmware senza intervenire in loco. Gli amministratori di sistema sono sempre informati: tentativi di scasso o forzatura di una porta vengono notificati con un segnale di allarme e lo stato della batteria segnalato in automatico.

Cilindro meccatronico compatto Kaba

Cilindro meccatronico Kaba, versione con elettronica integrata

KABA®
BEYOND SECURITY

CONTATTI: KABA SRL
info.it@kaba.com
www.kaba.it

Da Gunnebo le 5 regole d'oro per progettare varchi di sicurezza per spazi pubblici

a cura della Redazione

Lo spazio pubblico, per sua natura, è un luogo dove l'accesso deve essere possibile e idealmente agevole, ma non per questo illimitato: anche in questi luoghi è fondamentale regolare flussi e prevenire i rischi. Quali sono gli accorgimenti più importanti per implementare un corretto controllo degli accessi ai luoghi pubblici?

A differenza degli uffici privati, dove la composizione dell'insieme di persone presenti è generalmente costante o comunque prevedibile, la maggior parte dei luoghi aperti al pubblico sono frequentati da persone anche molto diverse fra loro, pur avendo tutte diritto di trovarsi lì. La progettazione di questi luoghi non deve scoraggiare o escludere nessun utente; allo stesso tempo è fondamentale che prevenga accessi indesiderati o pericolosi. Per questo è opportuno seguire alcune regole, come ci spiega **Tim Ward**, esperto globale di Gunnebo in questo settore, mentre **Mauro Bonetto**, Public Plus Manager di Gunnebo Italia, illustra la loro applicazione nella realtà italiana.
Per prima cosa, la soluzione di sicurezza va implementata rendendosi conto dei fisiologici tempi di adattamento degli utenti. Come spiega Tim Ward, per chi frequenta da tempo una biblioteca o un centro civico, trovarsi dall'oggi al domani davanti a barriere e tornelli è una sorpresa; gli utenti potrebbero non sapere come comportarsi. Il problema è che anche il personale potrebbe non essere in grado di spiegare le modalità di funzionamento e i motivi di introduzione del sistema. Per questo, è sempre importante procedere per gradi, attribuendo grande importanza alla comunicazione quando si introducono delle novità di questo tipo. Come segnala Mauro Bonetto, in alcune realtà italiane del trasporto pubblico (dove le soluzioni Gunnebo sono ampiamente diffuse) la novità costituita dalla timbratura in uscita dalle stazioni metropolitane è stata ampiamente preannunciata e preceduta da una fase in cui i varchi erano sempre aperti e la timbratura all'uscita facoltativa; la chiusura è stata graduale e ampiamente comunicata, e questo ha permesso di abituare personale e utenti al nuovo sistema.
Un altro aspetto da valutare con cura è l'opportunità di differenziare i livelli di sicurezza: anche nei luoghi pubblici, spiega Ward, alcune aree non sono affatto pubbliche, e sarebbe decisamente inefficace adottare sistemi di controllo uniformi per tutte le sezioni. Basti pensare agli ospedali, dove una regolazione degli accessi che consenta rapidi flussi e orienti senza creare ostacoli è opportuna, ad esempio, nei reparti di pronto soccorso, mentre l'accesso alle aree dove sono conservati farmaci deve essere consentito solo al personale autorizzato. Trovare soluzioni differenziate per ogni livello di sicurezza richiesto, ricorda Bonetto, non è difficile: la gamma di soluzioni disponibili è ampia, e con l'aiuto di personale qualificato è possibile identificare sempre la soluzione giusta per ogni situazione.
Anche nel controllo accessi l'equilibrio è importante – soprattutto fra il flusso possibile attraverso le barriere e quello atteso di persone che le utilizzeranno. Come illustra Ward, se il numero di varchi è insufficiente rispetto al numero di accessi previsti, è evidente che si formeranno code, con conseguenti colli di bottiglia e possibili frustrazioni. Non va inoltre mai dimenticato che, proprio per la natura pubblica dello spazio, è quasi impossibile prevedere se fra gli utenti ci saranno persone che richiederanno assistenza, e in quale misura, ma di questa possibilità va tenuto conto in quanto potrebbe rallentare ulteriormente il flusso e va controbilanciata con un'adeguata capacità di transito.
Un esempio di perfetto coordinamento fra capacità di flusso richiesta e fornita, come ricorda Bonetto, è dato dalle barriere alla stazione San Siro della linea 5 della metropolitana milanese, automatizzata e senza conducente, con treni che arrivano e ripartono ogni tre minuti e possono contenere fino a 500 persone. Per evitare inutili assembramenti in banchina e "arrembaggi" ai treni, potenzialmente pericolosi, le barriere Full-O-Stile di Gunnebo installate in questa stazione si bloccano automaticamente dopo il passaggio di 450 persone, e si riaprono dopo pochi minuti, quando le persone transitate in precedenza saranno ormai sul treno e avranno quindi lasciato spazio libero in banchina.
Se è importante non avere soluzioni sottodimensionate per evitare ingorghi, è d'altra parte controproducente installare macchinari che solo per la loro mole rischiano di inibire gli utenti e intimidirli - cosa che può avere risvolti positivi in siti di massima sicurezza ma che è normalmente inopportuna in un luogo pubblico. Come rileva Ward, oltre a rallentare i flussi, varchi immanenti e minacciosi possono lasciar presagire un livello di rischio superiore a quello reale e generare nei visitatori una preoccupazione inutile, pregiudicando la possibilità di un'esperienza positiva. Per questo, come spiega Bonetto, in molti luoghi quali musei e biblioteche sono presenti barriere Gunnebo, selezionate di volta in volta in base al livello di sicurezza richiesto ma sempre caratterizzate da un'estrema facilità d'uso e da un design accattivante che non respinge assolutamente gli utilizzatori.

Va infine ricordato che le barriere hanno una vocazione egualitaria: controllano tutti, senza fare distinzioni o preferenze, ed è giusto che sia così. Permettere a dipendenti o gestori dei luoghi pubblici di saltare i controlli senza un valido motivo non è generalmente una buona idea, come spiega Ward: il livello complessivo della sicurezza si abbassa e si lasciano spiragli nel sistema dei quali potrebbero approfittare persone non autorizzate. Coinvolgere invece il personale e spiegare che, esemplificando l'uso corretto dei varchi, tutti contribuiscono al buon funzionamento del sistema di sicurezza, è sicuramente una strategia più efficiente.
Tra l'altro, come rileva Bonetto, esistono esempi illustri. Le barriere Gunnebo sono state installate anche in sedi come Palazzo Chigi, dove, anche grazie alla facilità di utilizzo, molte importanti personalità le hanno utilizzate di buon grado, mostrando come non sia necessario creare corsie preferenziali: quando un sistema è efficiente, lo è per tutti!

GUNNEBO
For a safer world®

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

Pyronix, il Cloud come fattore vincente nell'evoluzione della sicurezza

a colloquio con Valeri Filanov, EMEA Sales Director di Pyronix
a cura della Redazione

Secondo una recente ricerca del Research and Markets, il mercato globale CHSS (Connected home security system) crescera' del 48% tra il 2016 e il 2020, un segmento nel quale Pyronix è uno dei piu' importanti attori. Quali sono le vostre strategie per sfruttare al meglio questa crescita?

A IFSEC-2014, la più importante fiera nel settore della sicurezza, avevamo introdotto la tecnologia Cloud, integrata con il sistema wireless Enforcer 32WE-APP. Questo e' stato il tema principale della fiera e di ogni altra manifestazione da quando è stata introdotta la **"Connected Home Security System"**. Inoltre, abbiamo presentato il concetto di integrazione video con il Cloud collegato ai dispositivi di antintrusione e di automazione domestica in un'unica piattaforma comune, accessibile dall'utente tramite una semplice APP. Due anni dopo il lancio del PyronixCloud con più di 2 milioni di notifiche push già inviate agli utenti, le telecamere cloud sono la realtà che il sistema si sta ampliando: per questo Pyronix ha introdotto sul mercato il sistema ibrido PCX46-APP. Abbiamo semplificato e migliorato la connettività dei nostri sistemi Cloud con l'introduzione della nostra SIM homecontrol e il concetto **smart security solution**. Abbiamo introdotto anche una notifica vocale push nella nostra App homecontrol, in modo tale che gli utenti non possano mai perdersi un importante evento. L'innovativita' che abbiamo lanciato sul mercato ci ha portato grandi soddisfazioni, ma siamo assolutamente

certi che questo e' solo l'inizio. Per questo motivo continuiamo ad investire in ricerca e sviluppo della nostra infrastruttura cloud, con l'obiettivo di integrare più prodotti e servizi che porteranno agli utenti soluzioni di sicurezza sempre più attraenti e accessibili.

L'integrazione tra i sistemi di sicurezza e automazione domestica (Home automation) e' uno dei campi di piu' immediata applicazione delle tecnologie IOT. Qual'e' la vostra visione in materia?

L'obiettivo di integrare i nostri sistemi con i dispositivi di automazione domestica è di fondamentale importanza per Pyronix. Devo dire che facciamo distinzione tra **home automation** e **"smart home"**. I nostri sistemi offrono già funzionalità di automazione. Attraverso l'App homecontrol gli utenti possono da remoto aprire e chiudere cancelli, accendere e spegnere le luci e così via. Stiamo continuando con questo sviluppo con l'obiettivo di integrare una vasta gamma di dispositivi di automazione wireless che permettono agli utenti di avere una gamma completa di servizi di automazione domestica.

Il nostro obiettivo finale è quello di giungere ad una soluzione di "casa intelligente", in cui la casa diventa parte integrante della **user experience**.

Una delle principali preoccupazioni degli utenti è la protezione dai pericoli di natura informatica: da un lato la tutela della privacy rispetto alla raccolta di informazioni sulle abitudini degli utenti; dall'altro, la possibilità di attacchi informatici per neutralizzare le difese fisiche. Come risponde Pyronix?

Pyronix risponde a queste minacce in modo proattivo e positivo. In qualità di produttore di sicurezza prima di tutto, Pyronix è in grado di portare le migliori conoscenze dei suoi sistemi di sicurezza e di applicarle al mercato dell' IOT. Ad esempio, il PyronixCloud è la porta attraverso la quale I prodotti Pyronix comunicano, e possono essere controllati tramite l'homecontrol App. Ma questo non significa che i dati sensibili devono essere conservati lì - in realtà, e' tutto il contrario. Il PyronixCloud non memorizza i dati sensibili degli utenti e questo non permette ai malintenzionati di accedervi. Inoltre, la nostra infrastruttura richiede tre verifiche per accedere alla centrale di controllo tramite l'App, un metodo altamente sicuro che va al di là della normale prassi del settore. Per Pyronix, la chiave per l'integrazione dei dispositivi IOT è questo focus diretto sulla sicurezza. Si parte dalla sicurezza, per costruire la funzionalità e l'usabilità intorno a quella etica.

L'integrazione intersistemica tra antintrusione, videosorveglianza, controllo accessi ecc si sviluppa anche a livello societario, con operazioni

M&A (fusioni e acquisizioni) che sono sempre più frequenti a livello globale. Ora con Pyronix parte del gruppo Hikvision, quali saranno le vostre strategie di business che porterete avanti?

Il modo migliore per rafforzare e consolidare la nostra presenza sul mercato è di crescere organicamente attraverso il continuo sviluppo di eccellenti prodotti per la sicurezza domestica. Questo è stato al centro della filosofia di Pyronix sin dai suoi albori, e siamo lieti quest`anno di festeggiare i 30 anni di attivita'. Adesso con Pyronix parte del gruppo Hikvison, la strategia per la azienda sara` quella di incorporare la convergenza delle tecnologie. Abbiamo in programma di integrare i nostri premiati sistemi di rilevamento antintrusione e portare nuove soluzioni che siano innovative e che ci permettano di continuare a mantenere una leadership di mercato. Il nostro impegno per far progredire il settore della sicurezza attraverso l'innovazione e gli investimenti in R & S continuerà, ma da adesso avremo dalla nostra parte il nostro nuovo partner Hikvision.

Pyronix HIKVISION

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

VideoSorveglianza Open Platform: da Centro di Costo a Business Tool con la soluzione 4K UHD Samsung WiseNet

a cura della Redazione

L'evoluzione della tecnologia di ripresa e di compressione video ha portato anche la VideoSorveglianza a considerare immagini con risoluzione sempre crescenti, rendendo la qualitá 4K UHD un elemento comune presente nelle soluzioni proposte da diversi costruttori.
Ma l'aumento della risoluzione e della qualitá video apre nuovi scenari e nuove problematiche in fase di implementazione e, successivamente, di gestione di un sistema di VideoSorveglianza.
L'implementazione di soluzioni con risoluzioni 4K UHD che, ricordiamo, equivale a 4 volte la risoluzione FullHD 1080p, porta ad un aumento delle informazioni disponibili all'interno della rete, in termini di occupazione di banda, occupazione di storage e gestione dei flussi video.
Senza una oculata progettazione, il rischio é che il tutto si traduca in un aumento dei costi sia iniziali per l'implementazione della soluzione, sia successivi per la gestione, che non giustifica l'investimento da parte degli utenti finali in una nuova soluzione o nell'aggiornamento dell'esistente.
E' importante, quindi, nel momento in cui si pensa ad una soluzione con risoluzione 4K UHD, considerare l'impatto che questa genera sull'infrastruttura di rete, oltre ai benefici concreti che puó portare agli utenti.
Ed é puntando su questi ultimi due elementi che la soluzione 4K UHD della serie **Samsung WiseNet** trova alcune risposte utili per progettare e realizzare sistemi basati su questa risoluzione.

H.265 e WiseStream

Un ruolo fondamentale, per la gestione di flussi video con risoluzione 4K UHD, viene giocato dall'efficacia degli algoritmi di compressione.
Tutte le telecamere 4K della gamma **Samsung WiseNet** implementano due novitá tecnologiche che sono state sviluppate per ottimizzare l'utilizzo delle risorse:

- la rispondenza allo standard di compressione video piú recente H.265 che, giá di per sè, porta ad una riduzione della banda necessaria;
- una ulteriore tecnica di compressione, denominata **WiseStream** che, associata all' H.265, porta ad una riduzione fino al 25% del flusso video, senza inficiare sulla qualitá dell'immagine.

E' ovviamente importante considerare che tutta la catena, dalla telecamera, agli apparati di registrazione, devono essere compatibili con lo standard di compressione **H.265 WiseStream**.

Soluzioni Edge based e Open Platform

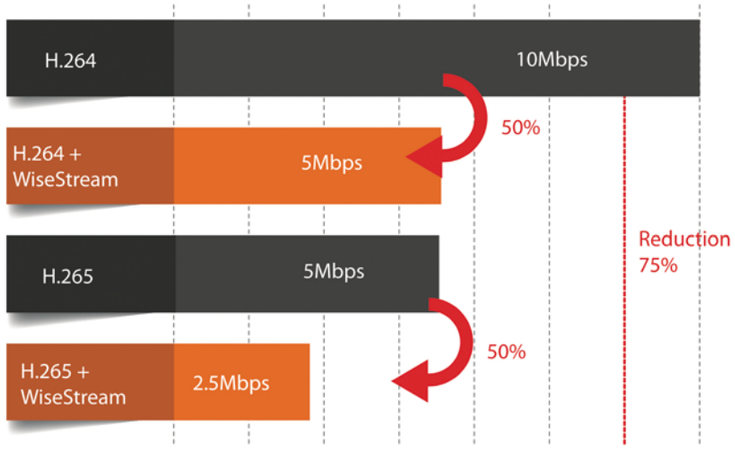
Diventa tuttavia riduttivo pensare che, con le nuove tecnologie, l'unico vantaggio sia quello di avere immagini live o registrate con una risoluzione maggiore, e non considerare la possibilitá di applicazioni e funzionalitá diverse ed innovative.
L'aumento di qualitá video rappresenta di per sè giá un vantaggio ed una motivazione forte all'investimento.
Ma sono altre le opportunitá che oggi vengono offerte e che aprono di fatto la possibilitá per nuove applicazioni che consentono, da un lato, di migliorare i processi di gestione della sicurezza degli ambienti e delle aree esterne ma, anche, di rendere fruibili agli utenti servizi legati alla business intelligence.
Da un punto di vista tecnologico, ciò che rende possibile queste funzioni é la capacitá di calcolo dei processori utilizzati all'interno delle telecamere che, oltre ad effettuare la compressione del segnale generato dai sensori, possono utilizzare parte delle risorse per attivitá di analisi e generazione di Metadata.
Il Metadata rappresenta la base su cui é possibile costruire le nuove piattaforme aperte di VideoSorveglianza, passando da un concetto di TVCC, ad un concetto piú ampio di Open Platform.
L'Open Platform rappresenta un interessante elemento di sviluppo e di crescita tecnologica e culturale del mercato in generale.
La tecnologia **WiseNet Samsung**, integrata nelle telecamere, é virtualmente al centro di una infrastruttura che, partendo dall'unitá di ripresa, risponde alle esigenze sempre piú complete di sicurezza, efficenza operativa, analisi video e supporto al business.

Il cuore dell'Open Platform: il DSP WiseNet III

Tutte le nuove funzioni e le nuove potenzialitá sono supportate da un processore di ultima generazione integrato nelle telecamere Samsung, chiamato **WiseNet III**.
Grazie all'Open Platform, é stato possibile consolidare partnership tecnologiche con altre aziende, contribuendo a fare crescere il livello tecnologico oggi disponibile, ed aprendo nuove opportunitá di utilizzo delle telecamere, con una ricaduta positiva sul business per tutti i player coinvolti, compreso gli utenti.
Le nuove funzionalitá rese disponibili con l'Open Platform possono facilmente essere integrate nelle telecamere con una logica simile a quella utilizzata per caricare una nuova App su uno smartphone.

Nuovi servizi grazie all'Open Platform

Le App disponibili per l'Open Platform aumentano le funzionalitá della telecamera, arricchendola di capacitá di analisi real-time per molteplici applicazioni.
Come risultato di questa attivitá, la telecamera, oltre a fornire immagini video, genera anche Metadata, che racchiudono tutte le informazioni risultanti dalla attivitá di analisi.
Tramite i Metadata generati a fronte dell'analisi video, é possibile inviare informazioni, ad esempio, su un numero di targa, sul numero di persone o veicoli presenti in un area o in transito da un varco virtuale.
Da qui, le molteplici nuove applicazioni possibili, che vedono le telecamere come uno strumento di ausilio



al business, ad esempio di un area commerciale o un ufficio pubblico.
L'analisi comportamentale e la possibilitá di identificare a fini statistici parametri come range di etá e genere, possibili con alcune delle App giá disponibili, diventano uno strumento utile per definire al meglio la "customer experience" all'interno di un punto vendita o per rendere piú veloce ed efficente la fruizione di servizi in una filiale di banca.
Analogamente, ottimizzando le stesse logiche per il controllo del traffico veicolare é possibile poter intervenire per ottimizzare il flusso e i tempi di percorrenza.
Un altro ambito importante in cui la logica di Open Platform porta a vantaggi tangibili é quello della sicurezza dei dati e della trasmissione in rete.
Una delle funzioni infatti oggi disponibile sulle telecamere Samsung con tecnologia Open Platform, consente infatti di garantire l'invio di flussi video criptati sulla rete, eliminando qualsiasi rischio di manipolazione e intercettazione dei dati.

Da centro di costo a business tool

E' chiaro, quindi, che risulta essere ormai riduttivo pensare che lo sviluppo tecnologico porti come unico vantaggio quello di poter fruire di sistemi di VideoSorveglianza con immagini sempre piú risolute e di qualitá.
I vantaggi offerti dalle soluzioni di ultima generazione vanno ben oltre, e aprono di fatto nuove opportunitá di utilizzo, e quindi di business, anche per gli utenti.
Tutto ció presuppone un cambio, oltre che tecnologico, anche di mentalitá e di modalitá di azione, passando dal concetto di semplice TVCC, Televisione a circuito chiuso, che giá nel nome indica elementi di limite, a soluzioni Open Platform, aperte, standard e pronte a cogliere le sfide del futuro.

Hanwha Techwin Europe

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

ProSYS™ Plus, il sistema di sicurezza "super ibrido" a piattaforma singola basato su Cloud di RISCO Group

a cura della Redazione

L'impegno di RISCO Group per l'avanguardia e l'innovazione: ProSYS™ Plus

ProSYS™ Plus, il nuovo sistema di sicurezza ibrido a piattaforma singola basato su Cloud di RISCO Group, è una soluzione dal carattere fortemente innovativo che conferma il costante impegno dell'azienda nella ricerca di soluzioni all'avanguardia e convergenti in grado di guidare il mercato. Il forte dinamismo, la vocazione per l'innovazione e l'attenzione per il supporto tecnico dei partner sono valori che hanno sempre pervaso la strategia di RISCO che, nata a fine degli anni '70 con il marchio Rokonet e come produttore di rivelatori professionali, si è evoluta nel tempo trasformandosi in fornitore di sistemi e arrivando ad affermarsi oggi come una società indipendente e leader a livello globale specializzata nella produzione, nello sviluppo e nella commercializzazione di un'ampia e completa gamma di soluzioni di sicurezza, impianti antifurto ad alte prestazioni, rivelatori e accessori.
L'offerta di RISCO, infatti, comprende prodotti cablati, wireless e ibridi per sistemi antintrusione pensati per la protezione di strutture residenziali, commerciali ed industriali, capace di rispondere in maniera completa e puntuale all'intera domanda di impianti di sicurezza. Tutte le soluzioni dell'azienda - dai semplici sensori fino ai complessi sistemi di sicurezza - sono conformi agli standard europei e permettono così di soddisfare anche i più stringenti requisiti di sicurezza di siti sensibili quali banche, infrastrutture critiche ed edifici governativi o pubblici. A conferma del ruolo di pioniere nello sviluppo di soluzioni che grazie alla tecnologia potessero far progredire l'intero mercato della sicurezza, RISCO annovera nel suo portafoglio prodotti numerosi brevetti di tecnologie di rilevamento all'avanguardia che aumentano notevolmente le prestazioni, riducendo l'incidenza di falsi allarmi. Si tratta di innovazioni uniche nel loro genere che consentono di distinguere in maniera estremamente precisa tra esseri umani e altre fonti di possibile interferenza per i canali a infrarossi e a microonde, sia all'interno sia all'esterno. Inoltre, l'azienda ha sviluppato una serie di rivelatori conformi agli standard di Grado 3 che vanno quindi a costituire la soluzione di eccellenza ideale per applicazioni industriali, commerciali o governative, capaci di garantire la massima affidabilità e immunità a falsi allarmi anche in ambienti critici e ad alto rischio. I rivelatori Grado 3 di RISCO offrono quindi prestazioni e qualità superiori, grazie anche alle esclusive analisi digitali messe a punto in quasi 40 anni di esperienza nel settore.
Tratto distintivo che caratterizza l'intera offerta RISCO è senza dubbio il cloud, considerato un vero e proprio modello di business. L'azienda, infatti, è stata la prima nel mercato della sicurezza ad aver riconosciuto e sfruttato le opportunità che questa tecnologia poteva offrire non più solo per aspetti tecnici e di supporto, ma scegliendola come base per tutte le sue innovazioni di prodotto, da **LightSYS™ 2** ad **Agility™ 3**, fino a

ProSYS™ Plus e all'innovativo sistema di controllo degli accessi **axesplus®**.

Il sistema di sicurezza "super ibrido"

ProSYS™ Plus è il sistema di sicurezza "super ibrido" studiato per progetti residenziali e commerciali su larga scala, particolarmente indicato nella gestione multi-sito, grazie all'integrazione con il software **SynopSYS Integrated Security and Building Management™**, che fornisce una soluzione semplice per il controllo e la gestione di sicurezza, rilevazione incendio, TVCC, accessi e molto altro. Inoltre, questa piattaforma è caratterizzata da un'architettura client-server aperta che favorisce l'integrazione di apparecchiature e software anche di terze parti.

Alla pari di tutte le soluzioni RISCO, **ProSYS™ Plus**, essendo conforme agli standard europei di Grado 3, permette di soddisfare anche i requisiti di sicurezza più stringenti grazie alle esclusive tecnologie di rilevazione di RISCO che forniscono affidabilità e immunità a falsi allarmi anche in ambienti critici, interni ed esterni, per livelli di sicurezza senza pari.

Progettata per indirizzare qualsiasi esigenza e offrire all'utente molteplici funzionalità, **ProSYS™ Plus** è una soluzione di ultima generazione basata su un'unica piattaforma hardware centrale adatta ad ogni tipo di applicazione - dalla più piccola alla più grande - e scalabile liberamente fino a 512 zone. In particolare, l'innovativo meccanismo di licenze RISCO *"pay as you grow"*, permette a installatori e system integrator di iniziare il progetto selezionando il numero esatto di zone richieste e di integrarle successivamente senza dover sostituire il sistema centrale. Ciò permette notevoli risparmi abbattendo il costo di future espansioni, semplificando la gestione e riducendo il valore del magazzino ricambi per gli addetti all'installazione e alla manutenzione.

ProSYS™ Plus sfrutta l'architettura ibrida, che combina accessori cablati, radio, mono e bidirezionali attraverso un collegamento sul RISCO Bus che consente di ottimizzare le installazioni e di effettuare diagnostica e assistenza da remoto.

ProSYS™ Plus, supportando le più avanzate tecnologie di comunicazione disponibili tra cui multi-socket IP,

2G/3G e WiFi, assicura ridondanza e resilienza, requisiti di fondamentale importanza per assicurare l'affidabilità di un sistema di comunicazione.

Inoltre, **ProSYS Plus™** si avvale del software di configurazione (CS) di RISCO, un applicativo con interfaccia multi-lingue, che consente la programmazione da remoto nonché la diagnostica e l'aggiornamento del firmware della centrale. In particolare, tramite questo software, gli installatori possono gestire e configurare il database dei clienti e degli impianti installati, programmare le centrali da PC, visualizzare localmente lo stato del sistema ed effettuare operazioni automatiche su gruppi centrali connettendosi alla centrale tramite un cavetto standard oppure da remoto via modem, GSM/GPRS o connessione TCP/IP grazie alle funzionalità offerte dal Cloud RISCO.

Le opportunità offerte dalla tecnologia cloud

RISCO Group è stato il primo player del mercato della sicurezza a riconoscere e sfruttare le opportunità che la tecnologia cloud poteva offrire agli utenti finali. Infatti, il cloud consente di coniugare al meglio semplicità di utilizzo e innovazione offrendo servizi e funzionalità aggiuntive che si integrano agli impianti già installati – purché connessi al cloud – andando a permeare le soluzioni RISCO di un forte valore aggiunto.

Essendo basata su cloud, **ProSYS™ Plus** offre una soluzione di sicurezza all'avanguardia e una completa gamma di servizi all'utente, che può disporre di un sistema che evolve nel tempo senza bisogno di sostituire l'installato e all'installatore, che ha invece l'opportunità di sviluppare fatturato anche sui clienti esistenti offrendo loro ulteriori servizi favorendone così la fidelizzazione, velocizzare il processo di installazione e semplificare la manutenzione.

Per clienti e installatori si aprono quindi nuove frontiere di gestione remota dei sistemi di allarme grazie all'utilizzo dell'app iRISCO disponibile per iOS e Android o di una interfaccia web, che offrono un livello di sicurezza e di controllo senza precedenti. Inoltre, oltre a consentire di controllare il sistema di sicurezza, l'innovativa funzione SmartHome che si aggiunge all'app iRISCO, permette, di gestire dispositivi domotici, assicurando un notevole risparmio in termini di denaro e di energia.

Grazie alla tecnologia offerta da **ProSYS™ Plus**, è possibile installare telecamere IP per interni ed esterni integrate con il sistema e richiedere, tramite VUpoint, immagini o video verifica in tempo reale e in alta risoluzione in qualsiasi momento e ovunque ci si trovi, su specifica richiesta o in risposta a qualsiasi tipo di allarme. In questo modo gli utenti hanno la possibilità di monitorare da remoto e di gestire completamente il proprio sistema di allarme: inserirlo o disinserirlo, escludere zone o richiedere immagini dalle fotocamere o dalle telecamere installate. Contestualmente, gli installatori possono interagire con le proprie centrali ovunque si trovino, potendo quindi configurare, aggiornare e controllare i sistemi senza interruzioni nelle prestazioni.

Commenta **Ivan Castellan, Branch Manager di RISCO Group Italia**: "Da sempre impegnati a fare innovazione, investiamo in Ricerca e Sviluppo per fornire delle soluzioni che rappresentino lo stato dell'arte del mercato per sicurezza e avanguardia. *Presenza locale a livello globale* è la strategia vincente intrapresa da RISCO Group e riproposta per il futuro: investire risorse e attenzione in tutti i mercati locali in cui l'azienda opera, potendo tuttavia contare su una visione globale e risorse tecniche e professionali provenienti da tutto il mondo. ProSYS™ Plus è la dimostrazione del nostro costante impegno nell'indirizzare ogni tipo di esigenza attraverso un sistema di sicurezza ibrido a piattaforma singola, pensato per offrire al cliente una soluzione senza pari in termini di sicurezza, protezione e di costo. Con ProSYS™ Plus, Risco Group offre una gamma completa di soluzioni avanzate pensate sia per le piccole-medie imprese che per le installazioni commerciali su larga scala, che sfruttano la stessa tecnologia. Basata sul Cloud RISCO, ProSYS™ Plus è una soluzione in grado di garantire tanto agli installatori quanto agli utenti finali l'enorme valore aggiunto garantito dal cloud, che permette di aggiungere servizi e funzioni anche sugli impianti precedentemente installati. È proprio il Cloud RISCO che ci ha permesso di differenziarci sul mercato integrando con una sola applicazione intrusione, video e in futuro anche domotica."

RISCO GROUP

CONTATTI: RISCO GROUP
Tel. +39 02 66590054
www.riscogroup.it

Lettori biometrici e tutela dei dati, la scommessa di IGTEK

a colloquio con Alessandro Facini, titolare di IGITEK
a cura della Redazione

Qual è lo stato dell'arte del mercato dei lettori di impronte digitali per il controllo degli accessi in Italia?
Oggi i lettori biometrici sono presenti in molti dispositivi di uso comune come Pc, Tablet o Smartphone ma, nonostante tale diffusione e conoscenza, il lettore biometrico in applicazioni legate alla sicurezza come il controllo degli accesi, rimane ancora un dispositivo di nicchia, insieme alle varie applicazioni "satelliti" come, ad esempio, l'utilizzo per comandare l'impianto anti intrusione o l'integrazione con la domotica. È indubbia la comodità dei lettori biometrici e la tecnologia sarebbe pronta da anni per un utilizzo a tutto campo: ci sono soluzioni idonee a tutti i settori, a partire dalle più semplici per il privato a quelle più articolate per le aziende, dalla piccola alla multinazionale, per una gestione avanzata degli ingressi, anche se la filiale o succursale aziendale si trova in un altro continente a migliaia di chilometri di distanza.
Il mercato offre tante soluzioni, quasi esclusivamente d'importazione, più o meno professionali. Senz'altro, la difficoltà nell'affidarsi ad un marchio invece che un altro, è quella di riuscire a valutare il livello di sicurezza e di affidabilità di prodotti spesso proposti in vaste gamme non compatibili e non integrabili tra loro.

Come nasce la sua azienda, quali prodotti ha sviluppato, a quali clienti si rivolge?
Ho iniziato lo sviluppo dei progetti dedicati ad aperture tramite riconoscimento dell'impronta digitale nel 2002, come collaboratore in un'azienda informatica, apportando la mia conoscenza nel settore dell'elettronica e delle comunicazioni. Nacquero i primi progetti proposti ed utilizzati per più aziende, con cui ho collaborato negli anni, per svariate applicazioni, inizialmente per lo più stand-alone come attivazione

di allarmi satellitari per auto, apertura di casseforti, apertura porte, abilitazione macchinari… ma anche più articolati come, ad esempio, i sistemi di apertura bussole delle banche con acquisizione dell'immagine dell'impronta digitale, della fotografia della persona e l'archiviazione separata con criptazione dei dati non ricollegabili tra loro se non opportunamente decriptati. Il passaggio a sistemi in bus con controllo da software fu spontaneo e quasi immediato. E' nata così l'architettura che è ancora alla base dei dispositivi che tuttora produco e commercializzo.
Nel frattempo ho intrapreso una mia attività imprenditoriale, dando vita ad IGTEK con la quale ho dato continuità ai miei progetti realizzando dispositivi di qualità e di sicurezza e l'impegno di offrire al cliente un elevato servizio tecnico, oltre ad un servizio di ricerca e sviluppo per soddisfare anche le richieste di prodotti "oem". L'assistenza agli installatori viene eseguita direttamente, ottimizzando i tempi di attivazione degli impianti semplici o complessi che siano.
I prodotti IGTEK si dividono principalmente in due categorie: quelli dedicati al controllo accessi e quelli oem. In quest'ultimi troviamo svariati dispositivi, non solo di tipo biometrico, dedicati a molteplici settori tra cui, per quanto riguarda la biometria, meritano nota i lettori dedicati all'apertura di casseforti di sicurezza nel mondo del lusso, oggetti quasi esclusivamente destinati all'esportazione. Per quanto riguarda il controllo accessi, IGTEK vanta una gamma prodotti altamente efficace per coprire tutte le richieste di mercato, spaziando dal settore privato con applicazioni per appartamenti o più strutturate per ville con gestione avanzata degli utenti, al settore industriale, commerciale (impianti nei supermercati), pubblico e militare con controlli accessi in varie caserme delle Forze dell'Ordine.

Biometria e privacy: qual è l'atteggiamento del Garante in questo momento? Quali sono gli accorgimenti da adottare per poter installare un sistema biometrico senza incorrere in sanzioni?
Negli anni passati, non è stato facile lavorare nei settori diversi dal privato, perché le procedure per ottenere l'autorizzazione per un impianto biometrico erano complesse e spesso non chiare, ma soprattutto, in generale, il garante disincentivava l'utilizzo di dispositivi biometrici sconsigliandoli se non in ultima soluzione per regolare gli accessi. I nostri dispositivi biometrici non salvano l'immagine dell'impronta ma solo il template (codice numerico ricavato da particolarità dell'impronta stessa dette "minuzie"), dal quale non è possibile risalire all'immagine dell'impronta che lo ha generato.
Recentemente il Garante della Privacy ha emesso delle importantissime linee guida che chiariscono le regole da rispettare e che, in parte, semplificano le procedure per la realizzazione di impianti biometrici, eliminando, in alcune casistiche, la necessità della richiesta di verifica preliminare al Garante. IGTEK a tal proposito ha messo a punto un software secondo tali linee guida che ha permesso, ad un nostro importante cliente, di raggiungere un accordo con il sindacato per l'utilizzo dei nostri lettori biometrici per regolamentare gli accessi dei dipendenti. I punti chiave sono la sicurezza nell'inviolabilità dei dati biometrici, con criptazioni degli stessi su più livelli e su tutte le linee di comunicazione,

la decentralizzazione della loro archiviazione, nonché procedure chiare e documentate sul funzionamento del sistema. Il tutto reso disponibile al dipendente che potrà scegliere se utilizzare il nuovo sistema biometrico o viceversa utilizzare gli strumenti tradizionali.

Biometria e domotica: quali sono gli scenari di integrazione tra rilevatori biometrici e dispositivi di automazione degli edifici?
Sono due settori molto vicini tra loro che continuano ad intrecciarsi da anni. D'altra parte, un lettore biometrico è un dispositivo di controllo accessi, ma è anche un accessorio per l'impianto di antiintrusione e quello domotico. Spesso i nostri lettori vengono utilizzati da system integrator o progettisti di impianti domotici per comandare attivazioni e scenari vari. Allo stesso tempo, per piccoli impianti domotici con funzioni di base come quelli richiesti in appartamenti, possono essere utilizzati i nostri kit lettore, scheda di rete e schede relay, con le quali si possono aprire i catenacci della porta blindata, accendere la luce dell'ingresso e disinserire l'allarme, semplicemente appoggiando il dito sul lettore all'ingresso di casa. Oppure comandare attivazioni da remoto come ad esempio la chiusura di tapparelle, il comando dell'allarme, l'accensione di luci… tramite comandi diretti o di scenari, utilizzando il proprio smart phone.

IGTEK

CONTATTI: IGTEK
info@igtek.eu
www.igtek.eu

Kaba exivo, un nuovo modo di intendere e gestire la sicurezza

a cura della Redazione

Tutta la sicurezza a portata di mano nel vostro smartphone o tablet ovunque voi siate!
Con Kaba exivo potete gestire e controllare gli accessi alle vostre porte anche quando non siete presenti in casa o in ufficio. Avete bisogno semplicemente di una connessione a Internet, tramite uno smartphone, un tablet o un PC: dal momento che Kaba exivo può essere gestito facilmente tramite il vostro browser, potete accedere al sistema ovunque voi siate e in qualsiasi momento.

Kaba exivo: Software as a Service!
Kaba, leader tecnologico dell'industria della sicurezza presenta **exivo**, la nuova soluzione che rivoluzionerà il modo di intendere e gestire la sicurezza di ogni giorno nelle piccole e medie imprese e nella vostra casa in linea con il nuovo mondo dell'"Internet of things".
Kaba exivo è il primo vero sistema professionale per la gestione della sicurezza, offerto in modalità "Software as a Service" sul mercato: non è necessario alcun PC o server dedicato, basta il dispositivo di controllo del varco, la connessione di rete ed un browser per accedere alla piattaforma Kaba web based. I costi mensili sono chiari e modulari in funzione della dimensione impianto e dei servizi richiesti.

La piattaforma centralizzata Kaba exivo opera su server con altissimi standard i di sicurezza, la protezione dei dati degli utenti è garantita, quindi, ai massimi livelli.

Aggiornamenti periodici della piattaforma garantiscono non solo la stabilità del sistema ma anche un continuo rilascio di nuove funzioni da utilizzare.

Con Kaba exivo, non siete soli, il vostro partner specializzato e certificato Kaba, se vorrete, vi potrà assistere e supportare nella fase di configurazione e nell'utilizzo della piattaforma in ogni momento; siete liberi di decidere cosa delegare o meno al vostro partner o se controllare tutto in totale autonomia.

La procedura per progettare, ordinare ed installare Kaba exivo è facile e veloce, potrete sempre estendere il sistema ordinando nuovi dispositivi e tessere direttamente dalla piattaforma web. I dispositivi vi arriveranno direttamente a casa o in ufficio e si configurano facilmente, in automatico, una volta connessi. Il sistema supporta lettori online, wireless e consente di introdurre anche sistemi di chiusura meccanici.

Kaba exivo è una soluzione facile e intuitiva ma anche comoda e flessibile: è possibile, per esempio, assegnare, modificare o revocare i diritti di accesso degli utenti in tutta semplicità e in qualsiasi momento.
Vantaggi in sintesi:

- Tutta la sicurezza a portata di mano nel vostro smartphone o tablet ovunque voi siate
- Gestione e monitoraggio degli eventi in mobilità ed in tempo reale
- Nessuna piattaforma Server o PC da dover gestire
- Costi chiari in funzione dell'impianto e dei servizi richiesti
- Contatto diretto con il partner che vi supporta e interviene su richiesta
- Facile da pianificare, ordinare ed estendere
- Piattaforma sicura. Tutte le informazioni sono protette
- Rapido montaggio: sistema subito disponibile ed utilizzabile dopo l'installazione dei componenti
- Gestione semplice e comoda dei diritti di accesso e dei componenti.

KABA®
BEYOND SECURITY

CONTATTI: KABA SRL
info.it@kaba.com
www.kaba.it

All'Elba il Meeting Concessionari e Installatori Autorizzati HESA 2016

a cura della Redazione

Si è tenuto il 12 e 13 maggio il **Meeting annuale del Concessionari e Installatori Autorizzati HESA 2016**, che ha visto una folta partecipazione di operatori nelle due giornate di lavori presso l'hotel Hermitage Biòdola all'Isola d'Elba. Una cornice incantevole, diventata negli anni un'attrazione ulteriore per i partner di HESA, storico e indiscusso protagonista del mercato italiano della sicurezza fisica.

Il tema conduttore dell'incontro di quest'anno è stata l'esortazione ad accettare la sfida (*Take the challenge*) che l'intero comparto della sicurezza fisica si trova davanti. Una sfida determinata dai molteplici e rapidi fattori di cambiamento nelle tecnologie, nelle richieste dei clienti e nella quantità e diversità dei competitori provenienti da altri settori, in fase di continuo aumento.

Tutti fattori che comportano difficoltà aggiuntive per gli installatori di sicurezza ma anche altrettante opportunità di crescita, sapendo utilizzare il sostegno offerto da partner strategici come HESA.

L'appello a guardare con attenzione al cambiamento in corso era stato già lanciato nelle ultime edizioni del Meeting, nelle quali era stata sottolineata l'esigenza di adeguare la figura dell'installatore di sicurezza alle novità che già si erano manifestate nel mercato.

Quest'anno il tema conduttore è stato invece la raccolta della sfida dell'adeguamento, per poter guardare avanti in uno scenario che si muove con estrema velocità.

Accettare questa sfida da parte degli installatori tradizionali di sicurezza significa fare un passo avanti, con la mentalità aperta al cambiamento e all'evoluzione della propria figura. Questo in sintesi il messaggio lanciato durante il meeting da **Carlo Hruby,** amministratore delegato del Gruppo milanese, che ha inoltre sottolineato: *"In un momento di grandi cambiamenti nel mercato, HESA mette a disposizione dei propri clienti ogni sostegno perché possano accettare e vincere la sfida, in un'ottica di vera e propria partnership. I migliori prodotti sul mercato offerti in esclusiva, le proposte di formazione qualificata, le agevolazioni e i servizi riservati sono il risultato dell'attenzione e dell'impegno che HESA dedica ai partner, che devono saper sfruttare al meglio per cogliere le opportunità che anche una fase come questa può comportare"*.

Un messaggio che riporta in primo piano il ruolo che HESA si è ritagliato nei suoi oltre quattro decenni di storia al vertice del mercato, costruendo con paziente lungimiranza una rete di partner (Concessionari e Installatori Autorizzati) che comprendono e apprezzano i valori di una collaborazione che ha caratteristiche uniche sul mercato nazionale e non solo. In un quadro globale in cui, come logica conseguenza della diffusione dei sistemi in rete nella sicurezza fisica, le modalità di distribuzione si avvicinano sempre più a quelle dei prodotti IT con tutte le specificità di questo settore, il ruolo del distributore che sappia offrire servizi e supporti operativi ai propri clienti installatori e li possa accompagnare verso i loro clienti finali sul territorio, fa veramente la differenza.

Una differenza sulla quale HESA ha costruito la propria storia e il proprio futuro.

Eccellenza nella sicurezza: le migliori novità tecnologiche al Meeting dei Concessionari e Installatori Autorizzati HESA 2016

a cura della Redazione

Il Meeting dei Concessionari e Installatori Autorizzati HESA è non solo un momento di bilancio e di confronto tra i più qualificati professionisti del settore, ma anche una vetrina delle proposte tecnologiche più avanzate presenti nel vasto catalogo HESA. Anche quest'anno l'incontro è stato dunque un momento fondamentale per conoscere in anteprima le novità introdotte nella gamma, che oggi rappresenta la più completa offerta di sistemi e prodotti professionali per la sicurezza, scelti tra le migliori tecnologie presenti a livello mondiale e resi disponibili insieme al più ampio programma di servizi al cliente.

Serie Quaranta – Nel cuore del prodotto

La centrale Serie Quaranta rappresenta il fiore all'occhiello della proposta di HESA riservata alla rete dei propri Concessionari e Installatori Autorizzati. In occasione del Meeting 2016, HESA ha offerto ai propri partner una sessione di lavoro dedicata alle importanti novità che si sono recentemente aggiunte e che sono oggi disponibili a magazzino, pronte per essere utilizzate dai migliori professionisti della sicurezza nelle loro realizzazioni. Un'occasione dunque per conoscere la nuova versione di firmware 2.0 che, come novità principali, introduce le mappe grafiche sulle tastiere touchscreen e l'integrazione delle telecamere tramite le app per dispositivi mobile. Durante i lavori sono stati poi presentati prodotti eccellenti come la sirena Serie Stile collegata su bus, il nuovo rivelatore Q-WDTC senza fili a effetto tenda per esterno a doppia tecnologia (disponibile nei colori bianco e marrone: modelli Q-WDTCB e Q-WDTCM), il rivelatore PIR senza fili Q-PIRD, e il rivelatore a doppia tecnologia senza fili Q-WDT. La presentazione ha riguardato inoltre una nuova e importante serie di rivelatori cablati, sia in versione PIR sia a doppia tecnologia, oggi disponibili in abbinamento alla centrale.

HESAVision – Una gamma completa per la videosorveglianza più evoluta

Il marchio HESAVision è sinonimo di affidabilità e innovazione nell'ambito della videosorveglianza e rappresenta una gamma completamente rinnovata che spazia dalla tecnologia analogica AHD combinata, a quella Over IP, con prodotti caratterizzati da standard qualitativi e prestazioni eccellenti: streaming dedicati alla registrazione in qualità Full HD e 2K (4 MegaPixel), visualizzazione Live e sui dispositivi mobile, una suite di software per la visualizzazione e la registrazione dei flussi su PC e un'applicazione per smartphone e tablet, HV Viewer, che permette di gestire qualsiasi telecamera o NVR in completa mobilità.

La novità di HESAVision presentata in anteprima in occasione del Meeting Concessionari e Installatori Autorizzati HESA 2016 è stata la gamma AHD. I prodotti che la compongono rappresentano la soluzione ideale per impianti di alta qualità, sia nuovi sia in sostituzione di sistemi analogici già esistenti, con un ottimo rapporto prezzo/prestazioni. La tecnologia AHD condivide con l'analogico la stessa tipologia di cablaggio, cavo coassiale, e quindi lo stesso tipo di infrastruttura, l'upgrade richiede la sola sostituzione delle telecamere e del DVR, con la possibilità di migrare anche in modo parziale e graduale. Tutto ciò si traduce in un notevole vantaggio sia di tipo economico che pratico. Inoltre, le telecamere analogiche 960H, registrate su sistemi AHD, migliorano ulteriormente le prestazioni in termini di qualità dell'immagine.

Le novità SAMSUNG - La nuova Serie WiseNet HD+ e molto altro

Per i Concessionari e gli Installatori Autorizzati HESA riuniti all'Isola d'Elba il Meeting 2016 è stato anche l'occasione per conoscere le importanti novità appena introdotte nella gamma SAMSUNG. Dalla Serie WiseNet HD+, una linea completa di telecamere e DVR FullHD 1080p over coax, alle nuove telecamere 4K, ovvero un range di telecamere Bullet, VandalDome e MiniDome con risoluzione 4K e compressione H.265, per una gestione ottimale delle risorse di rete, ai due nuovi NVR a 32 canali Serie XRN-2000 con gestione registrazione e live di immagini 4K e H.265, fino alla gamma di SpeedDome PTZ IP FullHD e HD con processore WiseNet Lite, caratterizzate da un rapporto prezzo/prestazioni particolarmente interessante. Si amplia inoltre la gamma di telecamere complete di plug-in preinstallato per applicazioni specifiche, con un range che oggi comprende un modello per lettura targhe, uno per Timelapse e uno per conteggio persone. Ma le novità non finiscono qui: nella famiglia WiseNet Lite entrano due nuove minidome antivandalo con ottica fissa e IR, di cui una (SNV-L6014RMP) certificata per utilizzo su mezzi mobili; sono inoltre disponibili la nuova versione della telecamera box WiseNet III Full HD con interfaccia in fibra ottica e quella della telecamera SNV-6013P, cui è stata aggiunta la funzione di conteggio persone, e due nuovi modelli di telecamera PinHole della serie WiseNet III con differenti ottiche, che si differenziano dai modelli precedenti per l'aggiunta dell'ingresso audio e dell'uscita video composito.

Oltre alle novità introdotte nella Serie Quaranta e nell'ampio catalogo di proposte per la videosorveglianza, nel corso del Meeting sono stati presentati altri prodotti di punta per la sicurezza antintrusione offerti da HESA – tra i marchi

distribuiti ricordiamo **OPTEX**, **UTC**, **DSC**, **JABLOTRON**, **TEXECOM**, **XTRALIS** - oltre alle soluzioni per l'integrazione e la continuità dei sistemi, con la presenza di **MILESTONE** e di **RIELLO UPS**.

MILESTONE – Soluzioni affidabili e versatili per l'integrazione dei sistemi

In particolare, di MILESTONE è stato presentato il software XProtect® VMS: potente, affidabile, facile da usare e impiegato in più di 100.000 installazioni in tutto il mondo. Sulla base di una vera e propria piattaforma aperta, XProtect VMS consente infatti l'integrazione con un'ampissima scelta di telecamere e soluzioni di business best-in-class, come il controllo degli accessi e l'analisi video. Tra i prodotti presentati anche l'innovativa serie di NVR Milestone Husky ™ che forniscono soluzioni di videosorveglianza completamente integrate e personalizzabili. Questa serie può essere personalizzata per soddisfare le esigenze di qualsiasi installazione di sorveglianza, da una piccola azienda a un impianto di sorveglianza complesso con più siti e centinaia di telecamere. Tra i prodotti di punta ricordiamo poi Milestone Arcus™, una piattaforma di videosorveglianza progettata per essere incorporata in dispositivi hardware. Tutti i prodotti XProtect VMS, Milestone Husky e Milestone Arcus sono compatibili con più di 5.000 encoder, telecamere IP e videoregistratori digitali (DVR) di quasi 150 diversi fornitori in tutto il mondo. Tutti i prodotti MILESTONE sono facili da usare e consentono agli utenti di visualizzare video in diretta, riprodurre registrazioni, indagare su eventi sospetti ed esportare prove video. Dunque soluzioni affidabili e versatili, che consentono agli utenti di aumentare in dimensione e complessità gli impianti in base alle proprie esigenze.

Riello UPS Vision Dual: la serie di UPS in versione tower/rack per chi esige un sistema di alimentazione con elevata protezione

Nel corso del Meeting Concessionari e Installatori Aurizzati HESA 2016 sono stati presentati i gruppi di continuità Vision Dual di Riello UPS, che comprendono modelli da 1100VA a 3000VA con tecnologia Line-Interactive ad onda di uscita sinusoidale. Installabili sia in configurazione tower che in armadi rack 19", i Vision Dual sono caldamente consigliati per la protezione dei dispositivi presenti nei moderni impianti di videosorveglianza. Infatti componenti quali telecamere, switch, router, DVR, server e monitor sono fortemente soggetti a guasti in presenza di perturbazioni di rete (sovra e sotto tensioni, variazione di frequenza e transitori).

Gli UPS Line-Interactive sono dunque ideali per la grandissima maggioranza degli impianti di videosorveglianza, dove si fanno apprezzare per il costo contenuto, per la facilità di installazione e i bassi costi di gestione. In coerenza con la filosofia Riello UPS *"Reliable Power for a Sustainable World"* i Vision Dual godono di un fattore di potenza in uscita di 0,9 e garantiscono prestazioni eccellenti con rendimenti pari al 98%, permettendo ridotti consumi energetici. Il display LCD retroilluminato fornisce indicazioni sullo stato dell'UPS, del carico e sulle condizioni delle batterie; i Riello UPS Vision Dual 2200VA e 3000VA possono essere abbinati a pacchi batterie esterni per aumentarne l'autonomia, arrivando a svariate ore con l'utilizzo delle versioni ER.

Infine i Vision Dual hanno un set di comunicazione assolutamente evoluto, multipiattaforma, compatibile con tutti i sistemi operativi ed ambienti di rete, con software di supervisione e shut-down Powershield3 incluso. Le interfacce presenti sono USB e RS232 ed è presente anche uno slot di espansione per schede di interfaccia di rete.

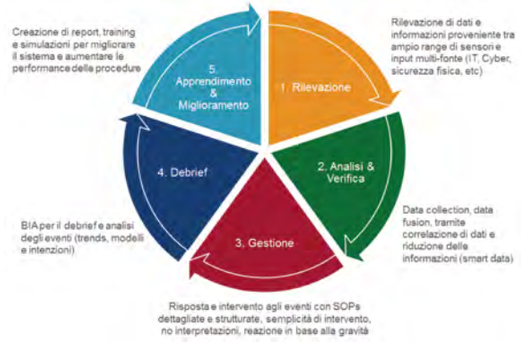
Minacce combinate, la nuova frontiera della sicurezza in banca

a colloquio con Maurizio Tondi, VP Strategy & Business Process Support Axitea
a cura della Redazione

Il profondo cambiamento in corso nel sistema bancario sta spostando sempre più l'attenzione verso le minacce informatiche o di tipo "combinato". Qual è la vostra visione sul tema?

Rispondo facendo una premessa e una domanda: ma i Big Data sono un bene o no? Dipende certamente dal campo di applicazione. Per chi deve, in una Control Room, in un Security Operation Center o all'interno di un CERT (Computer Emergency Response Team) o CSIRT (Computer Security Incident Response Team) gestire con tempestività, accuratezza ed efficacia migliaia di allarmi provenienti da decine di migliaia di sensori, stati dinamici ed informazioni multidimensionali in tempo reale, potrebbero essere un problema. Vale per ogni tipologia di industria e, certamente nel settore bancario dove la ricchezza di informazioni è strumento di grande qualità per la gestione del Cliente. Tuttavia disporre non tanto di una grande mole di dati, ma di quelli "giusti" e delle corrette correlazioni tra informazioni critiche - che provengono da domini fisico-logico ancora separati basati su tecnologie multivendor, nella complessità ed eterogeneità tecnologica delle infrastrutture di servizio delle Banche - è certamente la modalità più efficace per garantire qualità di servizio e di intervento. Evidentemente anche la Banca è "mission critical" da questa prospettiva; non solo, quindi, per la dipendenza del sistema transazionale, dove la riduzione del down time è cruciale, ma data la natura del servizio, dove la tempestiva gestione degli incidenti, degli eventi ed il relativo reporting è parte della gestione del rischio. E' qui che l'utilizzo di piattaforme moderne ed innovative per la gestione di situazioni di emergenza - **Situation Management** - può semplificare e rendere più efficace le modalità di gestione di allarmi e di intervento nel contesto di un CERT, iniziando da una corretta definizione delle SOPs (Standard Operating Procedures) degli operatori impegnati nella supervisione e nel controllo della sicurezza delle agenzie, delle filiali e delle persone. Una questione di "informazioni" ma anche di infrastruttura tecnologica per garantire continuità di servizio, sicurezza, integrità e protezione. In un contesto in cui la convergenza, se non l'integrazione tra impianti di sicurezza fisica e sistemi per la protezione informatica è evidente, oltre che necessaria. Le minacce e gli attacchi sono, infatti, sempre più sofisticati e trasversali e si basano su piani di penetrazione articolati per sfruttare vulnerabilità del domino fisico e di quello logico indifferentemente. Da sempre la Banca è un target preferenziale del cyber crime dove si concentrano ed intrecciano -

Processo di gestione attraverso le piattaforme di Situation Management

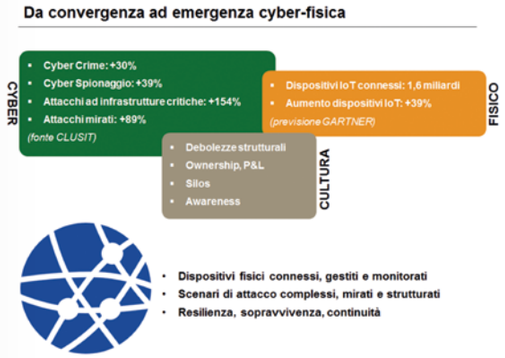


con modalità differenti che sfruttano competenze anche differenti ma che sono animate dallo stesso obiettivo criminoso - frodi, estorsioni, sottrazione di informazioni critiche, furti di identità digitali, ATM malware, fino ai più recenti spear phishing, APT (Advance Persistent Threats) e social media. Botnet e sistemi distribuiti sono in grado di lanciare sofisticati DDoS (Distributed Denial-of-Service) per inibire il servizio di una Banca a meno che non venga pagato un riscatto; attacchi ai social media attraverso falsi profili e account compromessi possono agevolmente ottenere informazioni mediante social engineering; mail falsificate ad-hoc provenienti dall'organizzazione o da colleghi possono indurre al rilascio di informazioni riservate e sensibili; codice malevolo che colpisce gli ATM prelevando denaro o manipolando transazioni (ad esempio: Ploutus, Tyupkin, GreenDispenser). Ma anche i non meno dannosi e pericolosi attacchi fisici agli ATM con più o meno sofisticati strumenti che, oltre alla sottrazione del denaro, provocano danni alle strutture ed evidentemente possono contribuire a creare un clima di insicurezza per il Cliente nella fase di interazione con l'ATM di agenzie sempre meno presidiate.

Quali sono le risposte che un Global Security Provider come Axitea può offrire alle mutate esigenze del sistema bancario?

Se il profilo di attacco è realmente integrato ed è strutturato per sfruttare tutte le debolezze dello spazio cyber-fisico, nonché quelle spesso più rilevanti dell'essere umano, la risposta deve essere necessariamente adeguata a questa escalation, a questo pericoloso innalzamento di profilo. La base è, innanzitutto, una **visione integrata** che includa consapevolezza, competenza e "cultura" della sicurezza da parte del personale; **metodologie innovative** per la gestione e valutazione del rischio e per la gestione programmata degli interventi, anche quelli manutentivi che possono mettere a rischio l'integrità o il funzionamento di un sistema od offrire un punto di ingresso nel sistema compromettendo così la sicurezza di informazioni ed asset critici. Pensiamo agli attacchi a qualche Banca internazionale portati attraverso le credenziali di accesso poco protette di un sistema di HVAC (Heating, Ventilation and Air Conditioning) con danni anche rilevanti in termini di immagine. Le minacce stanno emergendo come mai si era registrato fino ad oggi e, spesso, a ciò si aggiunge una debolezza strutturale nella gestione integrata della sicurezza da parte delle Aziende, per natura guidate dal business, dal P&L e dall'accettazione della "forza maggiore" e della "conformità normativa". Dall'evidenza che tutti gli attacchi del passato conosciuti, si sono dimostrati "trasversali" e hanno coinvolto elementi informatici, fisici, umani ed organizzativi, emerge 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. Ed in ultimo, ma certamente non meno importante, la disponibilità di **piattaforme tecnologiche** abilitanti e soluzioni per la gestione integrata della sicurezza della Banca. Axitea è, quindi, convinta che un approccio orientato alla "full security" possa coniugare e fondere in un'unica proposizione i servizi awareness (attraverso adeguata formazione, specializzazione e certificazione del personale coinvolto nelle procedure di sicurezza), le metodologie (un approccio di tipo olistico con attività ad esempio di assessment e penetration test attuate su tutto lo spazio cyber-fisico per supportare la Banca nella individuazione di potenziali punti di vulnerabilità ed attuare immediate procedure di remediation) e le soluzioni tecnologiche avanzate, come la realizzazione di un sistema di Situation Management. Per Axitea - che integra sia competenze e prerogative tipiche dell'istituto di vigilanza, centrali operative ed una consolidata esperienza nelle gestione degli allarmi e degli interventi, sia competenze specialistiche nella scouting tecnologico, nella progettazione, realizzazione e manutenzione di impianti di sicurezza anche complessi e personalizzati - la parola chiave è **"life cycle"**: una gestione continuativa della postura di sicurezza delle Aziende adeguata all'evoluzione delle minacce, modulata sul profilo di rischio ed in grado di evolvere secondo le esigenze ed i requisiti del "sistema" del cliente.

In che modo sviluppate il modello di Situation Management per una Banca?



In questo contesto anche la progettazione, la realizzazione o l'integrazione di un Situation Management, che nel caso delle Banche può essere l'asset tecnologico a supporto dell'organizzazione e dei processi sui cui opera il CERT, può avere elementi cruciali già inizialmente, nella fase di assessment dove è fondamentale effettuare una verifica a tutti i livelli dei potenziali e reali punti di vulnerabilità dell'azienda (varchi, ingressi, mezzi di trasporto, parcheggi, personale aziendale, fornitori, partner, sistemi informativi aziendali, sistemi tecnologici, dispositivi fissi e mobili, procedure, etc.) e di realizzare l'immediata messa in sicurezza di asset fisici, dati, infrastrutture, know-how, proprietà intellettuali, personale chiave, attività mission critical e di definire e implementare un processo di manutenzione continuativa focalizzato sul miglioramento e sul mantenimento del livello complessivo di sicurezza della Banca. Viceversa la presenza di sistemi legacy e modalità operative stratificate devono essere valutate con attenzione: le prime in termini di interoperabilità, flussi ed alimentazione di dati, informazioni, stati e segnali che devono - adeguatamente trattati e normalizzati - raggiungere i cruscotti operativi del Situation Management; le seconde per determinare con efficaci procedure standard che rappresentano, a fronte del rilevamento ed acquisizione di un allarme, la baseline comportamentale degli operatori, elementi cruciali per la gestione degli interventi con precisione, efficacia e misurabilità. Anche in funzione dei KPI di servizio che sono stati definiti e delle necessità di reportistica e compliance che le Banche in primis devono osservare. Il Situation Management - come piattaforma software aperta, scalabile e modulare - è in grado di correlare diversi sistemi e sensori e molteplici domini (customer service area, ATM, data center, cash vault, computer, rete, punti di accesso, porte, gate, etc.) consente di avere quindi in ogni momento il quadro complessivo della situazione, la gestione facilitata con procedure operative e, attraverso l'utilizzo di Business Intelligence Analysis (BIA), il supporto intelligente alle decisioni, il supporto intrinseco al filtraggio di informazioni, il riuso di sistemi di sicurezza e safety preesistenti, procedure di escalation e di collaborazione strutturata tra i diversi livelli gerarchici. Ciò si traduce in una maggiore efficienza nel processo decisionale (diminuzione degli errori) in scenari di emergenza e di routine, gestione delle risposte agli eventi critici con continuo miglioramento dell'intervento e riduzione del tempo di trattamento degli incidenti/eventi ed il completamento del ciclo con la creazione di report, training e simulazioni per migliorare il sistema e aumentare le performance delle procedure e la mitigazione complessiva del rischio.

axitea
SECURITY EVOLUTION

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

Dalle Control Room delle grandi banche i modelli di servizio su base PSIM per le moderne Società di Security

di Nils Fredrik Fazzini, general manager di CITEL spa

L'immagine è una composizione che intende solo dare una idea della diffusione delle soluzioni di CITEL Spa nella fascia alta del sistema bancario, Poste Italiane comprese; **una fascia di utenti che è stata anche la culla italiana del PSIM**, il sistema per l'informatizzazione della sicurezza fisica in architettura aperta su rete dati, con estensioni multifornitore, multimediale e multifunzione, comprese quelle funzionalità che assicurano la *compliance* a tutta la normativa in vigore riguardo alla sicurezza, la safety e la continuità operativa.

Il tema non è quello dei grandi gruppi bancari ma **dell'effetto che stanno producendo le innovazioni nate nelle loro Control Room** su piattaforme Centrax di Citel ora che a richiederle sono le **banche minori e gli Istituti di Vigilanza decisi a perseguire nuovi modelli di impresa** con un cambio di passo basato soprattutto sulle tecnologie di telegestione in architettura aperta multifornitore. Un modello adottato dalle grandi banche da almeno 15 anni e che ora viene preteso anche dalle banche minori in forma di servizio.

È quindi in corso un **processo evolutivo in cui Citel è coinvolta in pieno** e che sta portando una ventata di innovazione in chiave PSIM presso nomi significativi del settore della vigilanza, su un terreno che non è tanto tecnico quanto di affrancamento rispetto all'immagine stereotipata dell'Istituto di Vigilanza, per passare a **uno status di Società di Security come Centro Servizi specializzato, moderno, efficace**.

Ben venga quindi lo stimolo del settore del credito per creare modelli di servizio che hanno portato a risultati importanti dimostrati dalle statistiche OSSIF, condivisibili anche dalle banche minori verso cui stanno convergendo i recenti modelli di Società di Security.

Anche di questo si è parlato al **Convegno Banche e Sicurezza tenutosi di recente a Milano** nel maggio scorso, dove Nils Fredrik Fazzini, DG di CITEL Spa, è intervenuto sul tema dell'innovazione in chiave PSIM a fronte delle nuove minacce e i nuovi processi gestiti dall'intelligenza delle piattaforme, dalla loro interoperabilità e dall'interattività multimediale da Control Room che virtualizza le distanze.

Le banche minori, il PSIM e le società di servizi di security, la multifunzionalità

CENTRAX è il primo e più diffuso PSIM in Italia tra i grandi istituti di credito, ma **è sempre più accessibile anche alle banche di minori dimensioni**, che non possono pensare di dotarsi di una propria Control Room H24 ma che, comunque, non intendono fare a meno delle funzionalità e del livello di servizio che un PSIM assicura ai grandi utenti dotati di strutture interne.

La domanda di sicurezza fisica professionale da parte delle banche minori **converge con il tema dello stimolo alla crescita degli istituti di vigilanza e della loro evoluzione verso modelli di Società di Security informatizzate, in grado di soddisfare (e se possibile anticipare) una domanda che chiede servizi che vanno ben oltre il teleallarme tradizionale**.

In ogni caso le banche piccole e medie hanno le stesse esigenze delle grandi in termini di sicurezza e di compliance, ma non hanno la convenienza di dotarsi internamente dell'intera filiera informatizzata – dal centro di controllo e gestione (la Control Room) fino al sito protetto – e pertanto, esattamente come è già accaduto per l'informatica gestionale, si indirizzeranno verso soluzioni di servizio, di tipo consortile (ad esempio in combinazione con il fornitore di servizi informatici) o da fornitori di servizi di sicurezza purché specializzati e di affidabilità a tutta prova.

Quei fornitori specializzati e informatizzati esistono già: sono gli istituti di vigilanza che hanno già affrontato quel percorso evolutivo che porta ad affrancarsi dalla logica esclusiva dei teleallarmi chiusi, inadatti ad effettuare teleoperazioni in un ambito complesso e critico come quello dell'agenzia bancaria connessa su rete dati.

Dai sistemi chiusi della vigilanza al PSIM aperto, multiservizi e multimediale delle nuove Società di Security

Al contrario dei teleallarmi chiusi, infatti, **un PSIM conforme a tutti i requisiti è un sistema di telegestione aperto e autocontrollato che, come tutti i sistemi professionali ad alta resilienza: prescinde**

dall'affidabilità e abilità dell'operatore di Control Room e anche da quella dell'utente stesso:

- accetta soltanto le attività consentite dal profilo autorizzativo, guidando passo passo l'operatore lungo un processo di gestione che mette a disposizione in automatico oggetti contestualizzati per video-ispezione, per fonia digitale bidirezionale, per attivazioni correlate di dispositivi, per informazione e mobilitazione di risorse e servizi di terzi;
- inibisce le funzioni non autorizzate per il profilo dell'operatore, presentando solo quelle previste, segnalando i comportamenti anomali, fino a trasferire il controllo a un livello superiore o di emergenza in caso di ritardi di gestione, sequenze di operazioni sospette, reiterazione di operazioni non autorizzate;
- traccia e documenta gli eventi e la loro gestione.

Sempre in contrapposizione ai sistemi di teleallarmi chiusi monofornitore, il PSIM punta anche alla multifunzionalità per l'erogazione di una rosa completa di servizi, con soluzioni per il monitoraggio e **la telegestione di applicazioni sinergiche con la sicurezza: la safety, le teleportinerie e telereception, gli allarmi tecnici, il monitoraggio dei consumi**.

Tuto questo si traduce in una condizione di libertà di progettare l'evoluzione del sistema di telegestione che, nel caso di una Società di Security, vuol dire poter contare su soluzioni funzionali disponibili e collaudate a bordo del sistema di Control Room senza costringere il cliente a costosi interventi sugli apparati e sistemi già in esercizio.

La possibilità di adattarsi all'ambiente tecnico/funzionale esistente oltre il puro teleallarme è in effetti la chiave di volta per proporre nuovi tipi di servizio a valore aggiunto; ma la sua realizzazione è assolutamente vincolata a una sistemistica come quella di Centrax-PSIM, unica ad avere nel mercato un Ecosistema di soluzioni tecniche già fun-zionanti e referenziate da utenti di vari settori, oltre alle banche. Tutti accomunati dal rifiuto delle architetture chiuse monofornitore.

L'Ecosistema di Centrax-PSIM è alimentato dalle esperienze di oltre 100 sistemi nei vari settori dell'industria, del retail e del governo locale per applicazioni evolute, da circa 130 moduli di integrazione verso terze parti per l'interoperabilità di altrettanti apparati, sistemi, applicazioni, fino alle APP per dispositivi IOT, dagli smart-phone agli smart-watch.

La nuova Società di Security come Centro Servizi su base PSIM per il settore bancario (e non solo)

È già nei fatti da alcuni anni una transizione dei servizi della Vigilanza verso forme evolute di servizio, dopo essersi limitate ad eseguire nelle Control Room dei grandi utenti, servizi operativi con personale qualificato.

D'altronde, quando la tecnologia informatica è coinvolta – come nel caso del PSIM – si può essere certi che la spinta evolutiva potrà supportare in modo decisivo quelle vigilanze che intendono passare dalla fornitura di tempo-uomo per grandi banche ai servizi a valore aggiunto per banche di dimensioni minori, con servizi dello stesso livello di quello che le grandi banche ottengono con le proprie Control Room.

Oltretutto, nella valutazione del potenziale utente, **il PSIM è proprio quel tipo di sistema che – per sua stessa natura – dà quelle garanzie che inducono ad affidarsi a un servizio esterno:** gli eventi che si verificano all'interno della banca verranno gestiti secondo una procedura automatizzata e tracciabile per il tipo di evento, da un operatore guidato passo-passo, senza che sia tenuto a conoscere lo specifico sito essendo assistito dall'abbinamento visuale di mappe, planimetrie e sinottici dotati di oggetti dinamici, con flussi video pertinenti, con sequenze di azioni a pulsante per comandi contestualizzati.

Ma per ottenere una reale equivalenza rispetto al servizio ottenibile da un sistema interno alla banca è necessario che vengano rispettati **altri due paradigmi oltre al paradigma PSIM:**

• i**l paradigma della telegestione professionale**, per cui le connessioni Control Room – utente devono passare per una rete dati bidirezionale, con protocollo pubblico (come quello voluto dall'ABI), con la possibilità di indirizzare il singolo sensore/attuatore, con un grado di protezione al massimo livello previsto dalla norma e backup automatico su rete secondaria; in definitiva la **soluzione digitale che garantisce l'architettura aperta multifornitore e multimediale per la virtualizzazione della distanza** per dati, immagini, fonia;

• un **catalogo di applicazioni** standardizzate, basate sull'integrazione di prodotti e sistemi di mercato che la banca deve essere libera di adottare indipendentemente dal PSIM utilizzato; nella pratica, quindi, un portafoglio di soluzioni applicative e di moduli di integrazione pronti per l'uso e non da sviluppare su progetto a spese dell'utente, il che presuppone che il PSIM evolva continuamente dietro la spinta e la collaborazione di **un proprio Ecosistema ampio e diversificato composto da utenti e terze parti complementari.**

Le tendenze nell'evoluzione delle applicazioni interattive e multimediali con il coinvolgimento di Guardie Giurate

Negli ultimi anni i servizi che le banche hanno chiesto alla vigilanza sono cambiati in relazione all'andamento delle minacce e alla necessità di minimizzare i costi fissi / ricorrenti. Senza entrare – per ragioni deontologiche – nel rapporto causa-effetto, si può sostenere che nell'ultimo decennio:

- l'investimento delle banche si è concentrato sul rischio rapina, in particolare sugli erogatori temporizzati con teleasservimento a video-ispezioni da Control Room e coinvolgimento dei processi informatici; per questo motivo, associato alla videosorveglianza interattiva e dissuasiva da Control Room, il numero (e il danno) delle rapine brevi ha iniziato a scendere;
- le rapine lunghe tendono invece ad aumentare, in particolare negli sportelli più piccoli, ma possono essere contrastate dalla video-sorveglianza "intelligente" opportunamente correlata;
- la variante della rapina lunga, quella in versione di *comitato di accoglienza* – che riguarda anche gli sportelli più grandi – viene dato in crescita, ma può essere fronteggiato con una protezione completa del perimetro della filiale e dei vani critici, oppure con forme *intelligenti* di video-*patrolling*;
- i caveau sembrano tornati di attualità, probabilmente per aspettative crescenti sul bottino, e con rischi maggiori nei casi in cui il frequente alternarsi di fornitori di servizi (riferibile alle politiche acquisto a mezzo gara) non sia bilanciato da specifiche misure anti-infedeltà.

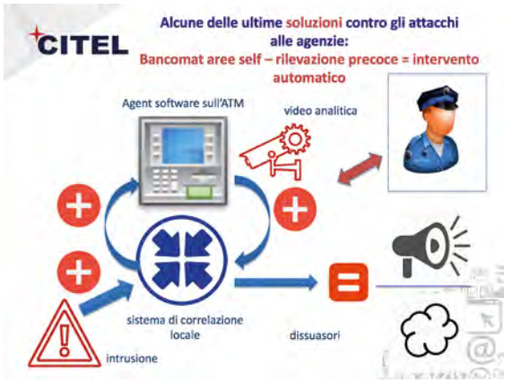
Nella casistica riportata, il ruolo del PSIM multimediale in architettura aperta non è solo utile ma indispensabile, sia per la banca che per chi si propone come fornitore di servizi. Si tratta infatti di applicazioni ad elevato grado di integrazione tra sistemi, compresi anche il sistema informatico della banca e quello di gestione degli ATM, interoperanti con il PSIM su flussi interamente informatici e quindi quasi istantanei, e con sistemi di patrolling e di videosorveglianza interattiva e bidirezionale a scopi dissuasivi.

I processi di telegestione interattiva in ambito bancario con il coinvolgimento della Società di Security

Le figure sono tratte dalla presentazione di Citel al convegno ABI Banche e Sicurezza 2016 – forniscono un'idea sintetica delle applicazioni che una infrastruttura PSIM può permettere, che è in uso corrente nelle banche maggiori, accessibile anche alle banche minori in forma di servizio.

Si tratta di applicazioni che sono state maturate e affinate nel corso di diversi anni tra i grandi utenti PSIM di Citel e che vedono oggi coinvolte le società di security più dinamiche in un ruolo di fornitore di servizi a valore aggiunto e non più in quello che subiva l'innovazione in un ruolo puramente esecutivo.

Si tratta di processi efficienti che sono stati maturati e affinati nel corso di diversi anni tra alcuni grandi utenti PSIM di Citel e che vedono oggi coinvolte le società di security più dinamiche in un ruolo di fornitore di servizi a valore aggiunto e non più in quello che subiva l'innovazione in un ruolo puramente esecutivo.



Bancomat e Aree Self-banking: processo per la rilevazione precoce per via informatica dell'attacco con reazioni dissuasive e interdittive immediate.

Caveau: protezione specifica anti-manomissione e anti-infedeltà della filiera da sensore a supervisore centralizzato.

Caveau: sistemi per l'accesso verificato e condizionato da procedura informatica.

Agenzia: video-ispezioni / verifiche automatizzate con algoritmi di videoanalisi centralizzati multivendor.

Come cambia la gestione del contante nella distribuzione al dettaglio

a colloquio con Roberto Licinio, Business Segment Manager Retail & CIT Italy di Gunnebo Italia spa
a cura della Redazione

Come si sta evolvendo a livello europeo la gestione della fisicità della moneta nella distribuzione al dettaglio, diventata il principale collettore del denaro contante, che rimane a livelli elevati malgrado gli sforzi delle istituzioni di riferimento per la virtualizzazione dei sistemi di pagamento?
Il contante suscita sentimenti contrastanti. Le istituzioni guardano con sospetto soprattutto i tagli più "pesanti" (500 euro, 1000 franchi svizzeri, 100 dollari USA, 50 sterline britanniche) che, grazie all'elevato valore concentrato in un volume minimo, sono ambite anche da operatori con motivazioni non cristalline; pratiche e normative a livello comunitario tendono a favorire l'uso delle forme elettroniche di pagamento, la cui tracciabilità è un serio ostacolo per evasione o transazioni illecite. L'attrattiva esercitata dal contante su chi intende delinquere preoccupa anche i retailer, consapevoli dei rischi derivanti dalla presenza di elevate quantità di monete e banconote nei negozi. D'altro canto, i vantaggi del contante - fra gli altri, l'assenza di costi e intermediazioni, l'immediatezza e la fiducia accordata alle transazioni in contanti anche dai clienti restii all'adozione di forme di pagamento più moderne - lo rendono irrinunciabile per il retail. Rendere più sicuro un mezzo di pagamento pratico e diffuso come il contante è l'obiettivo dei moderni sistemi di Cash Management, sempre più evoluti anche dal punto di vista dell'integrazione con il trasporto valori e il sistema bancario.

Quali sono le caratteristiche peculiari del mercato italiano rispetto agli altri paesi europei su questo tema? Quali sono gli orientamenti dei principali protagonisti nel nostro paese, sia in ambito retail che GDO?
Una certa diffidenza verso i sistemi di pagamenti elettronici è un fenomeno che caratterizza il nostro mercato, forse anche legato alla particolare demografia dell'Italia, fra le nazioni più "anziane" al mondo; l'uso del contante è di conseguenza più frequente che in altri paesi. La presenza di contante non è incompatibile con la sicurezza: i moderni sistemi di Cash Management sono stati progettati anche per questo. La GDO sta svolgendo un ruolo di apripista con l'introduzione di sistemi a ciclo chiuso sempre più efficienti e sicuri; alcune categorie di retailer particolarmente esposti ai rischi conseguenti dalla presenza di contante, come le farmacie, prendono esempio, anche grazie alla disponibilità di soluzioni compatte e convenienti, alla portata dei dettaglianti tradizionali. Le caratteristiche della distribuzione commerciale tradizionale italiana - frammentata, con catene lunghe, superfici piccole e logistica spesso subordinata ai dettami di un'edilizia plurisecolare - rendono necessarie queste soluzioni "su misura", per consentire anche ai dettaglianti un utilizzo del contante conveniente e sicuro.

Gunnebo è un'eccellenza europea nei sistemi di cash-management per il retail. Quali sono le caratteristiche delle vostre soluzioni in termini hardware e software per dare sicurezza e ottimizzare la gestione finanziaria del negozio?
L'eccellenza tecnologica delle soluzioni Gunnebo, garantita dagli investimenti costanti in ricerca e sviluppo che un grande gruppo multinazionale può permettersi, è sicuramente alla base del successo dell'azienda in questo segmento, ma non è il solo fattore critico. La varietà delle situazioni presenti nel nostro Paese - dalle grandi catene che per efficienza e modernità non hanno nulla da invidiare al resto d'Europa, ai negozi dei centri storici, dove a rapporti spesso sorprendenti fra fatturato e superficie si contrappongono situazioni logistiche a dir poco originali, che richiedono soluzioni particolarmente flessibili e creative - rende fondamentale la capacità del personale tecnico e commerciale di lavorare a fianco del cliente per identificare la soluzione migliore, assicurarsi che l'integrazione fisica e l'implementazione nel flusso di lavoro quotidiano avvengano nel modo migliore e che i risultati corrispondano pienamente alle aspettative. L'esperienza e la competenza dei professionisti Gunnebo sono parte integrante della soluzione, un aspetto senza il quale gli elementi tecnologicamente innovativi e le caratteristiche all'avanguardia dei macchinari non riuscirebbero a esprimere pienamente il loro potenziale all'interno del negozio.

Possiamo descrivere qualche storia di successo, in Italia e nel resto dell'Europa?
L'articolata struttura commerciale Gunnebo permette ai retalier di tutta Europa di rivolgersi a team che conoscono la realtà del mercato di riferimento; l'azienda è infatti multinazionale, ma mantiene un rapporto decisamente "locale" coni vari territori, e per questo Gunnebo Italia si concentra sui propri mercati di riferimento. Le applicazioni di successo sono numerose: basti ricordare gli ottimi risultati ottenuti con l'introduzione del sistema presso i negozi Leroy Merlin. SafePay™ ha permesso a questa grande insegna di focalizzare le squadre dei negozi sulla costruzione di una relazione unica con i clienti. La possibilità per il cliente di effettuare da solo il pagamento riduce lo stress per il personale di cassa, a favore di un focus maggiore sulla relazione con il cliente, sulla sua esperienza di acquisto e sui suggerimenti per migliorare i servizi.
SafePay™ è un sistema già apprezzato da molti retailer in Italia e in Europa per i numerosi benefici

che apporta: al personale, liberato dalla responsabilità della gestione del contante; al rapporto con il cliente, poiché il personale ha più tempo da dedicargli; come anche alle attività amministrative e contabili. Questo sistema di Cash Management a ciclo chiuso permette al cliente di eseguire da solo il pagamento in denaro, liberando il personale di cassa da compiti ripetitivi e faticosi e rendendo le operazioni di cassa più facili e sicure.

SafePay™ azzera il problema dei resti e delle differenze di cassa e identifica i falsi con un'affidabilità certificata dalla BCE. Grazie a SafePay™, il ciclo del contante dalla cassa al cash-in-transit è completamente chiuso e sicuro, e il flusso del denaro non è mai stato così semplice. Il sistema presenta, inoltre, una procedura di manutenzione semplice e immediata. SafePay™ è in realtà affidabile e robusto e di rado richiede interventi di manutenzione ma, nel caso in cui questa necessità si presenti, il sistema è totalmente controllabile da remoto: l'operatore può prendere contatto con il centro Help Desk SafePay™ di Gunnebo e procedere a una rapida risoluzione del problema, eliminando piccoli guasti (un oggetto incastrato nel contamonete, ad esempio) senza il fermo macchina e con costi di manutenzione praticamente azzerati.

Come tutte le soluzioni Gunnebo, SafePay™ è personalizzabile - nel caso di Leroy Merlin, ad esempio, sono stati adottati i colori dell'insegna ma, soprattutto la sua implementazione è seguita dal personale specializzato Gunnebo in modo che, in ogni punto vendita, possa avvenire nel modo più fluido possibile, rispettando le particolarità di ogni situazione e portando in tempi rapidi a poter fruire di tutti i vantagi offerti da questa soluzione.

SafePay™ è uno degli elementi che rafforzano la posizione di leadership di Gunnebo nel segmento del Cash management, ma le soluzioni di sicurezza per il retail riguardano anche numerosi altri aspetti, dai sistemi di regolazione dei flussi di transito e controllo degli accessi ai mezzi forti. Gunnebo si pone infatti come interlocutore unico per tutte le esigenze di sicurezza, grazie all'ampiezza della gamma di soluzioni offerte e alla capacità dei professionisti Gunnebo di adattarle perfettamente alle esigenze del cliente.

GUNNEBO
For a safer world®

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

Premio H d'oro 2015 Categoria INFRASTRUTTURE E SERVIZI

a cura della Redazione

Categoria: **INFRASTRUTTURE E SERVIZI**
Azienda installatrice: **SELCOM - Casavatore (NA)**
Denominazione e località dell'impianto: **Area Marina Protetta di Porto Cesareo**
Impianto realizzato: *Sistema di sicurezza integrato terrestre e marino*

La società **SELCOM** di Casavatore (NA) ha vinto il Premio H d'oro 2015 nella categoria Infrastrutture e Servizi per il sistema di sicurezza integrato terrestre e marino dell'Area Marina Protetta di Porto Cesareo, in provincia di Lecce.

Descrizione dell'impianto

Il contesto installativo in cui è stato implementato il progetto è rappresentato dall'**Area Marina Protetta (AMP)** di **Porto Cesareo**. Dinnanzi all'esigenza di una tutela adeguata ed efficace degli ecosistemi marini e costieri, le AMP rappresentano una risposta concreta grazie alla loro funzione di gestione e regolamentazione delle attività legate al mare, alla creazione di aree marine protette soggette a vincoli che le isolano dalle zone circostanti, alla protezione di determinati siti, ottenendo una gestione più ampia dell'area costiera marina.

L'impianto che è stato realizzato rappresenta un evoluto **sistema integrato di sicurezza terrestre e marino**, in grado di supportare e semplificare, rendendola più efficace, l'attività svolta dalla AMP di Porto Cesareo.

In particolare, il sistema è in grado di soddisfare i seguenti obiettivi:

- individuare tempestivamente situazioni anomale e di pericolo per le risorse dell'AMP (sversamenti di liquidi, presenza di natanti con caratteristiche non compatibili con il regolamento dell'AMP, presenza di pescatori non autorizzati o di pescatori subacquei, ancoraggio in zone interdette, sbancamento delle dune);

- monitorare le infrazioni al regolamento e studiarne le modalità per prevenirne la reiterazione;
- raccogliere dati statistici su tipo e luogo delle infrazioni più dannose in modo da individuare le migliori strategie di prevenzione;
- supportare le unità in mare durante le operazioni di pattugliamento congiunte AMP/ Capitaneria di Porto.

La soluzione si basa su un approccio integrato tra tecnologie quali la videosorveglianza, il monitoraggio territoriale, e l'analisi delle immagini.
L'intero sistema, dall'infrastruttura di comunicazione tra le postazioni di osservazione, alle videocamere, al sistema intelligente di monitoraggio del territorio, è basato su tecnologie completamente digitali.

Nell'ambito del progetto sono state installate telecamere fisse, PTZ e termiche (di queste, 1 fissa e 2 PTZ).

Le **telecamere di tipo "Speed Dome"** permettono di inquadrare vaste aree grazie al controllo del brandeggio e dello zoom, coprendo aree di ampio raggio e consentendo uno zoom della scena ripresa ed una inquadratura sufficientemente dettagliata per cogliere i particolari.
Le **telecamere fisse** permettono di visualizzare immagini di contesto e scene statiche e sono adatte quindi a controllare una determinata area della scena; nella fattispecie grazie la lente grandangolare consente la videosorveglianza delle installazioni realizzate.
La **telecamera di tipo "Termica Fissa"** fornisce un' analisi termica della scena, rivelandosi un ottimo strumento per la prevenzione degli incendi. Considerando che le infrazioni che più danneggiano le risorse dell'AMP avvengono di notte, condizione ideale per i pescatori abusivi, sub ed eventuali sversamenti di liquidi pericolosi in mare, le termocamere di sicurezza consentono di scorgere distintamente natanti e/o subacquei nella più totale oscurità e anche in presenza di condizioni climatiche avverse. Le termocamere inserite nel progetto sono studiate per applicazioni di sicurezza e sorveglianza a medio raggio e permettono di rilevare oggetti a una distanza di oltre 2.4 km.

Il sistema è costituito dai seguenti blocchi funzionali:
- Punti periferici di ripresa;
- Infrastruttura di rete a supporto del sistema:
- Centro di gestione e controllo del sistema.

I segnali generati dagli impianti di security sono remotizzati presso la Control Room, ovvero il locale preposto alla gestione del sistema e all'archiviazione dei flussi video. La **Control Room** è suddivisa in Sala Apparati, per le componenti hardware e software, e in Sala Regia, dove sono presenti le postazioni di gestione e visualizzazione dell'impianto.

Per la visualizzazione dell'impianto di security sono state realizzate tre sale regia: presso la sede dell'Area Marina Protetta, presso la sede della Capitaneria di Porto e presso l'avanposto della Capitaneria di Porto.

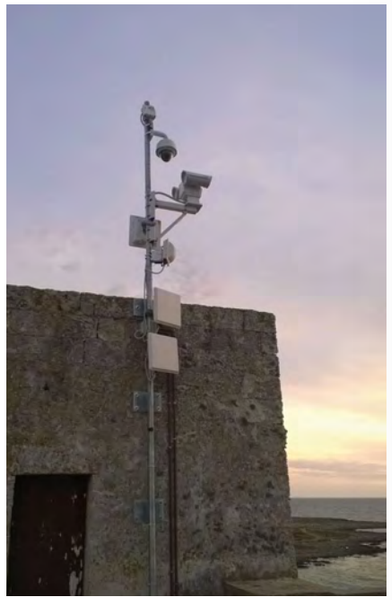
Per quanto riguarda l'infrastruttura di rete, è stata implementata una **rete wireless di tipo a maglia**, opportunamente dimensionata in modo tale da:

- supportare ampiamente la banda minima necessaria richiesta, essendo l'architettura caratterizzata da link radio sovradimensionati;
- garantire un'alta resistenza alle interferenze, mediante apparati affidabili;
- garantire la disponibilità delle frequenze e del numero di canali necessari a garantire la connettività di tutti gli apparati di campo.

Sono state realizzate interconnessioni tra le postazioni attraverso una rete a maglia rendendo la rete meno sensibile ai guasti dei collegamenti o dei nodi, poiché si instaurano percorsi alternativi garantendone così il funzionamento e aumentando la performance e l'affidabilità del sistema.

Il vero plus della soluzione implementata è una **piattaforma di gestione unica** in grado di fornire un'interfaccia unica e semplificata per la gestione delle immagini provenienti dalle telecamere, ma anche delle segnalazioni di allarmi provenienti dalle **centrali periferiche di antintrusione, controllo accessi e dal sistema di monitoraggio e sorveglianza della costa**.
Il vantaggio di utilizzare un'unica interfaccia diviene importante se si considera la correlazione tra le diverse segnalazioni di allarmi in un contesto installativo caratterizzato da una forte disomogeneità di apparecchiature. La piattaforma di gestione unica si pone come accentratore delle segnalazioni di allarme per dare all'operatore la possibilità di gestire, tramite un'unica interfaccia, le segnalazioni delle diverse apparecchiature
E' particolarmente interessante l'integrazione con il software di monitoraggio e sorveglianza della costa, tramite il quale è possibile associare gli allarmi alle registrazioni delle telecamere, sia termiche che di contesto.

Il sistema di monitoraggio e sorveglianza della costa è una soluzione integrata, sviluppata appositamente per la gestione del traffico marittimo costiero: esso visualizza in tempo reale i dati provenienti dai suoi sensori su una mappa raster o un grafico proprietario o ancora su una immagine satellitare georeferenziata. Per ogni oggetto visualizzato dal sistema è possibile ottenere le attuali coordinate geografiche. Il software di sorveglianza marittima permette di raccogliere ed elaborare dati provenienti da un radar, due termocamere e una stazione meteorologica. La forza del sistema è quella di generare in tempo reale un'immagine completa della situazione marittima costiera e di fornire gli strumenti per controllare le condizioni del traffico marittimo. Ogni natante che si trovi nella fascia controllata viene automaticamente tracciato e i suoi spostamenti vengono osservati in modo intelligente dal sistema, senza che sia richiesto l'intervento dell'operatore. In base ai criteri impostati dagli operatori, alcuni comportamenti dei natanti possono far passare il sistema di vigilanza dallo stato di semplice osservazione allo stato di allerta.



Gli eventi che possono essere segnalati sono:

- la violazione di una delle Zone "A" da parte di un natante.

- il superamento della velocità consentita all'interno delle zone B.

- lo stazionamento prolungato (ancoraggio) in Zona B.

Tutti e tre i comportamenti sono contrari al regolamento dell'AMP e possono quindi generare allarme. Gli operatori possono specificare i criteri che portano ad un allarme. I criteri di sorveglianza possono tener conto di tutte le variabili riferibili alla navigazione, ovvero:

- velocità;
- direzione;
- provenienza;
- violazione di determinate aree;
- sosta in determinate aree.

In seguito all'identificazione delle variabili che si vogliono applicare si possono poi creare gli eventi di allarme. Al verificarsi di uno degli eventi di allarme, il sistema può essere programmato per rispondere con:

- la registrazione della traccia continua degli spostamenti del natante;
- l'inquadratura con le telecamere e le termocamere;
- l'invio di allarmi via sms o via email.

La registrazione della traccia degli spostamenti e le videoriprese del natante avvengono in modalità sincrona e possono partire anche molto tempo prima dell'effettiva violazione che ha fatto scattare l'allarme. Infatti il sistema di monitoraggio, memorizzando continuamente il traffico costiero e aggiornando continuamente gli spostamenti dei natanti, può nel caso in cui scatti l'allerta per un determinato natante ricostruire lo storico dei suoi spostamenti, dal momento in cui esso è entrato nel raggio di azione del sistema. Non avendo i natati e le imbarcazioni l'obbligo di dotarsi di segnalatore AIS, il sistema di monitoraggio associa l'immagine ottenuta dalla termocamera alla traccia dell'imbarcazione. Sarà questa associazione ad identificare il natante.

Altro punto di forza del sistema è rappresentato dal software di controllo dei sistemi di videosorveglianza e di tutte le apparecchiature presenti nella rete, siano essi apparati trasmissivi o centraline di gestione allarmi. Tutto per poter avere il massimo dell'affidabilità e il completo controllo dei sistemi installati.

Materiali utilizzati

n. 8 telecamere PTZ; n. 2 termocamere PTZ; n. 8 telecamere fisse; n. 1 telecamera termica fissa; n. 7 lettori; n. 4 + 18 radio;n. 8 centrali antintrusione; n. 1radar; n. 26 monitor; n. 1 server; n. 1 switch di centrale; n. 3 work station; n. 3 sirene; n. 1 controller smart wireless lan; n. 8 UPS 1000VA; n. 3 UPS 2000VA

Grado di difficoltà, problemi e soluzioni

Complessità legata al fatto che i lavori sono stati effettuati su beni di interesse culturale (le torri saracene).

Caratteristiche particolari dell'opera

Sistema che integra molteplici tecnologie di sicurezza tutte gestite centralmente tramite un'unica piattaforma che ne correla i segnali riducendo i falsi allarmi e consentendo in tempo reale agli operatori di intervenire.

Staff e tempo impiegati per la realizzazione

6 mesi – 10 tecnici

Dichiarazione del committente sull'impianto

L'impianto restituisce alle antiche torri costiere distribuite lungo la costa l'originaria funzione di avvistamento, finalizzata oggi alla salvaguardia ambientale, e garantisce l'obiettivo della tutela day-night in un'area amplissima di elevato pregio naturalistico (siti SIC, Area marina Protetta, Parco Regionale). Questo costituisce il primo caso di utilizzo di un sistema complesso di videosorveglianza intelligente applicata ai reati ambientali.

Altra vigilanza, a chi fanno paura i servizi di un regolamento minore?

a cura di Raffaello Juvara

"Da qualche tempo convegni e media di settore trattano con assiduità il tema dell'"Altra vigilanza", mettendo sotto questa etichetta le attività, di carattere latamente assimilabile ai servizi di sicurezza ex art. 256 bis del Regolamento di Esecuzione, svolte da personale non decretato. Per il personale coinvolto si ipotizza un qualche tipo di autorizzazione a valle di percorsi formativi stabiliti per Decreto dal Ministero dell'Interno, il riconoscimento di uno stato giuridico certo – addirittura il riconoscimento di incaricato di pubblico servizio – la costituzione di un Albo, etc etc. Le scriventi Associazioni datoriali e Organizzazioni sindacali ribadiscono con forza che, aldilà delle fattispecie già normate, e cioè quelle relative agli addetti ai servizi di controllo delle attività di intrattenimento e ai servizi di accoglienza in ambito sportivo, non devono essere create repliche, in formato minore, delle figure titolari dei servizi di sicurezza sussidiaria."

Questo passaggio si trova nel ***cahier des doleances*** unitario inviato lo scorso 26 aprile ai vertici del Viminale dalle Associazioni di categoria e dalle Organizzazioni sindacali, per sollecitare giustamente l'intervento del Ministero per far rispettare le regole introdotte dai DM 269 e 115 che hanno definito i servizi di sicurezza di sussidiaria e i requisiti dei soggetti abilitati a svolgerli in esclusiva. Come spesso succede in Italia, chi si è adeguato alla norma sostenendo sforzi economici e organizzativi impegnativi, si è ritrovato il danno di subire la concorrenza al ribasso da parte di chi non si è adeguato e la doppia beffa di vederlo impunito per scarsità di controlli e mancate applicazioni delle sanzioni previste dalla norma stessa.

In questo documento unitario le parti sociali della vigilanza hanno anche espresso con forza la contrarietà alle ipotesi di qualificare gli operatori dei servizi diversi da quelli di sicurezza sussidiaria, paventando che la creazione di *"una seconda categoria di personale autorizzato generi una confusione ancora più grande tra i rispettivi perimetri di pertinenza"*. Timori generati dal fatto che *"uno dei principali problemi che la categoria sta affrontando è quello dell'erosione degli spazi di esclusiva competenza, in favore dell'abuso di figure non autorizzate e questo ai soli fini di risparmio sui costi ma a scapito dell'affidabilità e della sicurezza dei servizi erogati"*.

Secondo gli autori del documento, non si dovrà dunque parlare di "Altra vigilanza" quando ci si riferisce al mondo dei servizi che non sono contemplati dall'art. 256 bis del Regolamento di Esecuzione del TULPS. Questi servizi dovranno venire soppressi oppure, nella denegata ipotesi che ciò non risultasse possibile, si dovranno erogare senza alcuna forma di autorizzazione e di formazione del personale che li svolge, per evitare che clienti sprovveduti possano venire abbindolati da operatori senza scrupoli, che millantano di poter svolgere servizi di vigilanza in quanto muniti di autorizzazioni "minori".

Dal momento che da queste pagine trattiamo da anni il tema dell'evoluzione della vigilanza in ogni sua forma e da altrettanto tempo partecipiamo a eventi con rappresentanti del Ministero, associazioni di categoria e organizzazioni sindacali sulla comprensione e la conseguente gestione del fenomeno delle "altre vigilanze", riteniamo di poter esprimere qualche considerazione in merito.

Autorizzare significa "legittimare" o "consentire", da parte di un'autorità, a "fare qualcosa" nel rispetto di uno schema. In altre parole, significa indicare delle regole, alle quali il soggetto dovrà attenersi per avere il permesso (dall'autorità) di fare quella cosa. Non si vede perché, nello specifico, non debba essere in qualche modo autorizzato (e formato) chi accoglie, ad esempio, il pubblico in una banca o in una scuola, oppure verifica il movimento delle merci in uno stabilimento, in un supermercato, in un ospedale.

Abbiamo anche sollevato il non banale problema del profilo penale di queste figure, che si potrebbe gestire con una semplice previsione nello schema autorizzativo, quanto meno per evitare che ladri incalliti vengano messi a custodire i regali di nozze o il guardaroba di un museo, per non parlare di altre evenienze più incresciose. Inquadrare con regole chiare queste mansioni non servirebbe, oltre tutto, a delimitare con maggiore chiarezza il campo operativo riservato in esclusiva alle guardie giurate ed evitare le confusioni strumentali denunciate dal documento unitario?

Proseguiamo con un'altra domanda: i firmatari del documento hanno idea delle dimensioni del fenomeno che vorrebbero tenere sotto il tappeto come la cenere? Secondo le stime più recenti, equivale dalle due alle tre volte il comparto delle vigilanza regolamentata, ovvero tra 80.000 e 120.000 addetti in crescita, mentre i porti d'arma per guardie giurate – l'arma è necessaria per svolgere i servizi di sicurezza sussidiaria - sono diminuiti di quasi 10.000 unità solo nel 2015 **(leggi)**.

Questi numeri non sono di certo dovuti solo alla confusione da parte di clienti sprovveduti, ma a un deciso orientamento del mercato di cui i firmatari stessi sono perfettamente consapevoli, dal momento che hanno previsto da anni nei CCNL della vigilanza anche i "servizi fiduciari", equivoco sinonimo di "altra vigilanza".

Del resto, le principali imprese di sicurezza italiane

hanno già da tempo modificato il proprio modello organizzativo, con i servizi di sicurezza sussidiaria svolti da guardie giurate compresi in un più ampio spettro di prestazioni specialistiche. **Luigi Gabriele**, presidente di **Federsicurezza**, ha perfettamente fotografato questo irreversibile andamento, nell'intervento al convegno del 23 marzo sulla certificazione **(leggi essecome 2/2016 pg 96)**, e **Claudio Moro**, presidente di **ASSVigilanz**a, esprime nell'intervista che segue concetti analoghi.

Concludiamo con un'altra domanda, anzi due. Quante sono le aziende di "servizi fiduciari" o "altra vigilanza" a dir si voglia, che fanno capo direttamente o indirettamente agli istituti di vigilanza? Tra quelle ufficiali come denominazione, sede, organizzazione e CCNL e quelle "sotto traccia" utilizzate per combattere la guerra delle tariffe sugli stessi mercati, il comparto di questi servizi è fisiologicamente presidiato in forze dagli operatori della vigilanza fin dalla sua nascita. Quante sono le cooperative fittizie fatte nascere all'ombra di istituti anche blasonati, magari solo per rispondere alle esigenze dei clienti più importanti di avere servizi di "altra vigilanza" a prezzi competitivi?

Da qui l'altra domanda: non è che la perentoria richiesta di non regolamentare questa famigerata "altra vigilanza" derivi proprio dalla loro necessità (o voglia) di continuare a muoversi con aziende totalmente "libere", magari perché angustiati dall'eccesso di regole che rischiano di asfissiare quella "vera"?

ASSVigilanza, regole e sanzioni certe per la coesistenza della sicurezza sussidiaria e dei servizi fiduciari

a colloquio con l'avv. Claudio Moro, presidente ASSVigilanza
a cura di Raffaello Juvara

Servizi di sicurezza sussidiaria versus servizi fiduciari. Come si propone ASSvigilanza, l'associazione di settore con maggiore visione storica, su questo tema essenziale per il futuro della categoria?
Per quanto ci risulta, la gran parte degli Istituti di Vigilanza Privata hanno costituito società ad hoc o un ramo di azienda avente come oggetto sociale lo svolgimento dei servizi fiduciari a mezzo di personale specificamente assunto per svolgere tali servizi.
Non si ritiene, dunque, che vi possa essere contrapposizione tra le due attività purché si rispettino "le regole" anche in materia di appalto.
L'Autorità Nazionale Anticorruzione è intervenuta sul punto precisando che le stazioni appaltanti "debbano valutare l'opportunità di suddividere l'affidamento dei predetti servizi in più lotti funzionali caratterizzati da attività omogenee per natura".
Sulle modalità di affidamento degli appalti si è espresso anche il legislatore che, al titolo IV, art. 28 del nuovo codice degli appalti (in vigore dal 18.4.2016), ha precisato che l'operatore economico che concorre alla procedura di affidamento deve possedere i requisiti di qualificazione e capacità prescritti per ciascuna prestazione.

Parlando del CCNL, il fattore che fa la differenza sul costo delle guardie giurate ma non ancora sul riconoscimento da parte dell'utenza anche pubblica, quale sarebbe, secondo voi, il modo per superare una situazione che sta diventando insostenibile per le imprese "virtuose" della vigilanza?
Sarebbe indispensabile far rispettare, anche con riferimento alle private utenze, quanto previsto dalla normativa sugli appalti pubblici ed, in particolare da quanto previsto dall'art. 30 del sopra citato codice.

Tale norma impone che al personale impiegato nei lavori oggetto di appalti, deve essere applicato il contratto collettivo nazionale e territoriale in vigore per il settore e per la zona nella quale si eseguono le prestazioni di lavoro e prevede che nel caso di inadempienza contributiva o retributiva dell'appaltatore o subappaltatore, il Committente possa, a certe condizioni, versare direttamente agli istituti previdenziali ed assicurativi ed ai lavoratori interessati le somme dovute dall'appaltatore, detraendo il relativo importo dalle somme dovute all'affidatario del contratto.
Si dovrebbe inoltre tenere conto, come fa l'ANAC, del costo medio orario definito nelle Tabelle approvate dal Ministero del Lavoro e delle Politiche Sociali.
Tabelle che, per i settori Vigilanza Privata e Servizi Fiduciari, sono state fatte proprie dal Ministero del Lavoro e delle Politiche Sociali e che, lo scorso 21 marzo, sono state sottoscritte da tutte le parti sociali.

Ritenete più opportuno un CCNL che raggruppi vigilanza e servizi fiduciari o due separati?
Certamente un unico C.C.N.L. che permetta di poter intervenire sia sul contenuto delle mansioni che sul costo del personale.

Certificazioni: nel momento in cui il meccanismo sembra assestarsi, si sta ponendo il problema – ricordato nel documento unitario inviato ai vertici del Ministero dell'Interno lo scorso 26 aprile, firmato tra gli altri anche da ASSvigilanza – della gestione delle crisi in caso di revoca della licenza alle aziende inadempienti. Quali sono le vostre proposte a questo proposito?
Anche nell'incontro che si è tenuto il giorno 11 maggio u.s. al Ministero dell'Interno alla presenza del sottosegretario Sen. Filippo Bubbico, tutte le Associazioni di Categoria e le Organizzazioni Sindacali Nazionali hanno insistito su due punti ritenuti fondamentali:

Il primo punto è la qualificazione delle imprese di Vigilanza Privata a seguito dell'applicazione del D.M. 269/2010 e 155/2014.
Il processo di riforma normativa del settore, realizzato a partire dalla sentenza della Corte di Giustizia Europea del dicembre 2007, è ormai a regime. Il pieno rispetto dei requisiti minimi di qualità per aziende e operatori ed il correlato meccanismo di controllo e verifica, stentano però ad essere applicati e, quindi, a dare i risultati posti come obiettivo. Infatti, se da una parte si sono gravate le imprese di pesanti oneri per l'adeguamento alle prescrizioni, dall'altra non si sta procedendo con la dovuta celerità a sanzionare le aziende non in regola. Ciò fa sì che insistano sul mercato sia le aziende virtuose, sia quelle che non hanno adeguato le loro strutture alla normativa. Il risultato è perverso: infatti le aziende che agiscono fuori dalle regole, in virtù dei loro costi più bassi, possono praticare tariffe in *dumping*, con questo alterando la competizione commerciale e, in definitiva, ponendo una pesante ipoteca sull'affidabilità dei servizi e la sicurezza degli operatori, entrambi valori che rappresentano i *targets* della P.A.
Per interrompere questo circolo vizioso, riteniamo che la P.A. debba continuare ad operare in maniera incisiva in due direzioni:
- continuando a garantire l'efficacia e l'affidabilità dell'azione ispettiva e certificativa degli Enti accreditati. A questo proposito, riteniamo indispensabile la nomina del Comitato Tecnico di cui al punto 4) dell'art. 260 ter del Regolamento di Esecuzione del T.U.L.P.S.
- inibendo le attività delle aziende non conformi.
A tale fine, considerando che il termine ultimo per presentare il certificato attestante il possesso dei requisiti previsti dal D.M. n. 269 n. 115 e successivo Disciplinare del Capo di Polizia scadeva a settembre 2015, le Associazioni Datoriali e le Organizzazioni Sindacali, nel corso del predetto incontro che si è tenuto al Ministero dell'Interno, hanno chiesto l'invio di una circolare indirizzata a tutti gli uffici territoriali di Governo, nella quale, dopo aver ripercorso le tappe di costruzione del nuovo sistema normativo di settore (che si sono dipanate per ben otto anni) si disponga chiaramente che, data la piena efficacia del sistema, si dovrà procedere al ritiro della licenza

di polizia a quegli Istituti che risultino mancanti della certificazione o di valido contratto con un Ente di certificazione accreditato che abbia già fissato le date delle visite ispettive.
A seguito di quanto sopra, le Associazioni Datoriali e le Organizzazioni Sindacali firmatarie hanno, altresì, richiesto l'attivazione di tavoli congiunti presso le istituzioni preposte, nazionali e territoriali (Ministero, Prefetture), per gestire, anche a livello territoriale, i possibili effetti negativi sui livelli occupazionali che questa necessaria attività sanzionatoria potrebbe portare in un primo momento.
Inoltre, il Ministero dell'Interno ha precisato che, ai fini degli sgravi previsti dalla recente Legge di Stabilità, intende promuovere, presso tutte le altre funzioni pubbliche interessate, nonché presso il legislatore che, quale requisito obbligatorio per l'ottenimento di ogni beneficio/sgravio fiscali, vi sia la presenza delle certificazioni di cui al disposto dei D.M. 269/2010, D.M. 115/2014.
Un'altra misura che sicuramente contribuirebbe alla più rapida applicazione delle norme da parte degli Istituti di Vigilanza Privata, oltre a costituire uno strumento di trasparenza amministrativa, è la pubblicazione, da parte del Ministero dell'Interno, di un apposito elenco consultabile on line sul sito del Ministero dell'Interno (da tenere aggiornato), degli Istituti di Vigilanza Privata certificati.

Il secondo punto è il riconoscimento del C.C.N.L. di categoria quale elemento necessario per la tenuta dell'impianto normativo del settore.
Recentemente, un'azienda del comprensorio napoletano ha comunicato ai propri dipendenti la migrazione dal C.C.N.L. vigente, sottoscritto dalle OO.SS. comparativamente più rappresentative di comparto e da tutte le Associazioni datoriali, verso un contratto sottoscritto da un solo sindacato, (la Cisal) ed alcune Associazioni datoriali sino ad ora sconosciute e di rappresentatività quantomeno incerta.
Il fatto che esistano più contratti collettivi di lavoro riferiti agli stessi servizi, sottoscritti da sigle sindacali non rappresentative, rappresenta una anomalia, che favorisce il *dumping* e non tutela né le aziende virtuose, che sopportano, per questo, costi maggiori e perdita di servizi, né i lavoratori che si trovano esposti a subire condizioni peggiorative, pur di non perdere il posto di lavoro, come ad esempio, nei cambi di appalto, né le stazioni appaltanti, che si trovano spesso ad affrontare lunghi e costosi contenziosi. Fenomeni questo tipo costituiscono un *vulnus* alla efficacia del sistema della contrattazione collettiva, ed in definitiva alla tenuta delle relazioni sindacali del Paese.

Nel momento in cui i maggiori gruppi nazionali stanno assumendo l'assetto di "general security provider", secondo modelli consolidati a livello internazionale, nel quale i servizi di vigilanza ex TULPS sono solamente una parte di attività di facility management, intelligence, sistemi tecnologici ecc, ritenete che il modello associativo tradizionale della vigilanza possa continuare a rappresentare queste aziende o che sia, invece, necessario pensare a modelli diversi nel prossimo futuro?
Certamente il sistema associativo deve adeguarsi per comprendere anche le "nuove" ulteriori attività di security quali l'attività di steward negli stadi, i servizi di sicurezza sussidiaria nell'ambito dei porti, delle stazioni ferroviarie, delle ferrovie metropolitane, nonché nell'ambito delle linee di trasporto urbano, i servizi di controllo delle attività di intrattenimento e di spettacolo in luoghi aperti al pubblico o in pubblici esercizi, l'impiego di guardie giurate a bordo delle navi mercantili battenti bandiera italiana, che transitano in acque internazionali a rischio pirateria.

Genova, le più avanzate tecnologie di sicurezza per i Musei di Strada Nuova

a cura della Redazione

Inaugurazione del nuovo sistema di videosorveglianza di Palazzo Tursi e di Sala Paganini.

A meno di due mesi dalla delibera della collaborazione pluriennale che vede impegnata la **Fondazione Enzo Hruby** insieme al **Comune di Genova** per l'aggiornamento dei sistemi di sicurezza dei Musei di Strada Nuova, è stata portata a termine la prima fase del progetto, destinata alla protezione di Palazzo Tursi e di Sala Paganini, che custodisce al suo interno il celebre violino "Cannone".

L'intervento, interamente sostenuto dalla Fondazione Enzo Hruby, si è concretizzato nella completa sostituzione dell'impianto di videosorveglianza ormai obsoleto esistente a Palazzo Tursi con un sistema Over IP all'avanguardia e con nuove strutture di rete. L'utilizzo di telecamere IP ad alta definizione dotate di illuminatori a raggi infrarossi permette di ottenere immagini estremamente nitide in qualsiasi condizione di luminosità all'interno delle sale. Nella Sala Paganini le telecamere installate sono anche dotate di ottica varifocale motorizzata con gestione da remoto della messa a fuoco. Questo permette di ottenere una gestione ottimale e veloce anche in caso di manutenzione del sistema. La tecnologia Over IP di ultima generazione utilizzata offre la possibilità di implementare nel sistema algoritmi di analisi video evoluti, atti a controllare sia attività anomale, come intrusioni ed effrazioni, sia a dotare il complesso museale di strumenti utili per la gestione dei flussi dei visitatori e per il controllo della loro sicurezza. Il nuovo sistema è inoltre predisposto per rendere possibile, a completamento dell'intero progetto destinato ai Musei di Strada Nuova, la centralizzazione di tutti gli impianti in un unico punto di controllo, rendendo estremamente semplice e pratica la loro gestione. Per la realizzazione dell'intervento la Fondazione Enzo Hruby ha incaricato la società Umbra Control di Perugia, azienda Amica della Fondazione.

Un progetto di grande rilievo, che è stato inaugurato il 22 giugno con la conferenza stampa a Palazzo Tursi da **Carla Sibilla**, Assessore alla Cultura e Turismo del Comune di Genova, **Guido Gandino**, Direttore Direzione Cultura del Comune di Genova, e **Carlo Hruby**, Vice Presidente della Fondazione Enzo Hruby.

"Con questo progetto – **ha sottolineato l'assessore alla cultura e al turismo Carla Sibilla** – *si consolida il rapporto tra Amministrazione comunale e Fondazione Enzo Hruby che ha già dato ottimi risultati per la messa in sicurezza della Lanterna, uno dei simboli della nostra Città. Ora, con la decisione di avvalerci di questa preziosa collaborazione, vigileremo con un occhio ancor più attento sui tanti tesori conservati all'interno dei Musei di Strada Nuova. Nel ringraziare la Fondazione mi piace sottolineare* – conclude Sibilla – *quanto la sinergia tra pubblico e privato, che stiamo sperimentando anche in questa occasione, costituisca un sicuro elemento di sviluppo per la cultura nella nostra Città".*

"Il nostro obiettivo – **ha dichiarato Carlo Hruby, Vice**

Presidente della Fondazione Enzo Hruby – *è offrire adeguata sicurezza e piena accessibilità ai Musei di Strada Nuova e al tempo stesso realizzare un modello di riferimento per la protezione in ambito museale. A meno di due mesi dall'annuncio del progetto, abbiamo la soddisfazione di vedere compiuto il primo intervento, destinato a Palazzo Tursi e a Sala Paganini. Un progetto eccellente, che si caratterizza per l'impiego delle più avanzate tecnologie di videosorveglianza oggi disponibili a livello mondiale e come esempio di collaborazione virtuosa tra pubblico e privato. Ci auguriamo che questo intervento possa servire come modello per altre realtà analoghe presenti in Italia e a sensibilizzare altre pubbliche amministrazioni verso il tema della sicurezza del nostro inestimabile patrimonio culturale".*

LA SALA PAGANINI E IL "CANNONE" DI NICCOLÒ PAGANINI

Sala Paganini fa parte del percorso espositivo dei Musei di Strada Nuova e ospita – a Palazzo Tursi – il violino del grande virtuoso noto come il **'Cannone'**. Lo strumento è uno dei più grandi capolavori della liuteria cremonese e, per ragioni di conservazione, non viene suonato frequentemente. Sul suo stato di salute vigila il Comune di Genova con una commissione di esperti. Tornerà a suonare al **Teatro Carlo Felice di Genova il prossimo 27 ottobre, in occasione del concerto organizzato dalla Fondazione Enzo Hruby insieme al Comune di Genova**. Il concerto è inserito nella stagione sinfonica dello storico teatro genovese e verrà eseguito dalla violinista **Anastasiya Petryshak** accompagnata dall'**Orchestra del Teatro Carlo Felice.**

CONTATTI: FONDAZIONE ENZO HRUBY
www.fondazionehruby.org

Fondazione Enzo Hruby con Metrovox per la protezione di due mostre a Pompei e ai Musei Capitolini

a cura della Redazione

Due luoghi straordinari – l'**Antiquarium ottocentesco di Pompei e i Musei Capitolini di Roma** – fanno da sfondo a due mostre altrettanto eccezionali: *"Per Grazia Ricevuta – La devozione religiosa a Pompei antica e moderna"*, e *"La Misericordia nell'Arte. Itinerario giubilare tra i Capolavori dei grandi Artisti Italiani"*. Entrambe realizzate in occasione del Giubileo Straordinario della Misericordia indetto da Papa Francesco, sono visitabili fino al prossimo 29 novembre e vedono la **Fondazione Enzo Hruby** impegnata insieme alla società **Metrovox** - azienda Amica della Fondazione - per sostenere la protezione puntuale delle opere di maggior pregio esposte.

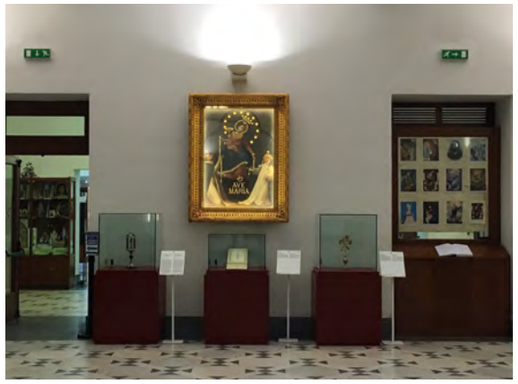
Organizzata dalla Soprintendenza di Pompei, dal Centro Europeo per il Turismo e Cultura presieduto da Giuseppe Lepore e dal Santuario della Beata Vergine del Rosario di Pompei, la mostra *"Per Grazia Ricevuta"* indaga il rapporto con il Divino nella sfera pubblica e domestica: attraverso le opere esposte, per la prima volta vengono messi a confronto i rituali e le offerte votive che gli antichi Sanniti e Romani di Pompei donavano alle divinità pagane con quelli che i Cristiani, ancora oggi, offrono al Santuario della Madonna del Rosario. Ne emerge uno stringente parallelismo che si perpetua in un rituale e in un "linguaggio" di offerte votive identiche nelle forme. A Pompei, oltre a questa mostra, l'impegno della Fondazione Enzo Hruby e di Metrovox è proseguito all'interno del Santuario della Madonna del Rosario, concretizzandosi nella protezione puntuale di importanti ex voto offerti al Santuario da Padre Pio, da Papa Benedetto XVI e da Papa Francesco.

"La Misericordia nell'Arte" è anch'essa una mostra di grande rilievo, promossa da Roma Capitale - Sovrintendenza Capitolina ai Beni Culturali e organizzata dal Centro Europeo per il Turismo e Cultura con il patrocinio del Ministero dei Beni e delle Attività Culturali e del Turismo. Il tema della Misericordia, proprio perché costituisce il cuore del pensiero cristiano, è stato oggetto nel corso dei secoli di moltissime opere d'arte. La mostra in corso ai Musei Capitolini propone al pubblico importanti testimonianze artistiche dedicate a questo tema. La prima sezione presenta un nucleo di dipinti testimoni della grande diffusione che il soggetto della *Madonna della Misericordia* ebbe nei secoli. La seconda sezione ha come oggetto *Le Opere di Misericordia*, per la prima volta descritte da Cristo stesso nel Vangelo di San Matteo. In mostra sono presenti dipinti e sculture che illustrano le varie opere misericordiose, tra cui si segnalano un bassorilievo di Pietro Bernini del Museo Nazionale di San Martino, la *Carità* di Guido Reni e un dipinto di Pierre Subleyras del Museo di Roma.

Come a Pompei, anche in questo caso si è resa necessaria una protezione puntuale delle più importanti opere esposte, sostenuta dalla Fondazione Enzo Hruby con la collaborazione di Metrovox, che ha realizzato l'intervento offrendo un proprio contributo concreto.

"*Con i progetti che sosteniamo in questi mesi a Pompei e ai Musei Capitolini* – dichiara **Carlo Hruby, Vice Presidente della Fondazione Enzo Hruby** - *si rinnova la proficua collaborazione della nostra Fondazione con il Centro Europeo per il Turismo e Cultura, con la società Metrovox e con la Soprintendenza di Pompei. Questi interventi, realizzati in contesti tra loro diversi - un importante museo, un edificio sacro e un parco archeologico - mettono ancora una volta in luce come le moderne tecnologie di sicurezza permettano, con soluzioni non invasive e costi contenuti, di conciliare le due esigenze solo in apparenza opposte di protezione e di valorizzazione del patrimonio culturale italiano"*.

"Stiamo collaborando ormai da tempo e continueremo in tal senso - sottolinea **Giulio Iucci, Amministratore Delegato della Metrovox** - *con grande entusiasmo, coinvolgimento e soddisfazione, alle iniziative di altissimo profilo proposte dalla Fondazione Enzo Hruby, mettendo a disposizione tutte le nostre competenze accumulate in anni di attività specifica nel settore dei Beni Culturali del nostro Paese"*.



CONTATTI: FONDAZIONE ENZO HRUBY
www.fondazionehruby.org

CONTATTI: METROVOX
www.grupposipro.it

AXIS Companion Line, la soluzione completa per la sicurezza delle piccole imprese

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

La soluzione **AXIS Companion Line** e il programma di assistenza per installatori **AXIS Companion Specialist** riuniscono i vantaggi della videosorveglianza IP in un'offerta completa, integrata e facile da usare, che permette a piccole imprese di adottare un sistema di sicurezza di rete avanzato, semplice, economico e a basso rischio.
AXIS Companion Recorder è l'unità di registrazione di rete a 8 canali con switch PoE integrato che abbatte i costi di installazione; porta USB per esportare i filmati; punto di accesso wireless. Il software per la gestione video AXIS Companion semplifica installazione e utilizzo con l'omonima app per accedere alle riprese e alla gestione da remoto tramite mobile.
Le telecamere IP offrono la videosorveglianza Day&Night con illuminazione a infrarossi integrata per interni o esterni e la risoluzione full HDTV o fino a 2 MP: supportano le tecnologie **Wide Dynamic Range** per condizioni di illuminazione difficili e **Axis Zipstream p**er ridurre l'occupazione di banda e lo spazio di archiviazione; sono dotate di slot microSD.

Centrale antintrusione wireless Proxinet W2

CAME SPA
(+39) 0422 2940
www.came.com

Proxinet W2 è una centrale programmabile a 99 ingressi radio e 6 ingressi filo, con le prestazioni della gamma **Proxinet** e la semplicità d'installazione dei sistemi wireless.
La centrale dispone di tastiera e display per gestire l'impianto e programmare i parametri funzionali, di una sirena per interni e di un lettore per chiave a transponder per inserire, disinserire e parzializzare l'impianto tramite chiave elettronica e dialogare in modalità Dual Band con tutti i dispositivi della gamma radio. Integra il comunicatore PSTN per trasmettere allarmi vocali e digitali verso istituti di vigilanza. I messaggi si impostano con la funzione Text To Speech, o si registrano dal microfono a bordo. Si può completare la centrale, con guida vocale, con il modulo GPRS per trasmettere allarmi in formato SMS, collegare via Internet al Cloud per il controllo remoto e gestire il sistema tramite l'**APP Came D**. Connessa su rete LAN, la centrale può dialogare con il sistema domotico per centralizzare e integrare i due sistemi.

La centrale Magellan MG5050 di Paradox

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

La centrale **MG5050** distribuita da **DIAS** costituisce una soluzione potente e flessibile particolarmente adatta per la protezione in ambito residenziale.
Supporta due aree del tutto separate, gestisce fino a 32 zone senza fili e assicura una protezione continua grazie a tre livelli di inserimento - perimetrale, notte e totale - e alla funzione StayD di **Paradox**, che consente di lasciare il sistema sempre inserito e si esclude quando si entra o si esce dall'ambiente protetto.
MG5050 offre semplicità di installazione, manutenzione e permette di ampliare con nuove prestazioni, il sistema già installato. Questa centrale supporta la linea completa di prodotti senza filo **Magellan** ed è compatibile con la tastiera TM50 touchscreen di Paradox con ampio schermo ad alta risoluzione di 5", disponibile in ben 7 colori e utilizzabile anche come cornice digitale. MG5050 è inoltre compatibile con il modulo PCS250 per rete GSM/GPRS con invio e gestione tramite SMS e con l'applicazione per smartphone iParadox disponibile per Android e iOs tramite il modulo IP150.

ELANFIRE: resistenza al fuoco e tecnologia del cavo

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

I cavi resistenti al fuoco sono utilizzati per alimentare e connettere tra loro apparecchiature di emergenza. Ad oggi sono 3 le tecnologie usate per produrre questo tipo di cavi.
Nel primo tipo il conduttore in rame è ricoperto con un nastro di mica. I conduttori isolati con XLPE e PPE non rispondono alla CEI 20/22 in quanto molto infiammabili. L'affidabilità del cavo è dunque proporzionale alla qualità della mica. Nella seconda generazione di cavi, viene usato invece il silicone. Anche in questo caso, la qualità molto economica lascia dubbi sull'affidabilità in caso di incendio.
ELAN ha sviluppato una terza tecnologia: E**LANFIRE (PH120)**, il cavo resistente al fuoco che utilizza la tecnologia mica senza impiego di XLPE o PPE. ELANFIRE ha dei conduttori isolati con una speciale mescola LSZH che rispetta tutte le normative, garantendo zero emissione di fumi tossici e una perfetta spelatura dei conduttori.
Tutti i cavi ELAN resistenti al fuoco, in particolare la gamma ELANFIRE, sono efficaci e affidabili per garantire il giusto livello di sicurezza.

Lettori d'impronte digitali ekey + domotica KNX

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

Lo standard internazionale KNX per l'automazione degli edifici rende collegabile in rete ogni singolo sistema, dall'illuminazione al riscaldamento e all'impianto d'allarme, offrendo l'aumento di comfort, sicurezza ed efficienza economica sia in edifici con finalità specifiche che in edifici residenziali.
Per la connessione dei lettori d'impronte ekey alla tecnologia KNX, ekey ha sviluppato l'**ekey home CV KNX**, che **sarà disponibile dopo l'estate**.
Il convertitore certificato da KNX converte le informazioni degli accessi direttamente in eventi KNX, rendendo possibile di controllare e gestire funzioni domotiche oppure concedere l'accesso all'edificio in base ai requisiti di una determinata persona.
Oltre ai vari convertitori (KNX, UDP, Wiegand), ekey offre anche la possibilità di accoppiare i lettori d'impronte con sistemi terzi usando direttamente un software development kit. Per maggiori dettagli vogliate consultare il depliant: http://goo.gl/FWEls0 oppure contattare italia@ekey.net

Amplificatori di potenza ERMES

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

ERMES ha messo a punto una nuova serie di amplificatori di potenza in IP con uscita per linee audio a 100V e in tre diverse potenze 80W, 160W e 320W con interessanti funzioni accessorie, fra le quali un ingresso audio a 0dB per collegare un segnale proveniente da un microfono o altra sorgente analogica.
E' così possibile implementare un impianto di amplificazione locale abilitabile in alternativa alla diffusione annunci Over IP. gestendo allo stesso tempo le priorità tra le diverse sorgenti sonore.
Si può anche collegare gruppi citofonici (pulsante di chiamata, microfono e altoparlante) per implementare postazioni per chiamate di emergenza da associare alla diffusione annunci Over IP.
In strutture complesse come alberghi, scuole o centri congressi, con questo gateway è possibile realizzare, oltre al sistema per la diffusione di annunci e di musica di sottofondo, sottosistemi di amplificazione locale per sale conferenza o di chiamata di emergenza per gli spazi calmi, come previsto dal D.M. 09/04/1994 – Regola tecnica di prevenzione incendi.

Nuove telecamere IP Fracarro

FRACARRO RADIOINDUSTRIE SRL
(+39) 0423 7361
www.fracarro.it

La nuova gamma di **videosorveglianza IP Fracarro** comprende diversi modelli di telecamere - bullet, dome, speed dome, a focale fissa e varifocali – caratterizzate dalla qualità video full HD anche in visione notturna, facilità d'uso e l'ottimo rapporto qualità/prezzo. Predisposte per l'utilizzo in ambienti interni ed esterni, sono compatibili con i DVR della serie **TRI Fracarro** e si interfacciano con qualsiasi dispositivo IP (standard Onvif).
La nuova gamma IP utilizza la rete LAN come vettore di trasmissione e di alimentazione (POE), con un protocollo di comunicazione standardizzato flessibile, per modulare il sistema secondo le differenti esigenze, con possibilità di espansione rispetto alle evoluzioni tecnologiche future. Ogni telecamera è identificata da un preciso indirizzo IP che il DVR acquisisce automaticamente, consentendo il telecontrollo in fase di programmazione e nel post-processing, anche da smartphone.
Con l'offerta Fracarro, l'installatore che sceglie l'IP può rispondere con professionalità alle esigenze del cliente.

SafePay™ di Gunnebo

GUNNEBO ITALIA SPA
(+39) 02 267101
www.gunnebo.it

Il sistema di Cash Management SafePay™ offre vantaggi notevoli rispetto ai punti cassa tradizionali: elimina gli errori nel conteggio dei resti e le differenze di cassa, identifica eventuali falsi (certificazione BCE) e consente al personale di cassa di fornire un miglior servizio ai clienti. Nella configurazione a ciclo chiuso, il versamento immediato dell'incasso rende inaccessibile il contante, azzerando il rischio di furti e rapine. Il software di back office permette di gestire in remoto le attività legate alla gestione manuale del contante. SafePay™ è veloce nel rendere il resto esatto, azzera i tempi di calcolo del fondo cassa e riduce l'immobilizzo necessario per l'avvicendamento al cambio turno, garantendo il ritorno sull'investimento in tempi rapidi. Installato in numerosi punti vendita della GD, DO e DS, SafePay ™ è anche personalizzabile con i colori dell'insegna. Il flusso di contante dalle casse al cash-in-transit non è mai stato così efficiente: rapido, sicuro e completamente chiuso dall'inizio alla fine.

Rivelatori passivi d'infrarossi Serie HE-100X

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

Progettati per proteggere porte e finestre con un doppio rivelatore PIR a tenda, i rivelatori passivi d'infrarossi **Serie HE-100X** distribuiti da **HESA** consentono di ottenere una valida protezione perimetrale. Disponibili nei modelli cablati e a basso assorbimento, offrono grande semplicità di installazione e di manutenzione. La protezione a tenda tramite coppia di sensori passivi d'infrarossi e le dimensioni contenute consentono l'installazione sul lato superiore di una finestra o di una porta. Per protezioni maggiori, sono disponibili con funzione antimascheramento e nella versione a doppia tecnologia con antimascheramento.
Funzionamento selezionabile in AND o OR; Funzionamento LED d'allarme selezionabile On/Off; Protezione antiapertura; Lente di Fresnel; Compensazione automatica della temperatura; Ampio spazio per l'alloggiamento del trasmettitore nelle versioni a basso assorbimento; Disponibili nei colori bianco e marrone; Disponibili nei nuovi modelli a doppio PIR con funzione antimascheramento e a doppia tecnologia con antimascheramento.

Aria di novità in casa Inim

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

Inim Electronics lancia sul mercato un'interessante novità via radio che arricchisce ancora di più il sistema wireless **Air2** per impianti antintrusione **SmartLiving**. Si chiama **Aria**, ed è una tastiera via radio per la completa gestione dell'impianto. Con Aria si può accedere alle stesse funzioni delle tastiere cablate **Concept** di Inim. Con un chiaro display grafico con icone intuitive e quattro comodi tasti funzione, è dotata di staffa a muro e da tavolo per collocarla a vista su un mobile. Grazie al suo design minimale, Aria è anche un raffinato elemento d'arredo. A bordo c'è un accelerometro che funziona da dispositivo anti-sabotaggio oppure da "risveglio" dallo stand-by. Un sensore di luminosità regola l'illuminazione del display e dei tasti in base all'ambiente circostante. C'è la funzione di spegnimento automatico, che si attiva in caso di allontanamento dal campo radio. La batteria dura ben due anni. Inoltre, nel caso in cui si desideri utilizzare un'alimentazione cablata, Aria offre anche un connettore dedicato.

InVue presenta CT100, sistema di protezione a libero tocco per fashion stores

NEDAP ITALY RETAIL
(+39) 02 26708493
www.omnisint.com

InVue, leader globale nella protezione dei prodotti a libero tocco, presenta il sistema **CT100** per i retailer che vogliono utilizzare smart devices in sicurezza. Sempre più rivenditori scelgono di migliorare la shopping experience del consumatore attraverso tablets e smartphones che sfruttano la realtà aumentata, controllano lo stock dei prodotti, mostrano video e immagini, fanno diventare più social il punto vendita e agevolano i pagamenti in cassa.
Tutto questo può venire svolto in totale sicurezza, grazie al sistema InVue **CT100** che protegge e allarma i dispositivi elettronici in modo semplice e comodo. Si compone di:
- Cover in policarbonato per la protezione da furti e abusi, resistente ad oltre 350 libbre di forza di tiro
- Base in metallo con sistema di allarme integrato, che funge anche da alimentatore a dispositivo attaccato
Chiavetta IR che allarma il dispositivo tramite sistema di trasmissione dati a infrarossi, non duplicabile.
Lo smart device può rimanere fisso alla base o essere spostato nel negozio, rimanendo protetto e allarmato.

La generazione dell`HomeControl

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

L'infrastruttura del **PyronixCloud** e l'**App Homecontrol**, per Android e iOS, consentono un accesso unico alla gestione e al controllo della casa tramite interfaccia IP crittografata in modo sicuro.
La semplicità nell'interfaccia con l`utente differenzia il sistema Pyronix dagli altri sul mercato.
PyronixCloud funge da piattaforma che permette a **homecontrol** + di comunicare e controllare con l'Enforcer 32-WE APP.
Letelecamere integrate, da interno ed esterno, permettono di guardare il video in streaming da casa come mai finora da un'unica applicazione.
Anche gli installatori possono programmare da remoto e diagnosticare con facilità il Sistema, utilizzando il software InSite UDL sulle comunicazioni IP.
La versione 10 del software **Enforcer** ha ridotto i tempi di installazione per la facilita e la semplicità d'uso del menu ridotto, che ha segnato il passaggio da sistemi di allarme standard alla generazione di Home Control. Fruibilita', funzionalità e innovazione sono al centro di questa rivoluzione dell'antintrusione, guidata da Pyronix.

Agility™3, il sistema di sicurezza radio bidirezionale

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

Agility™3 è il sistema di sicurezza radio bidirezionale di ultima generazione di **RISCO Group**, società indipendente leader a livello globale che sviluppa, produce e commercializza un'ampia gamma di soluzioni di sicurezza integrate. Agility™3 si basa su una tecnologia radio dual core con due canali radio simultanei con antenne separate: una per rivelare i segnali d'allarme, controllare e diagnosticare; l'altra per trasmettere le immagini. Utilizzando il Cloud RISCO e l'app iRISCO disponibile per iOS e Android, Agility™3 abilita la video verifica in tempo reale e la ricezione di immagini in caso di allarme in corso o su richiesta, tramite telecamere IP per interno ed esterno.
Dal design elegante, Agility™3 è una centrale progettata per il mercato residenziale e small business per raggiungere ogni angolo dell'ambiente da proteggere, garantire tempi di installazione rapidi e lavori strutturali minimi. E' integrabile con una vasta gamma di accessori per indirizzare ogni esigenza, anche di domotica, assistenza di anziani e bambini.

FACILE, la Centrale Antifurto con GSM e Scheda LAN integrato

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

Creata e realizzata negli stabilimenti **SAET, FACILE** utilizza le potenzialità della sorella maggiore DELPHI, adattate per applicazioni di taglio piccolo e medio. **FACILE** unisce semplicità e completezza funzionale, anche grazie all'applicativo dedicato che ne consente la configurazione e programmazione della centrale, nonché il download e upload del programma utente. Costituita da **8 ingressi a triplo bilanciamento, espandibile 32 o 160**, tramite modulo espansione ingressi modello SC8, o per mezzo di sensori a colloquio seriale di tipo current loop.
Il GSM può inviare allarmi fonia, allarmi puntiforme, comandi di attuazione. La **FACILE**, peculiare anche per la **Scheda LAN ETHERNET integrata** (IP Standard disponibile da Saet, modificabile dall'utente) che attraverso il **Web server integrato** con interfaccia utente locale o remota, permette di: Visualizzare lo storico, lo stato dei sensori e associazione zona/sensori e le relative messa in servizio / fuori servizio; La visualizzazione e gestione degli attuatori; La visualizzazione stato attivazione/ non pronto zone.
Per ulteriori info www.saetitalia.it/prodotto/sistema-antifurto-facile-cat-123

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.

Redazionali Tecnologie

Datix2App e Datix2Cloud: un connubio unico!

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

La serie **Datix**, brand di **SAVV srl**, include **Datix2App**, App Android per controllare il personale mobile, de-localizzato e isolato. Funzionalità specifiche permettono di gestire in modo semplice, razionale ed efficiente, "a portata di click", la forza lavoro, rilevando la presenza e le ispezioni svolte, con localizzazione GPS e monitoraggio di eventi pericolosi (SOS, uomo a terra).
Datix2App è multifunzione, unica nel suo genere, per semplificare procedure e razionalizzare risorse umane e di sicurezza degli Operatori isolati (L. 81/08 e DM 388/08).
Datix2App permette il **controllo di servizi e presenze in tempo reale degli operatori mobili, grazie a caratteristiche peculiari:**
Lettura NFC e scarico dati via connessione cellulare/WiFi - Localizzazione GPS - Sistema Uomo a terra - Gestione remota in real time
Datix2Cloud è il nuovo servizio software su infrastruttura virtuale in modalità SaaS (Software as a Service), per ricevere e consultare i dati trasmessi da dispositivi e App Datix dotati di connettività di rete TCP/IP (es. 2G, 3G, WiFi,...).

CLV-03 Sensori inerziali con contatto magnetico ad alta sicurezza integrato

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 per installazioni nelle zone dove il pericolo di scasso è più alto.
La loro sensibilità è paragonabile a quella della migliore sensoristica disponibile, compatibili con le schede di analisi più diffuse. Il contatto magnetico ad alta sicurezza integrato ne fa un dispositivo completo per la protezione di qualunque varco.
Sono disponibili nelle versioni a cavo e a morsetti. Quest'ultima consente l'adozione del pratico sistema plug per l'inserimento rapido di resistenze di fine linea.
Basandosi su tecnologia passiva, i sensori della serie CLV garantiscono grande affidabilità nel tempo e un'elevata immunità ai disturbi ambientali.
Sono prodotti interamente in Italia con 10 anni di garanzia. Accoppiati alle schede di analisi VAS di TSec, permettono la gestione puntuale di sensibilità molto elevate.

essecome security&safety

n. 03 maggio-giugno 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
Per Bjorkdhal
Nils Fredrik Fazzini
Alessandra de Juvenich

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Del Fabbro, 2
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
Bonazzi grafica S.r.l
Via Francia, 1
23100 Sondrio (SO)
Tel. 0342 216112
www.bonazzi.it

Partner essecome 3/2016

Satel ITALIA

Satel Italia srl
Via Ischia Prima, 280 - 63066 Grottammare (AP)

LIBERATI DEI CAVI.

AOD-200

Rilevatore
WIRELESS PER ESTERNI
DOPPIA TECNOLOGIA **PIR+MW.**

Per saperne di più, visita il sito: **www.satel-italia.it**