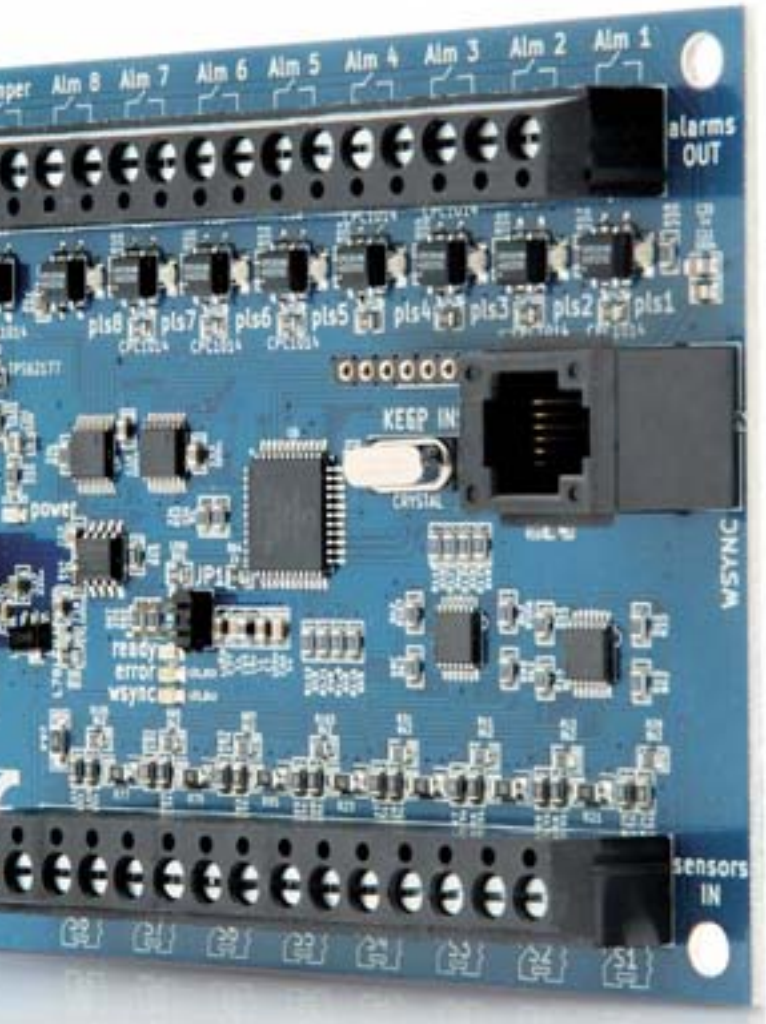
essecome
security&safety
01
2015 · ANNO XXXV-III
ISSN 2384-9282
PERIODICO DI INFORMAZIONE SU PERSONE, TECNOLOGIE E APPLICAZIONI DELLA SICUREZZA



SCHEDE DI ANALISI VAS

Il nuovo approccio alla protezione anti-scasso

Compatibilità completa con tutti i sensori inerziali passivi

Configurazione wireless con smartphone mediante sistema WSync™

WSync

Tsec
TECHNOLOGY FOR SECURITY
WWW.TSEC.IT

Pyronix®

www.pyronix.it

ENFORCERAPP

tecnologia bidirezionale senza fili

Prodotto inglese
con spirito italiano

installare senza inibizioni

AXIS COMMUNICATIONS

Qual è il modo migliore per gestire luce e ombra?

Simultaneamente.

Questo perché le telecamere di rete Axis con tecnologia ad ampio intervallo dinamico (Wide Dynamic Range, WDR) possono gestire luci forti e ombre scure nella stessa immagine. Inoltre sta a significare che è più facile individuare e identificare persone, veicoli e incidenti, non importa quanto siano difficili le condizioni di illuminazione. Sono il responsabile per la sicurezza in una centrale elettrica e WDR mi ha semplificato notevolmente la vita.

Per maggiori informazioni su WDR, l'utilizzo delle immagini e la soluzione di sorveglianza migliore per le proprie necessità, vedere la guida interattiva Axis all'indirizzo www.axis.com/imageusability

dahua TECHNOLOGY

Segnale video HD su coassiale. HDCVI versione 2.0

Sempre leader dell'innovazione HD

Dahua Technology è sempre all'avanguardia nel settore HD. La seconda generazione di telecamere HDCVI completa la sua gamma con i modelli 1080p/720p, obiettivi varifocale, accessori di trasmissione e un nuovo chip di trasmissione HDCVI integrato con l'ISP, inaugurando la seconda versione della tecnologia HDCVI di trasmissione del segnale video HD su cavo coassiale.

- **Telecamere 1080P/720P; disponibili fisse o varifocali o motorizzate, e speed dome PT**
- **Prestazioni HD ancora migliorata, ad un prezzo aggressivo**
- **Accessori per fibra ottica: ricevitori, convertitori ed extender sono già disponibili**
- **La tecnologia Dahua HDCVI è ad accesso aperto**
- **Sono stati venduti finora oltre 2 milioni di dispositivi HDCVI**
- **La tecnologia HDCVI 2.0, con HDcctv Alliance, è ora uno standard globale**

Principali modelli HDCVI :

4/8CH 1U Tribrido (HDCVI & Analogico & IP)
DH-HCVR7204/7208A-V2

4/8/16CH 1,5U Tribrido (HDCVI & Analogico & IP)
DH-HCVR7404/7408/7416L

4/8/16CH 2U Tribrido (HDCVI & analogico & IP)
DH-HCVR7804/7808/78165

Telecamera bullet IR HDCVI 720p/1080p da esterno
DH-HAC-HFW2120R/2220R-Z/VF

Telecamera dome IR HDCVI 720p/1080p antivandalo
DH-HAC-HDBW 2120R/ 2220R-Z/VF

Telecamera IR HDCVI, 2 Mp, 1080p, da esterno
DH-HAC-HFW22205

IFSEC 2015
16–18 Jun 2015 ExCel London, UK
Booth: E1300

CE FC ISO 9001:2000

Videotrend S.r.l.
Distributore ufficiale Dahua
Tel. 0362 1791300
www.videotrend.net / info@videotrend.net

DAHUA TECHNOLOGY CO., LTD.
No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

dahua TECHNOLOGY

4K

eKonomico e+ Kompleto

Prestazioni Ultra di visualizzazione e decodifica

4K è eKonomico
ad un prezzo accessibile fornisce migliore qualità

4K è Kompleto
offre una gamma completa di prodotti di alto e medio livello

Principali modelli:

4K Ultra HD IP Camera IPC-HF81200E	**4K Ultra HD IP Camera IR Fisheye antivandalo** IPC-EB(W)81200	**4K Super NVR 128 ch 2U** NVR608-128/608R-128-4K
4K Ultra HD IP Mini Bullet IR Camera IPC-HFW4800E	**4K Ultra HD IP Mini Dome IR Camera** IPC-HDBW4800E	**4K NVR 8/16/32 ch., 8 ch PoE, 1U** NVR4208/4216/4232-8P-4K

IFSEC 2015
16–18 Jun 2015 ExCeL London, UK
Booth: E1300

CE FC ISO 9001:2000

Videotrend S.r.l.
Distributore ufficiale Dahua
Tel. 0362 1791300
www.videotrend.net / info@videotrend.net

DAHUA TECHNOLOGY CO., LTD.
No.1199 Bin an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

Da Charlie Hebdo a Checkpoint Charlie, ovvero quando la sicurezza non significa più libertà

Il 2015 è cominciato in modo traumatico, gli attentati di Parigi hanno toccato le sensibilità individuali e collettive come era accaduto l'11 settembre 2001. Qualcuno ha osservato che, anche se i morti nella redazione di Charlie Hebdo e nel supermercato kosher siano stati molti meno di quelli ritrovati tra le macerie delle torri gemelle, i cambiamenti delle regole del vivere comune che deriveranno da questi ultimi episodi saranno di impatto almeno equivalente.

Tenendo sullo sfondo i grandi temi dell'integrazione, della tolleranza religiosa e delle libertà di espressione e di stampa, brutalizzati da questi attentati e dallo stillicidio di orrori che ci viene recapitato con sapiente regia quasi ogni giorno, ci rendiamo conto quanto i concetti di "libertà" e di "sicurezza" si ritrovino ancora una volta in drammatica contrapposizione, dove la prevalenza dell'uno comporta inevitabilmente l'annullamento dell'altro. Vediamo perché.

"Sicurezza" significa letteralmente "mancanza di percezione di pericolo". Quindi, ogni tipo di pericolo o di minaccia – per la salute, l'ambiente, i soldi, l'incolumità fisica, il lavoro e così via, fino alla sfera affettiva – comporta la ricerca di misure appropriate per prevenirlo ed evitarlo o, quanto meno, per ridurne gli effetti negativi. In altre parole, per "sentirsi sicuri". È partita da qui, fin dai tempi antichi, quella molteplicità di discipline, di competenze e di produzioni che oggi costituisce una parte cospicua del PIL mondiale. Basta pensare alla sanità e agli armamenti, per rendersi conto quanto l'idea di "mettere in sicurezza" o "fare sicurezza" sia riduttiva, se riferita alla sola prevenzione dei reati contro il patrimonio o la persona, alla quale viene abitualmente associato il termine "sicurezza".

Anche per definire la "libertà" si ricorre retoricamente a una "mancanza", in questo caso di vincoli al pensiero, all'espressione, all'azione, se non quelli inevitabili come le leggi della fisica e della convivenza sociale. Nell'era di internet, l'idea di libertà è sempre più correlata alla protezione dei nostri dati personali, nell'illusoria speranza che non vengano raccolti e catalogati da altri, privandoci in tal modo della libertà.

È intuitivo che le "mancanze" necessarie per avere sicurezza e libertà – rispettivamente la "percezione di pericolo" e di "vincoli" - possano coesistere solamente in condizioni di equilibrio o di armonia tra nazioni, tra persone, in natura, nel fisico di una persona eccetera.

Quando avviene uno scompenso, uno dei due concetti prevarrà inevitabilmente sull'altro, di solito con la supremazia della sicurezza sulla libertà, come è avvenuto dopo l'11 settembre e come sta avvenendo e avverrà dopo i fatti di gennaio 2015. Lo hanno fatto subito capire I giornali e i talkshow dei giorni successivi, più funzionali a farci elaborare il lutto per la perdita della libertà collettiva che per la morte dei vignettisti di Charlie Hebdo e dei clienti del negozio ebraico.

Cosa cambierà in concreto per i cittadini europei? In estrema sintesi, è partito un aumento dei controlli, con la conseguente caduta di ulteriori barriere a tutela della nostra privacy. I governi europei si stanno confrontando sulla fattibilità politica di aumentare i "Checkpoint Charlie", ovvero di punti di varco fisici e virtuali per poter controllare i movimenti delle persone, sia ai confini dei rispettivi stati che all'interno degli stessi.

Sul piano fisico, l'idea che qualsiasi luogo ad alta frequentazione debba venire considerato "obiettivo sensibile" dalle forze dell'ordine e, come tale, vada protetto con adeguati controlli agli accessi, è da tempo tradotta in realtà in paesi che convivono con il terrorismo, come, ad esempio, Israele. Come si è purtroppo visto, teatri, stadi e centri commerciali sono esposti al rischio di attentati come i treni e le metropolitane e, attualmente, sono tutti obiettivi più accessibili degli aerei, pur seminando altrettanto terrore nell'opinione pubblica che, per inciso, è esattamente quello che vogliono i terroristi di qualsiasi matrice.

È quindi prevedibile la diffusione di novelli "Checkpoint Charlie", forse senza Vopos e carri armati, ma dotati di sistemi di controllo-accessi, metal detector e soluzioni di analisi video e biometriche sempre più sofisticate, per il riconoscimento facciale e comportamentale delle persone in transito e il loro tracciamento.

Sul piano virtuale, i dati raccolti nei varchi fisici devono venire accentrati, analizzati, interpretati e confrontati con quelli provenienti dai "varchi" di altra natura, come i POS, le carte di credito, i siti internet, i cellulari, i telepass autostradali eccetera, per consentire alle "intelligence" di identificare i soggetti potenzialmente pericolosi, intercettarne i movimenti e prevenire possibili atti contro le comunità che devono proteggere.

Di conseguenza, di fronte alla preponderante e imprescindibile esigenza di "dare sicurezza" ai cittadini, si dissolve il diritto alla loro privacy e, quindi, alla loro libertà. Per qualcuno potrà sembrare uno scenario inquietante, ma è comprensibile che i più siano disposti a barattare volentieri gli ultimi brandelli di privacy/libertà, pur di ridurre le probabilità di trovarsi esposti a mitragliate per strada o coinvolti nell'esplosione di un attentatore suicida.

E poi, se pensiamo che la stragrande maggioranza delle persone ha già pubblicato sui social le proprie intimità, oppure le ha consegnate direttamente alle multinazionali del web per la ben meno nobile paura di sentirsi esclusi dai gruppi di acquisto - come sostiene Zigmunt Bauman con le sue teorie sulla "modernità liquida" (essecome 3/2014) - venire controllati a un Checkpoint Charlie in più da polizie che ci dovrebbero difendere non è forse un prezzo accettabile per la speranza di non fare la fine dei giornalisti di Charlie Hebdo?

Sommario

News

Technologies

Security for Retail

People

Denaro Sicuro

Vigilanza & Dintorni

Fiere

in copertina...

Il nuovo sistema antiscasso TSEC: alta sicurezza, bassa complessità, in un touch

Basato sull'analisi delle vibrazioni, la nuova architettura del sistema antiscasso TSEC, si fonda su due principali innovazioni: da un lato una nuova tecnologia sensoristica passiva, e dall'altro l'uso di moderne tecnologie elettroniche per arrivare ad elevatissimi livelli di sensibilità pur riducendo drasticamente sia la complessità della configurazione sia i costi di installazione.

I sensori inerziali della serie CLV sono costruiti sfruttando una nuova tecnologia magnetica, dove la massa vibrante viene tenuta in equilibrio non più dalla forza di gravità ma da campi magnetici tarati in maniera minuziosa nella fase di produzione.

Basate su moderni sistemi di controllo completamente digitali, le nuove schede inerziali della serie VAS sono in grado di sfruttare appieno la sensibilità dei sensori CLV.

Dotate di relais di uscita indipendenti per ciascun canale, sono compatibili con tutte le centrali di allarme in commercio. Il riconoscimento automatico delle resistenze di fine linea, sia per configurazioni con singolo sensore su ogni canale, che per quelle con collegamenti in serie di più sensori, assicurano la massima protezione da manomissioni sul cablaggio.

Nonostante la sofisticazione del sistema, la sua configurazione risulta però più semplice anche dei comuni sistemi che utilizzano sensori tradizionali a sfera o a lamelle. Grazie all'innovativo sistema senza fili WSync è infatti possibile utilizzare un comune smartphone per tutte le fasi di installazione, configurazione, taratura e manutenzione del sistema.

L'accessibilità economica del sistema lo rende fruibile anche negli impianti residenziali comuni determinando un livello di sicurezza fino ad oggi impensabile per questa tipologia di realizzazioni.

Quando il gioco si fa duro, sono i duri a giocare…

di Raffaello Juvara

Tokyo (Japan), 10 febbraio 2015

"Canon Inc. (Canon: Presidente e CEO Fujio Mitarai), ha annunciato oggi la Proposta di Offerta Pubblica in denaro (Offerta) agli azionisti della società svedese Axis AB (Axis: Presidente e CEO Ray Mauritsson) per vendere a Canon tutte le loro azioni in Axis. Il perfezionamento dell'offerta è soggetto a determinate condizioni. La azioni Axis sono quotate al Nasdaq di Stoccolma".

"L'Offerta è di natura amichevole e il Consiglio di Amministrazione di Axis ha deciso di raccomandare agli azionisti di Axis di accettarla. I tre principali azionisti di Axis, compresi i fondatori, che possiedono circa il 39,5% del totale delle azioni e dei diritti di voto in Axis, hanno deciso di accettare l'Offerta a determinate condizioni".

Stockholm (Sverige), 10 febbraio 2015

"Il Consiglio di Amministrazione di Axis, in base a considerazione di breve e medio-periodo, ha deliberato all'unanimità di raccomandare agli azionisti di Axis di accettare l'Offerta formulata da Canon".

"L'Offerta Pubblica lanciata da Canon agli azionisti di Axis per vendere a Canon tutte le loro azioni in Axis è al prezzo di 340 corone svedesi per azione. Questo prezzo rappresenta un premio del 49,8% sulla chiusura del 9 febbraio, del 64,4% sulla media delle chiusure degli ultimi 30 giorni lavorativi, del 70,6% sulla media delle chiusure degli ultimi 90 giorni lavorativi e del 35,6% sulla più alta quotazione raggiunta dalle azioni Axis (250,8 corone il 29 novembre 2013) dal momento delle quotazione al Nasdaq di Stoccolma del 27 giugno 2000".

Queste sono le aperture dei comunicati pubblicati il 10 febbraio 2015 nei siti di Canon e Axis, i protagonisti del deal che cambierà la storia della videosorveglianza a livello globale, con i quali sono stati resi pubblici i termini di una delle maggiori operazioni finanziarie mai avvenute nel mondo della sicurezza.

Il prezzo offerto di 340 corone (circa 32 euro) per azione corrisponde a un valore complessivo attribuito alla società svedese di circa 2,2 miliardi di euro, pari a oltre quattro volte il fatturato di 500 milioni realizzato da Axis nell'ultimo esercizio e oltre a quaranta volte l'utile netto di 50 milioni. Ma i pur rilevanti aspetti finanziari passano in secondo piano rispetto all'importanza strategica e politica del deal.

Come ha subito commentato Jon Cropley, capo analista di IHS, "questa operazione significa uno sviluppo enorme per il mercato della videosorveglianza. Fino all'anno scorso, Canon era un piccolo player in questo mercato, ma nel mese di agosto 2013 aveva rivelato le sue grandi ambizioni, quando il CEO Fujio Mitarai ha detto che le telecamere di sicurezza sarebbero diventate un "pilastro importante" per Canon e che quel mercato aveva "possibilità illimitate di crescita". Quindi, a giugno 2014 Canon ha comprato il più grande produttore mondiale di Video Management Software, la danese Milestone Systems, e ora si sta comprando il più grande produttore mondiale di videocamere in rete, la svedese Axis Communications. Tutto ciò dimostra quanto Canon abbia preso sul serio l'impegno di espandersi nel mercato dei componenti dei sistemi di videosorveglianza".

Fina dalle prossime settimane si capiranno gli effetti sul mercato. Forse non è un caso che Hikvision, il principale competitor a livello mondiale, abbia diramato il giorno dopo un comunicato stampa con gli strabilianti dati del 2014, con un fatturato di 2,82 miliardi di dollari in crescita del 60,3% sull'anno precedente e un CAGR (tasso medio di crescita) superiore al 53% nell'ultimo decennio. Ben poche aziende, in tutto il mondo e in ogni settore, possono vantare performance di questo livello.

Questi eventi e questi numeri stellari suggeriscono almeno tre considerazioni di ordine generale:

A. La crescita a ritmi galoppanti della videosorveglianza a livello mondiale. Come viene analizzato negli articoli che seguono di Jon Cropley e di Johan Paulsson, è un mercato in crescita a due cifre da almeno 5 anni e altrettanto farà nei prossimi, sulla spinta di una domanda crescente da parte di ogni categoria di utenti finali e in ogni area mondiale. I grandi numeri generati comportano l'interesse di competitori globali come Canon e di altre corporation che, con ogni probabilità, scenderanno in campo nei prossimi mesi; dall'altra parte, consentono lo sviluppo di aziende anche di dimensioni relativamente piccole con alti livelli di specializzazione;
B. L'industria della sicurezza in generale, e della videosorveglianza in particolare, è diventata un "obiettivo sensibile" di rilevanza politica. Con quello che sta succedendo nel mondo (crisi di teatro, terrorismi, separatismi) e lo sviluppo delle tecnologie dell'immagine (acquisizione, registrazione, interpretazione), diventate strumenti irrinunciabili per qualsiasi attività di intelligence, è ragionevole ritenere che i governi occidentali non intendano lasciare il dominio di un know-how diventato strategico, in mano solamente a costruttori cinesi. L'operazione Canon-Axis va forse letta anche in questo modo, così come il passaggio di Samsung Techwin al gruppo coreano Hanwua che, fra l'altro, è attivo anche nel campo delle forniture militari.
C. La concentrazione dei grandi vendor di tecnologie per la sicurezza oltre Oceano. Nell'editoriale di **essecome** 6/2014 avevamo denunciato la marginalizzazione in corso dell'industria europea della sicurezza, con le migliori aziende del nostro continente che possono aspirare solamente a essere ambite prede dei competitori globali, a causa della frammentazione del mercato interno. Milestone, Siemens SP e ora Axis sono i brand europei più noti passati sotto il controllo di competitori globali negli ultimi mesi, ma tutto fa pensare che siamo solo alle prime battute.

I trend secondo IHS per la videosorveglianza

contributo di Jon Cropley, capo analista di IHS per la videosorveglianza
traduzione a cura della Redazione

Secondo un nuovo white paper di IHS Inc (NYSE: IHS), l'industria globale della videosorveglianza potrà sottrarsi alla logica convenzionale del mercato resistendo alla tendenza di abbassamento del livello dei prodotti; ciò nonostante, crescerà più del 10% anche nel 2015. Nel 2014 aveva toccato 15 miliardi di dollari, con un aumento dell'11% rispetto al 2013. La cosa più importante è la previsione di raggiungere un valore di 23,6 miliardi di dollari entro il 2018, che corrisponderebbe a una crescita media annua del 12% per cinque anni consecutivi.

Jon Cropley, capo analista di IHS per la videosorveglianza e i servizi di security, sostiene che "il 2014 è stato uno degli anni più interessanti e caotici della storia recente per i produttori di videosorveglianza, sia per il mercato professionale che per quello consumer. Le forti diminuzioni del costo dei semiconduttori hanno determinato una nuova fase di concorrenza sui prezzi, con rilevanti cambiamenti di scenario a seguito dell'attività di acquisti e fusioni che ha interessato alcuni dei più importanti costruttori globali di prodotti e di software". Tuttavia, il settore della videosorveglianza può mantenere l'attuale livello di frammentazione della filiera produttiva e continuare a crescere per una serie di motivi, tra cui la riconoscibilità dei brand, le differenze (anche se sottili) fra le esigenze degli end-user nelle diverse aree geografiche e la continua differenziazione dei prodotti come, ad esempio, l'analisi video incorporata nelle telecamere. IHS ha previsto i seguenti trend per il settore nel 2015:

- La **differenziazione** sarà un market driver chiave per i tutti i produttori, distributori e integratori di componenti operanti nella videosorveglianza nei prossimi due anni.

- Le vendite di videocamere **HD TVCC** hanno superato 4 milioni di unità nel 2014, registrando un notevole aumento rispetto all'anno precedente. Data la forte performance di tecnologie, come la Composite Video Interface (CVI), l'Analog High-Definition (AHD) e la Transport Video Interface (TVI), nel 2015 le soluzioni analogiche continueranno a essere molto più vendute di quelle digitali e SDI. Nel corso dell'anno, si prevedono una forte competizione sui prezzi e ulteriori aggiornamenti incrementali dei prodotti.

www.hesa.com

HESA è sempre con te

Da oggi il mondo HESA è sempre con te con prodotti, promozioni e prezzi sempre aggiornati con un semplice click. Ovunque ti trovi puoi effettuare acquisti con la massima comodità attraverso il tuo tablet e utilizzando il negozio online ti assicuri sempre il miglior prezzo di acquisto, oltre alla possibilità di usufruire di vantaggiose promozioni.

Il catalogo online

Scopri il vantaggio di consultare il catalogo HESA sul sito con tutte le novità di prodotto e i prezzi aggiornati in tempo reale.

Versione mobile del sito

Scopri la comodità della versione mobile del sito HESA sullo schermo ridotto del tuo smartphone. Sempre con te, ovunque tu sia.

L'app HESA sul tablet

Puoi effettuare acquisti anche offline, compilare e inviare preventivi direttamente ai tuoi clienti. Scarica la nuova app HESA sul tuo tablet, è gratis!

Google play | App Store

HESA

SICUREZZA PROFESSIONALE IN CONTINUA EVOLUZIONE

HESA S.p.A. • Via Triboniano, 25 • 20156 MILANO • Tel. +39.02.380361 • Fax +39.02.38036701 • e-mail: hesa@hesa.com

- Il nuovo standard di compressione video **H.265** è stato uno degli argomenti più popolari del **Security China Show** tenutosi a Pechino in ottobre 2014, segnando una svolta nella videosorveglianza d'avanguardia.
- Nel 2015 la **Cina** emergerà come una regione dominante nello sviluppo dei prodotti, mentre ora il mercato è trainato principalmente dai centri R&D europei e nordamericani. Alcune società leader cinesi dispongono ora dei più grandi team al mondo dedicati a R&D della videosorveglianza. Con portfolio completi e prodotti dai prezzi competitivi, i produttori cinesi sono sempre più in cerca di opportunità nella scena mondiale per aumentare la propria presenza nei mercati stranieri.
- Un numero crescente di **produttori IT** tradizionali sta prendendo nota delle opportunità offerte dalla videosorveglianza; la migrazione dai sistemi analogici a quelli di rete ha cambiato il modo con cui molti sistemi di sicurezza vengono concepiti, costruiti e gestiti. Entro il 2018 il mercato globale dei componenti e dello storage per la videosorveglianza varrà più di 28 miliardi di dollari.
- Il **mercato consumer e "fai da te" (DIY)** che comprende i componenti venduti da retailers in negozio o online, nel 2013 valeva globalmente 953.4 milioni di dollari di cui il 47% dovuto a piccole imprese e end users commerciali. IHS si aspetta di vedere un maggior numero di produttori di componenti di videosorveglianza B2B - non B2C - interessarsi a questa fetta di mercato nel 2015, per completare la parte bassa della gamma di prodotti in listino.
- Si stima che i componenti di videosorveglianza venduti attraverso i **canali di distribuzione** nel 2013 valessero intorno al 55% del totale a livello globale, mentre a livello europeo erano del 60%. È prevista una crescita di queste percentuali, dato che i systems integrators e gli installatori approfitteranno dei vantaggi dell'acquisto di componenti attraverso questa modalità distribuzione.
- Nel corso del 2014 sono stati fatti esperimenti con **videocamere da indossare,** come elementi dei sistemi di videosorveglianza usati dalle Forze dell'Ordine. Nel 2015 ci si aspetta che vengano confermati gli ordini e vengano realizzate partnership a lungo termine. Le videocamere da indossare non solo sono utili come parti di un'ampia soluzione di videosorveglianza, ma possono anche contribuire a azioni di tipo politico finalizzate ad aumentare la fiducia negli agenti di polizia sul territorio.
- La cosiddetta **"Embedded vision - Visione incorporata",** la combinazione di sistemi integrati e computer vision, avrà nuove implicazioni nell'Advanced Driver Assistance Systems (ADAS) nell'industria automotive, con innovazioni che si rifletteranno nell'industria della videosorveglianza.

Tecnologie e sviluppi della videosorveglianza nel 2015 e oltre

contributo di Johan Paulsson, Chief Technology Officer, Axis Communications

Per tutto il 2014 e in tutti i settori, l'Internet delle cose è stato un argomento all'ordine del giorno, sia che riguardasse automobili smart che elettrodomestici intelligenti come i frigoriferi connessi al Web. Non sorprende, dunque, che sempre più consumatori e aziende siano consapevoli dei vantaggi offerti da una connessione a Internet: questo vale anche per i professionisti della sicurezza e per tutti coloro che vogliono tutelare la propria impresa.

Secondo le previsioni di numerosi esperti, il nuovo standard '4K Ultra HD' continuerà a essere uno dei temi più caldi, oltre che la naturale evoluzione in un settore che persegue immagini sempre più dettagliate e una copertura più ampia con le telecamere di videosorveglianza. Lo standard 4K per le applicazioni di videosorveglianza sarà sempre più diffuso a partire dal 2015. La qualità dell'immagine è un fattore chiave e sebbene tutti parlino dello standard 4K, la vera sfida consiste nell'ottimizzare la qualità dell'immagine per le proprie applicazioni di videosorveglianza, indipendentemente dalle condizioni di luce e ambientali. L'innovazione in questa area, ovvero lo sviluppo di una tecnologia capace di aumentare la qualità d'immagine per applicazioni avanzate di videosorveglianza, sarà il fattore trainante del settore. I progressi compiuti a livello della qualità dell'immagine hanno tuttavia introdotto nuove sfide per quanto riguarda la gestione delle risorse necessarie a supportare questa maggiore qualità. Questi progressi possono ad esempio avere un impatto significativo sui requisiti riguardanti la larghezza di banda della rete e l'archiviazione, e richiedere l'introduzione di metodi di compressione più efficaci.

Videosorveglianza come servizio (VSaaS) e cloud computing

La videosorveglianza come servizio (VSaaS) può essere utile per gestire e archiviare su cloud i filmati ripresi dalle telecamere. I sistemi di videosorveglianza installati in ambienti quali centri commerciali, parchi, banche, aeroporti e trasporti pubblici possono essere uno strumento efficace per prevenire il crimine o condurre le indagini. In alcuni casi, il rapido aumento della domanda di sistemi di videosorveglianza è la diretta conseguenza del crescente interesse verso la sicurezza registrato in ogni parte del mondo.

Secondo Transparency Market Research, il settore della videosorveglianza e dei servizi VSaaS dovrebbe raggiungere 42,81 miliardi di dollari entro il 2019, con un tasso annuale medio di crescita (CAGR) del 19,1% tra il 2013 e il 2019. Per quanto riguarda i sistemi, il settore della videosorveglianza basata su IP dovrebbe crescere rapidamente ad un tasso annuale medio del 24,2% durante il periodo di previsione (2013-2019).

Nel 2012, il settore hardware è stato valutato a 9,49 miliardi di dollari e dovrebbe crescere ad un tasso CAGR del 17,3% durante il periodo di previsione (2013-2019). Questo settore copre telecamere di videosorveglianza analogiche e basate su IP, unità di registrazione e archiviazione, codificatori e monitor. Nel 2012, la quota del segmento delle unità di registrazione e archiviazione ha raggiunto il 37% del settore hardware complessivo, seguita dalle telecamere di videosorveglianza col 32%. Nei prossimi anni, tuttavia, si prevede una diminuzione della quota delle unità di registrazione e archiviazione in seguito ad una diffusione sempre maggiore delle soluzioni di archiviazione basate sul Cloud (VSaaS). La quota della telecamere di videosorveglianza dovrebbe invece aumentare fino a raggiungere circa di 46% nel 2019 in seguito alla crescente diffusione delle telecamere di videosorveglianza basate su IP che offrono una migliore qualità delle immagini video e che dispongono di unità di registrazione incorporate.

È da vari anni che “cloud computing” è un termine di gran voga tra gli operatori del settore IT, ma è soprattutto ora che avvertiamo gli effetti di questa nuova era. Sia che venga utilizzato un ambiente di archiviazione pubblico, dove lo spazio sui server viene condiviso con altri clienti, o un ambiente privato, dove solo i propri dati e le proprie applicazioni risiedono su un sistema, il cloud computing offre tre vantaggi alla rete: ridondanza, scalabilità e trasferimento dei costi da spesa per capitale (CAPEX) a spesa operativa (OPEX). A seconda che il cloud sia in hosting o sia gestito internamente, un ulteriore vantaggio potrebbe essere la possibilità di affidare upgrade, aggiornamenti e patch (manutenzione periodica) a terze parti.

La scalabilità non è importante solo quando oc-

corrono più telecamere. Essa consente, infatti, di ottenere più potenza di calcolo e capacità di archiviazione quando è ad esempio necessaria una maggiore risoluzione o una velocità in fotogrammi superiore. Se ad esempio è necessario analizzare i dati video raccolti per determinare eventuali pattern a livello del traffico, ci si può avvalere di una capacità di elaborazione superiore che si paga solo quando necessario.

Una migliore gestione dell'Intelligent Video a bordo cameraè valida anche per applicazioni riguardanti infrastrutture di importanza critica. La potenza di calcolo addizionale può infatti essere utilizzata per archiviare mezzo milione di numeri di targa e catturare ad esempio le targhe delle auto che superano i 40 km/h. La videosorveglianza intesa come servizio è interessante anche perché offre la possibilità di aggiungere altri servizi, come quelli di monitoraggio remoto o di guardia.

Analisi, business intelligence e big data

Si prevede che a partire dal 2015 la tecnologia di analisi dovrebbe definitivamente decollare nel settore della videosorveglianza per consentire di ricavare dati utili da enormi quantità di informazioni strutturate e non (i cosiddetti "big data"). Grazie alla capacità delle telecamere di rete di fornire video a risoluzione più elevata e di connettersi da qualsiasi punto e in un qualsiasi momento, i reparti di videosorveglianza ricevono molte informazioni da più fonti. Per aiutare le organizzazioni a interpretare questa incredibile quantità di dati, compresi dati non strutturati come immagini e video, sono necessari maggiori strumenti analitici. Per aiutare a categorizzare e interpretare le informazioni, in modo da ottenere dati immediatamente utili, sono necessarie applicazioni più intelligenti.

Le tre V che caratterizzano i big data, vale a dire Volume, Velocità e Varietà, sono decisive per poter fornire informazioni di importanza vitale e i dati giusti nel momento giusto, durante una crisi. Partendo da dati più fattuali, come dati di videosorveglianza, dati di controllo degli accessi fisici e dati su attività informatiche e stabilendo successivamente utili associazioni, è possibile ridurre i costi attraverso la ricerca delle informazioni più pertinenti.

È in questo modo che la rivoluzione IP è in grado di trasformare una telecamera di videosorveglianza in uno strumento investigativo che può essere utilizzato per risolvere problemi dopo un incidente e diventare quindi un componente vitale di una catena preventiva. Utilizzando immagini video e sfruttando al contempo un'elevata potenza analitica, è possibile ad esempio scoprire pattern nel traffico degli avventori di un esercizio commerciale, analizzare i tempi di sosta in particolari punti del negozio o isolare colli di bottiglia. Se a tutto ciò si aggiungono altre fonti di dati strutturati e non strutturati, comprese tabelle di transito, elenchi di promozioni, dati sui prezzi di aziende concorrenti e dati provenienti da social media, un analista esperto è in grado di individuare relazioni e pattern inaspettati. Tutto ciò rappresenta un notevole vantaggio sulla concorrenza.

Compressione video e uso della larghezza di banda

Le tecnologie di compressione video hanno lo scopo di ridurre e rimuovere i dati video ridondanti affinché il file video digitale risultante possa essere trasmesso in modo efficiente attraverso una rete e memorizzato su unità disco. Con tecniche di compressione efficaci, è possibile ottenere una riduzione notevole delle dimensioni dei file con effetti minimi o comunque non negativi sulla qualità delle immagini. Se tuttavia la dimensione del file viene ulteriormente ridotta aumentando la compressione ottenuta con una particolare tecnica, è possibile che si notino effetti sulla qualità delle immagini.

Sono disponibili vari standard di compressione video compresi: Motion JPEG, MPEG-4 Parte 2 (noto semplicemente come MPEG-4) e H.264. Quest'ultimo rappresenta il più recente ed efficiente standard di compressione video ed è già diventato lo standard nel settore della videosorveglianza e in molti altri settori, come ad esempio il settore dell'intrattenimento. Allo stesso tempo, il continuo miglioramento delle telecamere, relativo ad esempio alla risoluzione d'immagine e alla sensibilità alla luce, aumenta il volume dei dati in uscita dalle telecamere e impone una compressione video più efficiente. Le case produttrici di apparecchiature di videosorveglianza devono far fronte all'aumento della risoluzione migliorando gli algoritmi di compressione H.264, affinché i costi per l'utilizzo della larghezza di banda e dello spazio di archiviazione non aumentino in modo incontrollato. L'impegno comune per trovare metodi di riduzione dei disturbi e ridurre la velocità di trasmissione deve essere accompagnato dalla ricerca di una nuova codifica video che consenta di ottenere risultati ottimali.

Oltre ai miglioramenti a livello dell'attuale standard di compressione H.264, lo standard H.265 è un'interessante tecnologia futura che sta rapidamente guadagnando interesse nel settore del broadcasting. Lo standard H.265 è in grado di ridurre in modo significativo i requisiti riguardanti la larghezza di banda e l'archiviazione (fino al 50%) in particolari circostanze e questa tecnologia dovrebbe essere introdotta nel settore della videosorveglianza nel corso dei prossimi anni. Essa verrà probabilmente introdotta per le telecamere ad alta risoluzione di fascia alta e si prevede che le tecnologie H.264 e H.265 continueranno a coesistere nel settore.

Conclusione

In conclusione, video e immagini di maggiore qualità come ad esempio quelli basati sullo standard 4K hanno bisogno di essere supportati da tecnologie adeguate per consentire ad aziende e organizzazioni di ottenere il massimo dai dati e trasformarli in utili insight non solo per scopi di sicurezza ma anche per migliorare l'efficienza e ottenere vantaggi commerciali. Questa dovrebbe essere la considerazione chiave per chiunque cerchi di capire quale sarà il prossimo grande sviluppo nel campo della videosorveglianza.

SuperLoLux HD2™

Nuove Camere CCTV JVC Super LoLux HD2

NOTTI D'ESTATE

DAL TRAMONTO ALL' ALBA CON SLL HD2

Combinando le alte prestazioni con la risoluzione FULL HD, la prossima generazione di telecamere Super LoLux HD2 (modelli EX) può offrire una superiore riproduzione dei colori anche con poca luce.

Le nuove telecamere JVC Super LoLux HD2 IP offrono eccezionali prestazioni e precisa riproduzione dei colori e sono equipaggiate con nuovi sensori CMOS sviluppati per ottenere eccezionali prestazioni in condizioni di scarsa luminosità, garantendo risoluzioni in full HD 1080p. La sensibilità è stata notevolmente migliorata rispetto alla camere della prima generazione e i nuovi modelli SLL HD2 (EX) garantiscono colori e dettagli impressionanti – senza l' utilizzo di LEDs – con livelli di luce di soli 0.05 lux.

I sei modelli della gamma SLL HD2 sono costituiti da tre camere box, due dome da interni e una dome da esterni grado IP66, ognuna con incluso il supporto multicodec M-JPEG, MPEG-4 e H.264 High Profile. E'stata inoltre migliorata la compensazione del controluce per rendere un'ottimale qualità dell'immagine, in particolare nelle zone difficili, l'eleborazione intelligente delle immagini assicura inoltre una ripresa ottimale indipendentemente dalle condizioni di illuminazione.

Precedente Telecamera SLL HD
(Immagine reale ripresa a 0.1 lux)

Nuova Telecamera SLL HD2
(Immagine reale ripresa a 0.1 lux)

- Nuova generazione sensibilità
- Eccezionali dettagli e colori
- Miglioramento delle prestazioni WDR

Per ulteriori informazioni sulle nostre soluzioni CCTV, si prega di visitare www.jvcpro.it/cctv.

JVC

Essecome entra nel 35° anno, con ottimi risultati e tante novità

a cura della Redazione

Nel febbraio del 1981 è uscito il numero 1 di **essecome**, la rivista fondata da Paolo Tura subito diventata una testata di riferimento per gli operatori della sicurezza fisica. Festeggiamo l'inizio del 35° anno di attività evitando ricordi e celebrazioni, perché troppe cose sono cambiate nel mondo della comunicazione e in quello della sicurezza, per non parlare del mondo circostante. Preferiamo, quindi, parlare di ciò che abbiamo realizzato nel 2014, e dei nostri programmi per l'anno appena iniziato, con l'impegno e l'auspicio di continuare a essere anche in futuro un punto di riferimento attendibile e qualificato per i professionisti di una materia che sta diventando sempre più importante per l'intera società.

In sintesi, il nostro programma si articola sulla evoluzione continua di **essecome**, sullo sviluppo di **securindex.com**, che lo scorso anno ha ottenuto risultati eccellenti, e sul lancio di un programma di **eventi** esclusivi, dedicati agli argomenti di maggiore attualità.

L'integrazione tra carta e web

Nel 2014 è stato completato il processo di integrazione tra il supporto cartaceo e quello digitale. La rivista bimestrale è diventata un **framework** di contenuti tecnici, scientifici e culturali che vengono puntualmente ripresi in **securindex.com** in forma di pdf globale e di post singoli.

In questo modo, anche gli articoli di elevato approfondimento che caratterizzano la linea editoriale di **essecome** vengono divulgati in rete, con il rilancio

spontaneo da parte dei lettori sui social più diffusi. Il risultato è duplice: l'aumento della visibilità degli articoli pubblicati su carta, e l'innalzamento dei contenuti postati on-line.

Sull'altro versante, le news più significative ricevute dalla redazione di **securindex.com** vengono approfondite dalla redazione della rivista, mediante interviste e informazioni aggiuntive, per realizzare articoli e servizi da pubblicare in **essecome**.

Il nostro obiettivo è la realizzazione di un'**unica piattaforma di comunicazione** per la diffusione delle informazioni e della cultura della sicurezza, utile e concretamente fruibile per tutti gli operatori e gli stake holders: clienti, progettisti, forze dell'ordine, amministratori pubblici, lavoratori del settore.

Le sezioni tematiche e i mercati verticali

La costituzione di una piattaforma unica di comunica-

zione viene sottolineata dalla suddivisione in sezioni tematiche e mercati verticali, presenti con la stessa grafica sia in **essecome** che in **securindex.com**:

- **News** e **Technologies** sono le sezioni interdisciplinari che raccolgono rispettivamente gli articoli di attualità di interesse generale e gli approfondimenti tecnici presentati dalle aziende per ogni applicazione di security, fire e safety. **Norme & Sentenze** è la sottosezione che raccoglie contenuti normativi e giurisprudenziali selezionati per importanza, mentre **Fiere ed Eventi** offre il calendario aggiornato delle manifestazioni fieristiche e congressuali di tutto il mondo, con articoli e presentazioni degli eventi più importanti di cui le nostre testate sono media partner.
- **Denaro Sicuro è dedicata principalmente alla sicurezza** e alla evoluzione strutturale del settore bancario e alla gestione del denaro contante (trasporto, contazione, custodia), con il contributo dei protagonisti della sicurezza bancaria e dei principali operatori italiani e stranieri del CIT.
- **Security for Retail** si rivolge agli operatori della distribuzione, il mercato verticale più importante per l'industria della sicurezza fisica, comprendendo i retailer internazionali, la grande distribuzione organizzata, i centri commerciali, i negozi di prossimità e le infrastrutture della logistica e del trasporto
- **Vigilanza & Dintorni è l'unic**a testata su carta e web dedicata alla vigilanza privata, per la quale tratta in modo specialistico gli aspetti normativi, contrattuali, tecnologici e gestionali
- **Fire & Safety** affronta le tematiche dell'anti-incendio e della safety, in particolare per presentare le soluzioni tecnologiche trasversali con la security
- **Cultura e Formazione è rivolta a**l grande tema della formazione professionale, della cultura della sicurezza e della "sicurezza della cultura" ovvero del patrimonio artistico nazionale, il principale asset del nostro paese.
- **Casamiasicura è la sezione dedicata al mercato residenziale e alla sicurezza della persona, che riprende la denominazione del motore di ricerca B2C per la promozione dei** fornitori diretti dell'utente finale.

Gli eventi di essecome

Gli eventi di essecome completano la piattaforma di comunicazione specializzata, offrendo un percorso a tema che copre i principali ambiti mercati verticali della sicurezza fisica. **Gli eventi di essecome** vengono sviluppati utilizzando tre formati: seminari riservati a inviti in location di prestigio – tavole rotonde a tema nell'ambito delle fiere settoriali più importanti – workshop organizzati con i Partner. Di ogni evento viene realizzato il servizio televisivo dal team di **Securindex TV** con interviste ai protagonisti, per la pubblicazione nel canale Youtube.

Nel 2015 sono previsti:

- **Security for Retail Forum 2015.** *Seminario a inviti* ***2 marzo*** *a Milano Palazzo delle Stelline*
- **Certificazioni e certificatori per il DM 115 (Vigilanza & Dintorni)** - *Roadshow - primavera a Milano, Roma, Bari*
- **Eccellenze tecnologiche per la sicurezza -** *Seminario a inviti - settembre in Franciacorta*

securindex.com, visitatori unici +48%

- **Security for Retail** - *Tavole rotonde a tema – 3-5 novembre a Sicurezza 2015 - Milano Rho*
- **Per una Città Sicura nell'Euroregione** - *Seminario a inviti - **dicembre a** Trieste*

Durante il 2014, sono stati effettuati importanti interventi nella piattaforma informatica di **securindex.com,** per migliorarne la funzionalità e la grafica, e renderlo idoneo a ospitare i contenuti di **essecome**.

I risultati hanno premiato questo impegno, come ha certificato **Google Analytics** che, nel 2014, ha registrato **54.220** sessioni, con **37.332** utenti (primi visitatori) e **115.772** visualizzazioni, con aumenti rispetto all'anno precedente rispettivamente del **28,2%,** del **48,1%** e del **29,9%.**

Secondo le certificazioni di **Mail Chimp**, in Q4/2014 sono state inviate **15 Securindex WIN** (Weekly Information Newsletter) ai nostri data base con oltre 10.000 indirizzi attivi complessivi, con un indice di aperture totali superiore al **30%** e di click totali del **2,7%.**

Sempre in Q4, sono state realizzate **20** campagne dedicate (**DEM**) per conto di Partner, che hanno ottenuto un indice di aperture totali del **32,7%** (aperture uniche **17,5%**) e di click totali del **3,9%**. La DEM del 7 novembre 2014 (CITEL) ha ottenuto **2074 click totali**.

Sempre nel 2014, Securindex.com ha pubblicato **118** notizie di interesse generale e **244** comunicati di Partner, che avevano ottenuto al 31 dicembre 2014 **89.308** visualizzazioni totali (media **366**).

I due Partner più attivi hanno pubblicato, separatamente, **21** comunicati con **5.104** visualizzazioni, e **19** comunicati con **8.195** visualizzazioni. Un altro Partner ha pubblicato il comunicato più visualizzato nel 2014, con **514** visite.

Tra le notizie di interesse generale, il post sull'acquisizione di IVRI da parte del gruppo KSM, pubblicato il 3 marzo 2014, aveva ottenuto al 31 dicembre **13.144** visualizzazioni.

Nota bene: La certificazione dei dati sopra riportati è disponibile a richiesta oppure è riportata da contatori direttamente accessibili dai visitatori di **securindex.com.**

Citel, quando “saper fare” viene “fatto sapere”

a colloquio con Nils Fazzini, Direttore Operations CITEL spa
a cura della Redazione

Nel rilevamento al 31 dicembre 2014, i comunicati di Citel pubblicati in www.securindex.com nel 2014 hanno ottenuto una media di 514 aperture ognuna, risultando over performing del 40% rispetto alle media globale delle news aziendali (366). A cosa ritiene sia dovuto l’interesse dei nostri lettori verso i contenuti che avete proposto?
È un risultato gratificante e ci dà una spinta ulteriore a continuare sulla strada che abbiamo scelto dall’inizio per la nostra comunicazione, quella della narrazione di un percorso aziendale vissuto insieme all’evoluzione del settore della sicurezza fisica in un contesto sempre più digitale. E penso che, per molti lettori, sia di interesse più generalizzato una notizia sulle tendenze di settore che su un singolo prodotto.
Abbiamo sempre puntato a condividere con gli utenti finali e con i fornitori complementari i progressi del settore della sicurezza fisica in Italia ed abbiamo avuto la fortuna di poterci confrontare con figure di tutto rilievo, con cui si può dire che abbiamo scritto a più mani la storia recente del settore. Partendo comunque da un presupposto di fondo: la sicurezza fisica va gestita come un qualsiasi processo aziendale secondo criteri ispirati all’efficienza e alle buone pratiche gestionali, e con l’informatizzazione come strumento ovvio per ottenere tutto ciò.
Abbiamo iniziato anni fa sostenendo che nella sicurezza fisica centralizzata bancaria l’Italia era davanti a tutti nel mondo, e che il motivo principale era l’architettura aperta multi fornitore, grazie al protocollo pubblico bidirezionale ad alta sicurezza e affidabilità voluto dall’ABI già nel 1979.

Può sembrare incredibile che un protocollo di comunicazione espresso da un’associazione di categoria possa cambiare la storia di un intero settore in un intero Paese, ma è quello che può succedere se quella spinta va nella stessa direzione di un movimento di fondo, accelerandolo.
E la direzione in questione è sempre stata per noi l’informatizzazione pervasiva, quella che ha prima occupato le aziende e le organizzazioni in genere e poi gli stessi individui con l’informatica personale; e quella che, in definitiva, ha messo in discussione le archi-

tetture informatiche chiuse, confinandole in contesti sempre più di nicchia.
Quindi una storia interessante, che viene letta volentieri in questi tempi: quella di un'Italia che anticipa di anni il perfezionamento e l'uso della tecnologia, che è il Paese dove il PSIM è nato, dove l'architettura aperta è diventata la regola, mentre nei Paesi più avanzati al massimo si è arrivati allo standard associativo per il video e, da poco, per il controllo accessi.

La DEM inviata il 7 novembre scorso per presentare l'e-book sull'Ecosistema Centrax ha ottenuto 2154 visualizzazioni totali (media generale 1952), con un numero di click totali davvero eccezionale: 2074 a fronte di una media di 172. In pratica, ogni lettore della DEM ha aperto l'e-book sull'Ecosistema Centrax, dimostrando un interesse molto elevato per quanto avete presentato. Possiamo riassumere il contenuto dell'e-book?
Il concetto di *Ecosistema* ha aiutato ad approfondire la narrazione del nostro percorso aziendale, associato all'evoluzione del settore in Italia, in quanto appropriato per la percezione intuitiva delle sinergie che possono nascere quando utenti innovativi e fornitori complementari e aperti contribuiscono a far evolvere un sistema come il Centrax-PSIM di Citel.
L'interesse ad approfondire oltre la curiosità iniziale si spiega con il fatto che per la prima volta nella stampa specializzata appare la combinazione dei concetti "*PSIM*" ed "*Ecosistema*", con il coinvolgimento, oltretutto, di numerosi incontestabili protagonisti del mercato quali soggetti attivi di interoperabilità in architettura aperta multifornitore.
Si può capire che sia interessante per gli addetti ai lavori sapere come si stanno muovendo gli utenti all'avanguardia; che poi è quello che abbiamo raccontato, evidenziando soprattutto il ruolo delle comunità composte dai grandi della finanza e dell'industria, insieme agli utenti di medie dimensioni; ma anche la svolta delle Società di Security più innovative, impegnate in una ridefinizione settoriale che - in chiave PSIM - punta a erogare in forma di servizio le nuove funzionalità agli utenti di dimensioni minori.
Con una precisazione importante, che va fatta. Un Ecosistema di tipo *industriale* e non naturale, si attiva e si mantiene con gli investimenti del suo produttore: le tante integrazioni di prodotti di terzi in ambito Centrax non ci sarebbero mai state se Citel le avesse fatte su progetto a spese del committente, e lo stesso vale per le funzionalità del PSIM. In effetti le inte-

grazione e le funzionalità di Centrax sono numerose perché sono state realizzate dal laboratorio Citel con investimenti interni e ritorni proiettati negli anni. Citel è infatti una società che fa profitti sin dalla fondazione, con una politica costante di reinvestimento per finanziare lo sviluppo tecnico indirizzato appunto al PSIM, alle sue funzionalità e all'alimentazione del suo Ecosistema lungo un percorso ultradecennale, come si conviene ai sistemi informatizzati.

Quali sono i vostri programmi per il 2015?

Abbiamo molta carne al fuoco, sia in laboratorio che nel mercato. Non possiamo entrare nel dettaglio perché l'informazione sulle novità passa prima dai nostri utenti ma possiamo dire che puntiamo decisamente sulle estensioni applicative di Centrax-PSIM dalla sicurezza fisica verso la safety dei lavoratori, il governo dell'efficienza energetica e la tele-portineria, in modo che l'utenza del sistema ottenga delle economie di scopo dall'infrastruttura di gestione che ha creato.

Sul piano delle prestazioni di sistema, Centrax-PSIM è stato potenziato particolarmente sul piano della multimedialità a fini di interazione efficace tra postazione di gestione e sito remoto. Quindi, non solo interfacce grafiche ma anche audio bidirezionale e in generale telefonia over-IP, non solo su strutture fisse ma anche su piattaforme mobili e apparati indossabili.

Per concludere con il fatto di maggiore valenza strategica, nel 2014 abbiamo completato una serie di progetti che ci hanno permesso di affinare e referenziare il modello del Building-PSIM in architettura aperta multifornitore. Sarà un filone di business importante per noi, che negli ultimi anni abbiamo lavorato duro su clienti di grande prestigio ed esigenze stringenti, ottenendo per contro di poter annunciare al mercato che abbiamo la possibilità di rispondere a capitolati di automazione integrale telegestita di edifici singoli e multipli in architettura PSIM.

Con questo - per concludere - daremo la possibilità ai nostri utenti e ai loro progettisti di orientarsi alle soluzioni realmente interoperabili, anche multi-fornitore, in contrapposizione al modello di building automation vincolato al fornitore unico.

Infrastrutture critiche più sicure con le termocamere FLIR

a colloquio con Giovanni Scaglia, Sales Manager Distribuzione Sud Europa e Africa Sub Sahariana FLIR
a cura della Redazione

Nello scorso dicembre, persone finora non identificate hanno superato le recinzioni della TAV vicino a Bologna in una notte di nebbia e hanno introdotto degli stracci infiammati in alcuni pozzetti di accesso alle dorsali in fibra ottica, bloccando la trasmissione dei dati, e, di conseguenza, paralizzando il traffico ferroviario all'altezza dello snodo più importante del paese alla vigilia delle feste natalizie.. Da alcuni giornali è stato evidenziato che i sistemi di videosorveglianza a protezione della linea – se ci fossero stati - non sarebbero stati in grado di riprendere né tantomeno di identificare delle persone di notte o in caso di maltempo. Come sarebbe possibile usare le videocamere termiche per questo specifico impiego?

Le termocamere producono un'immagine nitida anche nelle notti più buie. Diversamente da altre tecnologie, non hanno bisogno di alcuna luce per creare immagini ben definite, riuscendo a vedere anche attraverso nebbia leggera e fumo, praticamente in qualsiasi condizione atmosferica. Sono pertanto strumenti perfetti per la sorveglianza remota 24/7. L'immagine termica può essere utilizzata per tutti i tipi di applicazioni di sicurezza e sorveglianza a distanza, specialmente quando si devono rilevare potenziali intrusi nella totale oscurità, prescindendo dalla situazione meteorologica. Compito della sicurezza, dopo tutto, è proprio individuare qualsiasi minaccia, 24 ore al giorno. Le termocamere sono strumenti potenti, che consentono di individuare individui sospetti in totale oscurità, attraverso fumo e vegetazione leggera. Il contrasto termico è molto difficile da mascherare.

Anche se qualcuno tenta di nascondersi nell'ombra o fra dei cespugli oppure di mimetizzarsi, non può sfuggire all'occhio vigile di una termocamera.

Le termo camere, inoltre, non vengono saturate dalla luce del sole e producono un'immagine nitida praticamente in qualsiasi condizione meteorologica. Una delle parti più importanti di una termocamera è infatti il rilevatore. La maggior parte delle termocamere di FLIR Systems per la sicurezza e la sorveglianza utilizzano rilevatori a microbolometro non raffreddati

all'ossido di vanadio (VOx). Sebbene possano essere utilizzati altri materiali per produrre rilevatori a microbolometro, l'ossido di vanadio è superiore a tutti. I microbolometri all'ossido di vanadio offrono una qualità d'immagine superiore in ogni ambiente e consentono persino di inquadrare direttamente il sole o avere il sole nel campo visivo della termo camera, continuando a fornire un'immagine ad alto contrasto termico.

Esistono realizzazioni in altri paesi che possano venire utilizzate come riferimento di protezione di IC?

L'aeroporto di Monaco in Germania, ufficialmente chiamato "Aeroporto Franz Josef Strauss", situato a 28 km a nordest dalla città, utilizza le termocamere **SR-100** di FLIR Systems per proteggere il proprio perimetro esterno. L'aeroporto di Monaco è il secondo della Germania in termini di traffico di passeggeri, alle spalle di quello di Francoforte, al settimo posto in Europa e al ventottesimo a livello mondiale. Il "Franz Josef Strauss" copre una superficie di 1.560 ettari, con un rettilineo lungo circa 6 chilometri. Come in tutti i principali aeroporti, assicurare la sicurezza dei passeggeri, degli aeromobili e dei loro equipaggi, dello staff e di tutte le altre persone in transito è una priorità e le termocamere di FLIR Systems contribuiscono a garantire che nessuna minaccia passi inosservata. I responsabili dell'aeroporto hanno optato per il modello **FLIR SR-100**, che ha un'ottima portata ed è in grado di rilevare un obiettivo della taglia di un uomo a una distanza di circa 1,6 chilometri, offrendo un'eccellente combinazione di portata, qualità dell'immagine e prezzo. Le termocamere SR-100 sono state installate su un dispositivo di rotazione/inclinazione per poter monitorare dovunque vogliano. Le immagini generate dalla SR-100 viaggiano su fibre ottiche fino alla sala di controllo, dove è possibile controllare la rotazione/inclinazione e guardare le immagini su tutti gli schermi o sullo schermo a parete. Se viene rilevata una minaccia così si può agire immediatamente.

Quali sono le differenze in termini economici e delle altre prestazioni (p.e. l'analisi video) tra le videocamere termiche e quelle normali?

Nonostante una termocamera sia più costosa di una telecamera tradizionale, l'investimento per la protezione perimetrale è inferiore, poiché è necessario un numero minore di unità. Utilizzare meno telecamere significa anche un minore investimento per tutte le attrezzature ad esse collegate (tutto il necessario per mettere correttamente in funzione la telecamera e trasmettere il segnale video sugli schermi della sala di controllo). Tutti questi costi aggiuntivi devono essere moltiplicati per ogni telecamera.

Riducendo il numero di telecamere necessarie, la termografia consente ai clienti di realizzare risparmi significativi nelle infrastrutture e attrezzature necessarie per le telecamere. Inoltre, le termocamere non richiedono alcuna fonte di illuminazione: i sistemi di illuminazione non sono soltanto molto costosi da installare, ma richiedono anche una grande quantità di energia elettrica per restare accesi tutta la notte. In conclusione, anche se all'inizio le termocamere sono leggermente più dispendiose delle telecamere, si rivelano non solo la soluzione migliore, ma anche quella con un rapporto prezzo-prestazioni più favorevole.

Le termocamere di sicurezza permettono di vedere più lontano di qualsiasi altra tecnologia di visione notturna attualmente disponibile sul mercato, ma in certe situazioni, anche di giorno, funzionano addirittura meglio delle telecamere.

Un vantaggio offerto dalle termocamere durante il giorno rispetto alle telecamere è che le seconde possono venire accecate dalla luce diretta o riflessa del sole. Le termocamere, invece, non soffrono di questo problema. Le normali telecamere dipendono dal contrasto visivo per fornire informazioni sufficienti ai software di analisi video o per consentire al personale di sorveglianza di rilevare un intruso. Anche a distanze moderate, un contrasto colore debole può rendere inutili queste telecamere. Le termocamere non hanno questo limite. Gli esseri umani emettono molte più radiazioni termiche dell'ambiente circostante. Questo significa che i software di analisi video o l'occhio umano che visiona le immagini possono vedere molto più facilmente gli intrusi nel materiale video proveniente da una termocamera, rispetto alle riprese di una telecamera. Le termocamere inoltre generano un minor numero di falsi allarmi rispetto alle telecamere. Per esempio, un ragno che passa sull'obiettivo della telecamera, o i rami di un albero mossi dal vento, sono tra le numerose possibili cause di falsi allarmi. Le termocamere generano un minor numero di falsi allarmi per lo stesso motivo per cui hanno migliori prestazioni in termini di portata rispetto alle telecamere. Il contrasto termico è solitamente molto maggiore del contrasto visivo e, quindi, il software di analisi video può distinguere in modo molto più accurato tra un ramo mosso dal vento, ad esempio, ed un intruso che sta tentando di accedere all'area.

Sono possibili utilizzi in ambito forense?
Ai fini dell'individuazione di attività sospette in luoghi di interesse pubblico e non solo, la strumentazione di visione IR di tipo passivo risulta specificamente indicata, ed in particolar modo in condizioni di totale assenza d'illuminazione nonché in condizioni di nebbia o fumo. Tali immagini potrebbero essere infatti registrate automaticamente, e venire utilizzate per fornire elementi utili alle indagini preliminari da parte degli organi competenti. Le apparecchiature permetterebbero infatti di seguire azioni di boicottaggio, manomissione, intercettazione di individui attraverso l'uso di software intelligenti, che garantirebbero l'intervento dei corpi di sorveglianza preposti in tempo utile, ai fini dell'individuazione delle persone.
È ormai prassi comune l'installazione di dispositivi di sorveglianza di questo tipo presso tutti i siti militari e civili particolarmente sensibili (caserme, aeroporti, centri di munizionamento, aree di stoccaggio carburante, barche di lusso e petroliere).
La strumentazione in se non permetterebbe invece il riconoscimento facciale diretto da distanze considerevoli, come ci si aspetterebbe da una normale videocamera, che peraltro funzionerebbe solamente in condizioni di luminosità sufficiente.

Le videocamere termiche richiedono particolari livelli di formazione da parte degli operatori delle control room?
Tutte le termocamere FLIR sono caratterizzate da una facilità d'uso che ne rende l'utilizzo intuitivo e immediato. La formazione per l'operatore termografico è però di vitale importanza, poiché permette di rimanere costantemente aggiornati sui metodi di utilizzo delle termocamere, garantendo così il massimo risultato e riducendo tempi e costi di ispezione. L'Infrared Training Center di FLIR Systems ha pertanto creato un semplice ed intuitivo corso introduttivo online per l'utente che si avvicini per la prima volta al mondo delle termografia, disponibile al link http://support.flir.se/training/basic_it.
Una voce guida accompagna il visitatore in un percorso che lo porterà a conoscere le nozioni di base sulla termografia e sugli strumenti termografici, analizzando alcuni casi applicativi concreti. Ogni concetto è supportato da utili schemi e fotografie, che rendono di più facile comprensione i concetti illustrati. L'Infrared Training Center offre inoltre corsi in aula, sia per l'utente alle prime armi, sia per gli operatori più esperti. L'accesso al corso online è gratuito e non vincolato alla partecipazione ai corsi in aula.

A Expo 2015 l'immagine non sarà solo bellezza

contributo di Alessia Orlando

Expo 2015. Esposizione universale. Un viaggio sensoriale di gusti, profumi, suoni, esperienze, conoscenze per le vie dei continenti della terra, racchiusi in un unico spazio.
Esposizione, esporre, dal latino *ex-pònere* "porre fuori", ha in sé diverse accezioni come mostrare e mettere in evidenza, evocativi di una parola: "immagine". Ed è proprio "l'immagine" uno dei focus dell'Expo, sia essa racconto visivo di paradisi perduti, di biodiversità alimentari, di lavori esotici che come strumento di prevenzione e sicurezza.
Testimonianze dal pianeta e gestione ottimale devono equilibrarsi per la riuscita dell'evento. Expo e l'Italia passeranno agli annali, positivamente, solo se accanto al successo della manifestazione, funzioneranno anche gli ingranaggi che fanno muovere le lancette: l'organizzazione e la sicurezza, sinonimo di immagini e videosorveglianza. Perché se fondamentale rappresenta l'elemento "culturale, informativo e ludico" evidente all'occhio di tutti, non meno peso ha il controllo di una cabina di regia invisibile ma tangibile. Ecco perché l'Expo(sizione) rievoca "l'immagine", come chiave di lettura di un evento che dovrebbe fare convogliare, secondo gli osservatori, circa 20 milioni di visitatori tra il 1 maggio e il 31 ottobre. Un terzo della popolazione italiana.
È indubbio che questa istantanea planetaria dell'alimentazione mondiale, tra le sue sfaccettature, sia sinonimo di bellezza. E nel nostro secolo, "la bellezza", è immagine visiva. E proprio Canon, imaging sponsor di Expo 2015, ha creato un libro non da sfogliare ma da assaporare attraverso un racconto/percorso fatto di scatti "suggestionanti" ancor più che suggestivi. Firme note della fotografia descrivono con istantanee oniriche, pittoriche e anche selvagge, braccia che lavorano e cibi esotici che conquistano. L'amministratore delegato e presidente di Canon Italia, Enrico Deluchi, spiega come "i visitatori saranno guidati attraverso 9 tappe visuali che identificano i temi e le filiere alimentari - riso, cacao, caffè, frutta e legumi, spezie, cereali e tuberi, biomediterraneo, isole mare e cibo e zone aride - rappresentative di tutti i Paesi partecipanti". "Il nostro compito – afferma - sarà quello di consentire a queste immagini, realizzate da alcuni tra i più importanti fotografi al mondo, di esprimere tutta la loro forza e potenza grazie alle nostre tecniche di stampa". Ma Deluchi solleva anche un altro tema: l'immagine come volano per un miglioramento di quei paesi che, pur nella bellezza, vivono situazioni di profondo

Enrico Deluchi - presidente Canon Italia

disagio. “Da oltre 70 anni – sottolinea – la filosofia di Canon, racchiusa nella parola Kyosei, ci invita a contribuire al benessere della società e dell’ambiente”. In breve: vivere bene per il bene comune.
E il bene comune è anche il “prendersi cura”, mostrando più attenzione per gli aspetti meno poetici ma altrettanto fondamentali, come la sicurezza della città, dei cittadini e delle sue opere. Gli interrogativi sono tanti. Perché se da una parte gli “exposcettici” guardano al cantiere Expo/Milano con la “preoccupazione” che i lavori non si concluderanno in tempo, l’altro grande punto di domanda è: “Milano, la Lombardia e l’Italia sono pronte per il taglio del nastro?”.
Expo a vario titolo sfiora, tocca, coinvolge, sconvolge e travolge tutti. Venti milioni di visitatori significa migliaia di anime in più che vagheranno per le vie di Milano con delle necessità. Luoghi e mezzi per dormire, mangiare, divertirsi, spostarsi ma anche la sicurezza di essere tutelati in caso di eventi imprevisti, come un malore o uno scippo. Ma Expo non vede protagonista solo il “turista”, ma anche il semplice cittadino e il retailer. Il cittadino che pretende l’efficienza dei servizi e il Retail che oltre ai benefici per la sua attività, deve valutare gli eventuali furti e danni che potrebbe subire.
Accanto all’immagine di straordinario impatto mediatico-culturale, non si possono sottovalutare i rischi a esso correlati. Racchiudere in una città un giubileo pagano della dea terra, significa fare i conti con chi può vedere in Expo un punto nevralgico per colpire l’Occidente. Tavoli tecnici e tavole rotonde devono riunirsi perché tutto il mondo della sicurezza, pubblica e privata, risponda con forza e metodo. Che piaccia o no, l’Expo ci sarà.

Questo assioma crea la necessità di cooperazione a 360°. Qui ritorna Expo come immagine di sicurezza. *Ubi maior minor cessat*. E nello specifico il male maggiore è il pericolo dell’incolumità di tanti. Ecco perché anche il Retail ha l’obbligo di collaborare. Come? Migliorando le tecnologie di sicurezza per tutelare se stessi e gli altri.
La cronaca mondiale ci insegna quanto importante rappresenti la videosorveglianza privata, anche per il riconoscimento di autori di reati non solo predatori. Il caso parigino ne è una prova. Proprio il contributo delle telecamere del supermercato Kosher, in cui sono stati sequestrati 19 ostaggi dagli stragisti di Chiarlie Hebdo, è stato fondamentale per la cattura dei terroristi. In breve, anche il privato può fare la differenza per la sicurezza di tanti.
Per questo motivo sarebbe auspicabile creare una rete, un piano B, a livello istituzionale e privato, per costruire a priori uno scenario di ipotetico pericolo, trovando delle soluzioni ad hoc.
Come sottolinea, Gianna Detoni (?): “Nessuno può chiamarsi fuori: dobbiamo essere convinti dell’ineluttabilità di poter subire impatti anche significativi. Diventa urgente effettuare una valutazione del nostro livello di preparazione e pensare ad eventuali azioni per mitigare le minacce rilevate – aggiunge -. Occorre coinvolgere il Top Management della propria organizzazione, per ottenere risultati convincenti. Materiali quali la Corporate Security, la Business Continuity e il Crisis Management sono strategiche e pertinenti e offrono un valido supporto”. L’invito è chiaro: per gustare le portate del banchetto Expo, ogni ingrediente deve avere il giusto peso e ogni commensale deve sedersi nel posto assegnato.

Chi è pronto per Expo 2015 scagli la prima pietra

contributo di Gianna Detoni, presidente Associazione HI CARE

Sono diversi mesi che nei vari ambiti della sicurezza e della continuità operativa si discute del rischio Expo 2015. Non solo per Milano, ma per tutte le città d'arte o comunque per le mete turistiche italiane. La discussione non è banale perché se consideriamo che l'Expo 2010 di Shangai ha aggregato circa 60 milioni di visitatori, anche ipotizzando l'arrivo di una frazione di tale numero di viaggiatori (circa 7,5 milioni di biglietti già venduti a fine dicembre), le infrastrutture milanesi e italiane dovranno attrezzarsi a fronteggiare la gestione di una massa critica di persone davvero significativa. Alcune fonti stimano che almeno 20 milioni di persone visiteranno i padiglioni dell'Expo durante il periodo di sei mesi (dal 1° maggio al 31 ottobre). Sarebbe dunque ben giustificato l'entusiasmo per l'aspetto economico dell'evento, per i profitti che ne deriverebbero per settori come la moda, il turismo, l'alimentare e il made in Italy in generale. È una grande vetrina commerciale e come tale potrebbe aiutare a rilanciare la nostra economia. Tuttavia corriamo anche l'enorme rischio di mettere in luce le nostre inefficienze in materia di sicurezza e la pressoché totale mancanza di prevenzione nella gestione delle emergenze. Dobbiamo quindi fare in modo che tutto funzioni, nonostante lo scetticismo e la scarsa fiducia nelle capacità organizzative delle nostre Istituzioni. Una critica certamente non nuova, ma più che giustificata dagli innumerevoli precedenti e dalla portata di questa manifestazione che rischia di sconvolgere Milano e l'Italia.

Come si può evincere dal titolo, tuttavia, questo articolo nasce con l'intento di distogliere per un attimo il dito puntato contro gli organizzatori di Expo 2015 per rivolgere l'attenzione su quanto abbiamo fatto noi per la nostra organizzazione in vista dell'evento. Quanti tra noi hanno già fatto le opportune riflessioni sui probabili, o meglio certi, effetti di una manifestazione così imponente? Ecco alcune domande alle quali dovremmo provare a rispondere:

- Siamo pronti ad affrontare i problemi di traffico, di trasporto, le difficoltà nel reperire alberghi o di gestire il costo a volte triplicato degli stessi per i nostri visitatori?
- Se le nostre infrastrutture dovessero essere intasate (ospedali, metropolitane, treni, aerei, parcheggi e ristoranti) abbiamo pensato a come sopperire direttamente agli eventuali problemi creati al nostro Staff, agli stakeholder, alla nostra attività e alla nostra tecnologia?
- I fornitori che hanno un'influenza diretta sui nostri processi/servizi/prodotti critici, se ci devono raggiungere o se devono provvedere alla manutenzione della nostra continuità operativa si sono attrezzati? Glielo abbiamo chiesto?
- Abbiamo studiato strategie alternative per i potenziali incidenti?
- Siamo in grado di spostare alcuni processi critici fuori dal sito a rischio?Quanti di noi hanno effettuato una simulazione per la gestione delle nostre attività quando qualche milione di persone arriveranno a Milano
- portando culture e religioni diverse, parlando lingue diverse, e che potrebbero avere problemi di natura sanitaria, logistica o economica?
- Le nostre procedure di sicurezza fisica, già valide in periodi normali, sono adeguate rispetto alla criticità dell'evento?

- Abbiamo pensato alle nostre risorse critiche (oltre all'impatto sui processi) per tutelarle da eventuali conseguenze provocate dall'evento?
- Come saranno gestiti i soliti lavori straordinari che in genere nei mesi estivi rendono Milano un cantiere a cielo aperto? Saranno rinviati? Con quali conseguenze? Abbiamo pianificato interventi strutturali estivi nella nostra organizzazione?

Mentre sono tantissime le domande che ci poniamo e che vorremmo porre alle Istituzioni sulla loro preparazione a gestire i problemi della comunità (ad esempio la raccolta dei rifiuti, le telecomunicazioni, il fabbisogno energetico e il trasporto municipale/extra-municipale), dovremmo cominciare a preoccuparci in primis della nostra continuità. Nessuno può chiamarsi fuori da questo tipo di riflessioni: dobbiamo essere convinti dell'ineluttabilità di poter subire impatti anche significativi da un evento di questa portata, senza precedenti per durata e dimensione. Manca ormai pochissimo, quindi diventa urgente effettuare una valutazione del nostro livello di preparazione e pensare ad eventuali azioni per mitigare le minacce rilevate. Se queste riflessioni non sono state già fatte in precedenza, a maggior ragione occorre coinvolgere il Top Management della propria organizzazione - possibilmente in modo convincente - per ottenere risultati concreti in così poco tempo. Materie quali la Corporate Security, la Business Continuity e il Crisis Management sono assolutamente strategiche e pertinenti, visto il problema da affrontare, e offrono un valido supporto ai manager. Per non dover contare sempre e solo sulla capacità di reazione e sulla proverbiale "flessibilità" tutta italiana nell'affrontare problemi dopo l'accadimento. Dopotutto, una sana e opportuna prevenzione conviene anche economicamente.

Il Comune di Venezia sceglie Avigilon per la videosorveglianza

a cura della Redazione

Sfida

Una delle città più suggestive d'Italia si trovava nella necessità di installare una soluzione di videosorveglianza HD in grado di garantire la sicurezza ai residenti e ai turisti, proteggere gli edifici e i monumenti storici dagli atti vandalici e soddisfare i numerosi regolamenti in vigore in città.

- Mercato: Sorveglianza di aree pubbliche
- Location: Italia
- Partner: Venis S.r.l.

Prodotti utilizzati

- Software ACC
- Telecamera HD Pro da 8 e 16 MP
- Registratore video in rete
- Encoder video per segnali video analogici

Soluzione

Il personale del Comune di Venezia addetto alla sicurezza gestisce il sistema di videosorveglianza HD nel centro operativo di telecomunicazioni e videosorve-

glianza della polizia locale. Il centro occupa due sale e utilizza 12 monitor HD da 55 pollici installati a parete. Centri di controllo aggiuntivi sono ubicati presso un centro interforze in Piazza San Marco, presso il comando operativo provinciale dei Carabinieri di Venezia e presso il centro operativo della Polizia di Stato di Venezia. Il Comune di Venezia utilizza il software Avigilon Control Center (ACC) Enterprise con High Definition Stream Management (HDSM)™. Si tratta del sistema di registrazione centrale, ubicato presso il centro dati del Comune di Venezia, gestito da Venis, una società IT con sede in città.

Per proteggere tre importanti siti della città sono state installate telecamere HD Pro di Avigilon da 16 MP e 8 MP: Piazza Ferretto (la principale piazza di Mestre), Piazza San Marco e il Ponte di Rialto. Inoltre, tutti i feed video delle telecamere analogiche esistenti vengono convertiti in HD utilizzando gli encoder Avigilon. Il Comune utilizza inoltre i registratori video in rete (NVR, Network Video Recorder) di Avigilon per archiviare un minimo di sette giorni consecutivi di riprese di videosorveglianza. L'intera rete di videosorveglianza si basa su un'infrastruttura di fibra ottica MPLS (Multiprotocol Label Switching) costruita da Venis ma di proprietà del Comune di Venezia.

Vantaggi per il Comune di Venezia

- Protezione di residenti, turisti ed edifici storici
- Risparmio sui costi per il personale
- Relazioni migliori con le forze dell'ordine

Vantaggi della soluzione Avigilon

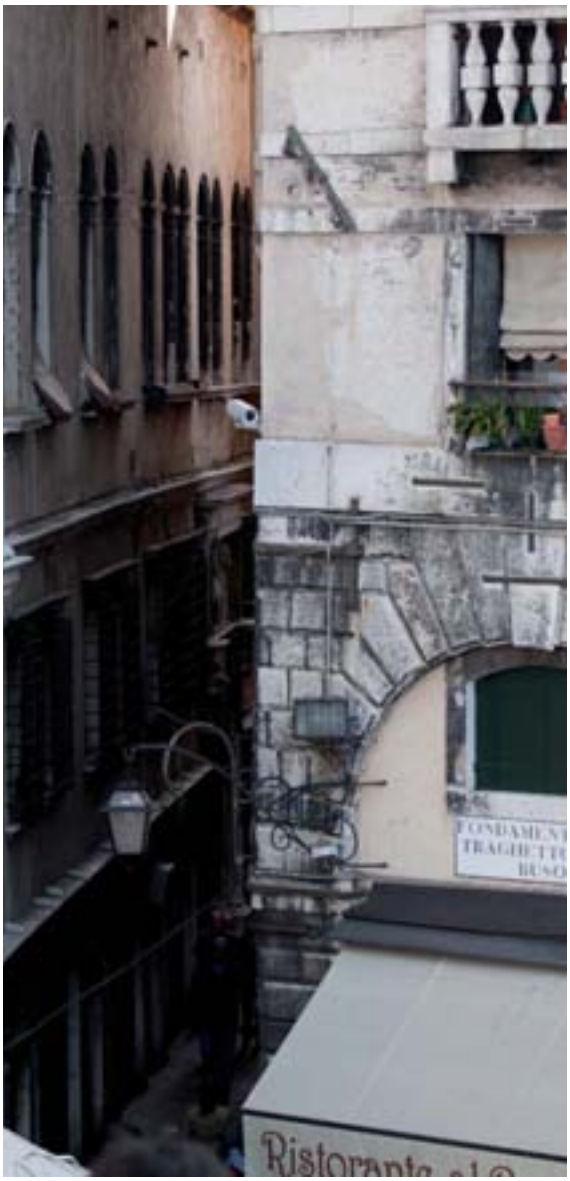
- Ricerche più rapide
- Prove inconfutabili per gli incidenti
- Alta qualità nei dettagli delle immagini

Il Comune di Venezia sceglie il sistema di videosorveglianza HD di Avigilon per proteggere i residenti, i turisti e il proprio patrimonio architettonico storico

Canali, ponti ed edifici mozzafiato fanno di Venezia una delle città più belle del mondo, come dimostrano gli oltre 50.000 turisti che la visitano ogni giorno. Adagiata lungo le coste dell'Italia nordorientale, la città sorge su 118 isolette separate da canali e unite da ponti. Il territorio del Comune di Venezia include isole e un tratto costieri, abbracciando due nuclei cittadini separati: Venezia, in laguna, e Mestre, sulla costa. A causa del paesaggio unico e del retaggio artistico di questa città, il controllo dell'area pone alcuni problemi logistici. In una città come Venezia non solo è importante assicurare la sicurezza dei residenti e dei turisti, ma è anche fondamentale proteggere i famosi edifici storici, famosi in tutto il mondo. In passato, i vandali hanno imbrattato il Ponte di Rialto con graffiti. Dopo essersi affidato per anni a un obsoleto sistema di videosorveglianza analogico, il Comune è passato a una soluzione video basata su IP a elevato tenore tecnologico, dotata di una piattaforma aperta. "Il sistema di videosorveglianza precedente, di proprietà comunale, era costituito da circa 60 videocamere analogiche a bassa risoluzione, molto difficili da analizzare", spiega Luciano Marini, comandante della Polizia Municipale di Venezia, che ha parlato anche dei problemi connessi al software e ai dispositivi di registrazione video in rete del sistema precedente. "Gli apparecchi di registrazione video si guastavano spesso, con perdita parziale dei feed e conseguente difficoltà a utilizzarli come prove". Consigliato da Venis, partner specializzato in sistemi di sicurezza, il Comune di Venezia ha scelto Avigilon per l'elevata qualità dei dettagli d'immagine offerta dalle telecamere Avigilon e per le efficienti funzionalità di archiviazione dell'intuitivo software ACC. Avigilon è stata scelta anche perché è l'unico produttore in grado di fornire telecamere ad alta risoluzione con un'ampia scelta di lenti. "Gli altri produttori non offrivano soluzioni comparabili in termini di risoluzione e neppure offrivano un'adeguata scelta di lenti per i diversi tipi di fotogramma", aggiunge il comandante Marini.

Qualità d'immagine di livello superiore

In Piazza San Marco, le due telecamere Avigilon da 16 MP sono state installate sul Campanile di San Marco, celate negli archi. Una telecamera fornisce una copertura della Piazza in direzione del Molo e l'altra è puntata verso l'Ala Napoleonica del Museo Correr. "Utilizzando telecamere ad alta risoluzione, come quelle da 16 MP, otteniamo immagini altamente dettagliate che possono essere visualizzate durante l'analisi delle registrazioni", spiega il comandante Marini, il quale aggiunge che la qualità delle immagini ha aiutato la polizia a risolvere alcuni casi. "Per ottenere gli stessi risultati, avremmo dovuto installare più telecamere sui monumenti vicini, con tutte le complicazioni del caso". In passato, il Comune era obbligato a sorvegliare le aree principali soggette a un traffico intenso o a vandalismi utilizzando più telecamere analogiche. "Con l'impiego di più telecamere era facile lasciarsi sfuggire fotogrammi importanti, sia



a causa del posizionamento sia a causa delle immagini sfocate", conclude Marini. "Le telecamere fisse ad alta risoluzione, invece, non pongono un simile.
"L'utilizzo di telecamere ad alta risoluzione, come quelle da 16 MP, ci consente di ottenere immagini estremamente dettagliate che è possibile visualizzare anche durante l'analisi delle registrazioni" afferma Luciano Marini, Comandante della Polizia Municipale di Venezia

Soluzione versatile e scalabile

Grazie alla piattaforma aperta del sistema HD di Avigilon, negli ultimi anni il Comune di Venezia ha potuto ampliare efficientemente la copertura di sorveglianza. Gli encoder di Avigilon hanno consentito agli agenti di affiancare le telecamere HD di Avigilon ai dispositivi analogici esistenti e oggi la gestione di tutte le telecamere risulta perfettamente integrata all'interno di un'unica piattaforma. Le funzionalità di ricerca avanzata del software Avigilon Control Center (ACC) hanno messo gli agenti in condizione di individuare gli eventi in tempi drasticamente inferiori rispetto a prima. "Troviamo il software ACC molto semplice da utilizzare. Grazie ad ACC le nostre ricerche sono molto più efficienti", ha dichiarato il comandante Marini che è rimasto inoltre molto colpito dalle funzionalità di zoom del software. "È straordinario poter visualizzare diverse parti della stessa immagine con livelli di zoom variabili e farlo in HD, continuando a registrare contemporaneamente il fotogramma intero".

Efficace strumento per la lotta alla criminalità

La possibilità di individuare i colpevoli di reati o atti vandalici è stato uno dei principali vantaggi derivanti dall'installazione del sistema HD di Avigilon. "In numerose occasioni il sistema di Avigilon si è rivelato un prezioso strumento di ricerca, anche per le indagini", ha commentato il comandante Marini. Le immagini ad alta risoluzione si sono rivelate utili per fornire prove inconfutabili alle forze di polizia locali. Oltre alle funzionalità tecniche, la soluzione HD di Avigilon ha offerto al personale del Comune di Venezia addetto alla sicurezza un ottimo rapporto tra prezzo e prestazioni. "I vantaggi si riscontrano quotidianamente", conclude il comandante Marini. "Ad esempio, per contrastare le attività commerciali non autorizzate in aree pubbliche, oggi possiamo impiegare un numero minore di agenti. In precedenza dovevamo verificare tutte le segnalazioni di commercio abusivo, mentre ora possiamo monitorare le aree interessate e compiere interventi mirati".
"In numerose occasioni il sistema di Avigilon si è rivelato un prezioso strumento di ricerca, anche per le indagini" conclude il Comandante della Polizia Municipale di Venezia.

CONTATTI

AVIGLION

www.avigilon.com

L'ecosistema Centrax

I fornitori complementari di Centrali di allarme intrusione e incendio e quelli di controllo accessi. Quarta parte

Le tre parti già pubblicate riguardavano la comunità degli utenti, quelle dei fornitori complementari di apparati e sistemi di videosorveglianza, e quelle dei dispositivi di teleallarme.

contributo di Bruno Fazzini, presidente CITEL SPA

Le centrali di allarme – intrusione e incendio

Nel trattarne l'integrazione, i sistemi di allarme sono stati suddivisi in tre aree:

- teleallarmi
- controllo perimetrale
- centrali di allarme – intrusione e incendio

(Le prime due aree sono state trattate in **essecome** 6/2014, le centrali in questo numero)

Note legali

Fatti salvi quelli di Citel e dei suoi prodotti, tutti i marchi citati nel seguito di questo documento sono utilizzati unicamente a scopo illustrativo per una fruibilità immediata da parte del lettore. Ciò detto, Citel dichiara espressamente di non avere su di essi nessuno dei diritti che appartengono esclusivamente ai legittimi proprietari.

Centrali di allarme intrusione e incendio

L'interesse del mercato e la richiesta

Premessa: le centrali antintrusione considerate sono quelle tipicamente connesse su reti LAN/WAN con protocolli bidirezionali che permettono una telegestione da Control Room orientata agli "eventi", non ai semplici "allarmi" per i quali si utilizzano invece i dispositivi trattati in precedenza come "teleallarmi".

L'interesse dell'utenza per la centralizzazione di impianti con centrali di allarme di produttori qualsiasi è quasi sempre il motivo dell'adozione di Centrax, soprattutto se si sente la necessità:

1. di gestire in maniera normalizzata e unificata **un certo numero di propri siti dotati di centrali anti-intrusione e antincendio, indipendentemente da marca, modello, epoca del loro acquisto**; è il caso tipico delle banche, del retail, ma anche di grandi imprese multi-sito;
2. di passare alla **gestione integrata e supervisionata di un impianto, singolo ma complesso e articolato**, con necessità di interazione tra apparati e sistemi di produttori diversi.

Nel **caso 1** l'esigenza è decisamente sentita da tempo ed è tipica di chi utilizza una Control Room interna di telegestione della sicurezza; meno sentita per chi è portato ad affidarsi su basi locali alle control room di società di security che forniscono anche il servizio di pronto intervento.

Nel **caso 2**, l'esigenza si è consolidata solo di recente; in passato il caso del supervisore unificato nel singolo edificio o non si poneva, lasciando separati i diversi sistemi, oppure l'integrazione avveniva nell'ambito della cosiddetta Building Automation in ambito rigorosamente chiuso mono-fornitore e ovviamente sbilanciato verso i tecnologici. Nell'ultimo decennio, però, quella chiusura protettiva, palesemente antistorica, ha portato – proprio nei grandi edifici e infrastrutture – alla crescita della domanda di una gestione separata della sicurezza fisica, con la richiesta di un PSIM basato sull'interoperabilità con accessi, video, safety ed emergenze a partire dalla centrale di allarme del sito, quasi sempre da preservare per non dover affrontare costosi rifacimenti dell'impiantistica antintrusione.

In entrambi i casi emerge comunque l'interesse dell'utenza ad ottenere l'integrazione con le centrali di allarme preesistenti per non rimettere mano agli impianti o per mantenere i fornitori abituali di prodotti e servizi: e questo spiega il numero elevato delle centrali di allarme, intrusione e incendio in fascia media e alta, che sono state integrate in Centrax.

La disponibilità e la collaborazione delle terze parti

Le centrali con protocollo proprietario integrate in Centrax sono tra le più diffuse nella fascia media e alta del mercato italiano. La disponibilità a fornire il protocollo è nettamente migliorata nel tempo grazie alla *moral suasion* esercitata dai grandi utenti di Centrax la cui massa critica ha dimostrato tutto il suo peso anche in questo settore, da sempre il più chiuso e protetto.

Le innovazioni introdotte con l'integrazione.

In una infrastruttura aziendale di sicurezza fisica la centrale di allarme è un elemento di condizionamento rilevante per il numero e l'importanza delle segnalazioni che gestisce, per i comandi che esegue e per i costi che implicherebbe una sua sostituzione. Pertanto l'alto numero di casi di integrazione multifornitore in ambito Centrax rappresenta – di per sé – l'origine di tutte le innovazioni di sistema o funzionali, essendo quella che ha fatto saltare l'assuefazione alle architetture chiuse a protezione dei *prodotti della casa* e la rassegnazione alle *non* scelte dei singoli moduli all'interno del sistema. È stato quello il passaggio chiave che ha portato al ripristino della competizione e della regola aurea dei sistemi aperti: la valorizzazione del pregi dei singoli moduli indipendentemente dal costruttore del sistema di supervisione, quindi la meritocrazia e l'innovazione nel suo corollario.

L'innovazione è consistita nella possibilità di trattare i segnali di singoli sensori in ingresso e di singoli attuatori in uscita senza essere costretti ad avere un unico costruttore sia per il centro che per la periferia. Una innovazione determinante per rendere accessibile il livello applicativo della gestione del singolo sensore riservato ai sistemi chiusi monomarca.

Il livello raggiunto dalle applicazioni

L'innovazione appena trattata porta alla possibilità di ottenere in un ambito aperto e multifornitore prestazioni avanzate di gestione da supervisore di solito riservate ai sistemi chiusi monomarca che prevedono la gestione per eventi trattando i segnali di ogni singolo sensore e l'azionamento di ogni singolo attuatore. Tale possibilità si può tradurre – tramite configurazione per eventi – in interventi appropriati,

tempestivi, efficienti, documentati, grazie alla possibilità di configurare processi di gestione con, ad esempio:

- la precisa rilevazione spaziale dell'evento e la possibilità di puntare strumenti di verifica associati, come la telecamera abbinata allo spazio di interesse
- la possibilità di correlare altri segnali per determinare con precisione il tipo di evento, la sua attendibilità, il suo decorso a fini di *situation management*, l'abbinamento alle procedure di intervento, la generazione automatico di un reporting accurato ottenendo quindi – su un piano più generale – di passare dalla semplice centralizzazione allarmi alla telegestione degli eventi senza rinunciare ai benefici dell'architettura aperta.

I sistemi di controllo accessi e varchi

Note legali

Fatti salvi quelli di Citel e dei suoi prodotti, tutti i marchi citati nel seguito di questo documento sono utilizzati unicamente a scopo illustrativo per una fruibilità immediata da parte del lettore. Ciò detto, Citel dichiara espressamente di non avere su di essi nessuno dei diritti che appartengono esclusivamente ai legittimi proprietari.

L'interesse del mercato e la richiesta

Nell'esperienza di Citel l'integrazione del Controllo Accessi in una sistemistica di supervisione multifunzionale è stata sporadica nel passato e semplicistica nella realizzazione, del tipo: un allarme di varco = un contatto per un ingresso su una centrale di allarme. Oppure due centralizzazioni distinte e separate con posti operatore specializzati nella control room del grande utente.

Negli anni recenti, però, la richiesta di integrazione è cresciuta sia per numero di casi che per livello di interoperabilità, e lo dimostrano il numero e il peso dei marchi nella figura, in larga parte integrati di recente in ambito Centrax.

E con l'integrazione cresce il livello qualitativo delle applicazioni, che vanno ormai ben oltre il consenso all'apertura di un varco, allargandosi a un ambito più generale della rilevazione del passaggio e della presenza. Grazie alle nuove tecniche di rilevazione di prossimità nelle sue varie forme, oggi si possono infatti rilevare, correlare e gestire anche il transito in genere e il tracciamento del passaggio lungo percorsi monitorati, aprendo alla telegestione nuovi campi di applicazione.

la disponibilità e la collaborazione delle terze parti
La collaborazione dei costruttori alla fine non è mai mancata, avendo tutti interesse a partecipare a progetti di integrazione, e si è tradotta in interoperabilità basata sempre su protocollo o SDK.

Le innovazioni introdotte con l'integrazione.
L'innovazione tecnico/impiantistica in ambiente multifornitore si è tradotta nel passaggio dalle connessioni con contatti on/off dei *controller* di varco del passato (e delle informazioni elementari che essi fornivano) all'interazione con la centrale di gestione eventi Novax o direttamente con il Centrax via LAN o bus seriale:

- con una struttura dell'impianto più compatta, protetta e tele-monitorabile
- con la disponibilità di un protocollo applicativo bidirezionale basato su un set completo di informazioni in entrata e di comandi in uscita oltre alla diagnostica centralizzata di funzionamento.

Le innovazioni funzionali hanno origine dalla possibilità di poter utilizzare tutto il set di segnali e comandi del protocollo del costruttore per poter effettuare una telegestione basata sulla percezione completa e tempestiva dell'evento e sull'attivazione delle misure congruenti.

In particolare sono stati raggiunti i massimi livelli funzionali nella gestione da supervisore anche grazie all'integrazione con la centrale di gestione eventi (Novax o altre marche con protocollo CEI 79/5-6):

- l'acquisizione via protocollo da parte della centrale di gestione eventi dei singoli allarmi di varco
- la correlazione tra segnalazioni via protocollo e input tradizionali ai fini della generazione di eventi corredati da una informativa completa
- la grafica di visualizzazione su posto operatore della posizione del varco e del contesto pertinente
- la possibilità di autorizzare da control room (o da dispositivi mobili) l'accesso al sito di lavoratori, manutentori e visitatori con profili di accesso personalizzati anche senza accompagnamento su percorsi obbligati
- la possibilità di una gestione centralizzata e unitaria anche in un contesto multi-sito con dotazioni eterogenee.

Il livello raggiunto dalle applicazioni – controllo accessi
Il livello applicativo raggiunto grazie alle suddette innovazioni ha toccato i massimi consentiti dallo stato dell'arte in applicazioni civili. A beneficiarne, nei casi di integrazione stretta con Centrax ai fini della telegestione sono state soprattutto l'efficienza dell'operatività, sia nel controllo accessi e varchi che nelle applicazioni di monitoraggio:

- riduzione dei costi di gestione dei servizi di accoglienza e presidio tramite automatismi locali e servizi centralizzati
- riduzione degli interventi inutili sul posto per false emergenze
- tele-interventi di manutenzione, ove possibile mediante riconfigurazione da remoto.

CONTATTI

CITEL SPA
(+39) 02 2550766
www.citel.it

Mirasys, il VMS che arriva dalla Finlandia

a colloquio con Elio Argenti, general manager Mirasys Italia
a cura di Raffaello Juvara

Nel segmento del VMS, snodo cruciale per la videosorveglianza, sono avvenute nel 2014 operazioni che hanno modificato gli equilibri consolidati del mercato a livello globale. Come si colloca in questo nuovo scenario l'outsider Mirasys, un'azienda finlandese che si era finora tenuta ai margini della contesa del primato tra i maggiori operatori?
Nel breve termine, non penso che ci saranno conseguenze stravolgenti; tutto continuerà ad essere gestito come prima, almeno all'inizio. Nel corso dell'anno si potranno comunque verificare situazioni che saranno diretta conseguenza delle operazioni avvenute nel 2014. Mantenendo la sua caratteristica di Sistema Aperto in ambito VMS, Mirasys avrà un'attenzione sempre più focalizzata sulle soluzioni anziché sui singoli prodotti. Questo significa avere maggiori possibilità di integrare o di integrarsi con altre soluzioni. Noi forniamo principalmente sistemi per applicazioni corporate multisito in progetti su larga scala, e disponiamo di un vasto ecosistema di partner: infatti collaboriamo direttamente con tutti i principali produttori di telecamere, di sistemi di analisi video e di controllo accessi, gli integratori di sistemi, ed i fornitori di servizi di sicurezza. Noi crediamo che la partnership con altre aziende sia il modo per fornire soluzioni che soddisfano qualsiasi specifica esigenza. Un movimento nei mercati creerà ulteriori opportunità commerciali, e le soluzioni Mirasys risponderanno in modo ottimale a queste nuove opportunità.

Qual è la storia dell'azienda e come è strutturata in Italia e nel mondo?
Mirasys è un'azienda finlandese con sede ad Helsinki. Fin dall'inizio, Mirasys ha sempre avuto il fine di essere un'azienda multinazionale. Ha iniziato le sue attività nel 1997 a Helsinki come azienda specializzata

nella sorveglianza in ambito bancario, dietro richiesta dell'Associazione Bancaria Finlandese, e si è evoluta da subito nell'ambito IP, intuendo la grandi potenzialità del mercato di questa tecnologia.
Mirasys ha uffici di vendita in oltre 40 paesi europei e nel mondo con oltre 50.000 clienti worldwide. Le videocamere attualmente connesse ai sistemi Mirasys sono circa un milione, e la società lavora con oltre 500 Partner e Distributori. Il software Mirasys supporta in modo nativo oltre 2200 modelli di telecamere IP delle maggiori case costruttrici, e praticamente tutte le telecamere analogiche.
Mirasys è presente in Italia dal 2010, sia con la vendita che con il supporto. Io credo che la presenza locale del supporto sia fondamentale, soprattutto per installazioni di una certa dimensione. La struttura italiana permette quindi un interfacciamento tra l'utenza locale e le strutture di Mirasys in Finlandia in caso di esigenze sia di natura commerciale che tecnica.

Quali sono i prodotti e le applicazioni di punta di Mirasys?

Mirasys ha due prodotti di base che sono VMS Pro, per medie installazioni, e VMS Enterprise per soluzioni Corporate, in modo da soddisfare al massimo livello le esigenze dei clienti. Il prodotto Enterprise è inoltre la base per passare da prodotto a soluzione. Infatti, utilizzando il sistema VMS Enterprise come base, è possibile integrare soluzioni di VCA (analisi video), AVM (video wall), ANPR+ (lettura targhe), FailOver ed altre funzionalità come Reporting e Server Expansion. Il software Mirasys è quindi, come detto in precedenza, pronto sia per essere utilizzato come singolo prodotto, sia per essere utilizzato in ambito di soluzioni complete. Spesso, durante la vita di un sistema di sorveglianza, ogni azienda deve affrontare diversi cambiamenti operativi riguardanti l'ambito della sicurezza, come l'utilizzo di outsourcing, l'aumento delle proprie sedi, l'integrazione con sistemi di sicurezza, o la necessità di centralizzazione. Quindi, in caso di modifiche operative, una buona soluzione iniziale fa la differenza tra l'acquisto di un nuovo sistema e l'ampliamento di uno già esistente. Scegliere Mirasys significa quindi guadagnare il diritto di scegliere, senza avere restrizioni nella futura evoluzione di un sistema.

Mirasys VMS Enterprise è la soluzione perfetta per le aziende e centri di sicurezza di qualsiasi dimensione. Estremamente flessibile e personalizzabile, può adattarsi a qualsiasi soluzione di sorveglianza. In aggiunta alla sua estrema adattabilità, la filosofia progettuale alla base di VMS Enterprise è sempre stata la facilità d'uso, rendendolo un sistema intuitivo, veloce da implementare e da utilizzare. Inoltre, l'estrema scalabilità di Mirasys VMS Enterprise permette di gestire centinaia di utenti, così come di server VMS. La forza della soluzione Mirasys è nella sua aperta modularità. Ciascun server può agire in modo indipendente, o come parte di una rete di server controllata da un server principale - o entrambi contemporaneamente. Tutte le nostre soluzioni sono intrinsecamente modulari.

Quali sono i vostri partner di canale e le strategie di distribuzione?

In Italia, Mirasys non utilizza i classici canali di distribuzione, come in passato ma si è in seguito preferito utilizzare un'altra strada. Il prodotto è distribuito attraverso nostri Partner o OEM: sono in pratica System Integrator ad alto valore aggiunto che hanno la possibilità di vendere sia i prodotti Mirasys che il loro prodotto OEM.

Questa impostazione ha permesso a molti System Integrator di essere indipendenti sul prodotto e di acquistare usufruendo delle stesse condizioni di un normale distributore; ma ha altresì permesso ad altri System Integrator di installare soluzioni di VCA e di lettura targhe, sulle quali non avevano una conoscenza approfondita, utilizzando un grosso supporto da questi nostri partner, in modo da presentare al cliente finale una soluzione installata che funzionava correttamente da subito.

Nel resto del mondo, Mirasys opera a livello globale attraverso filiali commerciali e agenti, in collaborazione

con i principali distributori, integratori di sistemi, fornitori di servizi di sicurezza e produttori di sistemi.

Ci parli dei vostri programmi per il futuro, sia nel mercato italiano che in quello globale.

Per quanto riguarda il mercato italiano, per la particolarità del prodotto Mirasys è orientata da tempo ad identificare System Integrator che adottino e propongano soluzioni Enterprise ai loro clienti, in modo da utilizzare il prodotto nella sua interezza. Certo, si possono proporre anche soluzioni molto semplici, ma in questa fascia ci si scontra normalmente con il prezzo che hanno quasi tutti i competitor.

Per quanto riguarda il mercato globale, ritengo che non esista una unica strategia. I distributori classici, che in Italia non sono utilizzati, in altre parti d'Europa funzionano. Quindi, come si vede, ci sono delle regole di base, ma effettivamente ogni Country applica quello che il mercato richiede.

Mirasys è in rapida crescita nel Regno Unito e Stati Uniti, che sono tra i mercati di sicurezza più grandi al mondo. In Finlandia, Mirasys è il leader di mercato. Il nostro obiettivo è quello di aumentare le quote di mercato anche nei principali paesi europei, tra cui l'Italia. In Asia, in questo momento Mirasys è focalizzata a crescere in Thailandia e India, e le opportunità offerte dal mercato asiatico rimarranno a fuoco per Mirasys nei prossimi anni.

Dal suo punto di osservazione e alla luce della sua esperienza pluriennale nel settore, come evolverà il mercato delle videosorveglianza in generale e del VMS in particolare?

Dal mio personale punto di vista ci sono due strade percorribili: la prima è quella che, tra un po' di tempo, altri brand seguiranno la strada intrapresa da Canon; quindi acquisizioni di aziende con un consolidato prodotto software da abbinare agli altrettanto validi prodotti HW di campo (intesi come telecamere).

L'altra strada è quella di continuare a crescere autonomamente ed a sviluppare funzionalità sul prodotto software in modo da incontrare le sempre più esigenti richieste del mercato; ad esempio, Mirasys VMS ha da offrire sempre più possibilità di integrazioni, non solo per il controllo accessi tradizionale, gli allarmi antincendio e sistemi POS, ma anche agli innovativi sistemi che si stanno sviluppando solo ora.

CONTATTI

MIRASYS
(+39) 02 36723101
www.mirasys.com

La visione artificiale per edifici che vedono

contributo di Gabriel Sikorjak, European Product Marketing Manager Omron Electronic Components

Le opportunità di acquisire immagini legate alla più recente elettronica di consumo potranno rivoluzionare la building automation, grazie anche alla completa integrazione con i sistemi di sicurezza.

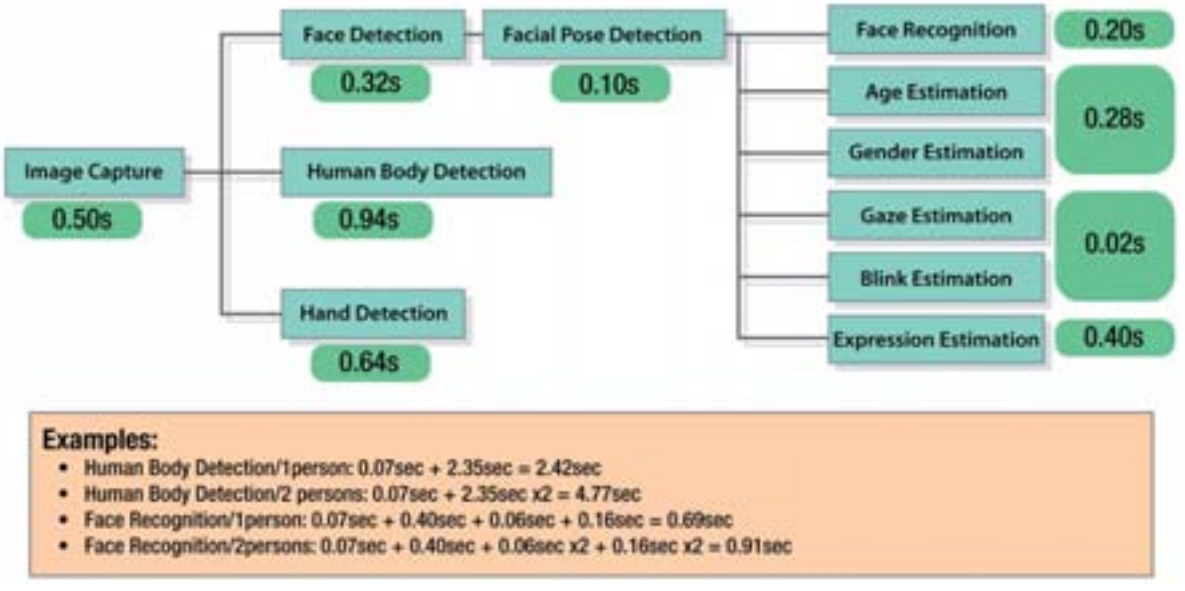
La visione artificiale si è ormai pienamente affermata nelle interfacce utente dei prodotti dell'elettronica di consumo. Ad esempio, alcuni telefoni sono in grado di riconoscere il legittimo proprietario e reagire di conseguenza, mentre varie console per videogiochi e vari televisori rispondono ai comandi gestuali, eliminando la necessità del telecomando e semplificando così l'accesso alle loro funzioni sempre più sofisticate.

In questo contesto, può apparire strano che le funzionalità basate sulla visione non si siano ancora affermate nei sistemi di automazione d'edificio. Molti edifici sono dotati di sistemi di TV a circuito chiuso, che però si limitano a trasmettere le immagini; l'interpretazione delle stesse è affidata all'operatore umano, che solitamente è responsabile solo della sorveglianza. Può accadere quindi che il rivelatore passivo a infrarossi (passive infra-red, PIR) spenga luci nel corso di una riunione, anche se la telecamera di videosorveglianza collocata nella stessa sala vede chiaramente le persone che la occupano.

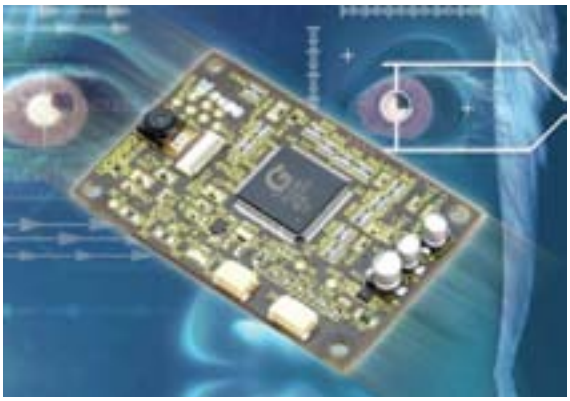
Le potenzialità nella building automation

I sistemi di automazione di edificio hanno requisiti applicativi molto più severi rispetto ai telefoni cellulari e alle console di videogioco, aziende innovative stanno tuttavia sviluppando tecnologie nate originariamente per prodotti consumer allo scopo di realizzare soluzioni adatte ad applicazioni professionali.

Utilizzando tali tecnologie, i sistemi di automazione degli edifici sono in grado di interpretare le immagini raccolte dalle telecamere. Possono, ad esempio,



Tempi di risposta per diverse funzioni di riconoscimento delle immagini



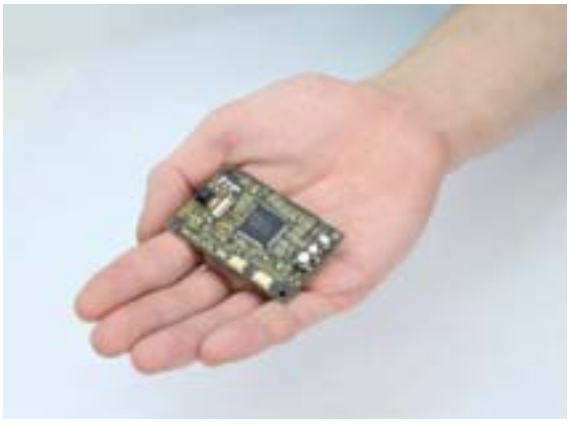
distinguere un essere umano da un gatto; rilevare gesti e reagire ad essi; valutare stati d'animo, età e genere delle persone, e perfino riconoscere uno specifico individuo. In prospettiva, i sistemi di sicurezza anticrimine e di building automation potrebbero essere integrati tra loro e sfruttare gli stessi moduli di visione. I dati raccolti potrebbero comandare reazioni automatiche, essere salvati o aggregati centralmente e inviati all'operatore solo quando necessario. Potenzialmente, negli uffici diverrebbe possibile riconoscere una persona al suo arrivo e regolare il riscaldamento e l'illuminazione secondo le sue preferenze. Nei sistemi di illuminazione di prossima generazione, inoltre, la regolazione di luce, aria condizionata e riscaldamento potrà essere comandata anche tramite gesti. Il prodotto HVC di Omron è il primo modulo di visione specificamente rivolto ad applicazioni quali l'automazione di edifici, disponibile anche in piccole quantità e immediatamente integrabile da qualunque progettista - senza alcuna necessità di comprendere i complessi algoritmi necessari per riconoscere gesti, facce ed espressioni, né il progetto ottico. Il modulo costituisce una soluzione plug-in totalmente integrata; lo sviluppatore può limitarsi a osservare i dati forniti in uscita e a configurare il sistema per prendere le decisioni appropriate in funzione del loro stato.

L'integrazione con le funzioni di sicurezza

Potendo rilevare in modo affidabile presenza, ubicazione e identità degli occupanti di una stanza, un modulo come HVC potrà in prospettiva consentire una completa integrazione tra i sistemi di controllo degli accessi e i sistemi che comandano gli impianti dell'edificio, esaltando le funzionalità di entrambi. Ad esempio, il modulo può identificare le persone per consentire o negare l'accesso; e può allertare il personale di sorveglianza se si rileva la presenza di persone non autorizzate in determinate aree, memorizzando fotografie provviste di una marca temporale. Il sistema può anche verificare se un ospite presente in una sala riunioni sia stato autorizzato ad entrare, oppure contare il numero dei visitatori nelle aree pubbliche. Senza dubbio, l'introduzione di sistemi di visione aggiungerà una nuova dimensione alla gestione degli immobili commerciali.

Il core-software del sistema

Moduli di questo tipo fanno affidamento su tecnologie consumer. In particolare, HVC è basato sul software di visione OKAO di Omron, un insieme di collaudatissimi algoritmi di riconoscimento delle immagini impiegati in oltre 500 milioni di fotocamere digitali, telefoni cellulari e robot di sorveglianza in tutto il mondo. Grazie a questo software, il modulo integra dieci funzioni chiave di rilevamento delle immagini, oltre a una telecamera e un'interfaccia esterna. Gli sviluppatori possono utilizzarlo per rilevare un viso, una mano o l'intero corpo umano e per implementare funzioni riguardanti il soggetto: riconoscimento facciale, rilevamento del genere, stime relative all'età e all'umore, l'espressione facciale, la direzione e gli atteggiamenti dello sguardo. Per tutti questi parametri il modulo fornisce un valore corredato da una valutazione di attendibilità, permettendo così al programmatore di configurare la reazione appropriata per ogni singola applicazione.
Tra le doti principali del modulo sono comprese la rapidità e ripetibilità delle risposte e la notevole distanza di rilevamento. Ad esempio, HVC è in grado di acquisire, rilevare e riconoscere un viso a una distanza di 1,3 m in 1,1 secondi, fornendo insieme alla lettura una stima del relativo livello di attendibilità. Il rilevamento delle caratteristiche legate allo sguardo richiede meno di un secondo.



Le dieci funzioni di riconoscimento delle immagini offerte dal modulo HVC di Omron

Il modulo, inoltre, è in grado di valutare l'umore del soggetto riconoscendo un'espressione facciale nell'ambito di un repertorio di cinque espressioni diverse. Può anche rilevare un corpo umano distante fino a 2,8 metri e una mano a un metro e mezzo di distanza. HVC implementa il software OKAO su una piattaforma hardware completa di telecamera, processore e interfaccia dati specificamente ottimizzata per questa applicazione, in termini di progetto digitale e ottico. Gli algoritmi necessari per implementare queste funzioni sono complessi e pesano molto sul processore, ma sono gestiti interamente all'interno del modulo. Pertanto i relativi calcoli, sebbene onerosi per la memoria e il processore, non impattano in alcun modo sul sistema host. Il modulo inoltre libera lo sviluppatore di sistema dalla necessità di dedicare tempo alla creazione e al test degli algoritmi, un compito complesso che richiede molto tempo.

Edifici speciali

La visione artificiale offre grandi potenzialità applicative nei sistemi di controllo e di sicurezza degli edifici, soprattutto in quelli destinati ad usi particolari. Nelle scuole, ad esempio, i moduli di visione possono distinguere un bambino da un adulto, oppure un dipendente scolastico da un estraneo, fornendo eventualmente opportuni allarmi. Negli ospedali i moduli possono riconoscere i singoli pazienti e perfino rilevare il loro umore, migliorando ampiamente la gestione sanitaria. Negli stabilimenti industriali il sistema può monitorare i visitatori segnalando quando si allontanano dai percorsi pedonali sicuri. Riconoscimento facciale e comandi gestuali sono da tempo disponibili in grandi volumi per l'elettronica di consumo. Soltanto oggi, però, si inizia a prendere coscienza delle potenzialità rivoluzionarie di queste funzioni nei sistemi di building automation.

ITEM	FUNCTION									
	FACE DETECTION	FACE RECOGNITION	GENDER ESTIMATION	AGE ESTIMATION	EXPRESSION ESTIMATION	FACIAL POSE ESTIMATION	GAZE ESTIMATION	BLINK ESTIMATION	HUMAN BODY DETECTION	HAND DETECTION
Horizontal Detection Area (Angle of view)	49deg									
Vertical Detection Area (Angle of View)	37deg									
Detection Distance (Reference)	1.3m	1.3m	1.3m	1.3m	1.3m	1.3m	1.3m	1.3m	2.8m	1.5m
Result output to system	Number Detected, Coordinates (X, Y), Size (pixels), Confidence	User ID, Score	Gender, Confidence	Age, Confidence	One of the 5 Expressions ("Neutral" "Happiness" "Surprise" "Anger" "Sadness") and Score, Positive or Negative Rate	Angle (horiz),, Angle (vert), Angle (roll), Confidence	Angle (horiz), Angle (vert)	Blink degree (Left eye, Right eye)	Number Detected, Coordinates (X, Y), Size (pixels), Confidence	Number Detected, Coordinates (X, Y), Size (pixels), Confidence

Security for Retail

Security for Retail Forum 2015, l'inizio di un percorso

Secondo il **Rapporto Intersettoriale sulla Criminalità Predatoria** prodotto annualmente da ABI/OSSIF, le rapine denunciate a danno degli esercizi commerciali censiti - tabaccherie, farmacie e distribuzione assieme a banche e uffici PT – hanno causato perdite per un totale di circa 30 milioni di euro nel 2013 e altrettanto i furti, compresi gli attacchi agli ATM, da tempo uno dei bersagli preferiti dalla delinquenza predatoria.

60 milioni di euro quindi il bottino complessivo dei reati predatori contro il sistema distributivo e le banche, che coinvolgono forze dell'ordine e magistratura, provocano allarme sociale e, quando serve in periodi elettorali, attirano anche l'attenzione della politica.

Passano invece nell'indifferenza totale gli oltre 2,5 miliardi che ogni anno vengono rubati in Italia dai clienti, dai dipendenti e dai fornitori del retail, pari al 75% del totale delle differenze inventariali registrate dalla rete nell'ultimo anno (3,1 miliardi). Secondo il Barometro dei Furti nel Retail, **ogni consumatore italiano si trova nel conto della spesa 94 euro in più** per la merce sottratta dai banchi dei supermercati e dei negozi di abbigliamento, elettronica eccetera. Una "disattenzione" dovuta in parte al fatto che la grande maggioranza dei furti in negozio non viene denunciata, fondamentalmente per due motivi: i singoli episodi sono in media di importo unitario inferiore ai costi diretti e indiretti che il gestore deve sostenere per la denuncia stessa; le norme italiane sulla privacy non consentono di utilizzare pienamente le tecnologie disponibili, anche nei confronti dei dipendenti infedeli. Si pensi, ad esempio, al limite di 24 ore per la conservazione delle immagini dei sistemi di videosorveglianza, che riduce sensibilmente la loro utilità; oppure agli impedimenti al controllo a distanza dei lavoratori, ai quali il Barometro attribuisce il 22% degli ammanchi, oltre 500 milioni all'anno.

La prevenzione attraverso sistemi, servizi e procedure è dunque l'unica difesa per il mondo del retail, diventato per legittima difesa uno dei principali mercati verticali dell'industria della sicurezza.

Security for Retail Forum 2015 è alla prima edizione organizzata in forma di seminario a inviti riservato agli operatori del settore, che si aggiunge ai talkshow aperti al pubblico in occasione delle fiere settoriali (Sicurezza Milano, CPEXPO Genova, Security Expo Roma, Medity Expò Capua).

Da questi incontri è stato sviluppato il modello di follow-up continuo, con la pubblicazione di analisi, approfondimenti e notizie provenienti da tutto il mondo nelle sezioni tematiche dedicate di **essecome** e **securindex.com**

Il Forum 2015 ha un'agenda intensa di tavole rotonde, relazioni e workshop, il cui scopo è di mettere a fuoco i problemi e cercare le risposte, per lasciare ai partecipanti delle informazioni utili per la loro attività "dietro al banco", reale o virtuale che sia. Tutti i lavori ruotano attorno a un tema: **l'evoluzione della gestione della sicurezza nel mondo della distribuzione per ridurre l'impatto delle differenze inventariali.** I prossimi appuntamenti saranno **Security for Retail Expo** a **Sicurezza 2015** e **Security for Retail Forum 2016.**

GLI EVENTI DI ESSECOME

SECURITY FOR RETAIL FORUM 2015

2 marzo 2015 - Milano, Palazzo delle Stelline

Seminario a inviti, riservato ai manager (Security, HR, IT) del Retail e della Grande Distribuzione e ai gestori dei negozi. Un appuntamento imperdibile, per affrontare con i più qualificati esperti i temi di maggiore attualità per il settore economico più esposto agli attacchi predatori:

- Andamento della criminalità predatoria nei confronti della grande distribuzione, retailer, negozi di prossimità a rischio (tabaccherie, farmacie, stazioni di servizio)
- Il 22% delle differenze inventariali in Italia è causato da infedeltà dei dipendenti: come poter utilizzare le tecnologie nel rispetto della privacy. Le innovazioni introdotte dal Jobs Act
- Come sta cambiando la figura del security manager nel mondo del retail
- Videosorveglianza, business intelligence, gestione inventari: verso un'integrazione sempre più efficiente per ogni tipologia di negozio
- Cash-management nei punti vendita: soluzioni convenienti anche per i piccoli esercizi

L'evoluzione del security manager nella distribuzione – 1

a colloquio con Armando Garosci, giornalista di Largo Consumo, rivista leader in Italia nell'analisi del retail e dei mercati dei beni di consumo
a cura di Raffaello Juvara

La figura del security manager nelle grandi aziende di commercio al dettaglio sta evolvendo a livello globale, in parallelo con l'evoluzione della stessa concezione di security nel sistema. Dal punto di osservazione di Largo Consumo, quali sono le parole chiave che stanno guidando questo processo?
In realtà, il ruolo del security manager è, allo stesso tempo, una risorsa strategica e operativa per la moderna distribuzione: è preposto a garantire la sicurezza globale attraverso la conoscenza di procedure, di sistemi, di tecnologie e di persone. A tutti gli effetti, egli è il responsabile aziendale per la sicurezza patrimoniale e si occupa di tutte le attività orientate alla prevenzione e per contrastare l'insorgenza di perdite legate a furti, frodi o truffe. Il security manager va considerato come un vero e proprio analista di *intelligence* in grado di interfacciarsi con i vari livelli dell'organigramma aziendale e di contribuire, in virtù delle proprie competenze particolari, ad assicurare e tutelare gli obiettivi di business.

In questo scenario, tra le diverse categorie di retailer (luxury, fashion, food, electronics, ecc.) e le catene di grande distribuzione, ci sono differenze sostanziali o l'evoluzione sta procedendo in modo trasversale e uniforme?
La minaccia alla proprietà è comune a tutti retailer, food e non food. Naturalmente differenti shopping

experience richiedono soluzioni coerenti con l'ambiente e comportamenti adeguati da parte del personale di sorveglianza e degli addetti vendita.
In generale, il libero accesso al prodotto nudo favorisce l'acquisto, la sua segregazione lo limita. Direi che i settori dell'elettronica e dell'abbigliamento hanno tuttavia trovato soluzioni adeguate a proteggere i prodotti senza comprometterne l'accesso. Nel grocery mi sembra invece che permangano criticità su alcune categorie, come le lamette o lo zafferano, che finiscono per trovarsi vicine alla cassa e sorvegliate, oppure si ricorre a display che limita-

no l'erogazione. Altre merceologie come i formaggi duri, o gli alcolici sono a rischio. Non mancano tuttavia le soluzioni tecnologiche per proteggerle, meglio se direttamente alla fonte. Le etichette RFID sono uno strumento efficace, e che ha affrontato e oggi superato le potenziali interferenze con certi pack o con i liquidi.
Le differenze inventariali rappresentano una minaccia di tipo multidimensionale per gli operatori retail di tutto il mondo, in quanto i fenomeni di taccheggio, i furti dei dipendenti e le attività della criminalità organizzata sono in costante aumento.
Queste problematiche particolari, unite alla crisi dei consumi ha reso la prevenzione delle perdite una priorità all'interno dei programmi dei retailer stessi, i quali si mostrano sempre più inclini a investire in metodi efficaci e a collaborare con gli specialisti per fronteggiare questa seria criticità per il business d'insegna. Gli operatori retail più lungimiranti sono impegnati a implementare soluzioni basate sulla tecnologia RFID, in grado di abbinare protezione e visibilità del singolo prodotto presso il punto di vendita. Di conseguenza, è più che legittimo attendersi che questa soluzione contribuirà a ridurre i casi di disassortimento, ampliare il livello delle vendite e migliorare la disponibilità stessa della merce a vantaggio dei clienti che accedono presso la superficie di vendita. In sostanza, è nella combinazione di metodi diversi che risiede la prevenzione delle perdite generalmente considerata come più efficace.

Ritiene che le competenze dei security manager attuali siano in linea con le esigenze dei grandi gruppi? Quali ulteriori capabilities vengono richieste oggi e quali, secondo lei, potrebbero venire maggiormente richieste in futuro?
In uno scenario sempre più complesso e articolato, il security manager deve costantemente tenersi aggiornato in modo da stare sempre al passo con i tempi, cercando di cogliere le nuove sfide imposte anche dal dinamico mondo del retail. Si tratta di una figura professionale che dovrà sempre di più consolidare le proprie capacità professionali in un'ottica di tipo manageriale e profondamente orientata all'innalzamento dei livelli di performance.
Di grande importanza è anche il ruolo della formazione rivolta al personale e coordinata dal security manager al fine di prevenire i furti: dipendenti motivati e appositamente qualificati possano essere messi in grado di individuare e di scoraggiare i fenomeni di taccheggio, effettuare controlli rigorosi al momento della consegna della merci da parte dei fornitori, seguire le procedure d'inventario e di prezzo.
Al security manager, è richiesto di avere una buona conoscenza dei processi aziendali, per individuare possibili punti deboli del sistema, perché i furti non avvengono solo in negozio, ma anche nei depositi e negli uffici.
Deve avere una buona conoscenza dell'evoluzione tecnologica, perché oggi la tecnologia rappresenta una parte significativa della minaccia. Ricordiamoci che anche i criminali si tengono al passo con i tempi e su Internet possono trovare utili ai ropri scopi. Inoltre, deve saper osservare la realtà, particolarmente quella locale, per interpretare le potenziali minacce.

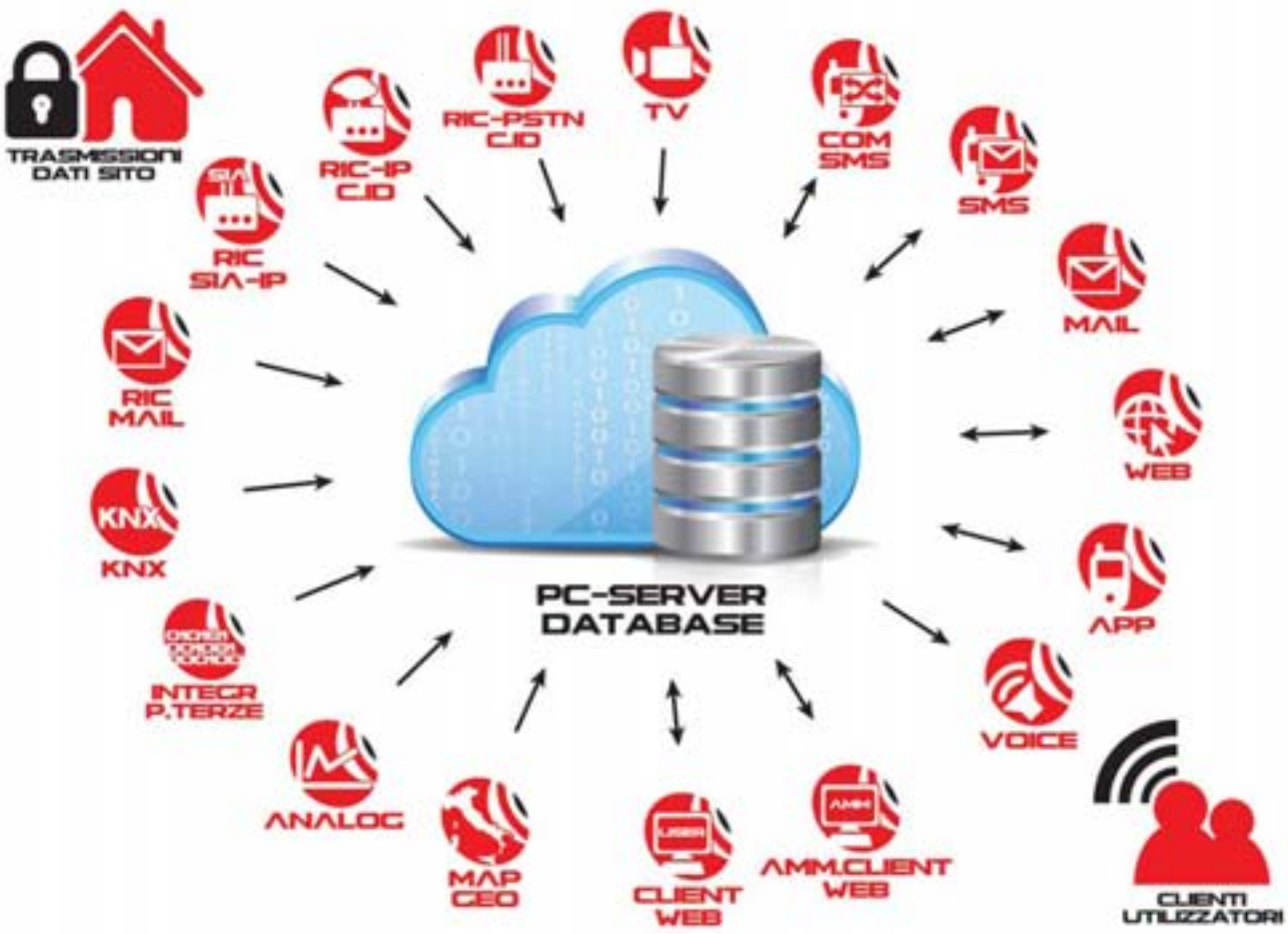
SICUREZZA E TELECONTROLLO SEMPRE IN TASCA

POINT SECURITY SERVICE

La piattaforma di supervisione Point Security Service (P.S.S.) è stato ideato e progettato in base alle reali esigenze degli operatori nel settore dei sistemi di sicurezza intrusione, rilevazione incendio, controllo accessi, tvcc e tecnologico. Point Security Service, così denominato, potrà, nella Sua flessibilità e potenzialità di elaborazione dati, portare questa piattaforma ad essere utilizzata per vari processi di manutenzione e post vendita evoluti.

Il software P.S.S è evoluto verso il mondo dei sistemi building automation per gestire una concreta e ideale area di lavoro e di processo di diversi protocolli, oggi usati in questo settore, come Konex, Profibas e protocolli PLC. Quindi, generando nel settore una nuova opportunità di crescita e sviluppo delle Aziende installative e grosse industrie legate al mondo della Security e Safety e della grossa distribuzione. Altro settore sviluppato a livello software e, con particolare attenzione dagli Operatori, è l'area Saving Energy, dove Skylab e i suoi informatici si sono concentrati per dare al massimo i risultati legati a questo software.

Sono state utilizzate competente e esperienze ad alti livelli di operatori del settore che hanno fatto crescere un focus group in scala nazionale dove finalmente possono usufruire di questo strumento per personalizzare i propri impianti, centralizzare le proprie tecnologie, utilizzando un modello di lavorazione intraprendente giovane e dinamica.



SKYLAB SOFTWARE - Via dell'economia 3, 31033 Castelfranco Veneto (TV)
Tel. 0302039010 - mail: info@pointsecurity.it - www.pointsecurity.it

L'evoluzione del security manager nella distribuzione – 2

contributo di Giuseppe Mastromattei, Head of Security Department H & M

La security aziendale evolve di pari passo con il sempre più veloce cambiamento ed innovamento tecnologico, e con esso cambiano le minacce e i rischi connessi.
Si rende pertanto necessario rivederne i contenuti lasciando definitivamente alle spalle il tipico approccio reattivo: ho un problema, lo risolvo adottando questa determinata soluzione o implementando una nuova attività che sia di supporto a una risposta efficace alla nuova minaccia.
La sicurezza, oggi deve essere un chiaro processo, condiviso e partecipato, affinché possa diventare uno strumento di *governance* efficace allo sviluppo, prima, e alla protezione, dopo, del business.
Si deve pertanto iniziare a parlare di "Sicurezza Partecipata"; ma prima è forse necessario analizzare in dettaglio quello che spesso, all'interno delle organizzazioni, viene troppe volte dato per scontato o peggio ancora, ignorato, ovvero, il "Sistema Sicurezza"
Il Sistema sicurezza è semplicemente un delicato compromesso tra elemento umano, interazioni sociali e supporto puramente tecnologico.
Come queste tre componenti interagiscano tra di loro è praticamente impossibile definirlo in maniera univoca, ma per poter rendere efficace tale definizione potrebbe risultare più semplice un'analisi fatta partendo dal "fallimento del sistema sicurezza".
Immaginiamo di avere un cruscotto su cui sono posizionate tre leve che rappresentano rispettivamente la componente umana, sociale e tecnologica ed utilizzare questo strumento per definire un piano operativo di sicurezza.

Partiamo dall'ultima delle tre: la **componente puramente tecnologica.** In questo caso il Security Manager analizza le offerte presenti sul mercato e, grazie alla tecnologia sempre più "user friendly" (è sufficiente accennare a quante possibilità oggi esistano utilizzando uno smartphone o meglio an-

cora un semplice tablet di ultima generazione) inizia a fare voli pindarici su soluzioni assolutamente idonee alla risoluzione dei problemi. La soluzione tecnologica scelta, spesso ha due fattori di insuccesso determinanti: Il prodotto non si dimostra all'altezza per svariati motivi, troppo complesso o troppo semplice e quindi inefficace ed inapplicabile, o peggio ancora, il fallimento si compie a causa di un coinvolgimento troppo ampio e fuori dalla portata gestionale dell'organizzazione. È il caso in cui la scelta ricade su di un applicativo che necessita di continue implementazioni e risorse dedicate: Il passo fatto è più lungo della gamba.
La perdita di credibilità che ne deriva, ma soprattutto la perdita economica derivante da tale investimento, connessa al non raggiungimento dell'obiettivo, rappresenta il più comune dei casi di fallimento del sistema sicurezza derivante dalla componente tecnologica.

Componente sociale. Qui è ancora più semplice, basti pensare all'onda emotiva successiva al disastro dell'11 settembre.
Ogni momento storico rappresenta un'opportunità di mandato per il responsabile della sicurezza (security manager), se questi è costantemente attento a quello che succede intorno al proprio modello di business. Il fallimento è però sempre dietro l'angolo e l'insuccesso del sistema sicurezza progettato in prevalenza sulla base della componente sociale male interpretata ha di solito un ottimo effetto iniziale ma risulta essere destinato a finire, o meglio a collassare, in tempi brevi a causa della mancanza di argomentazioni valide per gestire tale sistema una volta finita l'emozione iniziale, o meglio conosciuta sotto il nome di crisi.
Prima di affrontare l'ultima e forse la più importante delle tre componenti è opportuno inserire una breve considerazione riguardo il delicato tema delle consulenze esterne. In entrambi i casi in precedenza descritti, spesso si materializzano davanti all'ufficio del security manager fronde di sedicenti

esperti, auto referenziati, possessori di conoscenze sino al quel momento mai rivelate, con le quali porre fine alle problematiche di sicurezza presenti all'interno dell'azienda, sia attraverso l'utilizzo di tecnologie apparentemente innovative e funzionanti sia attraverso dettagliate analisi degli scenari esistenti, ma spesso non coerenti con le reali esigenze.

Il rischio in questi casi di ritrovarsi di fronte ad una pianificazione almeno annuale di incontri, riunioni, gruppi di lavoro, questionari, liste di controllo (check list), ma soprattutto imbarazzanti richieste da fare all'amministratore delegato, risulta essere troppo grande ed assolutamente non accettabile.

Detto questo non me ne vogliano i colleghi, consulenti e lettori, ma tale precisazione si rende necessaria al fine di tutelare quelle professionalità, che con competenza vivono la consulenza come vera e propria partnership supportando l'organizzazione con sistemi efficaci di analisi i cui risultati risultano da subito fruibili per tutte le funzioni aziendali coinvolte nel processo analizzato.

Infine, il fattore umano.

Senza scendere in argomentazioni letterarie e scientifiche, nel caso in esame si possono ricondurre la cause del fallimento del sistema sicurezza a tre cause ben specifiche: l'incompetenza, la corruzione e l'inconsapevolezza.

L'incompetenza è frutto di un'assenza legislativa con la quale vengono chiaramente definite le caratteristiche professionali proprie del security manager. Nonostante vi siano degli standard qualitativi riconosciuti, la formazione certificata del security manager non è richiesta, non essendo un obbligo di legge, dalle aziende che decidono di inserire all'interno della propria organizzazione tale funzione. È noto che spesso si ricorra ad esperti di "sicurezza istituzionale" provenienti dalle Forze di Polizia, con una grandissima esperienza nel campo della criminalità organizzata, ma spesso privi di conoscenze economiche, finanziare ed organizzative proprie di una azienda quotata in borsa.

Questi non rari casi sono facilmente riconoscibili in molte aziende, anche di rilievo internazionale, dove la maggior parte dei dipendenti non conosce personalmente il capo della sicurezza, ma sa benissimo dove sia ubicato l'ufficio o il dipartimento sicurezza, solitamente riconoscibile dalle porte blindate e da sistemi di controllo accessi all'avanguardia.
Senza dilungarsi troppo circa la corruzione è sufficiente individuare il security manager non solo per le competenze specifiche del ruolo ma, soprattutto, per l'integrità morale che necessariamente lo deve contraddistinguere. Questo ruolo, se soprattutto collocato in una posizione apicale all'interno dell'organizzazione aziendale, permette l'accesso ad ogni informazione di importanza strategica ed è pertanto fondamentale che ogni elemento umano del sistema sicurezza (staff, fornitori, consulenti) sia assolutamente di provata lealtà aziendale.
Infine l'inconsapevolezza, o meglio l'incapacità di analizzare obiettivamente ogni tipologia di rischio perché troppo radicato in convincimenti assurdi e pretestuosi.
Una volta determinate le caratteristiche del sistema sicurezza in modo tale da essere abbastanza lontani dalle esaminate cause di fallimento e quindi davanti ad un sistema di sicurezza quantomeno affidabile, inizia quella che è la fase più importante per il consolidamento e riconoscimento all'interno dell'azienda.
Oltre a rimuovere, da subito porte blindate e controllo accessi posti nei pressi dell'ufficio sicurezza è necessario coinvolgere ogni funzione aziendale a supportare un semplice quanto innovativo concetto di sicurezza aziendale: La sicurezza partecipata.
Partiamo dalla definizione.
Sicurezza partecipata vuol dire garantire una maggiore integrazione ed una migliore gestione del rischio, offrendo il massimo contributo a redditività e successo dell'organizzazione stessa. Ovvero, una responsabilità della tutela aziendale non più dispersa o confusa, ma definita in un processo chiaro, condiviso e fruibile per tutti.
Prima però di iniziare è necessario raggruppare tutte le "sicurezze" che spesso operano all'interno delle organizzazioni aziendali senza mai comunicare perché considerate delle attività diverse ed incompatibili tra di loro: un esempio su tutti è la scarsa collaborazione che esiste, nei molti casi in cui sono considerate funzioni ben separate, tra "security" e "safety".
Non è raro imbattersi in accese riunioni durante le quali si scatenano a vere e proprie battaglie tra il Security Manager e il Responsabile del Servizio Prevenzione e Protezione (RSPP): il primo perché pretende che le porte siano ben chiuse il secondo, ovviamente aperte per garantire il deflusso in caso di emergenza!
Raccolte le sicurezze disperse, comprese le componenti tecnologiche (IT), impiantistiche (Building) ed umane (Human Resources) inizia il delicato processo della comunicazione ovvero, definire, all'interno della funzione sicurezza una chiara strategia comunicativa da utilizzare con le altre funzioni aziendali.
Tale strategia dovrà essere incentrata su chiarezza e semplicità degli argomenti trattati e sempre orientata alle esigenze degli interlocutori.
Uno dei più comuni errori da evitare è quello di creare barriere comunicative e, soprattutto, assumere sempre un atteggiamento proattivo durante l'analisi di tutti i processi aziendali. Semplicemente: partecipazione ai processi aziendali rendendo la sicurezza pura funzione di sostegno, offrendo in ogni circostanza il massimo contributo.
Spesso capita di osservare durante incontri di condivisione di progetti o di valutazione di strategie commerciali, il security manager, se invitato, partecipare in silenzio, seduto in un angolo, intento a pensare a tutte le possibili sciagure che potrebbero capitare. Fermo in attesa di prendere la parola con il solo scopo di spaventare, i presenti, i quali dopo un attimo infinitesimale di stupore, ed acquisito in maniera ovviamente inconsapevole il rischio, continuano a discutere del progetto preoccupandosi di tanto in tanto di tranquillizzare il security manager con frasi del tipo: "anche in questo caso siamo consapevoli dei rischi, ma non ti preoccupare ti manderemo ogni dettaglio per le tue valutazioni in merito".
Dettagli che puntualmente non arrivano, salvo casi in cui, malauguratamente, una delle "profezie" si avvera. La strategia comunicativa è pertanto di fondamentale importanza per iniziare il processo di sicurezza partecipata all'interno dell'organizzazione. È ovvio che tutto deve ricevere il giusto consenso ed approvazione da parte dell'amministratore delegato e/o direttore generale, altrimenti ogni tentativo risulterà vano. Ma non subito.

Questo consenso dovrà essere ottenuto solo nella fase finale della strategia comunicativa: focalizzarsi immediatamente sul vertice aziendale è l'errore che più frequentemente viene commesso da inesperti security manager.

Si ritiene infatti che per ricevere un adeguato impegno (commitment), cioè identificazione e riconoscimento del ruolo, sia necessario e sufficiente "spaventare" adeguatamente il vertice aziendale, ipotizzando scenari apocalittici. (grande errore).

L'unico risultato ottenibile con questo approccio è una progressiva identificazione del security manager nel sottotenente Giovanni Drogo che viene assegnato alla Fortezza Bastiani, ultimo avamposto ai confini del Regno, posta a dominio di una desolata pianura chiamata "deserto dei Tartari", un tempo teatro di rovinose incursioni da parte di agguerriti nemici. Tuttavia, da tempo ormai non più minacciata la Fortezza, svuotata ormai della sua importanza strategica, rimane solo una costruzione arroccata su una solitaria montagna, di cui molti ignorano anche l'esistenza. (Il deserto dei Tartari, romanzo di Dino Buzzati. Pubblicato nel 1940).

Si parla pertanto di una vera e propria "comunicazione del rischio", cioè di comportamenti, parole ed altre interazioni che recepiscono e rispettano le percezioni dei destinatari dell'informazione, con lo scopo di fornire appropriati strumenti decisionali per una efficace gestione dei risultati emersi dall'analisi del rischio.

La comunicazione del rischio deve riguardare cosa la sicurezza fa, non solo quello che dice, ma e deve inoltre rappresentare nella forma comunicativa la componente emotiva nella percezione del rischio delle persone, consapevole che questa è diversa per ogni funzione aziendale.

Tale comunicazione sarà più efficace se pensata come dialogo e non come istruzione. Si avrà più successo se l'obiettivo è incoraggiare certi comportamenti, non semplicemente aspettarsi che i destinatari delle informazioni facciano ciò che i comunicatori desiderino.

Tutto ciò sarà possibile se gli obiettivi verranno chiaramente e in precedenza definiti:

· Sviluppare la conoscenza e la comprensione;
· Aumentare la fiducia e la credibilità;
· Prevenire e risolvere conflitti.

Tutto ciò adottando una terminologia semplice e un linguaggio chiaro, mantenendo costante la trasparenza degli obiettivi e delle strategie seguite durante ogni fase dell'analisi del rischio, condividendo la strategia e gli aspetti operativi di interazione con tutte le parti interessate e rendendo pubblici i risultati derivanti dall'analisi del rischio e delle politiche.

Il processo di comunicazione è probabilmente il più complesso da gestire in tutto il ciclo dell'analisi del rischio, difficile da generalizzare per quanto riguarda metodo e approccio ed è fortemente dipendente dalle condizioni sociali, economiche, culturali e politiche.

Sarà pertanto determinante agire sulla comunicazione del Rischio consapevoli dell'importanza della stessa al pari dell'analisi e della gestione del rischio stesso, all'interno di un unico e condiviso universo del rischio.

In un mondo in cui la velocità dei cambiamenti non è più controllabile, la Sicurezza diventa pertanto una questione di partecipazione e controllo dei processi aziendali in modo tale da poter consentire all'azienda di continuare a sviluppare e mantenere il proprio business in maniera sempre più consapevole ed efficace.

La sicurezza partecipata come strumento efficace di governance deve essere pertanto considerata un sistema fruibile e condiviso da ogni funzione aziendale per mantenere un'adeguata capacità competitiva superando eventuali incidenti con un approccio costantemente sempre consapevole per tutta l'organizzazione.

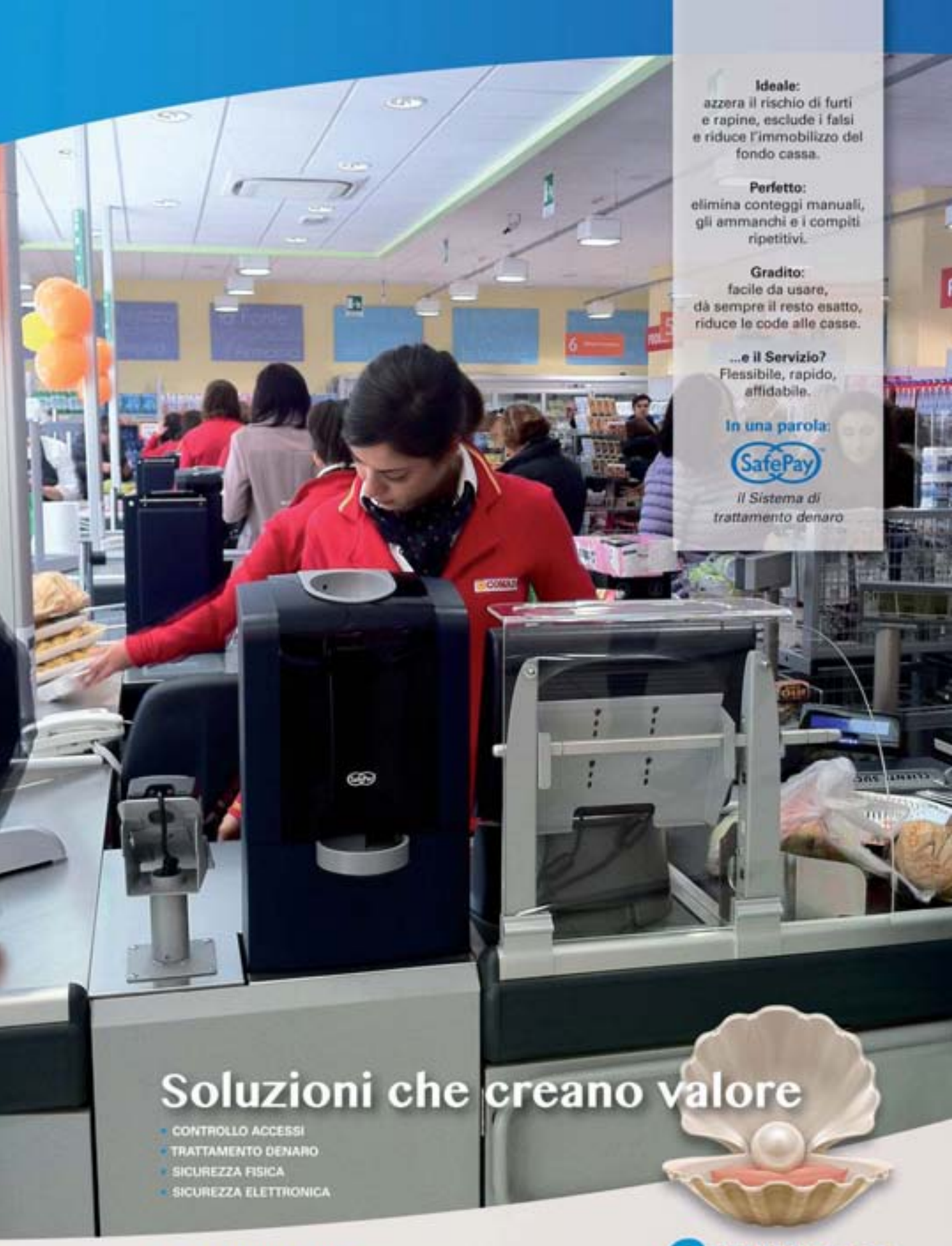
"La potenza è nulla senza controllo", era un famoso slogan pubblicitario degli anni passati, e un'azienda senza un chiaro sistema di *governance* non potrà rimanere competitiva negli anni. Soprattutto negli anni futuri.

Da Abercrombie & Fitch anche la sicurezza evolve

a colloquio con Gabriele Venuti, Asset Protection Manager di Abercrombie & Fitch e Hollister
a cura della Redazione

Partiamo da una valutazione di scenario. In qualità di Asset Protection Manager di due marchi simbolo del fashion giovanile a livello globale (Abercrombie & Fitch e Hollister), qual'è il suo punto di vista sull'evoluzione del ruolo del responsabile della sicurezza nel mondo del retail?

Sebbene non tutti i retailer abbiano ancora adottato la 'vendita omnicanale', questa nuova uniformità di esperienza del consumatore sembra ormai un futuro molto prossimo: il cliente potrà utilizzare simultaneamente diverse modalità per lo shopping, avrà la possibilità di unire la vendita classica in negozio con quella online tramite social media, smartphone, ecc., Già adesso puoi ordinare, pagare online e ritirare in negozio oppure ricevere la merce a casa, puoi controllare la disponibilità del prodotto dal PC e presentarti in negozio per acquistarla,...Il nostro ruolo deve contribuire a mantenere un'impeccabile precisione nell'allocazione della merce nei punti vendita e nei magazzini, riducendo al minimo le differenze inventariali. Le perdite non devono considerare solo il valore del prodotto o la mancata vendita, ma anche l'effetto diretto sulla soddisfazione del cliente. Immaginiamo, per esempio, il cliente che si presenti in negozio per ritirare il prodotto tanto desiderato e scopra che in realtà manca dal magazzino, nonostante l'applicazione mostri diversamente. Ecco che furti interni ed esterni, errori operazionali o amministrativi nelle spedizioni, giocano un ruolo fondamentale anche sul customer service e la fidelizzazione del cliente. Inoltre, non dimentichiamo i rischi connessi all'utilizzo delle tecnologie, basti pensare all'aumento di frodi con ricevute online, con carte di credito, resi merce fraudolenti, ecc su cui è necessaria un'attenta valutazione.



Ideale:
azzera il rischio di furti e rapine, esclude i falsi e riduce l'immobilizzo del fondo cassa.

Perfetto:
elimina conteggi manuali, gli ammanchi e i compiti ripetitivi.

Gradito:
facile da usare, dà sempre il resto esatto, riduce le code alle casse.

...e il Servizio?
Flessibile, rapido, affidabile.

In una parola:

SafePay

il Sistema di trattamento denaro

Soluzioni che creano valore

- CONTROLLO ACCESSI
- TRATTAMENTO DENARO
- SICUREZZA FISICA
- SICUREZZA ELETTRONICA

www.gunnebo.it

GUNNEBO
For a safer world®

Come viene impostata la security e la prevenzione delle perdite sul piano dell'organizzazione e del metodo, da parte di un manager operante in un gruppo internazionale?
È necessario creare un team eterogeneo di professionisti con un background analitico-operativo orientato alle attività proprie di retail security, come investigazioni interne ed esterne, analisi delle differenze inventariali, audit, formazione dei dipendenti ecc, ma anche capace di acquisire continuamente know-how specifici di store operation per conoscere e monitorare l'attività giornaliera dei punti vendita. Data mining e analisi post-inventariali permettono di controllare i trend e individuare le criticità su cui intervenire, non solo su quegli eventi che influenzano direttamente le differenze inventariali o varianze di cassa come, per esempio, i furti ma anche quelle perdite ritenute, entro una certa soglia, 'accettabili' per l'azienda come, per esempio, i prodotti danneggiati non rivendibili, che comunque incidono sul profitto. È necessario poi trasmettere costantemente queste conoscenze a tutti i livelli aziendali, sia verticalmente, dall'addetto alle vendite all'executive, sia orizzontalmente tra i dipartimenti. Si crea cosi una 'cultura di loss prevention', che molti considerano la chiave del successo per una significativa riduzione delle perdite.

Come supera il problema delle differenze normative tra un paese e l'altro, in particolare in relazione al trattamento dei dati personali dei clienti e dei dipendenti, un aspetto quest'ultimo molto delicato, alla luce dell'incidenza delle differenze inventariali attribuibili a furti interni?
Le aziende estere nel retail, soprattutto del mondo anglosassone, spesso non comprendono a fondo la particolarità della legislazione italiana, molto restrittiva su temi come videosorveglianza e controllo dei dipendenti sul luogo di lavoro. Ritengono il sistema italiano eccessivamente garantista anche nei confronti di quei lavoratori indubbiamente coinvolti in attività criminali contro l'azienda. Rispetto agli altri Paesi europei, forse ad eccezzione della Francia, in Italia riuscire a ridurre le differenze inventariali dovute a furti interni non è semplice, ma nemmeno impossibile, si cerca di lavorare sotto altri profili seguendo il concetto del 'control the controllable' (controlla il controllabile). Se ho difficoltà a reprimere le disonestà dei dipendenti, allora cerco di concentrare tutti i miei sforzi sulla prevenzione, creando una cultura di eticità e incentivando i dipendenti a segnalare i colleghi disonesti.

E, quindi, come affronta il problema del taccheggio, un problema particolarmente significativo nel fashion giovanile, in Italia e negli altri paesi?
Non c'è differenza tra i Paesi, il taccheggio commesso dai giovani, in gruppo o con la fidanzata, è un fenomeno costante, spesso spinto dall'appetibilità del prodotto in quanto 'cool', oppure spinto dalla voglia di trasgredire, tuttavia cio' che impatta in maniera significativa sulle differenze inventariali sono le bande organizzate e i ladri professionisti. Qualunque sia il tipo di ladro, il concetto di base è, ancora una volta, la formazione del personale: i dipendenti devono essere proattivi e prevenire l'accadimento dell'evento attraverso un'interazione indiscriminata verso tutti i clienti. Sottolineo che questa interazione non ha lo scopo primario di ridurre le perdite, ma punta ad un incremento della vendita e riduce la possibilità che il furto venga commesso solo come effetto secondario. Si limitano cosi' il numero di interventi degli operatori di sicurezza con l'eventuale fermo del ladro, un atto rischioso e costoso per l'azienda (per esempio il tempo che il dipendente spende per la denuncia alle forze dell'ordine), ma anche per lo Stato (es intervento forze dell'ordine, processo). Ovvio è che non sempre l'interazione 'soft' è efficace, in questo caso entra in gioco il nostro team, che è latente ma sempre vigile e operativo nel momento del bisogno.

Quali sono i supporti tecnologici attualmente disponibili di cui si avvale, e quali diverse applicazioni vorrebbe poter utilizzare?
Nonostante le ricerche abbiano dimostrato che l'efficacia dei sistemi di videosorveglianza come strumento di prevenzione diminuisca dopo i primi mesi dall'instrallazione, sicuramente sono una tecnologia molto utile per lo studio degli eventi criminali - modus operandi. Come efficacia preventiva ritengo invece l'EAS – protezione dei prodotti con placche antitacchaggio – molto piu' affidabile, nonostante le numerose tecniche adottate dai taccheggiatori per eludere il sistema. Data mining, software di business intelligence ed 'exception based reporting'

che identificano anomalie, red flags, trend permettono di conoscere a fondo le perdite non solo in temini di differenze inventariali causate da clienti e dipendenti disonesti, ma anche scoprire e ridurre gli errori umani (operazionali e amministrativi).

Quali interventi legislativi o modifiche normative richiederebbe per diminuire i problemi del taccheggio nei negozi in Italia?
Considerando il punto vendita come luogo criminogeno, cioé che genera criminalità, un'area dove continuamente avvengono taccheggi, borseggi, frodi, rapine, aggressioni, sono necessarie maggiori tutele per gli operatori privati che contrastano questo fenomeno. Spesso non solo le aziende devono investire per colmare quella sicurezza che lo Stato non riesce a garantire, ma a volte corrono il rischio di passare dalla parte del torto. Per esempio l'atto legittimo di arresto da parte di un civile si puo' facilmente trasformare in sequestro di persona. Inoltre, come sottolineavo in precedenza, sono necessarie normative piu' semplici e in linea con gli altri Paesi dell'Unione Europea, dove per esempio i tempi di registrazione di TVCC sono di 30 giorni. Infine, l'inasprimento delle pene nei confronti di coloro che praticano furti in esercizi commerciali come 'mestiere', vedi bande organizzate e ladri professionisti.

milestone

The Open Platform Company

Nel 2015, si avrà la svolta globale nel video IP nel settore retail dell'area EMEA

Ma perchè sono così tanti i retailer a cambiare?

Seconda parte

La prima parte è stata pubblicata in essecome n. 6/2014

contributo di Henrik Høj Pedersen, Milestone Systems Retail Business Dvp Manager, EMEA-APAC
traduzione a cura della Redazione

Conta Persone

Una delle applicazioni analitiche più naturali del VMS è il conteggio dei visitatori (Conta Persone oppure Footfall). La Conta Persone è normalmente ottenuta utilizzando dispositivi stand-alone, ma stanno aumentando le telecamere di sorveglianza dell'ingresso del negozio equipaggiate con un software per il conteggio delle persone, basato sulla ripresa delle immagini dei visitatori registrandone l'entrata e l'uscita dal negozio.

Il software Conta Persone produce un flusso di meta-dati che possono venire facilmente condivisi con le altre funzioni interessate e confrontati con gli scontrini di vendita. Questo tipo di controllo incrociato è un modo semplice per determinare quanto sia efficiente un determinato punto vendita. Se i visitatori di un negozio sono in aumento, mentre le vendite sono statiche o in diminuzione, questo potrebbe significare che il layout del punto vendita non è ottimale, con problemi di disponibilità o tipologia degli articoli oppure con altri problemi di gestione.

Analisi del tempo di sosta

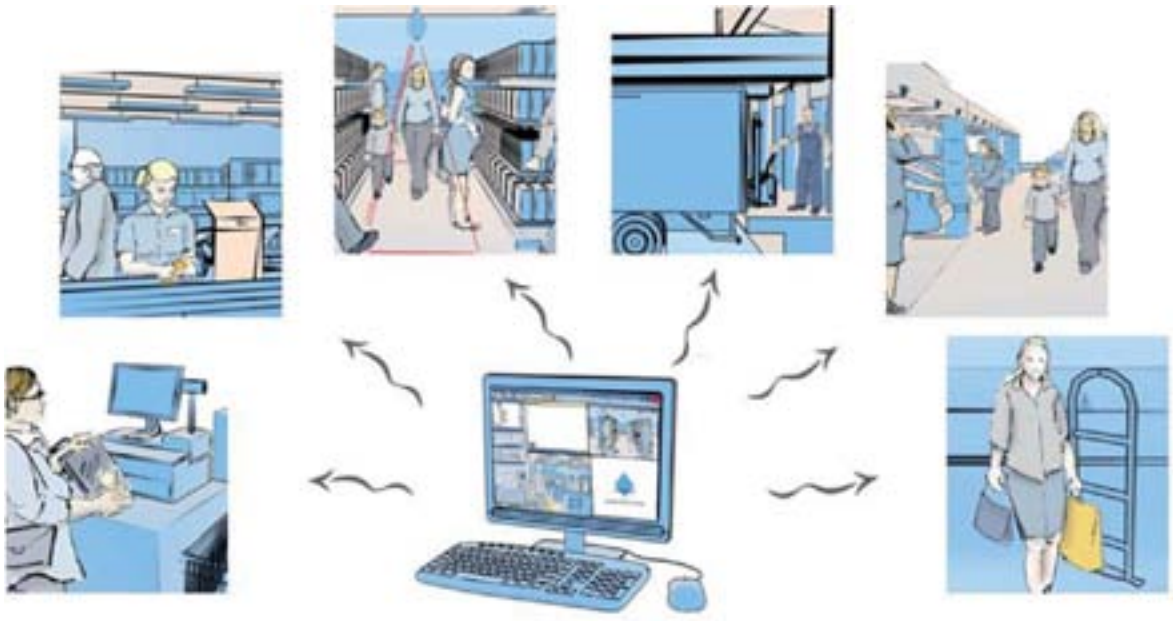
I nuovi sistemi video IP possono venire integrati con software che analizzano il tempo di sosta dei clienti, per aiutare a individuare quali corridoi e espositori funzionino meglio per attirare e trattenere i clienti. I sistemi possono anche analizzare il tempo di sosta assieme alle immagini di clienti che prendono in mano gli oggetti esposti e li mettono nei cestini. Ancora, può essere utile incrociare i dati dei tempi di sosta con i movimenti dei clienti che si sono conclusi con un normale acquisto. Ovviamente, se molti clienti si fermano a guardare un'offerta o un espositore e poi vanno via, è una chiara indicazione che qualcosa, in quell'offerta o in quell'espositore, non va bene. I gestori possono utilizzare la business intelligence per approfondire le cause e adottare i rimedi più opportuni.

Riconoscimento facciale

È possibile anche utilizzare le immagini dei clienti per analizzare i dati demografici, in particolare per raccogliere i profili in rapporto all'età e al sesso. La piattaforma aperta di Milestone può integrare anche produttori di software di riconoscimento facciale, per aiutare i gestori a determinare il livello di interesse di specifiche categorie di clienti per ogni tipologia di espositore. Questo software viene sempre più utilizzato per stabilire il numero di visitatori unici del negozio o di un singolo espositore.

Mappatura del calore

Per supportare questo tipo di intelligence, i proprietari dei negozi stanno aumentando i sistemi video IP integrati con software che offrono l'analisi della mappatura del calore. Le mappe di calore individuano le aree del negozio con maggior movimento e più elevato calpestio. Le mappe possono venire usate per capire come progettare al



meglio un negozio per ridurre i “punti neri” dove arrivano pochi clienti e anche per stimolare il flusso del pubblico attraverso il negozio affinchè si avvicini spontaneamente agli espositori con le merci di maggior valore. Le mappe di calore possono anche venire confrontate con i dati degli scontrini emessi dalle casse per verificare l’efficacia di un nuovo layout del negozio.

Gestione delle code

Oggi, i sistemi possono generare avvisi in tempo reale quando le code superano dei livelli pre-definiti. Questi avvisi devono provocare l’apertura di casse aggiuntive e l’accelerazione dei cicli di rifornimento delle merci, evitando in questo modo quelle brutte esperienze di cui tutti vorremmo farne a meno. Alcuni software intelligenti di analisi delle code possono venire integrati con i dati di calpestio all’ingresso del negozio, in modo che si possano aprire le casse aggiuntive prima che una nuova ondata di visitatori raggiunga le uscite.

Conclusioni

Aggiornare i software di video management (VMS) come il Milestone XProtect VMS, con XProtect Transact o XProtect Retail, è ancora considerato un passaggio ostico da qualche gestore. Invece, i retailer dovrebbero tenere presente che tre quarti delle loro differenze inventariali derivano dai taccheggi e dai furti dei dipendenti. Tenendo questo a mente, è chiaramente sbagliato avere un atteggiamento di chiusura verso il vantaggio di avere prove video facilmente accessibili e con l’orario registrato, da mettere insieme a specifiche transazioni (sospette) e agli scontrini di cassa. Sappiamo che questa possibilità riduce le perdite, come abbiamo potuto mettere alla prova presso clienti di alto profilo, in ogni parte del mondo.

Retailer globali della moda come Paul Smith e Prada hanno investito in VMS Milestone per i loro negozi in tutto il mondo per aiutare a ridurre le differenze inventariali e disporre di una piattaforma che consenta ulteriori miglioramenti operativi nel futuro. Una grande catena danese ha ridotto le differenze inventariali nei suoi negozi aumentando contemporaneamente il morale e la soddisfazione delle persone che lavorano dentro, perché ora sono in grado di distinguere chi è effettivamente leale e onesto sul lavoro.

A parte i benefici sulla prevenzione delle perdite, quando i retailer si accorgono dei vantaggi della business intelligence che i sistemi di video management più recenti offrono, l’affare diventa ancora più evidente. L’investimento in VMS Milestone e nei software di analisi dei nostri eco-partner possono ora offrire una business intelligence molto misurabile, giorno per giorno, che migliora l’esperienza in negozio dei clienti e aiuta i retailer a realizzare miglioramenti operativi in futuro, nemmeno immaginabili adesso.

Così, se non avete ancora pensato di usare il vostro sistema di videosorveglianza IP per avere dei benefici aggiuntivi alla mera prevenzione delle perdite, ora è arrivato il momento di farlo.

13 novembre 2014:

Presentato KeyCrime, il software predittivo usato dalla Questura di Milano

Durante la sessione di **Security for Retail 2014** tenuta nell'ambito di Sicurezza 2014, la **Polizia di Stato** ha presentato **KeyCrime**, il software predittivo utilizzato dalla Questura di Milano per l'analisi dei reati. Il suo ideatore, **l'assistente capo di PS Mario Venturi**, ha illustrato le scelte di impiego del programma, attualmente indirizzato al contrasto delle rapine nella città e nella provincia di Milano, un territorio con 3,8 milioni di abitanti per una superfice di 1.575 kmq. In base ai dati pubblicati dalla Questura, dal 2007, anno in cui è iniziata la sperimentazione, al 2013, le percentuale relativa ai casi risolti con individuazione degli autori di rapine ai danni di esercizi commerciali è raddoppiata, passando dal 27% al 54%. Sempre nel 2013, la risoluzione delle rapine ai danni delle banche ha raggiunto il 75%, mentre quella ai danni delle farmacie ha toccato il 76%. In alcuni casi, grazie alle capacità predittive del software, è stato possibile prevenire il fatto delittuoso, con gli agenti di Polizia che attendevano i criminali sul luogo dove avrebbero colpito. L'efficacia dell'effetto deterrente dell'azione della Questura di Milano è confermata dall'andamento delle rapine alle farmacie, diminuite del 25% nel corso del 2014. I risultati ottenuti sono stati oggetto di studi in ambito accademico nazinale e internazionale, fra i quali quello condotto dal Collegio Carlo Alberto di Torino, che ha evidenziato come l'impiego di **KeyCrime** in una città come Milano possa evitare un danno diretto di 3 milioni di euro all'anno, senza considerare i danni indiretti, i benefici e i risparmi per la pubblica amministrazione e la collettività.

Per contatti e informazioni scrivere a ***editor@securindex.com***

ONE

Grandezza 1:1

The only ONE...

ONE è il numero uno dei sensori digitali da esterno progettato da AVS ELECTRONICS per tutte le tue esigenze di sicurezza. Cinque modelli, un'avanzata dotazione tecnologica, l'innovativo accelerometro per un riconoscimento immediato del tentativo di manomissione, un'estrema precisione nella lettura dei segnali ambientali e innovative tecnologie antimascheramento sono i suoi segni di riconoscimento. ONE, il bello della sicurezza.

100%

AVS electronics® AVS ELECTRONICS S.p.A. Via Valsugana, 63, 35010, Curtarolo, (PD), Italy.
Tel. +39049 9698 411 - Fax +39049 9698 407 avs@avselectronics.com www.avselectronics.com

People

Il nuovo programma del CFS del gruppo HESA

a colloquio con Carlo Hruby, amministratore delegato HESA spa.
a cura della Redazione

Il Centro Formazione Sicurezza (CFS), attivo dal 2011, è una delle più importanti proposte formative del settore. Possiamo fare un bilancio di questi primi quattro anni di attività?
14 diverse tipologie di corsi replicati in ben 11 città italiane, con la partecipazione di oltre 350 aziende, sono numeri importanti ma che da soli non bastano ad esprimere la soddisfazione di aver dato vita ad un percorso formativo di alto livello e nemmeno esauriscono il nostro impegno. C'è infatti ancora tanto lavoro da fare affinché si diffonda in maniera capillare tra i professionisti della sicurezza la consapevolezza del valore che risiede in una adeguata formazione, da molti ancora sottovalutato. Questa è per noi una bella sfida, che ci entusiasma e che offre al dipartimento del CFS notevoli spazi di crescita e di sviluppo.

Quali sono le caratteristiche più significative della proposta formativa di CFS?
Innanzitutto il CFS si connota per essere un'iniziativa dedicata nello specifico ai professionisti della sicurezza, pensata per rispondere in maniera efficace a tutte le esigenze di formazione e aggiornamento legate alla loro attività. I corsi del CFS sono appositamente studiati per affrontare tutti i temi con i quali i professionisti del nostro settore entrano in contatto, sia attraverso lezioni frontali tenute da docenti esterni di alto profilo, sia attraverso sessioni interattive in aula durante le quali viene offerta agli installatori la possibilità di confrontarsi con gli altri operatori e condividere esperienze e suggerimenti. Un'altra importante caratteristica del CFS risiede nella tipologia dei corsi, che offrono una formazione di base su numerosi argomenti, dalle normative vigenti alla strategia commerciale, alle tecnologie, a prescindere dai marchi e dai modelli dei singoli prodotti ma andando piuttosto ad approfondire come realizzare una corretta progettazione e installazione dei sistemi o quale tecnologia – microonde, raggi infrarossi, laser, ecc. - scegliere in un determinato contesto.

Le proposte formative di CFS sono riservate ai clienti HESA o sono aperte a tutti gli operatori del settore?
I corsi del CFS sono aperti a tutti gli operatori del set-

tore fornendo agli installatori di sistemi di sicurezza una serie di aggiornamenti e l'acquisizione di nuove competenze per svolgere al meglio la propria attività e distinguersi da una concorrenza non sempre qualificata. E questo a prescindere dal fatto che siano già clienti HESA o meno.

Quali obiettivi si è proposto il gruppo HESA sviluppando un progetto formativo con questi contenuti e queste caratteristiche?

L'obiettivo principale che HESA si è proposta dando vita al CFS è quello di supportare l'evoluzione del settore elevando il livello e la crescita professionale dei suoi operatori, che oggi si trovano in un contesto competitivo sempre più difficile. È lo stesso obiettivo che ci ha spinti a creare un concorso come il Premio H d'oro o a dar vita ad un soggetto come la Fondazione Enzo Hruby. Crediamo infatti che sia compito di un'azienda come la nostra, che per prima ha introdotto la sicurezza elettronica in Italia, diffondere la cultura della sicurezza non solo all'interno del nostro settore, ma anche dargli una giusta visibilità all'esterno. C'è ancora molto lavoro da fare ma abbiamo raggiunto già molti traguardi che fino a pochi anni fa credevamo impossibili.

L'evoluzione delle tecnologie per la sicurezza è sempre più rapida, da una parte gli operatori a un continuo aggiornamento, dall'altra i formatori a "adeguarsi" in tempo ai nuovi contenuti. Come viene assicurato questo processo continuo da CFS?

La rapida evoluzione delle tecnologie di sicurezza si unisce all'altrettanto rapida evoluzione del mercato. In questo contesto, per rimanere competitivi, è di importanza fondamentale quella che noi chiamiamo la "formazione permanente", cioè l'aggiornamento costante sulle nuove tecnologie, sugli aspetti normativi in continua evoluzione e su quelli commerciali. Proprio in questo risiede il valore del CFS: offrire agli installatori di sicurezza l'opportunità di un continuo aggiornamento e fornire loro gli strumenti per intuire le

evoluzioni del settore e prepararsi in anticipo ai nuovi scenari competitivi. Oltre ai corsi di base, nella nostra proposta formativa vi sono moduli avanzati che consentono un costante e continuo aggiornamento. Per fare degli esempi concreti, nel primo trimestre del 2015 abbiamo un corso dedicato ai più recenti aggiornamenti normativi della videosorveglianza e della responsabilità nei confronti degli utenti finali, mirato a chiarire i nuovi obblighi che l'installatore è tenuto a rispettare in base alle più recenti sentenze nei tribunali italiani. Questo corso, tenuto dall'Avv. Valeria Finazzi, è dedicato agli operatori che hanno partecipato alle scorse edizioni di "Aspetti normativi della videosorveglianza e responsabilità dell'installatore". Approfondire questo tema ha un ruolo fondamentale nel nostro percorso formativo: se da un lato questo aspetto riveste infatti un'importanza cruciale nello svolgimento della professione, dall'altro c'è ancora una scarsa conoscenza in materia da parte degli operatori del settore. Colmare questa lacuna è una delle sfide che si è posto il CFS, attraverso il quale prendiamo l'installatore per mano e lo accompagnamo nel tempo in un percorso formativo.

Un altro fattore di cambiamento che interessa sempre più il settore è la crescita della componente "servizio" rispetto alla componente "prodotto fisico". Un cambiamento che comporta un approccio piuttosto diverso da parte degli installatori, in particolare nel rapporto con i clienti finali. Come affronta CFS questo tema?

A partire da una serie di considerazioni, fin dal 2006 la nostra azienda ha varato una strategia basata sul servizio, ovvero il valore aggiunto che è possibile offrire al cliente oltre il prodotto. In un settore come il nostro, dove la tecnologia ha raggiunto un alto livello di standardizzazione, investire su questo aspetto è molto importante per rimanere competitivi ed è un discorso che vale sia per noi fornitori sia per gli installatori. Attraverso il servizio questi ultimi possono infatti differenziarsi dalla concorrenza e rispondere con maggiore efficacia alle richieste della committenza. L'utente finale, prima ancora del prodotto, sceglie infatti il proprio installatore di fiducia, dal quale si aspetta un servizio di alto livello che l'installatore deve saper offrire. Una solida formazione di base che comprenda elementi commerciali, troppo spesso sottovalutati dal nostro settore molto (forse troppo) "tecnico", è dunque fondamentale ed è un aspetto al quale il CFS pone da sempre grande attenzione, con corsi dedicati alle tecniche di vendita che offrono interessanti spunti e simulazioni in aula.

Quali sono i temi più innovativi che CFS affronterà nel prossimo futuro?

Tutta l'attività del nostro settore è in continua evoluzione, sia per quanto riguarda le tecnologie, sia per quanto riguarda gli aspetti normativi e commerciali. Anche noi siamo perciò in evoluzione! Stiamo mettendo in cantiere delle novità importanti che per il momento non vogliamo svelare per non rovinare la sorpresa ai professionisti della sicurezza che seguono con attenzione e partecipazione le nostre iniziative.

Premio H d'oro 2014

a cura della Redazione

Categoria: **BENI MUSEALI**
Azienda installatrice: ***ELFORD 2 srl***

Denominazione e località dell'impianto: *Mostra "La ragazza con l'orecchino di perla - Il mito della Golden Age, da Vermeer a Rembrandt – Capolavori dal Mauritshuis" Palazzo Fava - Bologna*

Committente: *Museo della città di Bologna s.r.l.*

Tipologia di impianto realizzata: *Impianto antintrusione 3° livello CEI 79.3:2012, impianto di videosorveglianza, revisione e integrazione antincendio*

Data di ultimazione lavori: *Settembre 2013*

Con ben 342.626 visitatori è *"La ragazza con l'orecchino di perla. Il mito della Golden Age da Vermeer a Rembrandt"* la mostra più visitata in Italia nel 2014. Un record che fa particolarmente piacere anche al settore della sicurezza perché dimostra quanto la protezione sia indispensabile per la valorizzazione dei beni culturali. La sede di Palazzo Fava a Bologna ha potuto diventare lo scrigno di questa magnifica mostra a condizione che venisse garantita alle opere la massima sicurezza. Il risultato è stato pienamente raggiunto grazie ad un progetto eccellente di adeguamento dei sistemi esistenti, risultato finalista nella categoria dei Beni Culturali Museali del Premio H d'oro 2014, il concorso organizzato dalla Fondazione Enzo Hruby giunto alla sua nona edizione.

Descrizione dell'impianto

Per consentire ai locali di Palazzo Fava a Bologna di ospitare la mostra "Il mito della Golden Age da Vermeer a Rembrandt" e all'interno di essa l'esposizione del quadro celeberrimo di Johannes Vermeer noto come *La ragazza con l'orecchino di perla*, si è reso necessario adeguare i sistemi antintrusione e di videosorveglianza esistenti secondo le disposizioni impartite dalla società organizzatrice e dalle compagnie assicurative.

All'atto della presa in carico dei lavori risultava installato un sistema antintrusione da sostituire completamente e un sistema di videoregistrazione da integrare.

Gli impianti di sicurezza sono stati realizzati nel rispetto delle norme UNI EN 4 50131 allineate con le norme CEI 79.3:2012 che prevedono 4 classi ambientali, 4 gradi di sicurezza e 4 livelli di prestazione 2.

La scelta dei livelli di prestazione delle varie zone è diretta conseguenza dei rinforzi meccanici antieffrazione a porte e finestre realizzati al fine di considerare fisicamente compartimentali i vari ambiti espositivi.

Nelle aree con livello di prestazione 3 è previsto l'impiego di sensori volumetrici antimascheramento in tutti i locali, rilevatori sismici applicati alle inferriate, contatti magnetici antiapertura e rilevatori microfonici di rottura vetro cablati e avente grado di prestazione 3.

A protezione del coperto vetrato sul lucernaio della sala al piano terra sono previsti rivelatori microonde esterne aventi grado di prestazione 3.

Tutti i cavetti impiantistici risultano protetti da rivelatori volumetrici cablati antimascheramento di 3° livello.

Il cablaggio degli impianti antintrusione e di videosorveglianza è stato realizzato entro tubazioni e canalizzazioni separate da quelle di altri impianti, sfruttando per le parti a vista canalizzazioni ornamentali in rame e in PVC a cornice.

Ciascun oggetto esposto è munito di protezione antidistacco a contatto magnetico e/o fune realizzata con dispositivi wireless di 2° livello opportunamente interfacciate con l'unità centrale.

Per il montaggio h24 dell'area espositiva è stata allestita una control room sempre presidiata all'interno della quale sono alloggiati 6 monitor LCD 32" con schermo suddiviso in 16 riquadri per il monitoraggio live delle aree riprese. Una postazione PC dotata di software di supervisione ed una tastiera della centrale antifurto avvertono in tempo reale su mappa e mediante segnalazione ottico acustica di avvenuti allarmi e/o altre segnalazioni di guasto.

Una postazione pc dotata di software di supervisione

telecamere è dedicata all'immediata ricerca della sequenza registrata di eventuali azioni sospette, mentre è disponibile una stampante inkjet in qualità fotografica per la stampa istantanea di fotogrammi di particolare interesse per la contestazione immediata di ipotesi di reato.
Dalla postazione control room sarà possibile attivare il blocco delle porte d'accesso allo stabile così come allertare le Forze dell'Ordine e la control room remota dell'istituto di Vigilanza per il verificarsi di tentativi di rapina o altro.
La veicolazione delle segnalazioni di allarme verso la control room remota avviene mediante collegamento TCP/IP e periferica radio bidirezionale dedicata, oltre che mediante linea dati GPRS.
Il personale incaricato dal museo è avvisato simultaneamente mediante combinatore telefonico automatico operante contemporaneamente su linea urbana PSTN e cellulare GSM.

Tipologia dei materiali utilizzati

Q.tà	Descrizione prodotto
N.01	Centrale antifurto
N.76	Rivelatoreantimask 3°
N.17	Rivelatore antimask 2°
N. 30	Riv. Infrarosso passivo
N.09	Riv. Audio rottura vetro
N. 72	Riv. Sismico + cm
N. 36	Contatto magnetico 3° liv
N. 05	Barriera a microonde
N. 05	Tastiera da parete
N. 24	Concentratori 8 in 4 out
N. 05	Ricevitori wireless
N. 22	Minidome telecamera D/N
N. 01	DVR 16 ingressi samsung
N. 07	MONITOR LCD 32"

Grado di difficoltà problemi e soluzioni:
Tempi strettissimi per la realizzazione delle opere, difficoltà di passaggio cavi in edificio storico preservando l'estetica e limitando al minimo le opere murarie. Coordinamento con opere edili ed elettriche.
Necessità di attivare l'antifurto tutte le sere per ovviare ai problemi di affollamento cantiere. Per alcune settimane si è lavorato dalle ore 5.00 alle ore 14.00. Si è resa necessaria l'installazione di un sistema antifurto radio ridondante per proteggere le aree non ancora ultimate. Per il passaggio cavi sono state usate intercapedini tra i muri e lunghi fori praticati in diagonale in grado di congiungersi senza danneggiare l'intonaco..

Caratteristiche particolari dell'opera:
La presenza di un sistema di supervisione computerizzato all'interno della control room presidiata h 24 ha reso necessario l'interfacciamento dei sistemi di sicurezza con il software di gestione.

Staff e tempo impiegati per la realizzazione
N. 2 squadre da n.2 tecnici per 6 settimane consecutive.

Dichiarazione del committente sull'impianto:
Il committente si dichiara soddisfatto delle modalità di realizzazione, del rispetto dei tempi di consegna e del risultato estetico dell'opera.
La verifica positiva degli impianti da parte dell'ispettore assicurativo conferma la rispondenza di quanto realizzato alle specifiche progettuali.

CONTATTI

Fondazione Enzo Hruby
(+39) 02.38036625
www.accadoro.it

Stride la vampa…! 1ª parte

contributo di Valerio Weinberger

Per la nuova sezione tematica **Fire & Safety** ripresentiamo, a partire da questo numero, la serie di tre importanti articoli su grandi incendi di teatri avvenuti in anni recenti, pubblicati in **essecome** nel 2013. Gli articoli sono a firma di Valerio Weinberger, lo pseudonimo utilizzato da un esperto internazionale di teatri e luoghi di spettacolo, con il quale affronteremo il tema della sicurezza globale delle strutture permanenti ed estemporanee, nelle quali affluiscono e defluiscono grandi quantità di pubblico in archi temporali ristretti. Teatri, stadi, piazze sono luoghi potenzialmente a alto rischio di incendio (cinema Statuto a Torino nel 1983) di incidenti gravi (stadio Heysel a Bruxelles nel 1985) e di attentati (teatro Dubrovka a Mosca nel 2002). L'esame di quanto è avvenuto può servire a evitare che si ripetano episodi simili.

31 gennaio 1994 – Gran Teatre del Liceu, Barcelona
Fra le dieci e mezzo e le undici meno un quarto del mattino, mentre due operai lavoravano alla riparazione del sipario metallico che, in caso d'incendio, deve impedire la propagazione del fuoco dal palcoscenico alla sala e viceversa, le scintille prodotte dal cannello di un saldatore, forse azionato con superficialità e faciloneria, appiccarono il fuoco a una parte del sipario fisso posto nella zona alta del boccascena, per celare alla vista del pubblico i macchinari del palcoscenico. Alcuni frammenti di tessuto infiammati caddero al suolo, e per quanto i lavoratori si adoperassero per spegnerli, e sebbene fosse subito abbassato il sipario metallico, tutto fu inutile: le fiamme avevano già aggredito il sipario di velluto e salivano fino al graticcio e al tetto. Il fuoco era già fuori controllo quando i vigili del fuoco giunsero sul posto, soltanto pochi minuti dopo le undici. Forse ci fu un piccolo ritardo, perché gli operai

avevano tentato di spegnere l'incendio con i mezzi a loro disposizione invece di fare immediatamente una chiamata d'emergenza ai vigili del fuoco. E probabilmente, come durante le indagini è stato osservato, programmando lavori che implicavano operazioni di saldatura sarebbe stato più prudente smontare tutti gli elementi del sipario e dei tendaggi di boccascena. Sempre nel corso delle indagini fu osservato come gli impianti di spegnimento del Liceu non fossero al passo con i tempi e non corrispondessero alle normative più recenti e agli standard più aggiornati. Si legge negli atti del processo: «Tali erano l'incuria, il degrado e la scarsa considerazione dal punto di vista della sicurezza da poter affermare che la cosa più strana e sorprendente di tutta questa faccenda è come mai il teatro non fosse andato a fuoco prima…!».

Fortunatamente il fuoco non distrusse tutto il teatro: la facciata, il portico, il vestibolo, le scalinate, lo storico salone degli specchi e alcuni altri spazi risultarono indenni, circostanza che più tardi avrebbe favorito la rapidità della ricostruzione.

Il procedimento penale, dopo una richiesta da parte della pubblica accusa di una lieve pena detentiva e di una forte multa a carico del direttore tecnico del teatro e della sua assistente, per "imprudenza colposa", e di assoluzione per gli altri imputati (tecnici del teatro e operai di una ditta esterna incaricata dei lavori di saldatura), terminò nel febbraio del 2000 con l'assoluzione di tutti. Non mancarono le polemiche e uno degli imputati assolti, uno dei saldatori, affermò in seguito di avere una sua teoria sull'origine dell'incendio, ma di non poterla enunciare pubblicamente, e sostenne comunque che a suo avviso le misure antincendio presenti in teatro al momento dei lavori erano corrette, dato che erano presenti sei tecnici con estintori a portata di mano.

La sentenza accertò che l'incendio che aveva distrutto il teatro si era prodotto perché al momento non erano in essere tutte le misure di sicurezza del caso durante i lavori di saldatura, ma che tuttavia non era possibile individuare con precisione dei colpevoli. Gli unici due accusati rimasti, i responsabili della direzione tecnica del teatro, furono in ultima istanza assolti perché a loro carico non risultarono prove sufficienti a dimostrare che la competenza in materia di sicurezza in un caso di tal genere fosse in capo a loro.

L'incendio aveva provocato molta commozione nella società catalana e nel mondo dell'opera più generale. Occorre osservare che, come in nessun'altra città del mondo, a Barcelona il Liceu ha sempre rappresentato non soltanto un luogo caro agli amanti della musica e ai numerosissimi appassionati, ma soprattutto un autentico simbolo dell'identità cittadina, un emblema unificante dell'identità catalana più in generale. Fin dai primi mesi successivi all'incendio si moltiplicarono collette, offerte, donazioni spontanee. Alcuni fra i più importanti cantanti catalani (José Carreras e Monserrat Caballé, soltanto per citare due fra i più celebri) tennero diversi concerti all'aperto sulle Ramblas, poco lontano dalla struttura del teatro distrutto, destinando a favore della ricostruzione l'incasso realizzato con la vendita dei biglietti, e raccogliendo altri fondi e altre donazioni. Parallelamente fu deciso di non interrompere la programmazione teatrale, che proseguì utilizzando provvisoriamente teatri e auditori alternativi esistenti in città. Grazie all'appoggio delle istituzioni, al sostegno da parte di varie imprese e aziende, a contributi privati, il teatro fu ricostruito a tempo di record, riuscendo a riaprire le porte nel 1999. Rispetto ai due casi italiani, però, per i quali la ricostruzione ha richiesto tempi enormemente più lunghi, tanta rapidità non deve sorprendere. Nella sfortuna dell'incendio di Barcelona occorse una circostanza favorevole: fin dal 1986 erano già stati elaborati progetti per una ristrutturazione abbastanza radicale e per un ampliamento del teatro, con acquisizione di alcuni spazi adiacenti e quindi nel momento in cui si diede corso alla ricostruzione dopo l'incendio, un buon tratto di strada era già stato compiuto, almeno dal punto di vista della progettazione.

Il futuro già stava iniziando, e fu possibile procedere celermente all'attuazione del progetto esistente, che prevedeva l'ampliamento del teatro e la sua modernizzazione soprattutto dal punto di vista tecnico e della sicurezza.

Denaro Sicuro

Come cambia la sicurezza in banca – 1

a colloquio con Pietro Blengino, responsabile Physical Solutions di UniCredit Business Integrated Solutions
a cura di Raffaello Juvara

La sicurezza del sistema bancario in Italia nei confronti dei reati predatori ha compiuto passi da gigante negli ultimi anni, come viene certificato dai dati sulle rapine, diminuite dal 2007 al 2013 del 70%. Quali sono state le scelte chiave che hanno consentito questi risultati?
La fortissima riduzione del contante immediatamente disponibile in cassa è stata la chiave di volta nel contrasto alle rapine; a ciò si aggiunge che in questi anni le banche hanno investito molto in tecnologia, nell'impiantistica di allarme e nella videosorveglianza a distanza per consentire un intervento tempestivo da parte delle Forze dell'Ordine e garantendo nel contempo la massima sicurezza del personale della Banca, della clientela e non ultimo degli stessi operatori di polizia. Importante infine il ruolo giocato dall'ABI tramite l'Osservatorio Intersettoriale sulla Sicurezza (OSSIF) che ha lavorato intensamente per promuovere una ancora più stretta collaborazione tra Banche, Ministero dell'Interno, Prefetture e Forze dell'Ordine.

Quanto ha influito il rapporto con i fornitori, che in più di un'occasione, hanno sviluppato soluzioni a "quattro mani" con i responsabili della sicurezza delle banche?
Sicuramente i fornitori giocano un ruolo molto importante, forti soprattutto di una conoscenza diretta del mercato e delle soluzioni tecniche di ultima generazione. Un buon provider deve però essere anche proattivo e trasparente se vuole aspirare al ruolo di partner.

E quanto ha influito l'evoluzione tecnologica, in particolare l'avvento del video in alta definizione e dei sistemi in rete, che consentono di ottimizzare le installazioni e di centralizzare la gestione, con significativi vantaggi economici e funzionali?
La tecnologia è un elemento chiave quando si parla di sicurezza in agenzia. Ritengo che la centralizzazione e un'analisi strutturata delle informazioni siano decisive anche per disporre di alert mirati, utili a garantire una tutela tempestiva del personale e dei clienti.

I driver che guidano l'evoluzione del sistema bancario sono noti, guidati dalla virtualizzazione del rapporto con i clienti: diminuzione progressiva delle filiali, concentrazione del contante nei sistemi self-service e sua gestione affidata a service esterni utilizzo sempre più spinto delle soluzioni su mobile. Cosa resterà della filiale bancaria?

Cosa verrà chiesto ai fornitori di sistemi di sicurezza fisica?
La tecnologia ha rivoluzionato la nostra vita ed è mutata la modalità con cui ci si interfaccia ad essa. Assistiamo costantemente a progressi e cambiamenti e se anche nuovi attori si stanno affacciando al mondo bancario, non possiamo dimenticare che il denaro contante non scomparirà mai del tutto e ai fornitori di sistemi di sicurezza continueranno ad essere richieste misure per proteggerlo. Non dimentichiamo inoltre che le agenzie restano comunque un punto di riferimento sul territorio per il rapporto diretto con la clientela, specie per i servizi ad alto valore aggiunto come ad esempio la consulenza finanziaria; di conseguenza anche la protezione delle persone manterrà una certa rilevanza.

Tra i fornitori di sicurezza fisica si trovano anche gli istituti di vigilanza, a loro volta nel mezzo di un cambiamento epocale. Nel pieno della crisi economica generale, devono affrontare il cambio della normativa di riferimento e, soprattutto, il cambio della domanda da parte dell'utenza principale, in particolare proprio quella bancaria. Cosa si aspettano oggi le banche dagli istituti di vigilanza, e cosa propongono per superare le contrapposizioni strutturali sul prezzo che, in ultima analisi, non convengono neppure alle stesse banche utenti?
Si auspica una crescita con player che siano in grado di fornire servizi sempre più all'altezza della qualità richiesta dai clienti. Mi aspetto che il mercato favorisca i provider che puntano su servizi efficienti e all'avanguardia, che siano cioè in grado di accettare e fare propria la sfida del cambiamento.

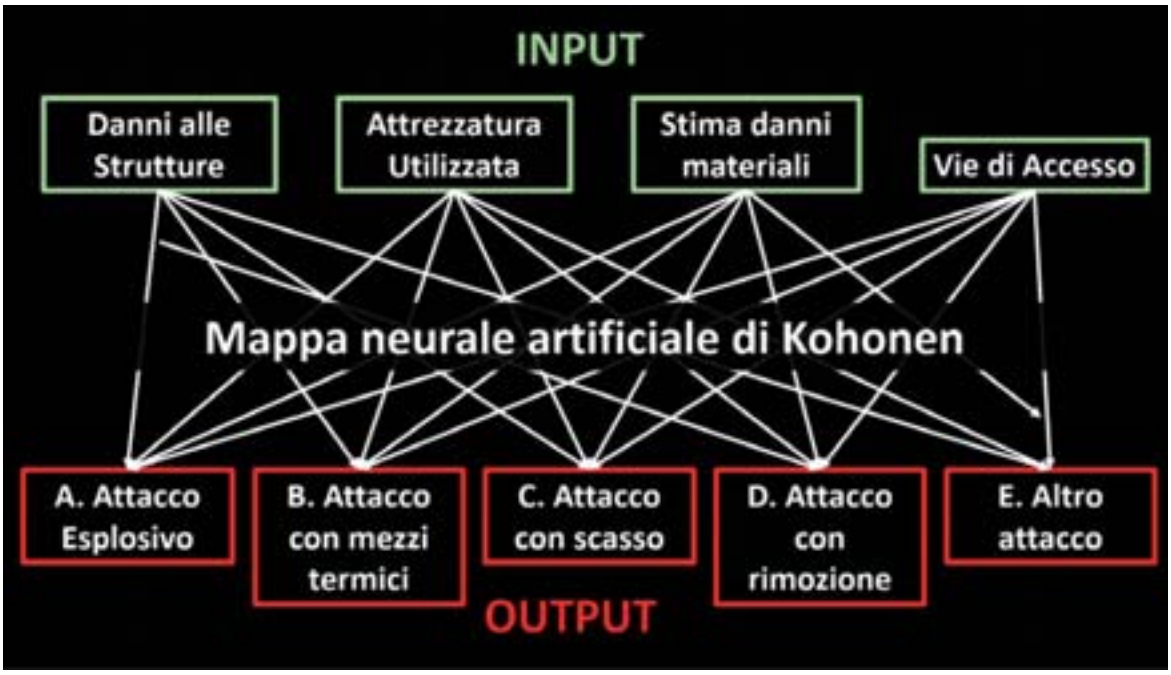
Per ultimo, come sta evolvendo la figura del security manager di una banca?
Il security manager è oggi una figura con forte rilevanza strategica all'interno della banca, un sistema in cui la sicurezza - specie quella legata al remote banking - è diventata parte integrante dei servizi e dei prodotti offerti alla clientela.
Questo significa che il security manager deve essere in grado di bilanciare la tutela della sicurezza delle persone e dei beni (fisici, informatici o reputazionali) con le esigenze del Business. Al fine di garantire un supporto costruttivo il security manager partecipa ormai sempre più spesso alle realizzazione di nuovi progetti (come ad esempio nuovi modelli e concept di agenzia oppure nuovi prodotti per l'online banking). Si tratta di una figura complessa cui vengono richieste sensibilità e conoscenze sempre maggiori congiunte alla capacità di interpretare la realtà in cui opera e anticipare quella futura.

Un nuovo modello di analisi per il rischio “attacco agli ATM”

a colloquio con Gaetano Bruno Ronsivalle, docente Tecnologie Informatiche Università Verona
a cura della Redazione

Quali sono i punti essenziali del modello di analisi del rischio di attacco agli ATM, che lei ha presentato alla Giornata della Sicurezza organizzata da OSSIF il 28 novembre scorso?
Il mio intervento descrive in cinque step i risultati delle recenti attività di ricerca svolte in collaborazione con OSSIF (Centro di Ricerca dell’ABI sulla Sicurezza Anticrimine) sull’analisi dei fenomeni criminali, con un focus specifico sulle diverse forme di attacco ai danni di impianti ATM. In particolare, ho avviato la presentazione con (1) una panoramica sull’architettura logica del modello di analisi del rischio, accompagnata da (2) alcuni dati rilevanti sull’evoluzione storica del fenomeno in esame. Mi sono poi soffermato (3) sulla classificazione neurale delle diverse tipologie di attacchi e (4) sulle funzioni generali del modello di analisi proposto. In conclusione, alla luce dei diversi output dell’indagine, ho ritenuto opportuno condividere con i partecipanti (5) alcuni suggerimenti e indicazioni metodologiche per un’efficace gestione del rischio di attacco agli ATM.

Procediamo con ordine e partiamo dal primo punto: quali sono, in sintesi, le caratteristiche fondamentali dell’architettura logica del modello che lei propone?
Nel descrivere il modello di analisi del rischio è possibile individuare tre dimensioni essenziali: (a) le finalità operative dello strumento in funzione delle esigenze dei responsabili della sicurezza, (b) gli “ingredienti” del sistema, ossia le variabili di input e le proprietà a partire dalle quali è possibile studiare e rappresentare il fenomeno, (c) gli output del modello.
Per ciò che concerne le finalità dello strumento, l’analisi è volta principalmente a valutare la probabilità che si verifichi un attacco ai danni di uno degli impianti ATM censiti all’interno del database di OSSIF. Inoltre, il sistema è in grado di restituire indicazioni dettagliate sulle diverse tipologie di attacchi, sulle eventuali perdite economiche e sulle correlazioni tra il rischio di attacco e i presidi posti

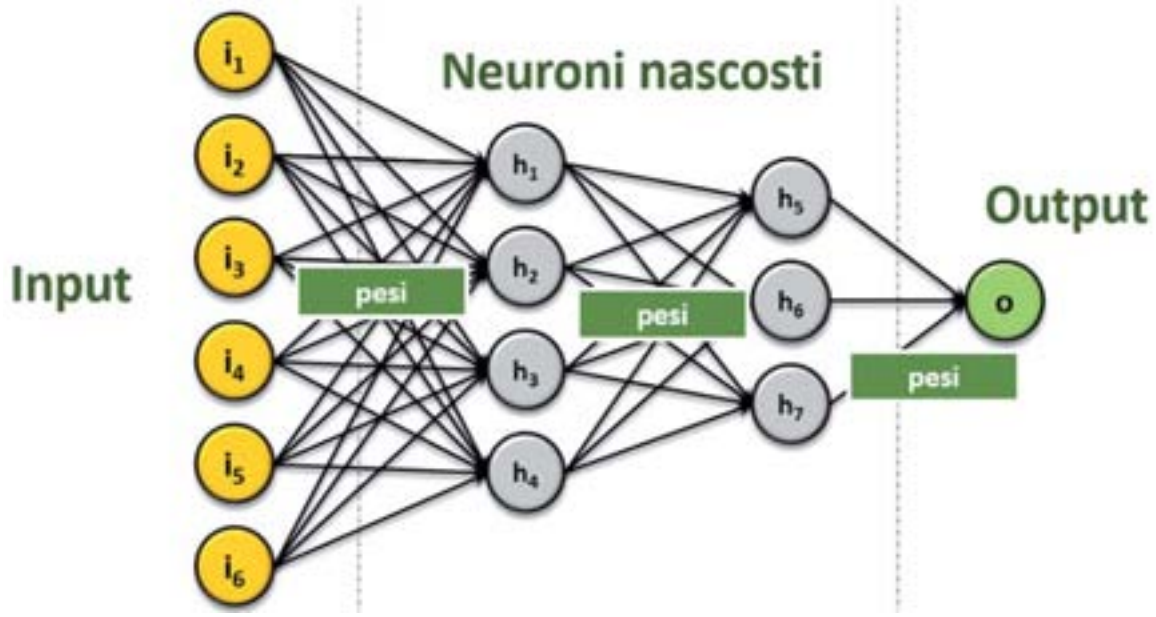


in essere nei diversi impianti.
A tal fine è necessario prendere in considerazione ed elaborare i dati storici relativi alla frequenza storica degli eventi, alla distinzione tra attacchi «tentati» e «consumati», alle differenti modalità di attacco, alle perdite economiche registrate e alle caratteristiche di ogni impianto.
Tutto ciò consente al sistema di generare, in tempo reale e per ogni ATM del territorio nazionale, un output prezioso a supporto dei processi gestionali delle banche: un vero e proprio indice di rischio "residuo" che esprime la combinazione della probabilità futura del verificarsi di un attacco, dei danni e delle perdite economiche che potrebbero derivarne e dal livello di efficacia delle misure di sicurezza che caratterizzano ogni singolo impianto.

Visto che il modello si basa sui dati inerenti l'evoluzione storica del fenomeno, al fine di inquadrare meglio il perimetro dell'analisi, può fornire qualche informazione generale sugli attacchi agli ATM e sulle relative perdite economiche negli ultimi anni?
Certamente! La base dati che supporta il modello di analisi include un censimento degli impianti e dei diversi attacchi (tentati e consumati) dal 2000 a oggi. Ciò ha consentito di studiare con estrema precisione e rigore scientifico le dinamiche che hanno caratterizzato il fenomeno in questo intervallo temporale, evidenziando alcuni dati macroscopici rilevanti per la nostra indagine:

- dal 2007 al 2014 gli attacchi ai danni di impianti ATM sono aumentati in modo rilevante. Si consideri, infatti, che l'incremento di eventi su base mensile è in media pari a circa il 200%. Una vera esplosione del fenomeno in meno di un decennio!
- il delta tra attacchi tentati e consumati, si è progressivamente assottigliato, in ragione di un presumibile incremento di "competenze" da parte degli attori criminali e una conseguente maggiore efficacia degli attacchi;
- la probabilità media di attacco mensile ai danni di impianti ATM è pari a circa 0,006498766, con punte massime di probabilità pari circa 0,03. Questi valori vanno contestualizzati in funzione dei danni materiali ed economici associati al fenomeno: ogni attacco potenzialmente produce, in media, una perdita economica pari a circa € 32.000,00, di cui almeno € 10.000,00 inerenti i danni arrecati alle strutture (a prescindere dall'effettiva sottrazione di contante dall'impianto).

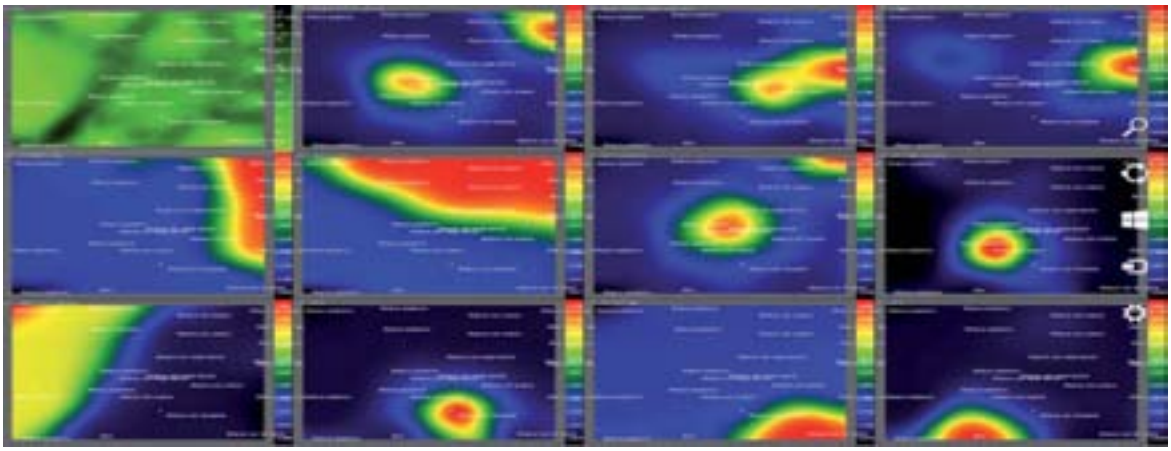
Mi sembra che questi pochi dati siano già sufficienti per giustificare l'interesse e il notevole livello di attenzione da parte delle banche nei confronti del fenomeno in esame.



Esempio di Rete Neurale Artificiale

Si tratta sicuramente di un fenomeno rilevante. In tal senso, qual è lo stato dell'arte nell'analisi degli eventi? Siamo già in grado di operare una distinzione tra le diverse modalità di attacco?
Sì. Questo è uno dei punti di forza del modello. Grazie ai dati presenti nel database è stata formulata una prima classificazione delle diverse tipologie di attacco, anche (e soprattutto) tenendo conto dell'evoluzione tecnologica degli ultimi dieci anni. In particolare, lo strumento di analisi ci consente di combinare le informazioni relative ai tipi di danni alle strutture, alle diverse attrezzature utilizzate (dagli agenti chimici al piede di porco, dalla fiamma ossidrica alla ruspa, ecc.) e alle vie di eventuale accesso all'agenzia al fine di "etichettare" ogni tipologia di attacco. La classificazione è attualmente supportata da una Rete Neurale Artificiale ad apprendimento non supervisionato (una Mappa di Kohonen, per l'esattezza), un software di Intelligenza Artificiale in grado di processare grandi quantità di dati associati ai diversi eventi della serie storica e restituire una mappa topologica delle diverse modalità di attacco. Grazie a questa attività di cluster analysis basata su tecnologia neurale, siamo riusciti a individuare e circoscrivere ben quattro tipologie complesse di attacco ai danni di impianti ATM: (a) attacco esplosivo, (b) attacco con mezzi termici, (c) attacco con scasso e (d) attacco con rimozione. Inoltre, per ciascuna tipologia è stata individuata un'area di informazioni che permette di approfondire anche le tecniche di progettazione e di conduzione dei singoli attacchi da parte degli attori criminali, nonché il loro attuale livello di competenze tecnologiche nell'uso delle diverse attrezzature. La Mappa di Kohonen, infatti, non fa altro che leggere fra le righe dei dati storici al fine di interpretare le possibili correlazioni fra le variabili in gioco e fornire informazioni sulla *forma mentis* e sul *modus operandi* del criminale. Un dato fra tutti: negli ultimi anni gli attacchi più "efficaci" sono stati portati a compimento mediante agenti chimici/esplosivi, con l'integrazione complementare di alcuni strumenti di scasso e/o mezzi termici. Ciò induce a ipotizzare un salto di qualità nella capacità "progettuale" dei responsabili degli attacchi…

Lei ha parlato di una Mappa neurale di Kohonen per classificare le tipologie di attacco. Può aiutarci a capire in modo semplice cosa sono le Reti Neurali Artificiali?
Le Reti Neurali Artificiali (RNA) sono sistemi avanzati di calcolo per l'elaborazione delle informazioni e possono essere implementate sia in termini di applicativi software, sia in termini di veri e propri dispositivi hardware (i cosiddetti PC neurali). Il loro funzionamento simula alcuni principi dei sistemi nervosi biologici e



si basa su una struttura reticolare di unità di calcolo - "nodi" o "neuroni artificiali" -, collegati mediante interconnessioni o archi pesati, la cui proprietà fondamentale consiste nella capacità di ottimizzare le caratteristiche interne al fine di produrre catalogazioni o previsioni in relazione ai dati di input. Ogni neurone è dunque in grado di ricevere input da altri neuroni e, in funzione del proprio stato di attivazione, generare o meno un singolo output, che costituisce quasi sempre un input per altre unità di elaborazione. Lo stato di attivazione di un nodo – o di eventuale non attivazione – dipende pertanto dai valori degli input e dai pesi delle connessioni. Si tratta, in definitiva, di veri e propri "cervelli" artificiali!

Perché ha deciso di adottare questi sistemi di calcolo, questi "cervelli artificiali", per l'analisi del crimine?

L'attacco ai danni di impianti ATM - come la rapina in banca e molti altri eventi criminosi - rappresenta un fenomeno complesso, quasi sempre difficilmente prevedibile mediante modelli matematici lineari. Ciò dipende essenzialmente dalla forte eterogeneità e interdipendenza dei molteplici elementi che lo determinano – sociali, economici, psicologici, geografici, ambientali, etc. Per fronteggiare questo problema si rende necessario utilizzare strumenti di analisi quantitativa avanzata che oltrepassano i confini della semplice aritmetica. Strumenti matematici addirittura in grado di "imparare" dall'esperienza e simulare la complessità di cui sono impregnati i fenomeni in questione. In tal senso, le Reti Neurali Artificiali costituiscono una risorsa insostituibile. Infatti, in perfetta armonia con la logica che governa il sistema nervoso di un essere umano, le Reti Neurali Artificiali sono state concepite in maniera tale da poter "apprendere" mediante un processo di "addestramento", ossia mediante la presentazione ripetuta di esempi relativi alla fenomenologia in esame o attraverso una serie di algoritmi di clusterizzazione dei segnali. In particolare, l'attività di apprendimento di una RNA consiste nella progressiva alterazione e definizione dei valori dei pesi delle connessioni fino alla condizione di "convergenza", intesa come uno stato del sistema in cui la rete è in grado di generare l'output ottimale o più adeguato, anche a partire da set di input non precedentemente analizzati. Tale proprietà di apprendere mediante un meccanismo distribuito e reticolare – in congiunzione con la definizione di neuroni ad attivazione non lineare - determina la capacità di una Rete Neurale Artificiale di interpretare e rappresentare la complessità di un fenomeno criminale.

Nell'introdurre la Mappa di Kohonen lei ha parlato di "apprendimento non supervisionato": esistono altre forme di apprendimento neurale?

Esistono vari algoritmi di apprendimento delle RNA. Ognuno di questi algoritmi dipende dalla natura dei dati da elaborare, dal parametro che definisce la velocità di apprendimento e dalla funzione che consente di modificare e correggere i pesi sinaptici. A seconda delle diverse combinazioni fra questi elementi, è possibile distinguere almeno tre tipi di apprendimento neuronale:

- apprendimento “supervisionato”, che prevede la presentazione di pattern di input e output attesi e dove la modifica dei pesi sinaptici dipende da una regola finalizzata a minimizzare l’errore, ossia il gap tra la risposta attesa e la risposta ottenuta, favorendo una discesa del gradiente della funzione di errore (Reti Back Propagation e Quick Propagation).
- apprendimento “non supervisionato”, che non richiede alcun set di output d’esempio, ma è condizionato esclusivamente dai pattern di input e dalla loro progressiva clusterizzazione mediante un algoritmo di tipo “competitivo” (Mappe di Kohonen o Self-Organizing Map);
- apprendimento di tipo “evoluzionistico, che si basa su particolari regole di ottimizzazione adattiva, attraverso veri e propri algoritmi genetici in grado di codificare delle stringhe genetiche artificiali, valutare le soluzioni proposte dai diversi nodi, per poi condizionarne la “riproduzione selettiva” e la vittoria sugli altri operatori.

Finora lei ha descritto la cornice teorica e la dimensione più descrittiva del modello. Può raccontarci come fa lo strumento a fornire delle informazioni a supporto dell’analisi predittiva e del processo gestionale?

Questa è la parte più interessante del nostro modello di analisi, poiché presuppone l’integrazione di una seconda tipologia di algoritmi neurali descritti precedentemente, quelli ad apprendimento supervisionato. In questo caso parliamo infatti di un Percettrone Multistrato (MultiLayer Perceptron), una rete neurale artificiale a due strati. Tale architettura è comunemente adottata per elaborare dati storici inerenti l’evoluzione di fenomeni non lineari (come quello relativo agli attacchi ai danni di impianti ATM) e simulare i meccanismi interni al fine di formulare generalizzazioni e previsioni probabilistiche. Qualcosa di molto simile al modello da noi precedentemente adottato per l’analisi del rischio rapina in Italia.

Nel caso specifico degli ATM, la Rete Neurale è stata addestrata con le variabili ricavate dalle serie storiche del db di OSSIF e dagli output della mappa di Kohonen: caratteristiche dell’impianto ATM (tipo di agenzia, tipo di ATM, collocazione, grado di resistenza, marca, ecc.), tipologie di attacchi, perdite economiche, dati sugli eventi passati e rischio esogeno (ambientale). Una volta raggiunta la convergenza, la rete è in grado di restituire, per ogni impianto ATM, un valore previsionale in corrispondenza dell’indice di rischio per ogni tipologia di attacco, dell’intensità della perdita economica attesa e del rischio residuo di attacco. In altri termini, è come se il Percettrone fosse capace di leggere i dati in modo “intelligente”, individuare le correlazioni fra le componenti del fenomeno e formulare una funzione complessa in grado simulare le dinamiche sottostanti gli eventi in esame.

Al di là dei risultati quantitativi, quali indicazioni generali e suggerimenti è possibile ricavare dall’analisi?

Gli output del modello permettono di ricostruire un identikit generico del profilo criminale del responsabile di attacchi ai danni di ATM, fornendo informazioni utili per definire una strategia di prevenzione e contrasto nei confronti del fenomeno. Ad esempio, grazie alla classificazione e alla segmentazione operate dalla Mappa di Kohonen, è possibile valutare la differenza sostanziale tra le competenze distintive di chi effettua una rapina in banca e di chi organizza un attacco ai danni di un impianto ATM. Nel primo caso, infatti, entrano in gioco abilità più incentrate sull’interazione fisica, per lo più connesse all’uso individuale di armi e alla gestione di un intervento in tempi eccezionalmente

GAETANO BRUNO RONSIVALLE
Docente di Tecnologie informatiche e multimediali · Università degli Studi di Verona
Docente di Informatica e di Tecnologie informatiche per la comunicazione · Università degli Studi di Cassino e del Lazio meridionale
Consulente scientifico di OSSIF ABI (Associazione Bancaria Italiana)

rapidi: competenze che, genericamente, potremmo ricondurre a quelle dell'assaltatore in campo militare. Nel secondo caso, invece, per mantenere la metafora militare, emerge una dimensione quasi ingegneristica della progettazione ex ante, dell'elevato livello di conoscenze tecnologiche, del lavoro interdisciplinare di squadra, assimilabile – *mutatis mutandis* - al profilo di un guastatore. Insomma, si tratta di due profili molto diversi che il responsabile della sicurezza deve poter fronteggiare mediante l'adozione di strategie mirate. E appare subito chiaro che nel caso degli ATM assume un ruolo fondamentale uno studio accurato dei modelli e di progettazione e delle procedure di attacco, un'analisi rigorosa della composizione del team criminale, una predisposizione di presidi per la mitigazione degli eventuali danni alle strutture. Per non parlare della necessità di un complessivo upgrade delle competenze tecnologiche del responsabile della sicurezza in funzione dell'evoluzione degli strumenti e delle metodologie di attacco.

Molto interessante. Ma fino a che punto i responsabili della sicurezza delle banche italiane sono disponibili a recepire le indicazioni che emergono dal modello?

Il modello proposto è semplicemente uno strumento di analisi a supporto delle ulteriori analisi che ogni responsabile della sicurezza svolge in modo dettagliato all'interno della propria azienda e non intende sostituirsi alle attività di intelligence interna. D'altra parte, l'architettura neurale proposta rappresenta una modalità avanzata di integrazione e razionalizzazione delle diverse esperienze dei responsabili della sicurezza coinvolti nell'indagine. Le funzioni del modello di analisi derivano infatti dalla condivisione delle diverse *best practice* delle banche, dalla composizione dei differenti approcci al problema e dalla sintesi ottimale di opposte rappresentazioni e modalità di gestione del medesimo fenomeno. Con un duplice vantaggio non indifferente: una crescente omogeneizzazione del vocabolario del rischio (fondamentale per un miglioramento complessivo delle prassi gestionali nell'ambito della sicurezza), accompagnata da una prospettiva analitica di sistema (resa possibile dal database di OSSIF) e non circoscritta ai dati relativi alla singola azienda.

Cosa succede alle banche italiane? La parola a FIBA/CISL

a colloquio con Claudio Quattrociocchi, delegato sicurezza FIBA/CISL Roma e Lazio
a cura della Redazione

Ci aiuta a fare il punto della situazione che sta attraversando il sistema bancario dal punto di vista dei lavoratori, dopo lo sciopero del 30 gennaio indetto dalle sigle sindacali nazionali contro il piano di riduzione delle retribuzioni e di tagli dei posti di lavoro?

Il sistema bancario italiano deve riscoprire la funzione sociale che lo ha sempre contraddistinto: raccogliere risparmi e trasformarli in impieghi. Le banche si sono invece zavorrate di crediti deteriorati per circa 300 miliardi di euro, dei quali almeno il 65% è stato erogato da figure apicali, dal direttore generale in su. Di conseguenza, almeno il 50% dei ricavi è destinato in accantonamenti su rischi verso la clientela, aumentando in proporzione il passivo dei bilanci. Per risolvere il problema, si è pensato bene di ridurre drasticamente il costo del lavoro e le teste dei bancari, aumentando invece i bonus e i compensi dei manager che hanno creato la crisi del sistema. FIBA-CISL ha raccolto più di 110 mila firme lo scorso anno per proporre un tetto alle ricompense dei manager. È stato depositato in cassazione ma è rimasto dormiente in parlamento.

Le banche devono adottare un nuovo modello centrato sulla professionalità dei dipendenti, investendo in una formazione "sana" per aumentarne le conoscenze, le capacità e le competenze. Non possono venire cancellati i diritti economici e normativi dei lavoratori con la scusa di una crisi, magari causata da scelte politiche, monetarie e bancarie miopi, basate esclusivamente sulla logica del tornaconto,

massimizzando i profitti degli azionisti e minimizzando i costi d'impresa. È un modello che deve venire aiutato da scelte politiche adeguate: non si può lasciare ai capitalisti esterni e alle multinazionali il patrimonio degli istituti di credito italiano che, guarda caso, hanno retto la crisi mondiale meglio delle banche estere. È invece di queste settimane la proposta del governo di varare un decreto legge (non si comprendono, fra l'altro, quali siano i motivi di

urgenza e necessità, previsti dalla Costituzione per i DL!) per trasformare le banche popolari in società per azioni, andando così a cancellare anni di storia di banca fondati sulle cooperative mutualistiche con voto capitario (una testa, un voto). Queste banche, lo dice la storia, hanno tenuto la crisi a differenza dei grossi colossi, hanno supportato il territorio, i cittadini, le famiglie, le aziende e, anziché premiare questo modello, lo si vuole cancellare.

Quali sono le proposte del sindacato per risolvere i problemi strutturali del sistema bancario italiano, caratterizzato da una presenza eccessiva di sportelli costruita prima del 2008 e "drammatizzata" dallo sviluppo prima dell'internet banking e ora dal mobile banking?

Il mondo cambia e bisogna stare al passo. Le operazioni allo sportello diminuiscono, riducendo anche i guadagni per le banche per effetto delle minori commissioni addebitate ai clienti che utilizzano i canali telematici. Le banche, a mio avviso, dovrebbero però focalizzare l'attenzione sui rapporti interpersonali con la clientela, ritornando a costruire relazioni fidelizzate, attraverso le quali intercettare gli interessi e le esigenze dei clienti. Le aziende di credito devono sfruttare le competenze acquisite dai dipendenti, da supportare con adeguati percorsi di formazione, per mantenere o aumentare la redditività anche attraverso servizi innovativi come, ad esempio, la consulenza alle imprese anche in campo fiscale e lo sviluppo dell'intermediazione immobiliare, conoscendo i costruttori e i bisogni capillari dei clienti. Per quanto riguarda la distribuzione degli sportelli, non dobbiamo dimenticare che il nostro territorio è morfologicamente diverso da quello degli altri paesi comunitari e, di conseguenza, stimare il numero giusto degli sportelli sarebbe azzardato e limitato. In ogni caso, non si dovrebbe pensare sempre e solo a tagliare i costi ma a come fare nuovo business. Ribadisco che la relazione con la clientela, oggi perduta, deve venire recuperata e rivalorizzata. Non desidererei che entrassero colossi internazionali con prodotti più economici e allettanti: penso che il cliente, che usa esclusivamente canali telematici spersonalizzando il rapporto con il bancario, impiegherebbe pochissimo tempo a scegliere la banca meno costosa…! L'evoluzione deve essere un'opportunità per complementare e implementare l'attività bancaria, ma non deve sostituire drasticamente il "fare banca".

I tagli dei costi, oltre a colpire le retribuzioni e la presenza sul territorio, potrebbero interessare anche il capitolo della sicurezza, ricordando che in banca la tutela dell'incolumità fisica dei lavoratori riguarda anche importanti aspetti di security?

Su questo argomento sarei molto cauto. “Ubi ius ibi societas, ubi societas ibi ius - dove c’è diritto c’è società”: il nostro ordinamento giuridico vigente tutela la salute come diritto costituzionalmente protetto e non alienabile. L’orientamento costante della cassazione esclude che il datore di lavoro possa “fare economia” sulla salute e la sicurezza dei lavoratori. Questa materia non ha bisogno di accordi poiché è lo stesso codice civile che impone ai datori di lavoro la responsabilità dell’organizzazione della massima sicurezza possibile. È dovere, obbligo, onere e onore dei rappresentati dei lavoratori per la sicurezza e delle organizzazioni sindacali vigilare affinchè venga rispettata la norma. Sarebbero inconcepibili tagli sulle politiche di salute e sicurezza dei dipendenti. Il benessere organizzativo, sinonimo di redditività e di produttività, si realizza attraverso la massima tutela e salvaguardia della salute dei dipendenti!

Negli anni passati, sono stati “esternalizzate” molte attività, fra le quali la gestione del denaro (conta a custodia) a soggetti terzi, che in alcuni casi – l’ultimo in Basilicata a dicembre – hanno prodotto ammanchi milionari che si sono riversati sulle banche appaltanti. Quali misure correttive vengono valutate in sede sindacale per evitare che si verifichino altri episodi del genere?
Le esternalizzazioni sono un nodo cruciale della trattativa. La concertazione di questi anni ha controllato e arginato forme estreme di esternalizzazione, volte sempre allo stesso fine: la riduzione del costo del lavoro. Ovviamente, le organizzazioni sindacali intendono continuare a salvaguardare tutta l’area contrattuale, regolando capillarmente le cessioni di rami d’azienda e le esternalizzazioni, contrastando le proposte inaccettabili di ABI. Per la tutela dell’occupazione, è indispensabile costituire dei presidi normativi. a livello nazionale. È cosa ormai risaputa che le cessioni di rami d’azienda e le esternalizzazione, oltre a causare inefficienze e problemi, siano solo finalizzate a perseguire in modo pedissequo la minimizzazione dei costi, per ottenere il massimo risultato con il minimo sforzo. Ma l’esperienza ci ha insegnato che, spesso, i costi risparmiati si sono solamente trasformati, come nei casi citati nella domanda, in “strane” sopravvenienze passive, provocate da scelte miopi che hanno ridotto drasticamente la competitività e la produttività delle banche. Questa è un’ulteriore conferma di quanto la deregolamentazione della normativa vigente, radicata sulla salvaguardia del modello di banca, sia già in partenza perdente. Solo attraverso il confronto si possono condividere obiettivi comuni: l’efficienza dell’organizzazione, la salvaguardia della salute dei lavoratori, l’aumento (o la difesa) dei margini d’intermediazione della banca.

Vigilanza e dintorni

Da ICIM la certificazione per la vigilanza e tutta la filiera della sicurezza

a colloquio con Paolo Gianoglio, direttore generale ICIM
a cura della Redazione

Il DM 115, entrato in vigore lo scorso mese di settembre, ha definito i termini per l'accreditamento degli enti di certificazione che dovranno certificare la corretta applicazione da parte degli istituti di vigilanza dei requisiti previsti dal DM 269/2010. Come valuta ICIM, uno dei più importanti enti di certificazione italiani, il percorso indicato dal Ministero dell'Interno?

Come ben sappiamo, il DM 115 era necessario per definire i termini per l'accreditamento degli Enti di Certificazione ma, di per sé, non è sufficiente per passare alla fase operativa delle certificazione degli istituti di vigilanza. Devono essere ancora definiti alcuni aspetti essenziali, quali le competenze specifiche richieste all'Ente di Certificazione, i parametri con i quali definire i tempi di audit, dove si deve concentrare l'attenzione del valutatore e altri ancora. In sostanza, manca il secondo livello di sviluppo del DM 115 ovvero le Regole Tecniche, senza le quali non è possibile dare attuazione al Decreto. Un livello al quale stanno lavorando il Ministero dell'***Interno e Accredia e che si dovrà concludere quanto prima***, per poter dare inizio alle verifiche e al rilascio delle certificazioni.

Da parte degli operatori, sono state espresse preoccupazioni sul possibile "ingorgo" che si potrebbe determinare a partire dalla prossima estate, quando i circa 800 istituti di vigilanza italiani attualmente operativi dovranno ottenere la certificazione entro settembre, per stare nei termini previsti dal DM 115. Quali risposte può dare ICIM?

Se le Regole Tecniche venissero pubblicate a breve, vale a dire al più tardi entro marzo, i tempi per verificare e certificare tutti gli istituti di vigilanza italiani sarebbero congrui e compatibili con le capacità operative del sistema di certificazione nazionale. Il problema, semmai, sta dalla parte degli istituti di vigilanza: quanti di loro sono pronti, sul piano organizzativo e documentale, per iniziare il percorso di certificazione

a partire da aprile? Quanti di loro sono effettivamente informati sugli adempimenti che devono attuare? Per questo motivo, ICIM ha in programma di organizzare un road show dopo la pubblicazione delle Regole Tecniche, indicativamente in tre tappe (Milano, Roma e Bari), per dare a tutti gli istituti di vigilanza le informazioni necessarie per prepararsi adeguatamente e in tempo utile alle verifiche, così da evitare il temuto ingorgo a settembre.

ICIM nasce nell'ambito dell'industria meccanica, con successivi ampliamenti a altri settori fra i quali l'anti-incendio, la safety e l'energia. Quali sono i presupposti che vi hanno portato a prendere in considerazione anche la vigilanza privata?

I presupposti da cui siamo partiti sono tre. Il primo è la nostra indiscussa leadership nella certificazione di prodotti nel segmento "sicurezza passiva" (i mezzi forti e le serrature) che, assieme a quello della "sicurezza attiva" (sistemi elettronici di rilevamento e gestione dati) e dei "servizi di sicurezza" (vigilanza, trasporto valori), compone il settore della "sicurezza fisica". Segmenti che stanno convergendo sotto la spinta dell'evoluzione tecnologica e del mercato, che sempre più richiede operatori in grado di dare risposte complete e coerenti. Il secondo è la nostra attenzione alla certificazione delle figure professionali. In questo momento è in corso l'accreditamento di ICIM per i serraturieri e i tecnici di casseforti in base alla nuova Norma UNI 11557. La certificazione delle figure professionali interesserà inevitabilmente l'intero settore della sicurezza, a partire da quanto già prevede il decreto (certificazione del professionista della security aziendale secondo la norma UNI 10459) fino ad arrivare – per le aziende che vorranno distinguersi sul mercato per la qualità del servizio offerto - alla qualificazione dei front men che si interfacciano con gli utenti finali di qualsiasi categoria. Infine, ICIM è leader in Italia nella certificazione dei contact center, in relazione alle Norme UNI 11200 – EN 15838 che, pur non afferendo alla sicurezza, costituiscono un back-round di competenze molto utile per le control rooms degli istituti di vigilanza che, come dispone il DM 269, devono essere certificate in base alle Norme UNI 11068 – EN 50518.

In conclusione, ICIM è in grado di proporsi come un unico Ente di Certificazione di riferimento per le imprese di sicurezza che operano sul mercato in modo globale, con misurabili benefici organizzativi e economici.

In quale modo avete impostato l'acquisizione delle competenze specifiche del settore nei termini previsti dal DM?

Negli ultimi 25 anni ICIM ha sempre approcciato i nuovi ambiti di certificazione avvalendosi di specialisti esperti in ognuno di essi. Il nostro modello di business prevede di acquisire le migliori competenze disponibili sul mercato. Di recente ci siamo mossi in questo modo, per esempio, per la certificazione degli operatori Fgas (gas fluorurati) e per i serraturieri, e altrettanto stiamo facendo per gli istituti di vigilanza, nei confronti dei quali ci presenteremo con il supporto di specialisti che dispongono di esperienze maturate ai massimi livelli della categoria.

Security, safety, anti incendio, gestione energetica e comfort climatico: sono funzioni del building che stanno convergendo verso piattaforme di gestione integrata e, quindi, verso gestori unici fra i quali le control rooms degli istituti di vigilanza potranno svolgere un ruolo sempre più importante. Quali contributo potrete offrire alle control rooms, in relazione alla vostre competenze consolidata nei vari ambiti del building?

Come già accennato, dalla nostra esperienza nel campo dei contact center deriva una conoscenza approfondita delle problematiche degli indicatori di performance, un aspetto critico comune con le control rooms di sicurezza. Le finalità di una control room sono chiaramente diverse da quelle di un contact center, ma conosciamo bene gli aspetti che hanno in comune dal punto di vista organizzativo e gestionale.

Di pari importanza ***è la nostra focalizzazione sulla qualificazione delle competenze degli operatori*** a contatto con il cliente, Il cosiddetto "ultimo miglio", cruciale nel processo di erogazione di qualsiasi servizio, a maggior ragione per quelli che interagiscono con la sicurezza delle persone.

Vorrei però sottolineare che le competenze che ICIM ha acquisito in materie trasversali quali i sistemi di ge-

stione della salute e sicurezza sul lavoro, i sistemi di gestione dell'energia e della building automation, l'utilizzo di sistemi di produzione di energia basati su fonti rinnovabili e la validazione di modelli di misurazione dei consumi energetici, la protezione anti incendio, convergono a costituire un valore aggiunto di grande rilevanza per un gestore di sistemi integrati che intenda operare secondo logiche di mercato tese non solo al rispetto degli obblighi di legge ma orientate a fornire un servizio di elevata qualità che soddisfi le sempre maggiori aspettative dei propri clienti. In questa logica, anche la recente normativa ISO sui sistemi di gestione per la continuità operativa (ISO 22301 "Business continuity") o sui sistemi di gestione della conformità agli adempimenti legislativi (ISO 19600 "Compliance management") rappresentano l'evoluzione di ciò che entro pochi anni sarà richiesto alle imprese che vogliono raggiungere e mantenere posizioni di leadership del proprio mercato in un contesto in cui le evoluzioni tecnologiche porteranno necessariamente a modificare le regole del gioco.

Sarà possibile superare lo storico equivoco del sillogismo *"certificazione = adempimento formale = costo superfluo"*, dando un valore aggiunto alle imprese anche in termini di sviluppo del loro business?

A questa domanda, le risposte sono due. La prima dipende da quanto il Ministero dell'Interno e Accredia sapranno e potranno tenere alta l'asticella delle certificazioni. Da quanto si è potuto vedere fino a questo momento, i presupposti sono incoraggianti e sembra chiara l'intenzione di non far scadere le certificazioni a livello di mero adempimento formale, da "comprare" al minor prezzo possibile, considerando come voci di spesa non tanto il corrispettivo per l'Ente di Certificazione, quanto l'impegno che l'impresa vorrà dedicare all'adempimento delle indicazioni del DM e delle norme che lo stesso prevede.

A quest'ultimo aspetto si collega la seconda risposta: dipende dall'approccio alla certificazione delle imprese stesse. Quanto più le imprese recepiranno le norme come schemi utili per migliorare la propria organizzazione e attribuiranno alle fasi di verifica il significato di test di efficienza, tanto più lo sforzo complessivo per la certificazione diventerà un investimento produttivo. In quest***'ottica***, la reputazione dell'Ente di Certificazione contribuirà a dare valore aggiunto alle verifiche, offrendo un accredito ulteriore alla reputazione dell'impresa certificata.

Il DM 115, vantaggi e svantaggi secondo l'esperto – 2

La prima parte è stata pubblicata in essecome n. 6/2014

contributo di Vincenzo Pinzolo di ING Progetti – Barberis Consulting

Continuità: il DM 115.2014 prevede che la certificazione di conformità degli istituti di vigilanza abbia durata triennale, prevedendo una verifica iniziale, una prima sorveglianza entro i 12 mesi successivi, una seconda sorveglianza entro 24 mesi e una verifica di rinnovo della certificazione prima della scadenza. Inoltre, almeno una verifica durante il ciclo di certificazione deve essere fatta con breve preavviso (cinque giorni lavorativi). Dulcis in fundo, è possibile effettuare verifiche anche senza preavviso. Anche se tale continuità di verifica potrebbe spaventare gli istituti, coglierei il vantaggio di avere la registrazione continua di parte terza della conformità alle norme di riferimento. In caso di qualsiasi contenzioso con terzi, inclusa la pubblica amministrazione, potrebbe rivelarsi un interessante aspetto positivo.

Abbattimento dei costi assicurativi: un'opportuna gestione dei rapporti con le compagnie assicurative, facendo leva sull'innalzamento dei livelli di buona qualità, non potrà che portare all'abbattimento dei relativi costi.

Analisi obiettiva e professionale: il coinvolgimento di enti di certificazione opportunamente accreditati presso ACCREDIA o altro Organismo di accreditamento europeo e presso il Ministero degli Interni assicurerà un'analisi obiettiva ed altamente professionale agli istituti. Essere accreditati presso ACCREDIA significa assicurare elevati standard organizzativi e referenze elevate in termini di formazione, addestramento ed esperienza specifica di settore per tutti i valutatori in essere. La certificazione è comunque un momento di crescita per qualsiasi organizzazione. Il risultato si tradurrà in termini potenziale arricchimento concorrenziale sul mercato della security.

SVANTAGGI

Non possiamo trascurare gli evidenti svantaggi che potranno derivare da una più o meno corretta applicazione del DM 115.2014:

Costi supplementari: sui punti previsti dal Regolamento attuativo del Capo della Polizia-Direttore Generale della pubblica sicurezza si giocherà la partita extra-costi per gli istituti. L'applicazione di criteri di campionamento già in uso da parte di enti accreditati (Rif ACCREDIA) per differenti standard di certificazione (Ex ISO 9001) porterebbe a costi per gli istituti proporzionali annualmente a circa 1/3 delle proprie sedi sul territorio nazionale. Non trascurerei anche i costi legati alla tempistica annuale di verifica periodica di conformità.

Tempistiche: le tempistiche attuative da parte degli istituti dovrebbero rispettare le seguenti date:

03.09.2015

- avere un sistema di gestione della qualità conforme alla UNI 10891 certificato da un organismo di certificazione indipendente opportunamente accreditato presso ACCREDIA o altro Organismo di accreditamento europeo
- avere nelle categorie previste una centrale operativa conforme alla UNI 11068 (o meglio alla EN 50518) certificata da un organismo di certificazione indipendente opportunamente accreditato presso ACCREDIA o altro Organismo di accreditamento europeo
- avere un Security Manager opportunamente formato e conforme alla UNI10459 certificato da un organismo di certificazione indipendente opportunamente accreditato presso ACCREDIA o altro Organismo di accreditamento europeo
- avere un certificato di conformità agli standard fissati da norme tecniche (leggi UNI 10891, UNI 10459, UNI 11068 e prossimamente EN 50518) ovvero al decreto Ministro dell'interno 269/2010 rilasciato da un Organismo di certificazione opportunamente accreditato presso il Ministero degli Interni da trasmettere al Prefetto competente territorialmente.

03.09.2017

- avere nelle categorie previste una centrale operativa conforme alla EN 50518 (se già certificata conformemente alla UNI 11068 alla data del 03.09.2014) certificata da un organismo di certificazione indipendente opportunamente accreditato presso ACCREDIA o altro Organismo di accreditamento europeo

Ad oggi: non esiste Regolamento attuativo del Capo della Polizia-Direttore Generale della pubblica sicurezza, non c'è notizia di alcun ente di certificazione indipendente opportunamente accreditato presso ACCREDIA per certificare secondo le UNI 10891, UNI 11068, UNI 10459, non esiste alcun Organismo di certificazione opportunamente accreditato presso il Ministero degli Interni.

Oneri tecnici: la transizione dalla UNI 11068 alla EN 50518, peraltro figlia del DM 269.2010 e dell'armonizzazione normativa di settore legata all'aspetto comunitario e non direttamente legata al DM 115.2014, comporterà per gli istituti dotati di centrali operative appartenenti alle categorie legate alla certificazione obblighi di natura tecnico/strutturale/organizzativo non già previsti. A puro titolo di esempio:

- Requisiti minimi porte, finestre, oscuranti e serrande conformi a EN 1627 classe di resistenza 4 (RC4)
- Requisito minimo guscio conforme a EN 62305 per la protezione contro la folgorazione
- Bussola d'ingresso composta da due porte interbloccate (tranne emergenze). H max 2,5 mt - L max 1,1 mt
- Area tra le due porte < 6 mq. Requisito minimo di resistenza antincendio conforme a EN 13501-2 o >= REI 30
- Requisiti minimi serrature conformi a EN 12209 per conformità classe di resistenza 4 (RC4)
- Requisito minimo ventilazione conforme a EN 13779
- Requisito minimo area libera intorno a cavi e tubazioni < 1,5 mm

Ovvia conseguenza la necessità di affidarsi ad un professionista, esperto del settore e di grande affidabilità, per la progettazione delle centrali operative o l'adeguamento delle stesse, con tutti i costi del caso.

Scelta temporanea dei partners: certamente non è apparsa felicissima la scelta del Ministero degli Interni e di ACCREDIA di effettuare delle prove generali di verifica finalizzate alla messa a punto degli strumenti operativi di cui al Regolamento attuativo del Capo della Polizia-Direttore Generale della pubblica sicurezza, in collaborazione con enti di certificazione in corsa per l'accreditamento ed istituti campione.

CONTATTI

ING PROGETTI srl
(+39) 081 19369982
www.ingprogetti.it

CONTATTI

BARBERIS CONSULTING
(+39) 0131 777082
www.barberisconsulting.it

Gli eventi di Essecome a Sicurezza 2014

14 novembre 2014:

Vigilanza & Dintorni
Droni e cloud saranno strumenti del cambiamento?

Hanno partecipato:
Andrea Menegazzi (ANIVP), Lino Busà (Assicurezza), Antonio Staino (Assovalori), Marco Giannico (Aelettronica Group), Andrea Arneri (SAVV).

L'incontro del 14 novembre organizzato da **essecome** ha messo innanzitutto in evidenza la convergenza, tra le associazioni presenti, sulle opportunità derivanti per l'intera categoria dall'entrata in vigore della nuova normativa, dopo il recepimento di alcuni emendamenti ritenuti essenziali quali i requisiti patrimoniali nei termini previsti dal Codice Civile. **ANIVP, *Assicurezza,*** e **Assovalori** hanno convenuto sul valutare l'adempimento ai dettami dei decreti ministeriali come un momento di crescita professionale e di selezione del settore, anche attraverso l'opportuno utilizzo delle tecnologie disponibili.
Un tema di rilevante interesse è di conseguenza il supporto che i fornitori di tecnologie specifiche possono dare agli istituti per "mettersi in regola",

all'indomani dell'entrata in vigore del **DM 115,** che determina i requisiti richiesti agli enti di certificazione per essere ammessi alla lista presso il Ministero dell'Interno. Le tecnologie offerte dai partecipanti alla tavola rotonda (Aelettronica e SAVV) sono rivolte direttamente alla documentazione delle attività svolte dagli istituti a favore dei propri clienti (gestione allarmi, pronto intervento, controllo ronde), e rientrano di conseguenza tra le forniture "sensibili" ai fini della certificazione delle prestazioni dell'istituto.

Andrea Menegazzi (ANIVP) *ha ricordato l'impegno di* ***ANIVP*** *per la definizione dei decreti ministeriali 269/2010 e 115/2014, sottolineando la necessità di certezze sul fatto che una normativa che impegna le aziende sul piano organizzativo e patrimoniale sia realmente applicata da tutti, con l'estromissione dal mercato degli inadempienti attraverso l'applicazione certa e omogenea delle sanzioni previste.*

Lino Busà (Assicurezza) *ha sostenuto la necessità che l'****Autorità tutoria,*** *dopo aver imposto regole che determinano significativi aumenti dei costi per le aziende che le rispettano, si adoperi ora per consentire un recupero dalla parte dei ricavi, anche attraverso l'incremento delle attività da affidare alla vigilanza privata (p.e. controlli a bordo dei treni, maggiore partecipazione alla sicurezza delle infrastrutture critiche ecc).*

Antonio Staino (Assovalori) *ha richiamato il concetto della libertà d'impresa nella determinazione dei prezzi, dopo aver osservato puntualmente gli adempimenti previsti. Ha inoltre evidenziato che l'impegno aggiuntivo richiesto al sistema del trasporto valori per garantire la* ***Business Continuity*** *in caso di interruzione dell'attività o di default di imprese che non rispettano le norme, potrebbe rappresentare una potenziale distorsione del mercato a danno delle imprese più virtuose.*

Marco Giannico (Aelettronica Group) *ha presentato la realtà nata dall'intesa tra due produttori di sistemi di centralizzazione di allarmi* ***(Eos Tech e Proservice****) per far rinascere lo storico marchio Aelettronica Group, in un mercato che richiede sempre più qualità e competitività. La conoscenza diretta degli operatori, maturata in decenni di attività, consente di interpretarne al meglio le esigenze, in particolare nell'attuale momento di mercato.*

Andrea Arneri (SAVV) *ha illustrato le caratteristiche delle nuove realizzazioni su cloud per i sistemi di controllo ronde, che permettono numerose prestazioni aggiuntive, di sicuro interesse per le imprese di vigilanza più avanzate. Arneri ha sottolineato l'importanza della volontà a evolvere espressa dagli imprenditori del settore, che potrebbero trovare un valido 'apporto da parte delle tecnologie più evolute, anche per adempiere alle normative in atto*

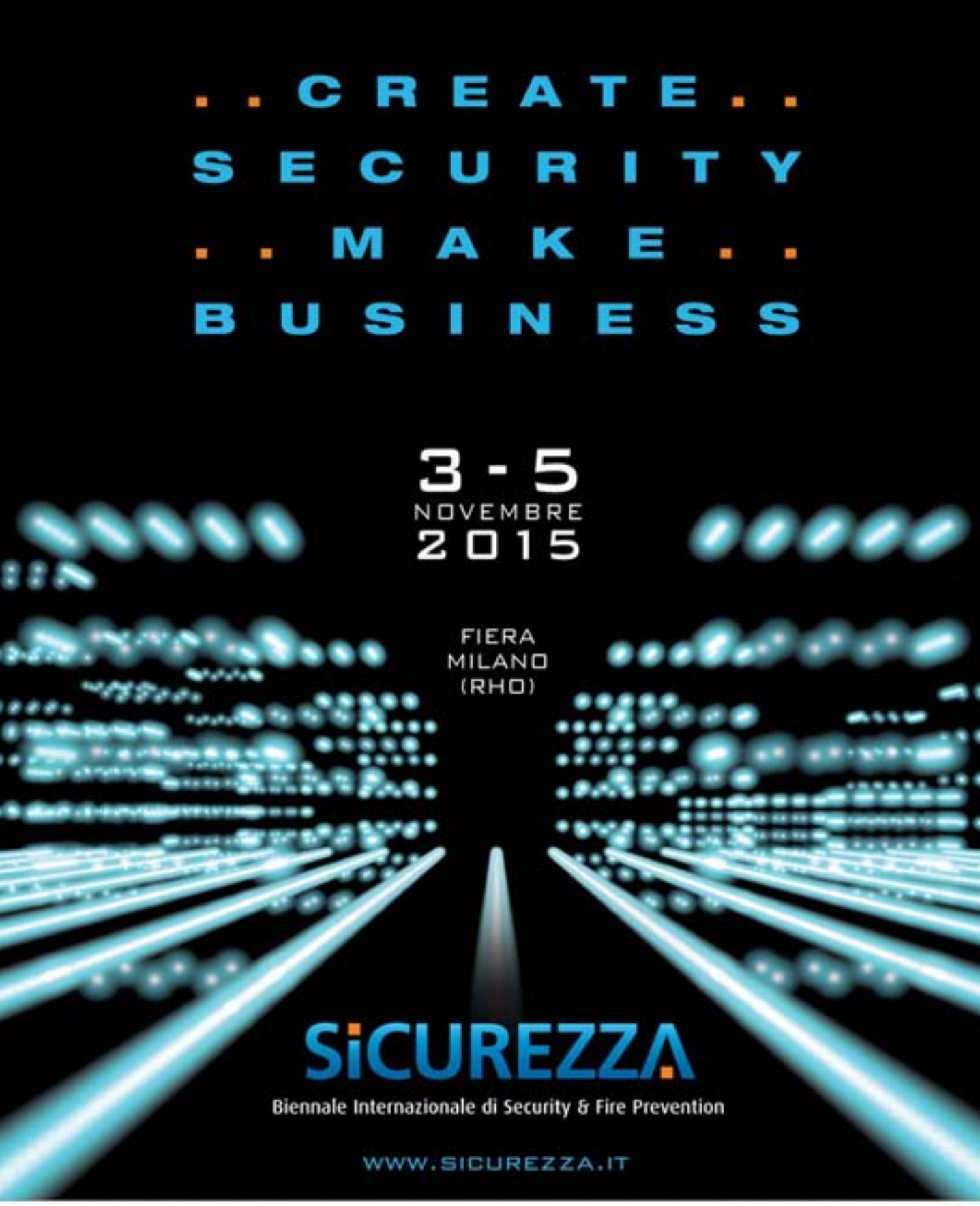
Per contatti e informazioni scrivere a
editor@securindex.com

Sicurezza 2015 annuncia la nuova data: dal 3 al 5 novembre

a cura della Redazione

Strumento di politica industriale a servizio del mercato e driver di sviluppo, questo è primariamente il ruolo delle fiere B2B. Ecco perché, viste le numerose richieste avanzate da espositori e autorevoli rappresentanti del settore, **SICUREZZA**, la Biennale Internazionale dedicata a Security & Fire Prevention, annuncia che la prossima edizione sarà dal **3 al 5 novembre 2015**.

Dopo gli importanti risultati del 2014 (29.000 mq, 512 espositori, 20.301 visitatori), **SICUREZZA** realizza così la strategia che la sposta negli anni dispari, ponendola come unica manifestazione autunnale nel panorama internazionale nel suo anno di svolgimento e innovativa occasione di business, mantenendo ferma la collocazione a novembre, particolarmente favorevole al settore.



INTERNATIONAL NETWORK

EXPOSEC
www.exposec.tmp.br

FISP
www.fispvirtual.com.br

Follow us on

EXPO MILANO 2015

FIERA MILANO

Official Partner

SICUREZZA 2015 sarà caratterizzata non solo da un nuovo calendario, ma anche da un concept rinnovato che avrà come filo conduttore l'**integrazione:** alla security, che rimane il suo core business, si affiancano settori sinergici, aprendo una finestra sul mondo dell'"**Internet of Things**" in cui le "cose" diventano smart e dialogano tra loro e tutto – dalle infrastrutture, al mondo industriale, fino ai singoli - si collega in una unica rete. Un ambito in cui la security si mostra sempre più elemento chiave di progresso.

Partendo dalle eccellenze della security, l'edizione 2015 di **SICUREZZA** vedrà dunque un ampliamento dell'area dedicata alla **domotica e agli edifici intelligenti** e maggiore attenzione alla **cyber security**. Spazio verrà dato inoltre alla **sicurezza stradale** che comprenderà sia soluzioni di urban lighting che veicoli speciali e sistemi GPS, mentre non mancheranno prodotti e servizi antincendio sia per quanto riguarda la rilevazione che lo spegnimento.

Vista la sempre maggiore convergenza tra i settori, anche la **safety** troverà una sua collocazione, consentendo lo sviluppo di interessanti sinergie con FISP (International Fair of Safety and Protection), la manifestazione di Fiera Milano che si svolge in Brasile, leader in questo settore in Sud America.

L'appuntamento con SICUREZZA 2015 è dunque dal 3 al 5 novembre 2015.

SICUREZZA

Invernizzi Group, un riferimento per il Made in Italy

contributo di Nicola Bortolazzi, project manager di Invernizzi Group

Invernizzi Group presenta cinque eventi per promuovere i prodotti del settore sicurezza in mercati in grande crescita: **Brasile, Marocco, USA, Turchia e Azerbaijan**

1 – ISC Brasil
Fiera internazionale che si svolge ogni anno a San Paolo (Brasile) presso l'Expo Center Norte nel mese di marzo. È un appuntamento molto importante per tutta l'America Latina dove circa il 70% dei visitatori proviene dallo stesso Brasile, dagli Stati Uniti d'America e dall'Argentina. Il Brasile è per tutti gli operatori italiani un mercato molto difficile da approcciare, soprattutto per coloro che propongono prodotti ad alto contenuto tecnologico e che quindi necessitano di un contatto locale in grado di seguire il post vendita, ma le probabilità di successo e le prospettive di successo sono altissime. *Questa fiera è da tenere in considerazione perché uno dei principali eventi in sud America e con un'alta fidelizzazione.* (www.iscbrasil.com.br)

2 – ISAFE
Fiera internazionale che si svolge ogni anno a Casablanca (Marocco) presso l'International Fairgrounds of Casablanca nel mese di aprile. Le aziende presenti e le strutture che ospitano l'evento non sono ancora paragonabili agli standard europei ma il potenziale di sviluppo è altissimo. L'interesse per questo mercato è sensibilmente aumentato grazie agli ampi margini di crescita registrati in questi anni (PIL in media sopra al 3%) e alle manovre politiche promosse dalla monarchia costituzionale. *Questa fiera è da tenere in considerazione perché l'unico evento di settore in questo stato e uno dei pochi presenti in tutto il nord africa.* (www.isafemorocco.com)

3 – ISC West
Fiera internazionale che si svolge ogni anno a Las Vegas (Stati Uniti d'America) presso il Sand Expo & Convention Center nel mese di aprile. È in grado di offrire la possibilità di entrare nel mercato americano o incrementare le proprie quote di mercato grazie alla presenza di oltre 23.000 operatori professionali. L'Italia è un attore principale nell'economia statunitense con oltre 27 miliardi di euro di esportazioni e nel settore sicurezza molte realtà importanti hanno già aperto filiali in loco per soddisfare al meglio la domanda. *Questa fiera è da tenere in considerazione perché è il miglior evento in America, una vera piattaforma internazionale.*

4 – ISAF
Fiera internazionale che si svolge ogni anno ad Istanbul (Turchia) presso l'Istanbul Expo Center nel mese di

REGISTER FOR FREE TODAY

COUNTER TERROR EXPO

21-22 APRIL 2015 | OLYMPIA LONDON

3 WORLD – INTERNATIONAL SECURITY FOR AN EVOLVING WORLD – INTERNA

The event for those in the public and private sectors tasked with sourcing and delivering protection against terrorist threats

- **Attend** live demonstrations and workshops
- **Network** with over 9,500+ public and private sector attendees
- **Meet** 300+ exhibitors showcasing the latest counter terrorism products and solutions
- **Discover** practical solutions on mitigating the threat of terrorism
- **Hear** from thought leaders on the future of global security

Save £50 by registering for your free exhibition pass at

WWW.COUNTERTERROREXPO.COM/IND03

Your unique registration code is Ind03

Co-located with

Follow us on

Supporting associations

Invernizzi Group, da 20 anni al fianco delle aziende italiane, si occupa di promuovere alcuni tra i migliori eventi del settore sicurezza ed antinfortunistica nel mondo.
L'agenzia è diventata un punto di riferimento per tutti quegli imprenditori che desiderano esportare i propri prodotti e diffondere il Made in Italy all'estero. Grazie alla collaborazione di aziende altamente specializzate è in grado di offrire assistenza in tutta la fase organizzativa: allestimento stand, viaggio-soggiorno, trasporto merce, servizio hostess ed eventi collaterali.
La mission aziendale è quella di sostenere le aziende nel loro processo d'internazionalizzazione creando nuove opportunità di business e migliorando la conoscenza delle dinamiche economiche globali.

settembre. I commenti su questa manifestazione sono tra i più disparati ma sta di fatto che circa 300 espositori si danno appuntamento per confrontarsi e fare affari nel centro finanziario ed economico della Turchia. Tante aziende italiane sono già rappresentate da operatori locali poiché la penetrazione nel mercato è – in certi casi – difficile causa barriere culturali e linguistiche ma ci sono margini di business per tutti. *Questa fiera è da tenere in considerazione perché è un hub strategico per il medio oriente. (www.isaffuari.com)*

5 – Cips Capian
Fiera internazionale che si svolge ogni anno a Baku (Azerbaijan) presso il Baku Expo Center nel mese di ottobre. Di certo non il primo nome che balza nella classifica delle fiere di settore ma questo appuntamento – che si svolge in contemporanea ad una fiera della costruzione – può diventare davvero un asso nella manica. Questo territorio gode di ottima salute economica grazie alle fonti energetiche, a un fondo sovrano che investe molto nelle infrastrutture e non ultimo la posizione geografica; sarà il paese che ospiterà la prima edizione dei giochi europei (manifestazione multisportiva per atleti europei) e si candidò perfino per le olimpiadi. Le istituzioni italiane sono molto attente a quest'area e si sentirà sicuramente parlare molto di questo progetto. *Questa fiera è da tenere in considerazione perché è una sfida avvincente per poter entrare in un mercato fino ad oggi poco conosciuta.* www.cips.az

ALESSIO ELETTROSICUREZZA SRL
(+39) 0423 493602
www.alessioelettrosicurezza.it

Point Security Service (P.S.S.)

La piattaforma di supervisione Point Security Service (P.S.S.) è stato ideata e progettata in base alle reali esigenze degli operatori nel settore dei sistemi di sicurezza, antintrusione, rilevazione incendio, controllo accessi e tvcc. Point Security Service può essere utilizzata per i processi evoluti di manutenzione e post vendita, è volta ai sistemi di building automation, per gestire una concreta e ideale area di lavoro e di processo di diversi protocolli, quali Konex, Profibas e PLC, e rappresenta una nuova opportunità di crescita per le aziende legate al mondo della security&safety e della grande distribuzione. Particolare attenzione è stata dedicata allo sviluppo dell'area Saving Energy. Sono state utilizzate competenze e esperienze degli operatori del settore per creare un focus group su scala nazionale e poter usufruire di questo strumento per personalizzare i propri impianti, centralizzare le proprie tecnologie, utilizzando un modello di lavoro intraprendente giovane e dinamico.

AVOTEC SRL
(+39) 0362 347493
www.avotec.it

Dispositivi per segnalazione incendio certificati CPR

AVOTEC, che da oltre quindici anni progetta e produce prodotti ad elevato contenuto tecnologico, punta su affidabilità, innovazione e design per rispondere a richieste sempre più attente ed esigenti per la sicurezza, e per **creare idee e innovazioni**. Lo studio e l'applicazione delle più moderne tecnologie, la ricerca di soluzioni personalizzate, l' operare in regime di qualità fanno di **AVOTEC** un gruppo di lavoro all'avanguardia, riconosciuto a livello internazionale.
A completamento della gamma di prodotti certificati secondo le norme EN 54, **AVOTEC** propone due serie di pannelli certificati EN 54-3 (parte acustica) + EN 54-23 (parte ottica): **AVD V e DOA V.**
Entrambi sono certificati come prodotti tipo "O" garantendo una maggiore versatilità di installazione. Lampeggio sincronizzabile con altri AVD V o DOA V; illuminazione messaggio "ALLARME INCENDIO" a led rossi ad alta efficienza; trasduttore di tipo piezo per un'ottima potenza acustica, con possibilità di scelta tipo di suono; consumo contenuto.

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

NV-5: il rivelatore d'infrarossi digitale ad alte prestazioni

Il rivelatore di movimento passivo d'infrarossi NV-5 di **Paradox** sostituisce il modello **NV-500,** impostosi per anni per la rilevazione precisa e altamente stabile, la copertura completa dell'area 10x10 metri con angolo di 90°, l'alta immunità ai falsi allarmi, e una serie di caratteristiche che l'hanno reso il prodotto più avanzato nella sua categoria.
Gli algoritmi e le analisi digitali di NV5 assicurano prestazioni precise e accurate, gestite dal comando elettronico digitale. A seconda delle condizioni ambientali, il rivelatore NV-5 può essere facilmente configurato con le impostazioni su 4 livelli.
NV-5 mantiene inalterata l'affidabilità del modello NV-500, anch'esso con tecnologia avanzata di elaborazione del segnale, ottica accurata e facilità di installazione. La nuova versione è dotata di squadretta a snodo per il fissaggio a parete o a soffitto ed è disponibile in due modelli: PX-NV5 con immunità agli animali domestici e PX-NV5SC con fasci antistrisciamento.

EKEY BIOMETRIC SYSTEMS SRL
(+39) 0471 922 712
www.ekey.net

ekey e Rittal, accesso biometrico ai centri calcolo

Rittal ha sviluppato in collaborazione con **ekey** una soluzione sicura per accedere sia a singoli rack di server sia a grandi centri dati. **Rittal** ha un'esperienza pluridecennale nella sicurezza informatica. La gamma di prodotti va dai sistemi di monitoraggio per controllare l'affidabilità operazionale di server, alle casseforti per dati informatici e alle soluzioni per camere di sicurezza.

I lettori d'impronte **ekey** sono stati integrati nel sistema di monitoraggio **Computer Multi Control CMC III** attraverso un'interfaccia standard (protocollo Wiegand). CMC III consiste in un'unità di comando centrale che interagisce con i vari sensori di temperatura, umidità ecc. Oltre ai sistemi classici di accesso, codici numerici o lettori di badge, da subito è disponibile anche la soluzione con lettore d'impronte digitali **ekey**. Con questa soluzione biometrica, si inizia una strada nuova per controllare e monitorare l'accesso ad aree riservate, garantendo anche una sicurezza ottimale ai centri dati.

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

Chubbsafes Evolve: I mezzo forte evoluto

Da **Gunnebo** arriva **Chubbsafes Evolve**: una cassaforte ergonomica, certificata EN 1143-1, con apertura automatica motorizzata e battente senza maniglia privo di fori. **Evolve** è stata studiata per chi quotidianamente si trova a utilizzare un mezzo forte, e questo è evidente nella comodità di accesso al contenuto, che avviene agendo sulla tastiera nella parte alta del battente.

Quel che differenzia **Evolve** dalle altre casseforti della sua categoria è il design, elegante e moderno, con finitura satinata e bordi arrotondati e smussati. Disponibile in tre misure con uno o due ripiani spostabili e, su richiesta, ripiano e cassetto scorrevole, **Evolve** ha una linea che favorisce l'altezza rispetto alla profondità; questo rende agevole riporre e prelevare anche oggetti piccoli, e consente alla cassaforte di adattarsi con notevole flessibilità a spazi diversi, all'interno di abitazioni, uffici o negozi.

Come tutte le casseforti ChubbSafes, Evolve è prodotta da **Gunnebo**, azienda leader nel proporre soluzioni di sicurezza vincenti.

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

I nuovi rivelatori per esterno Xtralis serie ADPRO PRO-E

HESA presenta i nuovi rivelatori passivi d'infrarossi per esterno serie ADPRO PRO-E di Xtralis**.** La nuova serie si aggiunge all'importante famiglia di rivelatori ADPRO PRO, con un'ampia gamma di modelli per soddisfare ogni esigenza di protezione perimetrale, con un ottimo rapporto qualità-prezzo. I rivelatori ADPRO PRO forniscono un'affidabilità incomparabile e una precisione di rilevamento nelle condizioni ambientali più avverse, utilizzando la tecnologia degli infrarossi passivi (PIR) abbinata con ottiche a specchio di precisione ed un'avanzata elaborazione digitale del segnale (DSP). La nuova serie PRO-E si distingue per la rilevazione di intrusi che strisciano, camminano o corrono a velocità comprese fra 0.2 e 5m/s e per la rilevazione avanzata di manomissione, che segnala un allarme se l'allineamento del rivelatore viene alterato, in aggiunta al tradizionale contatto antiapertura. L'altezza di fissaggio fino a m 4 consente di ridurre il rischio di vandalismi.

ISEO SERRATURE SPA
(+39) 0364 8821
www.iseo.com

Con Argo App, apri la porta a distanza anche con Iphone

I dispositivi di controllo accessi della linea **ISEO Zero1, serie Smart**, funzionano con **Argo,** la nuova applicazione gratuita di **ISEO,** disponibile per tutti gli smartphone e iPhone. Con App Argo, si possono abilitare tutti i telefoni Bluetooth Smart Ready (iOS, Android o Windows) all'apertura della porta, fino a 10 metri. Con App Argo, l'amministratore può autorizzare l'accesso fino a 300 utenti senza software aggiuntivi o connessione internet aggiungendo, cancellando o modificando le autorizzazioni. È anche disponibile lo storico degli ultimi 1000 eventi per ogni porta, con report inviabile via e-mail.
Gli aggiornamenti gratuiti del software dei dispositivi di controllo accesso consentono all"utente di usufruire delle nuove funzionalità del sistema. I prodotti compatibili con Argo (cilindri e maniglie elettroniche, serrature motorizzate, lettori di credenziali, etc.) si amplierà sempre più numerosi. Si possono utilizzare diverse credenziali di apertura: tessere ISEO, tessere e tag MIFARE e tutti gli smartphone con tecnologia NFC e Bluetooth Smart.

KABA SRL
(+39) 051 4178311
www.kaba.it

Nuova linea di prodotti Kaba Whiteline

Il portfolio dei prodotti **Kaba** si rinnova con la nuova linea white: da oggi tutti i dispositivi di controllo accessi Kaba sono disponibili anche nella colorazione bianca. La nuova linea è particolarmente adatta alle architetture ed edifici moderni. Grazie alla nuova linea white, **Kaba** amplia il suo portfolio di prodotti. Da oggi infatti il lettore, il cilindro digitale e la c-lever compact sono disponibili anche nella versione white. Tutti i componenti di controllo accessi, dal design pluripremiato, hanno una finitura lucida elegante e si integrano in modo perfetto nelle architetture ed edifici moderni.
Apriporta, chiusure motorizzate, varchi o porte automatiche possono essere gestiti e controllati con i lettori, antenne e sistemi di chiusura **Kaba** nella versione in bianco o nero. La nuova linea white è stata presentata all'ultima edizione del Security Essen 2014 insieme a molte altre soluzioni sempre altamente innovative dedicate al mondo del controllo accessi. Lettore e antenne di controllo accessi Kaba Whiteline.

PYRONIX
01709 700100
www.pyronix.com

Sorveglia la tua abitazione, ovunque tu sia!

La APP HomeControl+ è compatibile con Android e iOS e permette di controllare la centrale Enforcer32-WE APP utilizzando lo Smartphone come una tastiera wireless. Con l'infrastruttura Cloud (www.PyronixCloud.com, Pyronix offre all'utente una piattaforma semplice e sicura per connettersi alla centrale da remoto tramite l'App HomeControl+. Dallo Smartphone può inserire/disinserire le Aree, conoscere lo stato, escludere i sensori, leggere lo storico degli eventi, attivare le uscite domotiche. Con le Notifiche Push, avrà gli aggiornamenti in tempo reale dello stato del sistema ovunque sia, utilizzando l'HomeControl+ e il PyronixCloud. Presto HomeControl+ sarà aggiornata integrando i sistemi anti intrusione Pyronix con la gestione del video tramite PyronixCloud per verificare le immagini attraverso l'App HomeControl+, oltre al controllo della centrale di allarme PyronixCLoud infine consente all'installatore abilitato di collegarsi alla centrale e programmare e diagnosticare le proprie installazioni da remoto.

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

SAET Italia presenta la nuova centrale FACILE

La **Saet Italia** presenta la nuova Centrale Antifurto modello **FACILE** con **GSM e Scheda LAN integrato.** Realizzata presso gli stabilimenti **SAET, FACILE** offre le potenzialità della più grande **DELPHI,** adattate per applicazioni medie e piccole. **FACILE** è semplice e completa, anche per l'applicativo che consente la configurazione e la programmazione, e il download/upload del programma utente. È dotata di **8 ingressi a triplo bilanciamento, espandibili a 32 o 160** con modulo espansione mod. SC8, o di sensori seriali current loop**. I**l modulo GSM può inviare allarmi fonia e puntiformi e comandi di attuazione. **FACILE** dispone della **Scheda LAN ETHERNET integrata** (IP Standard di Saet, modificabile dall'utente) che, attraverso il **Web server integrato** con interfaccia utente locale o remota, permette di visualizzare: storico; stato dei sensori; associazione zona/sensori e le relative messa in servizio/fuori servizio; stato e gestione degli attuatori; stato attivazione/non pronto zone.

VIDEOTREND SRL
(+39) 0362 1791300
www.videotrend.net

Dahua presenta la Mini Speed Dome IP da 3”

Grazie al grado di protezione IP66 la telecamera può resistere anche alle condizioni atmosferiche più avverse. È inoltre certificata con grado di protezione antivandalo IK10. Utilizza un nuovo obiettivo con zoom ottico 3x. La compressione H264 genera uno stream video con un bit rate inferiore, riducendo così lo spazio di memorizzazione su hard disk. L'angolo di visuale dell'obiettivo arriva a 116,5 gradi fornendo un'ampia area di monitoraggio. Il corpo della fotocamera SD32203S-HN è realizzato in una lega di alluminio molto più solida rispetto ai materiali usati nei modelli precedenti. Il meccanismo di movimento verticale (TILT) si avvale di una trasmissione a cinghia invece che ad ingranaggi, migliorando così la precisione e il mantenimento dei presets e riducendo il rumore.
Il motore ad alta velocità offre una velocità massima di rotazione (Pan) sino a 240°/s ed una velocità di inclinazione (Tilt) di 160°/s che rendono la SD32203S-HN una vera telecamera ad alta velocità di posizionamento.

VIDEOTREND SRL
(+39) 0362 1791300
www.videotrend.net

Il nuovo sistema Dahua iHCVR con face detection

Il sistema iHCVR, basato sulla tecnologia proprietaria High Definition Composite Video Interface (HDCVI), è un DVR di nuova generazione con face detection, registrazione di uno snapshot e creazione di un file dei volti. I prodotti della serie iHCVR possono anche acquisire un'immagine istantanea del volto ed un filmato per 20 secondi.
Facile da usare come un sistema analogico, offre un video fino a 720p in High Definition.
I rilevamenti facciali, i movimenti, le istantanee di allarme e i video possono essere caricati sul Cloud, come Skydrive e Dropbox con sicurezza e risparmio dello spazio di archiviazione.
Può inoltre realizzare la connessione di rete p2p attraverso la scansione dei QR code ed il login al sito web (www.easy4ip.com).
L'iHCVR è economico, ad alte prestazioni e di facile utilizzo.

ELENCO FIERE

SECURITY FOR RETAIL FORUM 2015
02-03-2015
Palazzo delle Stelline, Milano

ISC BRASIL
10-03-2015 13-03-2015
Sao Paulo, Brasile

SECURITY EXPO
25-03-2015 28-03-2015
Sofia, Bulgaria

ISAFE
08-04-2015 11-04-2015
Casasablanca, Marocco

MIPS MOSCOW
13-04-2015 16-04-2015
Mosca, Russia

ISC WEST
15-04-2015 17-04-2015
Sands Expo, Las Vegas, NV

COUNTER TERROR EXPO
21-04-2015 22-04-2015
Olympia, Londra

MIDDLE EAST ENERGY SECURITY SUMMIT
21/04/ 22/04/2015
Abu Dhabi, UAE

IFSEC 2015
16-06-2015 18-06-2015
Londra, Inghilterra

AFRICAN BUSINESS CONTINUITY AND EMERGENCY REPONSE SUMMIT
18/08/2015 19/08/2015
Johannesburg, South Africa

CPSE EXHIBITION 2015
29-10-2015 01-11-2015
Shenzhen, Cina

SICUREZZA 2015
03-11-2015 05-11-2015
Milano, Italia

essecome security&safety

n. 01 gennaio –febbraio 2015

ISSN: 2384-9282

Anno XXXV-III
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Nicola Bortolazzi, Jon Cropley, Gianna Detoni, Bruno Fazzini, Giuseppe Mastromattei, Alessia Orlando, Johan Paulsson, Henrik Hoj Pedersen, Vincenzo Pinzolo, Gaetano Bruno Ronsivalle, Gabriel Siorjak, Valerio Weinberger

SEGRETERIA DI REDAZIONE
redazione@securindex.com

GRAFICA/IMPAGINAZIONE
servizio interno dell'editore

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Bozzini 3/A
Milano - Via Montegani, 23
Tel. +39 02 36757931

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

STAMPA
PINELLI PRINTING Srl
Via Redipuglia 9 - 20060 Gessate (MI)
Sede Operativa: Via E. Fermi 8 - 20096 Seggiano di Pioltello (MI)
Tel. 02.9267933 - Fax 02.9266527
www.pinelliprinting.it

Partner Essecome

ABERCROMBIE & FITCH	www.abercrombie.com	56, 58-59
ALESSIO	www.alessiosicurezza.it	50-99
AVIGILON	www.avigilon.com	2-34
AVOTEC	www.avotec.it	99
AVS ELECTRONICS	www.avselectronics.it	63
AXIS COMMUNICATION	www.axis.com	I ROMANA
CITEL	www.citel.it	21-23,35-38
COUNTER TERROR	www.counterterrorexpo.com	97
DAHUA	www.dahuasecurity.com	2-3, 102
DIAS	www.dias.it	99, IV copertina
EKEY BIOMETRIC SYSTEMS	www.ekey.net	100
EMMEVIEMME	www.emmeviemme.com	62
ERMES	www.ermes-cctv.com	59
FLIR	www.flir.com	15, 24-27
FONDAZIONE HRUBY	www.fondazionehruby.org	68-69
GUNNEBO	www.gunnebo.it	57, 100
HESA	www.hesa.it	65-67-100
H&M	www.hm.com	51-55
HI CARE	www.hi-care.eu	30-31
ICIM S.P.A.	www.icim.it	85-87
IFSEC	www.ifsec.co.uk	95
IHS	www.ihs.com	10, 12
ING PROGETTI	www.ingprogetti.it	88-89
INVERNIZZI GROUP	www.invernizzigroup.com	96-98
ISEO SERRATURE	www.iseoserrature.it	101
JVC	www.jvcpro.it	17
KABA	www.kaba.it	101
LARGO CONSUMO	www.largoconsumo.info	48-49
MILESTONE SYSTEMS	www.milestonesystems.com	60-61
MIRASYS	www.mirasys.com	39-41
OMRON	www.omron.com	42-44
PYRONIX	www.pyronix.com	II copertina, 101
SAET ITALIA S.P.A.	www.saetitalia.it	102
SATEL ITALIA	www.satel-italia.it	III copertina
SICUREZZA - FIERA MILANO	www.sicurezza.it	92-94
T-SEC S.P.A.	www.tsec.it	I copertina
VIDEOTREND	www.videotrend.net	2-3, 102

PENSA
DIVERSAMENTE

VERSA Plus

Satel Italia srl
via Ischia Prima, 280
63066 Grottammare (AP)
tel. 0735 588713
fax 0735 579159
info@satel-italia.it
www.satel-italia.it

Satel
ITALIA

Sempre al tuo fianco

Siamo da sempre al fianco dei nostri distributori qualificati con un servizio unico e le migliori soluzioni di sicurezza.

dias
Sicurezza quotidiana.

www.dias.it