essecome security&safety 01

Periodico di informazione su persone, tecnologie e applicazioni della sicurezza

2016 · ANNO XXXIX · ISSN 2384-9282

Smart Security Solution di Pyronix: La soluzione completa per soddisfare anche il progetto più esigente

Smart Security Solution include diversi componenti che offrono la soluzione "tutto incluso" ai problemi di sicurezza tipici del settore commerciale e residenziale. Grazie alla soluzione completa con centrali di sicurezza, comunicazione GPRS, servizio SIM HomeControl, infrastruttura PyronixCloud, video e possibilità di controllo remoto tramite App e software di gestione, **Smart Security Solution** consente agli installatori di configurare il sistema per ogni progetto commerciale o residenziale.

Si inizia con la centrale di sicurezza: **Enforcer 32-WE APP** e **PCX46 APP**, una gamma di centrali ibride e wireless bi-direzionale, approvate dall'ente indipendente **IMQ** al 2° e 3° livello nella **Norma EN50131**. Modulari, le centrali di sicurezza combinano molte opzioni programmabili con facilità sia d'installazione che d'uso. Assieme ai prodotti c'è un'ampia gamma di periferiche **Pyronix** cablate e/o wireless, inclusi i rilevatori per l'esterno filari e wireless XD, che offrono un'eccezionale protezione delle aree esterne delle proprietà e la massima sicurezza, rilevando l'intrusore prima che entri nei locali.

La comunicazione delle centrali **Pyronix** è un ulteriore elemento della soluzione. Il modem DIGI-GPRS, approvato secondo SP5, il massimo livello EN di sicurezza delle comunicazioni, offre un canale di comunicazione sicuro ed affidabile, consentendo alle centrali di comunicare in contemporanea con utente, con l'installatore e la vigilanza. La soluzione di comunicazione GPRS è completata da **HomeControlSIM**, la scheda SIM roaming Pyronix, che offre con una semplice iscrizione annuale il servizio DATI continuativo al sistema; in questo modo, gli installatori non devono più preoccuparsi della copertura del gestore DATI nell'area dei loro clienti, e i clienti non devono controllare il credito residuo.

Smart Security Solution è unica anche per compatibilità con il Pyronixcloud e l'App per smartphone HomeControl+. PyronixCloud funge da gateway tra centrali di sicurezza e l'app, garantendo ulteriore sicurezza attraverso una doppia password e una comunicazione totalmente criptata al livello di AES-256. PyronixCloud può essere utilizzato sia dagli utenti che dagli installatori. Gli utenti master hanno la possibilità di gestire il proprio sistema, attivando/disattivando lo smartphone degli utenti, modificando le autorizzazioni per le notifiche push per ogni utente. Agli installatori, invece, PyronixCloud offre la gestione di diversi sistemi da un unico account PyronixCloud e di personalizzare l'app HomeControl+ con il logo della propria società, per incrementare la visibilità del marchio aziendale.

L'app HomeControl+ per Android e iOS consente agli utenti un accesso immediato da remoto per inserire/disinserire le aree, controllare lo stato dei sensori connessi alla centrale, escludere sensori, controllare le uscite domotiche e visualizzare la memoria di eventi. Questa esclusiva possibilità di utilizzo semplifica l'interfaccia tra utente e sistema di sicurezza, elevando Smart Security Solution da tradizionale sistema di sicurezza a sistema integrabile nello stile di vita dell'utente, in grado di offrire benefici reali.

L'ultimo elemento di **Smart Security Solution** sono le telecamere HomeControl IP (LAN e WIFI) da 1,3 megapixel. Le telecamere per interno con possibilità di brandeggio orizzontale e verticale e le telecamere bullet per esterni, entrambe con visione notturna IR, permettono la trasmissione dello streaming live del video.

Sommario

Sommario

Eco-Savvy Series 2.0

4-Megapixel IP Camera

- 4M@20fps; 3M@25/30fps
- Triplo stream video
- IP67 e IK10
- Analisi video integrata
- Ultra WDR (Wide Dynamic Range) fino a 120dB
- Zoom ottico 30x (telecamere speed-dome)

4Mp · 1080p FULL HD · ICR D/N · IP67 · PoE · IK10

Le telecamere Dahua della serie Eco-savvy2.0 sono in grado di fornire prestazioni più elevate grazie al nuovo processore Ambarella S2LM che offre maggiori vantaggi con l'aggiunta di nuove funzioni tra cui la cui la risoluzione 4MP, WDR e analisi video. Inoltre, il sensore e la struttura meccanica delle nuove telecamere sono state migliorate per raggiungere una qualità di altissimo livello. Tutte queste innovazioni rendono la serie Eco-savvy2.0 di Dahua una soluzione con un ottimo rapporto prezzo/prestazioni e, quindi, ideale per una vasta gamma di applicazioni nella videosorveglianza in alberghi, fabbriche, negozi, edifici commerciali e nel terziario.

Modelli raccomandati:

>> IPC-HFW5121/5220/5221/5421E-Z <<

>> IPC-HDBW5121/5220/5221/5421E-Z <<

>> SD59212T/220T/230T-HN (2MP) <<

>> PC-HDBW4120/4220/4221/4421E <<

>> IPC-HDBW4120/4220/4221/4421F <<

>> SD50220T/230T-HN (2MP) <<

CE FC RoHS ISO 9001:2000

www.dahuasecurity.com

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

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

2016, cosa cambia nell'industria della sicurezza

Nel cantiere permanente del riassetto del comparto della sicurezza, i lavori stanno procedendo a pieno ritmo, con notizie quasi quotidiane di acquisti e di fusioni che modificano non solo gli assetti societari dei protagonisti ma anche il loro profilo industriale. I deal vengono in genere annunciati come operazioni a matrice prevalentemente finanziaria ma, nella maggior parte dei casi, si individuano robuste motivazioni di business, in un mercato che sta richiedendo tecnologie sempre più sofisticate e integrate con i servizi di gestione e, di pari passo, operatori sempre più trasversali e "profilati".

L'affidabilità del fornitore sembra aver assunto una portata molto più ampia e determinante di quanto avesse in passato. Oltre a capacità tecnica e solidità patrimoniale, i grandi utilizzatori richiedono garanzie di continuità operativa e, nelle forniture più delicate, il DNA societario dell'intera filiera, dai produttori di componenti al system integrator finale. L'attuale scenario politico internazionale impone infatti attenzioni inusitate per la compatibilità tra fornitori e utilizzatori, anche per applicazioni che non rientrano necessariamente nella sfera militare.

I principali deal degli ultimi dodici mesi vanno forse interpretati con questa chiave di lettura. Ad esempio, l'OPA amichevole lanciata da Canon nei confronti di Axis Communications e il passaggio di Samsung Techwin ad Hanwha, gruppo coreano operante nel real estate e nelle forniture militari, sembrano rispondere sia a logiche industriali che a esigenze di riequilibrio sul fronte della videosorveglianza e sarà interessante sapere se e come avrà seguito la notizia di un possibile take over riguardante Avigilon girata il 20 gennaio scorso. Sarebbe un'altra mossa importante nella partita in corso in questo comparto strategico.

Altro fronte in grande spolvero è quello degli accessi fisici e dell'antintrusione, soprattutto per l'attivismo delle aziende nord-americane in Europa, anzi in Germania. Mentre Vanderbilt ha acquistato i prodotti di sicurezza da Siemens, Allegion (il ramo sicurezza "spinoffato" da Ingersoll Rand) ha conquistato Simons Voss, costruttore di serramenti meccatronici di gamma alta. Due operazioni nel segno dell'importanza della protezione fisica degli accessi e dei perimetri di aree ed edifici sensibili, confermata dalla crescita dei produttori specializzati in recinzioni passive, integrate con sempre maggior frequenza con i sistemi di sicurezza attiva.

E' probabilmente correlato a questo il maggior interesse per i sistemi di gestione integrata e risposta agli eventi (PSIM Physical Security Information Manager) che si trovano al vertice della gerarchia funzionale nelle strutture complesse. Se, alla fine del 2015, Nice ha ceduto a un fondo di investimento israelo/statunitense il ramo d'azienda specializzato, al quale IHS aveva attribuito la leadership mondiale del comparto, si possono immaginare motivazioni di profilo strategico che si comprenderanno in futuro.

Per finire, dalla fusione tra Johnson Controls e Tyco Fire & Security sta nascendo il leader mondiale nella building automation e security integration, un gigante da 32 miliardi di dollari di fatturato che dichiara di voler già fare altre acquisizioni per crescere ancora e cambiare i paradigmi del comparto.

Noi, con i 6 miliardi scarsi fatturati dall'intera filiera della sicurezza tecnologica e dei servizi di vigilanza, possiamo solo stare a guardare…

riscogroup.com/italy

RISCO GROUP

VUpoint

VUpoint di RISCO Group, è la rivoluzionaria soluzione per la verifica video live che integra perfettamente Telecamere IP con i sistemi di sicurezza professionali RISCO.

Utilizzando il Cloud RISCO, VUpoint offre la possibilità di visualizzare immagini video dal vivo potendo così monitorare siti commerciali e residenziali.

Per maggiori informazioni visitate il sito **www.riscogroup.it**

RISCO Group S.R.L | Via Robecco, 91 – Cinisello B (MI)

Guarda il video di VUpoint su YouTube!

App Store | Facebook | Play Store | iRISCO

ZeroWire

ANDROID APP ON Google play

Available on the App Store

ZeroWire, prodotto da UTC (United Technologies Corporation), è un innovativo sistema di sicurezza senza fili con funzioni domotiche e prestazioni all'avanguardia. Semplice da utilizzare, viene fornito con un transceiver Z-Wave® integrato di serie, consentendo agli utenti di attivare luci, termostati e serrature da casa o da remoto tramite app disponibile per dispositivi iOS e Android.

HESA

www.hesa.com

Perché ho presentato l'emendamento alla Legge di Stabilità 2016 per il bonus fiscale da 15 milioni per videosorveglianza e vigilanza

a colloquio con l'on. Gianfranco Librandi, deputato di Scelta Civica
a cura di Raffaello Juvara

Martedì 22 dicembre 2015 il Senato ha approvato, con 162 voti favorevoli e 125 contrari, il disegno di Legge di Stabilità 2016 (A.S. 2111-B) nel testo licenziato dalla Camera, sul quale il Governo aveva posto la questione di fiducia. E' stato quindi approvato anche l'emendamento proposto dal relatore on. **Gianfranco Librandi** di Scelta Civica al comma 982 che "istituisce per l'anno 2016 un credito d'imposta per 15 milioni a favore delle persone fisiche che, al di fuori della loro attività di lavoro autonomo, installano sistemi di videosorveglianza digitale ovvero stipulano contratti con istituti di vigilanza per la prevenzione di attività criminali". Un successivo decreto ministeriale definirà le modalità applicative della norma.
Abbiamo intervistato l'on. Librandi, per chiedergli quali siano state le motivazioni che lo hanno spinto a presentare questo emendamento e quali siano le prospettive di coinvolgimento delle categorie che compongono il settore della sicurezza interessate dal provvedimento rispetto alla definizione del decreto attuativo ma, soprattutto, rispetto a un possibile dialogo con il Governo per affrontare in modo organico il tema della sicurezza partecipata. Un tema rilevante non solo sul piano dell'ordine pubblico e, come tale, di pertinenza del Ministero dell'Interno, ma anche per numerosi altri Dicasteri come Sviluppo Economico, Giustizia, Beni Culturali, Infrastrutture, solo per citarne alcuni.

L'emendamento che ha presentato alla Legge di Stabilità relativo al recupero fiscale per l'acquisto di sistemi di videosorveglianza e di servizi di vigilanza da parte di cittadini privati è stato interpretato dagli operatori della sicurezza privata – che in Italia, tra fornitori di tecnologie e istituti di vigilanza, occupa circa 60.000 persone con un fatturato superiore a 6 miliardi di euro – da una parte come un segnale positivo di interesse del governo per la diffusione dei sistemi di sicurezza; dall'altra come un intervento che avrà scarso effetto per l'esiguità dello stanziamento (15 milioni). Quali sono stati i presupposti alla base della presentazione dell'emendamento e alla sua definizione in questi termini?
Il principio generale alla base della presentazione del mio emendamento è stato "Italiani, per garantirvi sicurezza, non comprate la pistola ma usate il cervello". Recenti fatti di cronaca ci hanno mostrato la propensione di molti italiani a difendersi con le armi. E' una scelta che mi spaventa, non mi piace l'idea di trasformare il mio Paese in un Far West, dove vince chi spara per primo.
E poi gli echi delle tragedie che giungono quasi quotidianamente dagli Stati Uniti, dove secondo recenti statistiche una famiglia su tre detiene armi, dovrebbero convincerci che questa non è la via giusta da seguire.
Esistono molti altri strumenti, in primis i sistemi di videosorveglianza e di vigilanza, che ci permettono di difenderci in modo efficace e ritengo sia un dovere dello Stato promuovere la loro diffusione, anche attraverso sgravi fiscali legati al loro acquisto.
E' proprio questa la ratio del mio emendamento.
Certo, concordo sul fatto che uno stanziamento di 15 milioni di euro sia modesto, come ho in più occasioni fatto presente al Viceministro Morando nel corso della discussione della Legge di Stabilità in Commissione Bilancio.
Ho percepito su questo tema una diffusa condivisione da parte di molti colleghi e perciò confermo in questa occasione il mio impegno a lavorare per far sì che ulteriori risorse siano destinate al finanziamento di questi sgravi; al momento ritengo comunque importante che sia stato condiviso ed approvato il concetto della necessità di sostenere economicamente l'acquisto e l'utilizzo di queste strumentazioni e servizi per la sicurezza domestica

Secondo i dati elaborati da diversi osservatori, basati sui rilevamenti dell'ISTAT e del Ministero dell'Interno, negli ultimi anni la criminalità predatoria comune ha spostato sempre più l'attenzione verso gli obiettivi più indifesi, come i negozi e soprattutto le abitazioni, con conseguenze pesanti in termini di allarme sociale e di costi per la collettività. Si può pensare a un programma organico per la loro messa in sicurezza, partendo proprio da questa Legge di Stabilità?
Sì, credo che si possa ma soprattutto si debba pensare ad un programma organico, continuativo e strutturale per la messa in sicurezza delle abitazioni e dei luoghi di lavoro, che ha preso il via con l'approvazione dell'emendamento alla Legge di Stabilità che ho proposto.
Per quanto in generale il numero dei reati in Italia tenda a diminuire, come confermano i dati recentemente pubblicati dal Ministero dell'Interno, i furti sono comunque reati che creano forte allarme sociale e preoccupazione per i cittadini, che vengono colpiti non solo nel loro patrimonio ma anche nell'intimità della loro vita privata e famigliare.
Serve un piano organico di sicurezza che promuova la diffusione capillare, anche ma non solo attraverso sgravi fiscali, di una serie di strumenti, la videosorveglianza e la vigilanza innanzitutto, ma anche ponti radio per collegamenti con le forze dell'ordine o serramenti anti sfondamento, che garantiscano sicurezza e tranquillità ai nostri cittadini.
Ed in quest'ottica ritengo sia fondamentale il contributo degli operatori della sicurezza, che con la loro esperienza possono aiutare noi politici a preparare un piano di difesa efficiente ed efficace.
Incontriamoci e lavoriamo insieme per il bene dei nostri cittadini!

Nel testo finale del comma 982 approvato dal Senato, la definizione delle modalità applicative della norma vengono demandate a un successivo decreto ministeriale. Considerando la complessità della materia, anche in relazione alla definizione dei requisiti tecnici degli apparati e di rispondenza alle normative vigenti dei fornitori, è prevedibile un coinvolgimento dei rappresentanti delle categorie interessate nella stesura del decreto attuativo? Quale sarà il ministero al quale verrà demandata la definizione del decreto?
Come ho già sostenuto in precedenza, credo che in un settore delicato e particolarmente complesso da un punto di vista tecnico come quello della sicurezza risulti fondamentale che il Ministero che avrà l'incarico di definire il Regolamento attuativo possa avvalersi dell'esperienza e della competenza degli esperti del settore. La creazione di un tavolo di consultazione tecnica - di cui mi farò promotore - sarebbe certamente un forte valore aggiunto e permetterebbe l'approvazione in tempi brevi di un Regolamento operativo che darebbe il via a nuovi investimenti nel settore.
Non dobbiamo perdere tempo, i nostri cittadini non lo meritano.

Chi deve gestire le minacce combinate? La sicurezza fisica o il dipartimento IT?

sintesi dell'articolo di Peter Houlis, managing Director di 2020 Vision System
pubblicato da Security Briefing – IFSEC Global
traduzione a cura di Federica Guizzo

Sono all'ordine del giorno i rapporti su attacchi informatici a sistemi di rete, di comunicazione e di informazione sponsorizzati da stati, gruppi estremisti e bande criminali organizzate; di conseguenza, i professionisti della sicurezza sono sempre più consapevoli della cosiddetta minaccia di tipo "combinato".

Un sondaggio condotto da BSI ha rivelato che a rappresentare la principale minaccia per la sicurezza delle informazioni sono i dipendenti cosiddetti "malintenzionati": il furto di informazioni e di dati viene infatti realizzato dal personale interno dell'organizzazione e da partner di fiducia. Si tratta, in altri termini, di *insider threat (minaccia interna)*.

Sebbene la pirateria costituisca una grave minaccia per la sicurezza dei dati (e molti esperti di Internet convengono che nel prossimo decennio gli attacchi informatici siano destinati ad aumentare), è solo uno dei modi in cui è possibile perdere le proprie informazioni. In realtà, ogni dipendente e ogni visitatore rappresentano una potenziale minaccia.

"Le lingue lunghe affondano le navi"

La perdita di informazioni può avvenire attraverso colloqui informali (per utilizzare il motto risalente alla seconda guerra mondiale, loose *lips sink ships*, ovvero letteralmente "le lingue lunghe affondano le navi"), l'uso improprio dei social media, la negligenza o l'utilizzo scorretto nelle fasi di registrazione e di trasferimento dei dati o a seguito di atto doloso o intenzionale di una persona di fiducia *"per ragioni quali la fama, la cupidigia, l'attitudine, interessi contrastanti o errate convinzioni"* (S. Bellovin (2008:7).

I metodi comprendono le intercettazioni, la rimozione delle apparecchiature informatiche aziendali o dei dati su supporto cartaceo, le fotocopie, il download su USB o dispositivi personali, il traffico illecito di e-mail, le fotografie mediante fotocamere digitali dei telefoni cellulari, ecc.

Nella mia azienda, come nella maggior parte delle aziende attuali, le informazioni (elenchi clienti, obiettivi di vendita, dati finanziari, dati relativi a dipendenti e fornitori, ecc.) esistono sia in formato cartaceo che elettronico, rendendole pertanto vulnerabili alle minacce sia a livello fisico che cyber.

Per svolgere le attività necessarie al buon andamento dell'azienda, i nostri dipendenti gestiscono quotidianamente informazioni di ogni tipo. Trattandosi dunque di un bene prezioso, è indispensabile tutelare tali informazioni da perdite accidentali o intenzionali durante il relativo trattamento o registrazione.

Il principale metodo fisico per ridurre la perdita di dati consiste in una politica di sicurezza del personale, poiché l'anello debole nella catena della sicurezza è costituito proprio dalle persone, sia per negligenza che per intento. Secondo l'*HMG Security Policy Framework* (Quadro normativo in materia di sicurezza del Governo del Regno Unito – aprile 2012: 31), *"la sicurezza relativa al personale è volta a garantire l'attendibilità, l'integrità e l'affidabilità dei dipendenti, degli appaltatori e del personale temporaneo"*.

Le pubblicazioni quale *Holistic Management of Employee Risk* (HoMER), a cura del CPNI e di PW Consulting (2012), forniscono alcune indicazioni utili su come implementare una politica di sicurezza rivolta al personale. A prescindere dalle indagini preliminari all'assunzione, si parla, tra le altre cose, di controlli in corso d'opera, valutazione del personale e formazione sulla consapevolezza in materia di sicurezza, per garantire che i dipendenti siano perfettamente al corrente delle minacce relative a tale ambito.

Politica della sicurezza delle informazioni

È possibile ridurre i rischi mediante una politica di clean desk (o di "scrivania pulita"), l'utilizzo opportuno dei social media e la corretta gestione e conservazione delle informazioni o dei dispositivi. Una politica della sicurezza delle informazioni fornisce le istruzioni utili per utilizzare, gestire, archiviare ed eliminare in tutta sicurezza le informazioni sensibili.

È fondamentale gestire e monitorare l'accesso alle informazioni da parte dei visitatori, e ciò si potrebbe tradurre, molto semplicemente, nel registrare ogni visitatore e seguirlo per tutta la durata dell'accesso. È necessario inoltre garantire che i luoghi in cui vengono memorizzati i dati siano protetti e che i documenti cartacei siano custoditi in tutta sicurezza. I PC non devono essere lasciati accesi e gli utenti devono disconnettersi quando si allontanano dalla propria postazione.

Un altro metodo efficace per limitare l'accesso a, da e nei pressi di una struttura è il sistema fisico di controllo accessi (ACS – *Access Control System*), che può fornire preziose informazioni su chi si trova all'interno della struttura, e dove e quando è consentito sostare in un dato luogo. Unitamente alla sorveglianza video, il

sistema di controllo accessi diventa uno strumento prezioso che consente di individuare e di analizzare, successivamente, gli eventi.

Oggi, la sicurezza fisica degli edifici in termini di serrature, sbarre e imposte è ovviamente fondamentale per quanto riguarda gli elementi di protezione, come nel caso dei sistemi antifurto progressivi.

Analogamente, è indispensabile proteggere i dati quando sono fisicamente in movimento: i dipendenti devono infatti considerare la sicurezza durante il trasporto su veicoli dei dispositivi informatici o delle informazioni. Antifurto per auto, archiviazione in sicurezza o dispositivi nascosti alla vista sono tutti metodi di sicurezza fisici, semplici ed efficaci, domestici o a uso professionale. Anche l'applicazione e la risposta sono aree di competenza del mondo della sicurezza fisica.

Le minacce di tipo combinato ai sistemi fisici e logici richiedono metodi di difesa sia fisici che logici: il cosiddetto approccio convergente. Se esiste nel mondo fisico, probabilmente la responsabilità spetta alla sicurezza fisica.

Al contrario, se esiste nel ciberspazio, come nel caso dei pirati informatici, allora la responsabilità è a livello di IT. Per fare un esempio, parliamo degli elementi di sicurezza logici o cyber quali l'autenticazione di accesso e i controlli delle autorizzazioni, gli antivirus e i sistemi di filtraggio dei contenuti, i firewall e le difese di rete. Ridurre i rischi richiede evidentemente il collegamento e la cooperazione di più elementi specifici delle varie discipline.

Convegno del Garante: La società sorvegliata, i nuovi confini della libertà

a cura della Redazione

In occasione della decima Giornata europea della protezione dei dati personali, il **Garante per la protezione dei dati personali** ha organizzato a Roma, presso l'Aula del Palazzo dei Gruppi parlamentari, il convegno dal titolo "La società sorvegliata - I nuovi confini della libertà" al quale hanno partecipato avvocati, magistrati, sociologi, giornalisti e il Sottosegretario alla Presidenza del Consiglio dei Ministri, **Marco Minniti**. Il convegno ha affrontato le problematiche derivanti dal rapporto tra privacy, sicurezza e controllo mettendo a confronto diverse opinioni.

Il presidente dell'Autorità Garante, **Antonello Soro**, ha sottolineato come tutti i cittadini siano soggetti ad un controllo continuo ed invisibile, riconducibile sia al potere pubblico che a quello dei privati. A ciò rimandano anche due recenti sentenze della Corte di Strasburgo, depositate il 12 gennaio 2016, una in materia di controllo datoriale dei lavoratori e l'altra in materia di intercettazioni da parte dei servizi, che confermano l'esistenza di nuovi confini della libertà e la necessità di regole precise in materia per evitare che venga meno la libertà stessa.

Soro ha ripreso il tema, più volte affrontato in passato, dei rischi connessi allo sviluppo di tecnologie sempre più invasive per la creazione di processi di raccolta e conservazione dei dati relativi, in particolare, alle attività su web dei singoli. Ogni attività sul web viene infatti analizzata da processi matematici (algoritmi) che tracciano il profilo degli utenti individuando le sue abitudini e interessi e, quando richiesto dal ricercatore, i livelli di rischiosità del soggetto profilato. Tuttavia, questa mole di informazioni rischia di creare una matassa informe di dati inidonea a tutelare la sicurezza ma solo limitativa del diritto alla riservatezza dei singoli. Problemi drammatizzati nell'attuale contrasto al terrorismo internazionale: i governi europei si stanno interrogando su come affrontare questa minaccia con il pericolo che, nella contrapposizione tra il diritto alla riservatezza e la tutela della sicurezza traverso la sorveglianza, prevalga quest'ultima, in base al principio dei vasi comunicanti.

Durante il convegno sono emerse opinioni divergenti su come i governi europei debbano affrontare la minaccia terroristica, ossia se una limitazione del diritto alla riservatezza dei singoli sia o meno un reale strumento per prevenire e contrastare gli attacchi, in particolare ad opera dell'Isis.

Secondo il sociologo Maurizio Ferraris nei sistemi

democratici la privacy non esiste, poiché la libertà non è un principio fondamentale a livello sociale; mentre il sociologo Giuseppe Roma individua nella democrazia, in quanto sistema resiliente, lo strumento per contrastare il terrorismo, poiché essa accetta una diminuzione dei diritti pur di salvaguardare la sicurezza. Diversamente, Marco Minniti, ritiene che il rinnegare i principi di libertà e limitare i diritti personali costituirebbe una sconfitta per l'Occidente e una vittoria per i terroristi. Per prevenire gli attacchi è necessario che via sia uno scambio di informazioni tra i vari stati.

RIFERIMENTI NORMATIVI

Italia

Codice in materia di protezione dei dati personali (**Decreto legislativo 30 giugno 2003, n. 196**)
(testo su http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196)

Allegati al Codice:

- Allegato A.1. - Codice di deontologia - Trattamento dei dati personali nell'esercizio dell'attività giornalistica
- Allegato A.2. - Codice di deontologia - Trattamento dei dati personali per scopi storici
- Allegato A.3 - Codice di deontologia - Trattamento dei dati personali a scopi statistici in ambito Sistan
- Allegato A.4- Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi statistici e scientifici
- Allegato A.5. - Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti
- Allegato A.6. - Codice di deontologia e di buona condotta per i trattamenti di dati personali effettuati per svolgere investigazioni difensive
- Allegato A.7. Codice di deontologia e di buona condotta per il trattamento dei dati personali effettuato a fini di informazione commerciale
- Allegato B. Disciplinare tecnico in materia di misure minime di sicurezza
- Allegato C. Trattamenti non occasionali effettuati in ambito giudiziario o per fini di polizia
- Tavola di corrispondenza dei riferimenti previgenti al codice in materia di protezione dei dati personali

Europa

Unione europea

- Carta dei diritti fondamentali dell'Unione europea
- Trattato di Lisbona
- Direttiva 1995/46
- Direttiva 2002/58
- Direttiva 2009/136
- Direttiva 2009/140
- Direttiva 2006/24
- Decisione del Consiglio 2008 615 GAI sul potenziamento della cooperazione transfrontaliera
- Decisione del Consiglio 2008 616 GAI sull'attuazione della decisione relativa al potenziamento della cooperazione transfrontaliera
- Decisione quadro del Consiglio 2008 977 GAI sulla protezione dei dati personali trattati nell'ambito della cooperazione in materia giudiziaria e penale

Consiglio d'Europa

- Convenzione europea sui diritti umani (testo su http://www.echr.coe.int/Documents/Convention_ITA.pdf)
- Convenzione 108/81
- Protocollo addizionale alla Convenzione 108/81
- Convenzione 185/2001 sulla criminalità informativa
- Protocollo addizionale alla Convenzione 185/2001

In particolare:

Art. 8 CEDU Diritto al rispetto della vita privata e familiare

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Sentenza Corte di Strasburgo del 12 gennaio 2016 in materia di controllo datoriale dei lavoratori

La Corte dei diritti dell'uomo è intervenuta sul tema del controllo datoriale sulla mail aziendale del dipendente, statuendo che, pur trattandosi di una ingerenza nel diritto alla vita privata del lavoratore, tale controllo è tuttavia compatibile con la Convezione dei diritti dell'uomo e dunque legittimo.

Security for Retail

SECURITY FOR RETAIL FORUM 2016

23 febbraio 2016
Palazzo delle Stelline, Milano

Security for Retail Forum 2016 è un seminario a inviti riservato agli operatori professionali della sicurezza del mondo della Distribuzione Organizzata e dei rappresentanti delle categorie degli esercizi commerciali di prossimità. E' l'appuntamento annuale esclusivo organizzato da **essecome/securindex.com** per affrontare e approfondire i problemi e presentare le soluzioni per la tutela del patrimonio aziendale del settore maggiormente esposto agli attacchi della criminalità predatoria.

In questa edizione si parlerà di:

Milano, città sicura per i negozianti? • ***Infedeltà dei dipendenti: cosa permette il Jobs Act***

Videosorveglianza e Loss Prevention • ***Soluzioni per la sicurezza del denaro in negozio***

Verrà inoltre presentato il **Laboratorio per la Sicurezza**, un progetto di aggregazione "post-associativa" per i security manager della Distribuzione.

14:00-14:30 Registrazione dei partecipanti

14:30
Sicurezza in vetrina, il punto della situazione
Raffaello Juvara
direttore essecome/securindex.com

14:40
Milano, città sicura per i negozi?
Questura di Milano, Comune di Milano, Associazioni di categoria

15:25
Il Barometro Mondiale dei Furti nel Retail 2015
Alberto Corradini
CheckPoint Systems

15:45
Soluzioni integrate per la sicurezza nei PdV
Maurizio Tondi
Axitea spa

16:00-16:30 Coffe break

16:30
L'uso proattivo della video sorveglianza per la prevenzione delle perdite
Pietro Tonussi
AXIS Communications

16:45
Infedeltà dipendenti, cosa permette il Jobs Act
Avv. Ezio Moro
giuslavorista Foro Torino

17:30
Gestione intelligente del denaro, ma in sicurezza
Luigi Rubinelli
Conforti spa

17:45
Presentazione del Laboratorio per la Sicurezza
Jerome Bertrume, Giuseppe Mastromattei, Federico Saini

18:30-19:00 Cocktail buffet

PARTNER

Gli interventi a Security for Retail Forum 2016

L'USO PROATTIVO DELLA VIDEO SORVEGLIANZA COME CONTRIBUTO ALLA PREVENZIONE DELLE PERDITE

La video sorveglianza degli esercizi commerciali è e sarà un sistema efficace per la prevenzione delle perdite, per le frodi e per la sicurezza del locale. Senza dubbio, così come succede per altri tipi di tecnologia utilizzate, l'effetto dissuasorio della telecamera perderà la sua efficacia man mano che i delinquenti conosceranno i limiti e i difetti del sistema di video sorveglianza. Le nuove tecnologie permettono di sanare alcune di queste limitazioni, aumentando il livello di difficoltà per i delinquenti ed elevando l'efficienza del sistema stesso, migliorando il ritorno degli investimenti. L'uso proattivo del sistema video consente di fare un'analisi più dettagliata dell'investimento da realizzare.

SOLUZIONI INTEGRATE PER LA SICUREZZA DEI PUNTI VENDITA

La sicurezza fisica dell'ambito Retail è un concetto sempre più integrato in termini di sistemi di allarme, video sorveglianza evoluta, automazione degli edifici, sicurezza delle persone che lavorano nel punto di vendita, della merce presente e controllo di tutta la filiera di distribuzione. Inoltre l'estensione degli attacchi e degli atti predatori allo spazio cyber-fisico, indirizza necessariamente anche l'ambito Retail e punti vendita. Dal mondo fisico, attraverso vulnerabilità tradizionalmente legate alla localizzazione (posizione periferica, viabilità, etc.) ai flussi di traffico (picchi di acquisto, code, etc.) , ai pattern compartimentali di dipendenti e consumatori, a consuetudini e debolezze strutturali e a fragilità tecnologiche (reti wireless, POS, tags, etc.); dal cyber, attraverso attacchi ai siti di e-commerce, al furto di carte di credito, identità ed atri dati sensibili anche sfruttando la diffusione dei social network. La risposta efficace per garantire coerentemente contromisure di difesa e protezione, passa per una forte integrazione tra formazione e professionalizzazione del personale dei punti di vendita, aumentando la consapevolezza dei consumatori/clienti e adottando tecnologie innovative inserite nella catena del servizio dalla prevenzione/rilevazione degli allarmi e delle situazioni di pericolo, alla gestione della situazione di rischio fino all'intervento.

GESTIONE INTELLIGENTE DEL DENARO, MA IN SICUREZZA

La società Conforti ha percorso, in più di un secolo, i corsi e ricorsi delle situazioni sociali che hanno determinato esigenze differenti nel tempo, corroborate dall'evoluzione tecnologica che ha contribuito a trasformare significativamente i tempi di azione e reazione nel "gioco di guardie e ladri". Fin dagli anni 80 ha sviluppato, assieme alla ricerca di materiali e soluzioni innovative per la resistenza fisica all'effrazione, sistemi elettronici e logiche per la protezione degli ambienti a rischio e per la gestione della sicurezza denaro introducendo funzionalità innovative in armonia con le nascenti esigenze del mercato che si andava spostando verso il trasferimento del contante tra gli esercizi commerciali e le banche e le sale conta. Oggi, che il rischio furto-rapina si è significativamente spostato sulle attività commerciali, Conforti non manca di proporre soluzioni tecnologicamente avanzate per la custodia intelligente del contante nelle diverse applicazioni d'uso e nei diversi contesti di rischio.

Security for Retail Forum 2016: quando la sicurezza del negozio non è solo un fatto privato - 1

di Raffaello Juvara

Occuparsi della sicurezza del commercio al dettaglio significa occuparsi di un settore che rappresenta il 25% del PIL italiano, impiega centinaia di migliaia di persone e investe 3 miliardi di euro all'anno in prodotti, soluzioni e servizi per la protezione delle merci e del denaro che movimenta. In tutti i Paesi, il commercio al dettaglio interagisce con le rispettive popolazioni come un'Infrastruttura Critica a ogni effetto, considerando le conseguenze che potrebbero derivare da eventuali interruzioni operative nella filiera.

In genere, questo tema viene affrontato esaminando i dati quantitativi dei reati predatori commessi a danno degli esercizi commerciali, ma con una curiosa asimmetria.

I media parlano di solito dei cosiddetti "reati predatori", ovvero dei furti e delle rapine subiti e denunciati all'Autorità giudiziaria dagli esercenti delle diverse categorie, il cui bottino complessivo si è attestato da qualche tempo attorno a 60 milioni di euro all'anno, compresi gli sportelli bancari e gli uffici postali con i loro bancomat, diventati la preda preferita dai malviventi (dati OSSIF/ABI 2015).

Quasi nessuno, al di fuori della cerchia degli addetti ai lavori, parla invece dei 3 miliardi all'anno di "differenze inventariali" patite solamente dai grandi Retailer, dovute per l'87% a furti dei clienti, appropriazioni dei dipendenti e truffe dei fornitori, secondo i dati dell'unico osservatorio che se ne occupa a livello internazionale, il Barometro Mondiale dei Furti nel Retail.

Solo gli ammanchi riconducibili alle appropriazioni da parte dei dipendenti ammontano a quasi 700 milioni di euro, oltre 11 volte il bottino complessivo dei reati predatori denunciati da tutte le categorie commerciali. Forse perché i gestori denunciano all'Autorità giudiziaria solo i casi più gravi o perché questa particolare microcriminalità è diffusa ovunque, il fenomeno non crea allarme sociale come i furti e le rapine ma costa al sistema distributivo oltre l'1% del fatturato, con un ribaltamento sui consumatori stimato in 208 euro all'anno per famiglia, oltre 90 euro a persona.

Il tema della sicurezza nel commercio al dettaglio non si esaurisce però con l'analisi dei reati predatori - dalle rapine a mano armata nelle boutique del lusso alle confezioni di prosciutto mangiate prima di passare alla cassa del supermercato - e delle relative precauzioni adottabili. I negozi sono, da sempre, anche un simbolo dei gruppi sociali ai quali appartengono e, come tali, bersagli naturali (e facili) dei rispettivi antagonisti.

Qualsiasi vetrina può venire infranta in occasione di disordini e sommosse in quanto icona da distruggere o magazzino da saccheggiare (vedi articolo successivo) ma, purtroppo, può anche diventare bersaglio di attacchi terroristici, come hanno dimostrato gli attentati di Parigi nel 2015. Oltre a racchiudere soldi e merci che interessano ai malviventi comuni, gli esercizi commerciali sono anche luoghi frequentati dalle persone normali che, malauguratamente, sono il vero bersaglio dei terroristi.

Tragica evoluzione, che ha trasformato i "luoghi della

normalità" - negozi, ristoranti, teatri, discoteche, alberghi eccetera – in altrettanti *soft target* per terroristi, definizione che sottintende l'impossibilità materiale da parte degli Stati di difenderli direttamente, come avviene invece per i siti considerati "sensibili" per la sicurezza pubblica. Questo obbliga un passaggio di livello nella valutazione dei rischi ai quali è esposto un punto vendita e nella conseguente configurazione delle misure di protezione, in un quadro di "sicurezza partecipata" di ancor maggiore rilevanza di quanto fosse in precedenza. Il dialogo e la collaborazione tra gli organi di polizia impegnati a difendere la sicurezza pubblica e gli operatori privati che devono tutelare il patrimonio aziendale possono infatti risultare determinanti per mitigare i rischi che attualmente minacciano l'intera Europa.

Un'esperienza consolidata di quanto possa essere positiva questa interazione è fornita dai sistemi di videosorveglianza installati all'interno e all'esterno degli esercizi commerciali. Quante volte i responsabili di un delitto commesso anche altrove sono stati identificati e rintracciati dalle forze dell'ordine, grazie alle riprese delle telecamere posizionate davanti all'ingresso del negozio? Oggi, un sistema evoluto di videosorveglianza digitale con analisi video può raccogliere e selezionare molti più dati dei precedenti sistemi analogici, dati utilizzabili sia per la tutela dell'esercizio commerciale che per le attività di intelligence preventiva e di investigazione forense da parte delle Forze dell'Ordine.

Le modalità di condivisione dei dati raccolti da un sistema di videosorveglianza privato, le regole e i termini per la conservazione delle immagini, ma anche la stessa configurazione dei sistemi devono essere dunque al centro di un dialogo permanente tra le Forze dell'Ordine e gli esercenti di ogni categoria commerciale, almeno quanto la condivisione delle procedure da adottare in caso di minaccia e la formazione specifica degli operatori. Esemplare a questo proposito la collaborazione tra Questura e farmacisti di Milano, che ha prodotto risultati eccellenti in termini di individuazione dei responsabili e di riduzione delle rapine commesse ai danni delle farmacie del capoluogo lombardo, grazie alla capillare formazione degli operatori e all'utilizzo di KeyCrime, l'esclusivo software predittivo a disposizione degli investigatori milanesi.

I grandi Retailer internazionali, la Grande Distribuzione Organizzata e i negozi di prossimità hanno diversi buoni motivi per cercare le soluzioni più adatte a tutela della propria attività, nella consapevolezza dell'indissolubile interazione tra sicurezza pubblica e sicurezza privata.

Per questo è necessario promuovere e rafforzare il dialogo tra tutti gli attori coinvolti nella sicurezza del commercio al dettaglio: i rappresentanti delle Forze dell'Ordine, i security manager del Retail e della GDO, le categorie di esercenti, i fornitori di tecnologie e servizi di sicurezza e, non ultimo, il decisore politico, per dare le risposte adeguate a chi "fa sicurezza", sia in forma diretta che partecipata. E' nell'interesse di tutti, nessuno escluso.

Security for Retail Forum 2016: quando la sicurezza del negozio non è solo un fatto privato - 2

di Raffaello Juvara

I violentissimi disordini sociali scoppiati nel 2011 in molte città della Gran Bretagna, prendendo di mira negozi di ogni genere con saccheggi e incendi, hanno rappresentato una doppia svolta nell'ordine pubblico internazionale. Da una parte, l'impiego dei social da parte dei dimostranti per organizzare gli assembramenti, impedendo alla polizia di intervenire in tempo per fermare gli attacchi, ha costituito un precedente riutilizzato successivamente nelle manifestazioni di piazza in ogni parte del mondo; dall'altra, i disordini del 2011 sono stati anche la prima occasione in cui Scotland Yard ha utilizzato in modo massivo l'analisi delle immagini raccolte dalle telecamere installate nelle strade per identificare i responsabili dei saccheggi.

Quanto successo nel 2011 è stato riesaminato in un articolo pubblicato di recente da un sito inglese specializzato in security, che affrontato il tema dell'importanza delle componenti passive per la protezione di un negozio *"soprattutto nell'era dei social media, dove i partecipanti agli scontri sono in grado di coordinare le loro attività, disperdersi velocemente da un posto per radunarsi nuovamente in un altro dove non vi sia la presenza della polizia per continuare a saccheggiare e a provocare danni. In un rapporto del 2011 sui disordini che hanno coinvolto le città del Regno Unito, il* ***Riots Communities and Victims Panel*** *ha dichiarato che i social network e le riprese televisive dei funzionari di polizia che osservavano la gente mentre 'saccheggiava a più non posso' hanno alimentato i disordini di Londra e delle altre città del Regno Unito."*

"I disordini civili e i relativi saccheggi degli esercizi commerciali sono un problema che i proprietari dei negozi che si trovano sulle vie principali delle città conoscono molto bene e al quale dovrebbero essere preparati. Nell'ambito di una battaglia continua e ormai tristemente nota per i negozianti, i produttori di serrande di sicurezza stanno rilevando l'importanza non solo di ricorrere a serramenti di sicurezza per una protezione efficace, ma anche di utilizzare il giusto tipo di serranda. Qualunque sia la causa, sia che si tratti di cortei di antagonisti o disordini provocati da qualsiasi forma di problema sociale, i tumulti, i saccheggi e le azioni con rilevanza anche penale possono propagarsi molto più rapidamente di quanto le forze dell'ordine riescano a sostenere con la mobilitazione e l'impiego dei loro uomini. Il saccheggio non è l'unico problema a interessare i negozianti e le altre attività commerciali che si trovano sulle vie principali delle città. Anche l'incendio doloso è una delle conseguenze degli scontri e, poiché molti proprietari dei negozi vivono all'interno dello stesso edificio o negli appartamenti sovrastanti,

la sicurezza dei locali potrebbe essere anche una questione di vita o di morte."

Il contributo mette in luce aspetti che rendono ancora più grave il tema della sicurezza dei negozi, dove la questione di vita o di morte è tristemente testimoniata da tutti i commercianti che hanno perso la vita per venire depredati degli incassi e delle merci e dalle più recenti vittime di attacchi terroristici.

Security for Retail è un'iniziativa editoriale nata per contribuire alla ricerca e alla divulgazione di soluzioni utili per ridurre i rischi dei commercianti di ogni categoria, rispetto alle minacce che li riguardano.

Il security manager nel retail secondo Federico Saini

a colloquio con Federico Saini, Profit Protection Manager – South Europe Adidas
a cura di Raffaello Juvara

Come viene affrontata dai grandi retailer internazionali l'evoluzione In corso nella security, determinata da una parte dalla trasversalità IT/Phy delle minacce, dall'altra dalla multifunzionalità dei sistemi e delle infrastrutture, concepiti in origine per security e loss prevention e oggi utilizzabili ad altri scopi, per esempio la business intelligence?
Stiamo vivendo un forte momento di crescita delle tecnologie volte a supportare il business. Il problema è che spesso queste tecnologie sono sviluppate dai dipartimenti IT e retail senza il coinvolgimento dei dipartimenti loss prevention e, di conseguenza, spesso i prodotti sono vulnerabili. Una volta la security si doveva "scontrare" solo con i visual. Per esempio, la tendenza a esporre i prodotti più belli/costosi nelle aree più a rischio, oppure la posizione dei sensori antitaccheggio spesso non andava a braccetto con la miglior posizione da un punto di vista security e cosi via. Oggi coinvolte ci sono anche le tecnologie IT, come ad esempio gli iPad o i chioschi per la consultazione dei prodotti in store, le vendite on-line (come click and collect), le tecnologie CCTV per lo studio dei flussi della clientela, sistemi di pagamento innovativi. Chiaramente tutte queste implementazioni portano all'apertura di nuovi rischi. In aggiunta, alcune tecnologie come, ad esempio, la citata videosorveglianza, possono essere utilizzate sia a scopo di business intelligence che per fini di sicurezza, creando problemi sulla gestione dei sistemi a causa delle differenti finalità degli stessi. Fondamentale è poi la sicurezza IT per evitare possibili

intrusioni nei sistemi aziendali da parte di terzi ed evitare frodi che possono costare care alle aziende. Oltre ai dati confidenziali dell'azienda, bisogna anche pensare ai dati sensibili dei clienti che si avvalgono dei nostri sistemi per portare a termine acquisti e che sono trattati dalle aziende.

Le minacce che oggi possono riguardare i punti vendita di un retailer internazionale non sono solamente determinate da atti predatori (rapine, furti, taccheggi) ma anche da atti dimostrativi (antagonismi, anarchismi) e terroristici, difficilmente prevenibili. Come si possono mitigare gli effetti di queste tipologie di attacchi?
L'unica maniera per mitigare gli effetti di queste tipologie di minacce è la formazione del personale responsabile dei negozi. Purtroppo, non si può essere preparati su tutto ma seguendo un'accurata formazione sulla gestione delle emergenze, ci si può adattare meglio ai casi specifici. Nozioni basilari come conoscere le vie di fuga e sapere dove queste portano, conoscere il proprio ambiente di lavoro anche in maniera più ampia (il centro commerciale, l'outlet), sapere come silenziare il cellulare, sapere quali ambienti possono essere chiusi a chiave e quali no, chi contattare e come descrivere l'evento sono i fondamentali per affrontare le emergenze. Purtroppo, questo tipo di formazione viene spesso solo fatta in maniera teorica e superficiale quando invece le prove dal vivo ripetute nel tempo sarebbero le più indicate. In Italia siamo culturalmente un po' poveri da un punto di vista di esercitazione sulle emergenze, anche se ci sono già notevoli miglioramenti rispetto al passato.

La continuità operativa di un punto vendita in relazione a eventi negativi (naturali, accidentali, volontari) è un elemento importante anche per il risultato economico di un retailer. Come può essere realizzata l'integrazione tra security e business continuity sul piano organizzativo?
Negli ultimi anni la prevenzione in termini di health and safety ha fatto passi da gigante sia da un punto di vista formativo che di prevenzione. Sia per una necessità di legge che per etica, le grandi multinazionali hanno implementato le funzioni di health and safety in Italia al punto da raggiungere ottimi livelli che sono spesso presi come esempio per implementare la sicurezza anche negli altri paesi. Ora è subentrato un nuovo tema oltre la prevenzione, il dopo emergenza. Anche noi in Adidas stiamo lavorando sulla business continuity in quanto crediamo che la tematica sia alquanto delicata e attuale. Non si era mai lavorato sul come sopravvivere a un'emergenza. La security è solo un tassello di questa complessa macchina, che coinvolge non solo la maggior parte dei partner interni ma anche quelli esterni. Basti pensare alla logistica con i magazzini esterni, eventuali server custoditi presso terzi e così via. Il poter accorciare i tempi di recupero da un'emergenza o essere in grado di utilizzare vie alternative per fare business è fondamentale per contenere le perdite, non solo da un punto di vista strettamente economico ma anche da un punto di vista servizio al cliente. Un esempio che mi viene in mente è la crisi che ha vissuto la Grecia di recente con la chiusura delle banche. L'impossibilità di versare contante e la mancanza di operatività finanziaria per un'azienda sono punti veramente critici e vanno risolti in maniera efficace e rapida per la continuità operativa e la sicurezza dei dipendenti. Grazie a un piano attuato con diligenza, si sono evitati impatti negativi sulle attività.

Tra le principali cause di differenze inventariali c'è l'infedeltà dei dipendenti che, secondo i dati forniti dal Barometro Mondiale dei Furti nel Retail, in Italia ha inciso nel 2014 per il 23% del totale delle differenze, un dato in linea con la media europea. Come viene affrontato il problema in Italia, dove le norme a tutela della privacy impediscono l'utilizzo pieno dei controlli a distanza dei dipendenti?
Il tema dell'infedeltà dei dipendenti è sempre un tema caldo e attuale. Il nostro approccio in materia è volto molto alla prevenzione soprattutto perché la repressione come diceva lei non è sempre possibile per via dei limiti imposti dalla legge. La formazione dei nostri dipendenti sul rispetto delle procedure è fondamentale. Il corretto rispetto delle procedure da parte dei manager e, di conseguenza, degli

addetti alle vendite rende più facile l'individuazione di eventuali problematiche e anche le tempistiche per la risoluzione risulteranno più brevi con effetti minori. Anche formare il management su come identificare eventuali situazioni sospette e come prevenire dando la corretta percezione di controllo è fondamentale per contenere le attività illecite. Oltre a questo, anche l'analisi dei dati (flussi di merce, differenze inventariali, operazioni cassa, audit…) è un altro ottimo strumento per l'individuazione di comportamenti scorretti e/o fraudolenti. In caso d'individuazione di atti illeciti, è fondamentale collaborare con le risorse umane per intraprendere i passi necessari senza esporre l'azienda a cause civili/penali.

Qual è oggi il profilo ideale del security manager di un grande retailer internazionale? Sono richieste competenze specifiche diverse da altri mondi (finanza, banche, trasporti ecc)?

Il mondo della sicurezza sta cambiando rapidamente. Mentre all'inizio la sicurezza era una forza preposta a reagire alle varie problematiche, si è poi passati alla prevenzione per arrivare ai giorni d'oggi nei quali viviamo una nuova fase di sviluppo per questo ruolo. Oggi il security manager, o per meglio dire Loss Prevention, deve avere anche ottime conoscenze in materia retail e business/finance in quanto solo facendo parte integrante del business si può creare la giusta prevenzione e salvaguardia dei profitti. Il retail è un settore molto particolare, quindi non è detto che professionisti specializzati in altri settori con competenze specifiche siano più adatti al ruolo. Per esempio, un security manager specializzato nella logistica può dare un contributo importante sulla parte distribuzione del prodotto, ma non è detto che

abbia competenze nella gestione del punto vendita e degli addetti alla vendita. Nel mondo retail, ci vuole un giusto mix di competenze e soprattutto un'ottima conoscenza delle dinamiche che si sviluppano nel punto vendita per conciliare il proprio ruolo con le esigenze di mercato e dell'azienda stessa. La cosa che potrebbe aiutare è invece creare uno spazio di incontro tra i vari esperti del settore nel quale condividere esperienze e opportunità per poter affrontare problematiche comuni in maniera più completa.

Jobs Act e videosorveglianza nei punti vendita: un workshop AXIS Communications per scoprire le ultime novità normative e tecnologiche

a cura della Redazione

Nell'ambito della riforma del lavoro e delle modifiche introdotte dal Jobs Act in materia di controllo a distanza dell'attività dei lavoratori e videosorveglianza, uno dei settori maggiormente coinvolti dalle nuove normative è sicuramente il Retail.
Quando parliamo di tecnologia al servizio del Retail, ci riferiamo agli ambiti più disparati: dalle applicazioni di security (la videosorveglianza) alla non security (safety in aree critiche) fino alla business intelligence. L'utilizzo più diffuso delle telecamere di rete e degli altri dispositivi di videosorveglianza IP rimane la cosiddetta "*security degli asset*", ovvero il monitoraggio degli investimenti effettuati dal singolo punto vendita e la prevenzione delle perdite (loss prevention). Ma ai responsabili della sicurezza di ogni catena di retail o punto vendita interessa molto conoscere come **poter utilizzare le telecamere** e gli altri dispositivi di videosorveglianza per contrastare in particolare un fenomeno che, secondo il Barometro Mondiale dei Furti nel Retail, è costato in un anno ai Retailer **678 milioni di euro, pari al 23% del totale delle differenze inventariali registrate in Italia nel 2014.**
Per tutti questi motivi **Axis Communications**, leader mondiale nel mercato dei sistemi con tecnologia video di rete e principale promotore della transizione dalla videosorveglianza analogica a quella digitale, ha organizzato lo scorso 1 dicembre 2015 presso la propria sede di Milano, un workshop dedicato a illustrare le **principali modifiche apportate dal**

Jobs Act in materia di controllo dei lavoratori e videosorveglianza nei punti vendita, per fornire un contributo concreto a questa importante e complessa tematica.
Nel corso del workshop, durante il quale sono intervenuti due avvocati giuslavoristi, **Roberto Alberto** e **Ezio Moro** del Foro di Torino, oltre a numerosi operatori della distribuzione al dettaglio, sono stati analizzati gli ultimi decreti attuativi del Jobs Act, per adeguare la disciplina dei rapporti di lavoro all'attuale realtà economica e tecnologica.
Tra le innovazioni introdotte, tre punti sono particolarmente rilevanti per l'intera filiera della sicurezza:
• L'abrogazione del divieto di controllo a distanza dei lavoratori.
• La possibilità di utilizzare apparecchiature di controllo per la tutela del patrimonio aziendale.
• La possibilità di utilizzare la videosorveglianza per fini connessi al rapporto di lavoro, nel rispetto della vigente normativa privacy.

L'incontro è stata un'importante occasione di confronto tra esperti e operatori del settore, con momenti di interazione tra i partecipanti con i professionisti e i rappresentanti di Axis Communications sull'argomento trattato. In un contesto come quello attuale, caratterizzato da numerosi dubbi e incertezze sulla corretta applicazione del nuovo articolo 4 della Legge n. 300/1970, il workshop ha messo in evidenza l'importanza dell'utilizzo proprio e improprio delle telecamere, della conoscenza delle aree di applicazione e delle soluzioni offerte dai professionisti del settore su un tema delicato e in costante evoluzione.
In questo senso un contributo importante può arrivare dalla professionalità dei team di Axis Communications: un gruppo di professionisti pronti a offrire tutta l'assistenza di cui ogni azienda necessità in un contesto sempre più complesso, in cui le normative spesso cambiano con una rapidità tale per cui è necessaria una consulenza personalizzata e su misura per conoscere le potenzialità del video di rete.
"Il nostro valore aggiunto – commenta **Pietro Tonussi, Business Developer Manager Southern Europe Axis Communications** – *è quello di poter assicurare la giusta soluzione ad ogni singola esigenza. Non a caso al workshop sul Jobs Act hanno partecipato manager della sicurezza provenienti da differenti realtà (moda, lusso, GDO, ecc.), ciascuno con le sue peculiarità e con le proprie esigenze di prevenzione e di monitoraggio dei punti vendita. Ognuno di essi, inoltre, si trova a dover gestire bisogni differenti a seconda dell'ubicazione del singolo punto vendita, con caratteristiche che cambiano a seconda dell'area soggetta a furti e situazioni critiche. Ed è proprio in questi casi che diventa fondamentale la qualità offerta dalle soluzioni Axis."* – aggiunge Tonussi.
Ci sono inoltre contesti in cui Axis Communications può diventare un partner tecnologico importante per l'aggiornamento dei propri prodotti, seguendo le disposizioni del Garante della Privacy e dei decreti attuativi portati avanti dal Jobs Act.
"Privacy mask, blurring, enchription sono caratteristiche presenti sulle telecamere Axis che permettono di proteggere la privacy personale. Senza dimenticare che se invece il singolo punto vendita si trovasse in una situazione critica, in presenza di frodi o di eventi particolari, Axis Communications ha la possibilità di garantire in ogni situazione la qualità d'immagine che le Forze dell'Ordine necessitano per scopi investigativi o forensi con l'aiuto di funzionalità come HD, Lightfinder, Wide Dynamic Range e altre soluzioni innovative." – conclude Pietro Tonussi di Axis Communications.

Numerose sono le soluzioni Axis Communications per il Retail. Un prodotto ideale per piccoli punti vendita è la AXIS F34, una soluzione di sorveglianza accessibile e discreta a quattro telecamere, dotata di hardware e software necessari per un sistema completo e integrato di monitoraggio e gestione video da remoto.
AXIS F34 fa parte di una serie di prodotti basata sul concetto di telecamera di rete destrutturata, vale a dire composta da sensori ottici con lente inclusa collegati con un cavo a un'unità principale che funge da corpo della telecamera, in grado di offrire la massima flessibilità agli installatori. La piccola unità sensore può infatti essere montata in modo discreto o in spazi ristretti, mentre l'unità principale può essere posizionata a distanza ovunque vi sia spazio.

Per approfondire l'argomento non perdete l'opportunità di parlare direttamente con Axis Communications che sarà presente all'evento Security for Retail Forum in programma il 23 febbraio a Milano presso il Palazzo delle Stelline.

Jobs Act, è possibile il controllo dei dipendenti in negozio, ma…

a colloquio con l'avv. Ezio Moro, del Foro di Torino
a cura della Redazione

Cosa è realmente cambiato, in generale, sui controlli a distanza dei lavoratori rispetto alla disciplina precedente a seguito dei decreti introdotti dal Jobs Act?

Vorrei chiarire subito che, sul tema dei controlli a distanza, non vi è stata alcuna "rivoluzione copernicana"; più semplicemente, il nuovo art. 4 dello Statuto dei Lavoratori tiene conto dell'evoluzione tecnologica e tenta di contemperare le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore nello svolgimento della prestazione di lavoro.

La nuova formulazione della norma introduce tuttavia alcune significative novità.

In primo luogo, si distingue da un lato gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori; dall'altro, gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa (PC, telefoni, tablet etc) e gli strumenti di registrazione degli accessi.

I primi possono essere installati ed utilizzati, previo accordo sindacale o autorizzazione ministeriale, non solo per esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma anche per esigenze di tutela del patrimonio aziendale. I secondi non necessitano di accordo/autorizzazione.

Per quanto riguarda poi le procedure autorizzatorie, si prevede che, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, l'accordo sindacale possa venire stipulato, oltre che con le singole RSA / RSU, anche

con le associazioni sindacali comparativamente più rappresentative sul piano nazionale; in caso di mancato accordo, è possibile richiedere l'autorizzazione direttamente al Ministero del Lavoro e delle Politiche Sociali.

Infine, si riconosce la facoltà per il datore di lavoro di utilizzare le informazioni raccolte attraverso i suddetti impianti e strumenti a tutti i fini connessi al rapporto di lavoro, a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e dell'effettuazione dei controlli, nel rispetto dei principi del Codice della Privacy.

Ancora oggi, dunque, sono consentiti esclusivamente i controlli c.d. preterintenzionali, ossia quei controlli che sono l'effetto indiretto della presenza di sistemi di controllo, il cui fine principale è quello di soddisfare esigenze organizzative, produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale.

Questo significa che, pur se oggi non vi è più un espresso e generalizzato divieto di controlli a distanza sull'attività del lavoratore attraverso strumenti tecnologici, il datore di lavoro non può legittimamente utilizzare strumenti ed impianti che abbiano quale unico fine quello di controllare continuativamente la qualità della prestazione ed i ritmi di lavoro da parte del lavoratore.

Il controllo della prestazione lavorativa non può, in altre parole, estendersi al punto da eliminare ogni zona di riservatezza e di autonomia del prestatore di lavoro.

Ora è possibile utilizzare legittimamente i sistemi tecnologici a tutela del patrimonio aziendale in negozio per contrastare atti di infedeltà del personale?

Certamente sì. La nuova formulazione della norma prevede espressamente che i sistemi di controllo tecnologici possono essere utilizzati non solo per esigenze organizzative e produttive ovvero di sicurezza del lavoro, ma anche per esigenze di tutela del patrimonio aziendale. Inoltre, innovando rispetto al passato, si prevede che le informazioni raccolte attraverso tali sistemi possono essere utilizzate a tutti i fini connessi al rapporto di lavoro e, dunque, anche a fini disciplinari.

Esemplificando, il datore di lavoro si potrà avvalere delle immagini registrate da un sistema di videosorveglianza quale prova per contestare e sanzionare eventuali ammanchi di denaro o sottrazioni di beni aziendali da parte dei dipendenti.

Si è quindi superata la teoria dei "controlli difensivi", elaborata dalla giurisprudenza sotto la vigenza della vecchia norma, in base alla quale il divieto di controllo a distanza dei lavoratori non si applicava nel caso in cui il controllo fosse diretto ad accertare comportamenti illeciti dei lavoratori e non riguardasse direttamente od indirettamente la prestazione lavorativa.

Occorrerà, però, prestare molta attenzione al fatto che oggi, a differenza che in passato, le informazioni raccolte attraverso gli impianti e strumenti tecnologici possono essere legittimamente utilizzate a condizione che il datore di lavoro provveda ad informare il lavoratore sulle modalità di utilizzo di tali strumenti e sui controlli che si riserva di effettuare.

Questo significa che d'ora in avanti la partita circa l'utilizzabilità in giudizio di tali informazioni si giocherà, oltre che sulla presenza, ove necessario, dell'accordo sindacale o dell'autorizzazione ministeriale, anche sulla prova dell'esistenza di idonei regolamenti e *policy* aziendali circa le regole poste dal datore di lavoro sull'uso degli strumenti tecnologici e sui relativi controlli.

Controlli che dovranno avvenire nel rispetto dei principi del Codice Privacy (liceità del trattamento dei dati, pertinenza, correttezza e non eccedenza del trattamento).

Occorrerà, dunque, per ciascun strumento ed impianto adottare specifici regolamenti aziendali da pubblicizzare adeguatamente, pena il rischio di non potere utilizzare in giudizio le informazioni raccolte.

Al riguardo, è illuminante un recente provvedimento del Garante della Privacy (provvedimento n. 450 del 30.7.2015) con il quale è stato sottolineato che l'assenza di una specifica *policy* circa la modalità di utilizzo degli strumenti aziendali può determinare una legittima aspettativa del lavoratore di confidenzialità.

Dunque, per ogni singolo impianto o strumento occorrerà predisporre un apposito regolamento al fine di:

i) individuare quali siano le modalità di utilizzo ritenute normali e consentite;

ii) adottare opportune misure organizzative e tecnologiche volte a prevenire il rischio di utilizzi impropri in modo da limitare i controlli successivi;

iii) esplicitare quali sono le informazioni memorizzate temporaneamente e per quanto tempo e chi vi può accedere;

iv) se, in quale misura e con che modalità il datore di lavoro si riserva di effettuare controlli;

v) prevedere una gradualità nei controlli, prevedendo prioritariamente dei controlli su dati anonimi ed aggregati e solo successivamente controlli individuali;

vi) specificare quali provvedimenti di natura disciplinare il datore si riserva di adottare in conseguenza delle irregolarità eventualmente riscontrate.

In questa materia, diritto del lavoro e diritto della privacy saranno sempre più strettamente intrecciati.

Ordinary, Intelligence, Special: quale security player è corretto usare per l'anti taccheggio?

a colloquio con con Luigi Alfieri, presidente di CSA Security
a cura della Redazione

Secondo i dati forniti dal Barometro Mondiale dei Furti nel Retail, nel 2014 le differenze inventariali sono costate 2,95 miliardi di euro al solo gruppo di retailer italiani che partecipano alla ricerca condotta da Checkpoint System. Il dato, pur ancora molto elevato, è in discesa per il secondo anno consecutivo, grazie agli investimenti in sistemi e servizi di prevenzione, con questi ultimi utilizzati dal 75% del campione intervistato. Qual'è il valore aggiunto apportato ai retailer da un'organizzazione specializzata come CSA Security?

Non ci è dato conoscere il campione di aziende del retail, utilizzato nella ricerca condotta dalla Checkpoint System, ma a prescindere dalla loro composizione, il dato relativo ai 2,95 miliardi di euro è oggettivamente un valore critico.

La ricerca della maggiore redditività, da parte di dette aziende, non può prescindere dall'impiego di società specializzate in sistemi di sicurezza e/o di prevenzione, con il precipuo fine di monitorare, studiare e combattere il fenomeno delle perdite attraverso azioni ad hoc in relazione alle peculiari caratteristiche di ogni azienda.

La specifica preparazione ed esperienza, per quanto riguarda i servizi, determina risultati concreti che migliorano non solo i dati inerenti le perdite, bensì anche il "livello di salubrità ambientale" che con l'eliminazione o la riduzione di *shoplifther* all'interno dei punti vendita, favoriscono non solo le stesse vendite ma generano nell'immagine collettiva degli avventori del negozio l'idea di un **"ambiente sicuro"**.

Immaginate di essere all'interno di un negozio per l'acquisto di un prodotto e potere osservare, girando per gli scaffali, uno *shoplifter* che tenta o ruba un prodotto.

Questa esperienza, negativa per chiunque, scoraggia l'acquisto generando in alcuni un senso d'insicurezza dando pulsione al proprio allontanamento dall'area insicura, in altri genera l'idea di poter "replicare" il comportamento criminale, trasformando il cliente "sano" in uno *shoplifter* improvvisato.

Facile pensare che l'incontrollata frequenza degli eventi negativi conduca alla esponenziale possibilità che i due casi accennati possano drasticamente evolvere al peggio.

Ad aggravare le cose, sono le perdite determinate dagli *"insider"* che colpiscono con tecniche, nella maggior parte delle volte più raffinate degli *outsider*, ovvero con maggiori informazioni relative ai sistemi di sicurezza oltre che agli agenti di sicurezza impiegati nelle strutture, con particolare riferimento a quelli *undercover*.

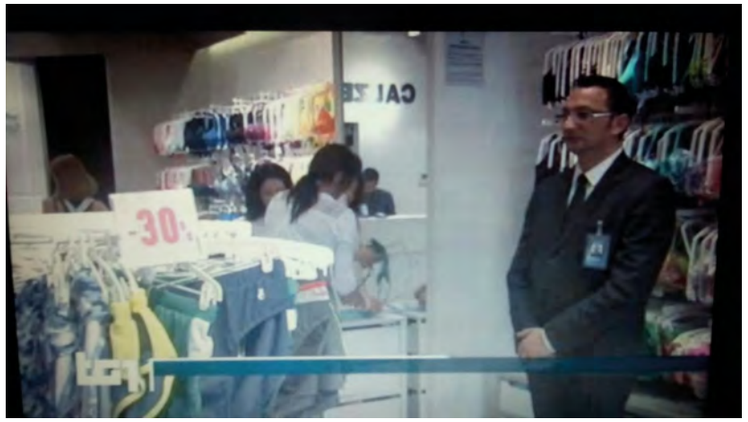
La risposta ad una così complessa situazione ambientale, non può essere affidata alla sorte dovendo ricorrere necessariamente ad una strategia chiara che

possa determinare, con certezza, i costi da considerare nel budget da dedicare ad ogni singolo negozio.
L'alternativa è subire passivamente le conseguenze delle perdite stesse.
L'atteggiamento ricorrente delle aziende del retail spesso sposa l'idea che la "cura" non può essere più costosa del "male" (perdite), anche se la forte competitività, in tutti i settori, ha finalmente portato molti a pensare di investire in servizi specializzati per arrivare a contenere e controllare le perdite, senza essere soggetti ad oscillazioni improvvise nella curva di analisi delle perdite stesse che causano anomalie in tutte le divisioni delle aziende con particolare riferimento, poi, al conto economico.
La CSA Security ha fatto del settore retail il proprio core business, specializzandosi e sviluppando specifico know-how che permette alla propria clientela livelli di controllo delle perdite sicuramente sostenibili e in alcuni casi con risultati eccezionali.
La capillare presenza di operatori su tutto il territorio nazionale, la specifica esperienza in tutti i settori del retail, la storicità della CSA Security in campo investigativo e di sicurezza e lo sviluppo di un metodo di contrasto ormai più che collaudato, sono valori di eccellenza che ci permettono di essere partner strategico di numerose e importanti aziende del retail.

Tra le principali cause di differenze inventariali c'è l'infedeltà dei dipendenti che, sempre secondo il Barometro, in Italia ha inciso nel 2014 per il 23% del totale delle differenze. Come possono contribuire gli operatori di sicurezza per mitigare questa situazione, nel rispetto delle norme a tutela della privacy dei dipendenti?
Si parlava prima di *"insider"* indicando con tale termine i dipendenti di una determinata struttura che, forti della loro posizione lavorativa, delle conoscenze ambientali (sistemi di allarme, telecamere, bug nelle procedure di vendita, operatori della sicurezza ecc…) agiscono, spesso indisturbati, sottraendo merce presente nei luoghi di lavoro.
Indiscutibilmente parliamo di soggetti con un più alto profilo di pericolosità rispetto agli *outsider*, in relazione alla maggiore possibilità di agire indisturbati.
Spesso gli *insider* sono gli autori dei furti più clamorosi per non dire costosi e, proprio per questo motivo, l'impiego di personale di sicurezza, deputato al contenimento delle perdite, deve avere una profilazione particolare, non di basso livello, affinché il denaro speso dai retailer possa essere portato a rendita e non a perdita.
Il mercato italiano della sicurezza offre ai retailer la possibilità di poter utilizzare all'interno delle proprie strutture operatori per servizi fiduciari, investigatori e guardie giurate che, attraverso i loro servizi determinano il controllo delle perdite, aumentando la redditività.
Le attuali normative, per quanto sotto alcuni aspetti fumose, indicano la strada da seguire e i criteri per il loro impiego, non tralasciando le note che delineano il raggio di azione che non deve essere oltrepassato a danno della privacy dei dipendenti.

Guardie giurate, operatori investigativi, addetti fiduciari: a quali criteri si devono attenere i retailer per impiegare correttamente le diverse figure di operatori di sicurezza?
La domanda è tutt'altro che semplice e impone una linea chiara nell'esposizione di un concetto che cercherò di trasferire senza troppi sofismi o richiami continui ad articoli di legge.
Preso un insieme di operatori denominato ***"Security Player"*** dobbiamo classificare tre sotto insiemi che chiameremo ***"Ordinary"***, ***"Intelligence"*** e ***"Special"***
La scelta di denominare il primo insieme *"Ordinary"* si basa proprio sulla caratteristica di questo tipo di operatori che nel mercato italiano sovente sono chiamati portieri oppure operatori fiduciari che assolvono a funzioni di sicurezza ordinarie, quali attività di portierato per la custodia, la sorveglianza, la fruizione di immobili, ivi compreso il controllo degli accessi e la regolazione del flusso di persone e merci, dove non sussistano le particolari esigenze di sicurezza di cui al D.M. n.269/2010.

Il gruppo *"Ordinary"* non può assolvere anche alle funzioni del gruppo *"Intelligence"* e *"Special"*.
La seconda categoria *"Intelligence"* appartiene ai dipendenti delle agenzie investigative (è richiesta la licenza ex art. 134 T.U.L.P.S. per l'esercizio specifico) comunemente chiamati "operatori antitaccheggio investigativo".
Tali operatori è possibile impiegarli solo attraverso un mandato investigativo commissionato all'istituto per *"…le attività di investigazione, ricerche e raccolta di informazioni per conto di privati, ivi comprese quelle relative agli ammanchi di merce ed alle differenze*



inventariali nel settore commerciale…". Le funzioni di questo gruppo si estrinsecano in una serie di controlli procedurali atti alla redazione di rapporti/ report informativi contenenti, a titolo esemplificativo, indicazioni dei reparti maggiormente colpiti, indicazioni dei malfunzionamenti dei dispositivi di difesa passiva, ovvero la mancata attivazione degli stessi da parte del personale dipendente, indicazioni delle deficienze procedurali di tipo logistico nel processo di approvvigionamento della merce, ovvero nel processo di vendita della stessa, anche attraverso l'individuazione di errori nei titoli di acquisto dei clienti dei locali commerciale con conseguente errata consegna di merce, generante differenze inventariali in minus o plus. L'individuazione di *shoplifter*, attraverso attività di osservazione statica e dinamica, riprese video/fotografiche, **col fine di comprendere le tecniche utilizzate dagli stessi per sottrarre la merce dalla struttura commerciale** e utilizzando, laddove necessario, anche lo strumento dell'intervista, utile a rendicontare in maniera più dettagliata i report informativi richiesti dal retailer.

Il gruppo *"Intelligence"* può assolvere anche alle funzioni del gruppo *"Ordinary"* ma non quello *"Special"*.
Infine, la terza categoria, quella denominata *"Special"* appartiene alle Guardie Particolari Giurate (G.P.G.) dipendenti da Istituti di Vigilanza Privata (è richiesta la licenza ex art. 134 T.U.L.P.S. per l'esercizio specifico); tale denominazione deriva dalla speciale disciplina riservata alle G.P.G.
L'attività si concretizza nella sorveglianza di beni esposti alla pubblica fede, nell'ambito della distribuzione commerciale, finalizzata, mediante osservazione, sia di persona che a mezzo impianti di videosorveglianza, a prevenire il furto e/o il danneggiamento dei beni stessi. Il servizio va espletato di norma in uniforme e con l'arma.

Il gruppo *"Special"* può assolvere esclusivamente alla sua funzione essendogli vietato espletare quanto previsto per il gruppo *"Intelligence"* e *"Ordinary"* fatto salvo quanto previsto dalle particolari esigenze di sicurezza di cui al D.M. n.269/2010.
Tralasciando le altre attività in ambito sicurezza, quella relativa al contenimento delle perdite, riguarda principalmente il gruppo ***"Intelligence"*** e ***"Special"*** lasciando al gruppo ***"Ordinary"*** solo una funzione di deterrenza indiretta senza alcuna possibilità di poter surrogare le altre due figure.
Nota importante per i retailer è che i gruppi soggetti ad autorizzazione di polizia (ex art. 134 T.U.L.P.S.) devono attenersi alla preventiva comunicazione dei nominativi alla prefettura competente in merito alle liste dei propri dipendenti che devono possedere i requisiti richiesti dall'art. 11 del medesimo Testo Unico circa l'idoneità morale, pena il licenziamento. Inutile sottolineare l'importanza di tale requisito in ambiente retail.

Quali sono le competenze richieste a un operatore investigativo impiegato in un punto vendita, che lo differenziano dalle altre figure?
La capacità di effettuare un ragionamento induttivo e deduttivo per costruire e riconoscere il profilo criminale dello shoplifter sommata alle doti di comunicazione

sintetica e alla spiccata capacità di osservazione differenziano l'investigatore in ambito retail da ogni altra figura del settore della sicurezza.
Non esistono scuole specifiche per questo tipo di attività, gioca pertanto un ruolo chiave l'esperienza nel settore con particolare attenzione all'essere capace di adattarsi ai diversi ambienti (es. Supermercati, Negozi di abbigliamento, boutique di lusso ecc...), così come la formazione acquisita all'interno della/e aziende ove si è prestato servizio.

Descrizione Profilo	*Attività consentite*												
Gruppi	Controllo accessi	controllo afflusso e deflusso clienti	controllo parcheggi	controllo area per individuazione shoplifter	attività investigativa sui dipendenti	Controllo scontrini per controllo differenze inventariali	report informativi/investigativi	Intervistare uno shoplifter	chiamare le FFOO per denunciare uno shoplifter	Controllo CCTV in Control Room	Vigilanza attivà sui beni esposti alla pubblica fede	Prevenzione reati di dannegiamento	Licenza richiesta
Ordinary attività di portierato per la custodia, la sorveglianza, la fruizione di immobili, ivi compreso il controllo degli accessi e la regolazione del flusso di persone e merci	√	√	√										
Intelligence attività di investigazione, ricerche e raccolta di informazioni per conto di privati, ivi comprese quelle relative agli ammanchi di merce ed alle differenze inventariali nel settore commerciale.	√	√	√	√	√	√	√	√					√
Special sorveglianza di beni esposti alla pubblica fede, finalizzata, a prevenire il furto e/o il danneggiamento dei beni stessi. Il servizio va espletato di norma in uniforme e con l'arma.									√	√	√	√	√

Quali sono le caratteristiche peculiari di CSA, sul piano organizzativo e della formazione?
In un clima di forte competizione commerciale per il mondo dei retailer, ove le strategie di saving sono all'ordine del giorno e la frontiera dei network utilizzati nel passato, cede il passo alle organizzazioni capaci di dare copertura in ambito nazionale o internazionale come la CSA Security, la capacità di erogare servizi a 360° con personale alle dirette dipendenze della nostra azienda genera vantaggi al committente ineguagliabili, sia dal punto di vista della qualità oltre che della capacità di fare economia di scala.
Avere CSA Security come unico referente permette la riduzione non solo dei costi, bensì anche dei tempi necessari per interfacciarsi con le moltitudini di aziende, quando il "parco fornitori" è ampio.
Il senso logico di creare una struttura capillare e, quindi, di offrire su area internazionale l'erogazione dei servizi fa di noi un provider strategico capace di assicurare, anche attraverso garanzie tangibili, risultati eccellenti.
L'organizzazione costruita dietro ad ogni singolo operatore è una macchina collaudata da ormai 18 anni fatta di dipartimenti operativi, legali, risorse umane, che si preoccupano di erogare formazione tanto in sede quanto *on the job* sempre con personale Senior, veterano del settore.
Una particolare nota va fatta al dipartimento IT che permette alla nostra azienda di erogare servizi con un alto livello informatico oltre che informativo.

La cassaforte in negozio dev'essere intelligente ma soprattutto sicura!

a colloquio con Luigi Rubinelli, CEO di Conforti spa
a cura della Redazione

L'ultimo Rapporto Intersettoriale sulla criminalità predatoria di OSSIF ha riportato che nel 2014 l'indice di rischio rapina dei punti vendita della DMO (Distribuzione Moderna Organizzata) è aumentato a 14,6 per gli attacchi riusciti e 18 per quelli tentati. In pratica, quasi un punto vendita su cinque ha subito un tentativo di rapina, in controtendenza rispetto a tutti gli altri settori monitorati dal Rapporto. Come si può spiegare questo andamento?

Il rischio "predatorio" è un rischio che esiste da sempre laddove esistono dei valori. Il rischio è una situazione possibile determinata dal pericolo, in questo caso dall'esistenza del valore che, però, assume connotazioni relative in funzione della considerazione che le persone o il mercato danno a questi valori. Un ricordo familiare può avere un valore affettivo inestimabile anche se il valore commerciale è irrisorio. Un computer che contiene i progetti di un'azienda o di un professionista, ha un valore commerciale di poche centinaia di euro, ma un valore enorme per chi lo perdesse. Quindi l'idea di Sicurezza deve essere strutturata per i singoli casi e settori, per individuare quali siano i pericoli esistenti e quali siano le probabilità che questi pericoli si possano trasformare in perdita di valori, anche non necessariamente venali.
La società Conforti ha percorso, in più di un secolo, i corsi e ricorsi delle situazioni sociali che hanno determinato esigenze differenti nel tempo, corroborate dall'evoluzione tecnologica che ha contribuito a trasformare significativamente i tempi di azione e reazione nel "gioco di guardie e ladri". Fin dagli anni 80 ha sviluppato, assieme alla ricerca di materiali e soluzioni innovative per la resistenza fisica all'effrazione, sistemi elettronici e logiche per la protezione degli ambienti a rischio e per la gestione della sicurezza delle casse servizio. Sono state introdotte funzionalità innovative, in armonia con le nascenti esigenze del mercato che si andava spostando verso il trasferimento del contante tra gli esercizi commerciali e le banche e le sale conta.
Ma non è solo la tecnologia che nell'ultimo ventennio ha modificato i termini di confronto tra le parti. Si è aggiunta una mutata condizione sociale dovuta ai flussi migratori e, in questi anni, la crisi economica ha acutizzato questa situazione favorendo l'utilizzo di

contante a causa della ridotta fiducia dei risparmiatori negli Istituti di Credito. Sostanzialmente, sono mutati gli obiettivi della criminalità e spesso anche le motivazioni. Le banche, che beneficiano degli investimenti in sicurezza degli anni passati, oltre ad una ridotta dotazione del contante per il diverso profilo commerciale assunto, non sono appetibili come certe attività di vendita al dettaglio, diventate obiettivi primari del rischio predatorio. I supermercati concentrano gli incassi dei molti negozi di quartiere ormai spariti, le tabaccherie diventano centri di pagamento, le stazioni di servizio, le farmacie, ecc. In sostanza, attività un tempo considerate a basso rischio, oggi si trovano ad essere ad alto rischio senza aver sviluppato la necessaria esperienza organizzativa e tecnologica.

Quali sono le soluzioni oggi disponibili per proteggere il denaro e, di conseguenza, il personale e i clienti nelle diverse tipologie di punti vendita, dagli ipermercati ai negozi di prossimità a rischio, come le tabaccherie e le farmacie?

Per contrastare la sottrazione di denaro contante, è sicuramente efficace il metodo di non renderlo "preda" facile e veloce. Noi non crediamo che possa mai avvenire la completa virtualizzazione dei pagamenti per ovvie considerazioni di diritto, ma anche per le "falle" nella sicurezza che il mondo dell'informatica dimostra ogni giorno e per la scarsa fiducia che la gente ha degli Istituti di Credito. Quindi, per ora e nei prossimi anni, una soluzione valida rimane quella di non lasciare disponibile il contante superfluo, non necessario per le operazioni in corso. Il contante in eccesso può essere immagazzinato in ambiti sicuri per una successiva contabilizzazione e movimentazione in condizioni protette. Questa prassi è nota da tempo e attuata con casse di deposito temporaneo assoggettate a programmazioni temporali più o meno sofisticate. Da non trascurare, tra i rischi di cui si tratta, che esiste anche il rischio infedeltà ovvero la possibilità che avvengano sottrazioni di denaro da parte del personale dipendente. Quindi, oltre al rischio rapina, nello studio di soluzioni di sicurezza si deve considerare anche il rischio furto e il rischio infedeltà. Il contenitore che custodisce il denaro in eccesso durante il giorno, tipicamente ai fini antirapina, se lo custodisce anche durante una o più notti, non può essere solo un contenitore metallico, ma una struttura intelligente e molto robusta. Sistemi che consentono l'utilizzo di contenitori leggeri e poco impegnativi, es. i macchiatori di banconote, sono in alcuni casi efficaci, ma molto costosi nel tempo, anche perché soggetti a manutenzione continua, oltre che a guasti o attivazioni improprie. Conosciamo i disguidi e i costi di un innesco di tali sistemi.

Parliamo alla fine di sistemi di custodia intelligenti del denaro con contabilizzazione diretta presso l'Istituto di Credito, che riducono efficacemente il rischio rapina e infedeltà e dovrebbero ridurre anche il rischio furto. E' noto che non sempre avvengono prelievi quotidiani nei punti vendita e, quindi, possono restare ingenti somme custodite durante i periodi senza presidio di personale. Per questo motivo, il punto vendita diventa un obiettivo a rischio elevato non solo per la sottrazione del denaro ma anche, e a volte soprattutto, per i danni collaterali come la distruzione di infissi e arredi e della struttura stessa del negozio, oltre al fermo attività e al danno di immagine. Se il contenitore di sicurezza è una Cassaforte con la "C maiuscola", adeguata a resistere il tempo necessario per assicurare un intervento certo, si ottiene un ottimo effetto deterrente, perché un'azione palesemente difficile costituisce un rischio troppo elevato per chi la compie, mentre riduce l'impegno di chi provvede ad evitarlo. E' naturalmente scontata la presenza di un sistema di allarme altrettanto efficiente e efficace.

Quali sono le proposte di Conforti?

Questi concetti si traducono in un prodotto altamente resistente, molto intelligente sia per il controllo della sua sicurezza, sia per la regolare gestione delle operazioni che lo utilizzano. Conforti, oltre alle innovative proposte di protezione fisica con funzionalità evolute, propone casseforti intelligenti con uno o due accettatori di banconote collegabili in rete (attualmente su piattaforma Knox) per l'accredito diretto presso l'Istituto di Credito e contemporaneamente con Mercurio, il sistema di monitoraggio in tempo reale sviluppato da Conforti per il controllo delle funzionalità della cassaforte e delle apparecchiature contenute. Non solo, è possibile che la cassaforte Conforti si colleghi con il sistema di allarme per scambiare informazioni e centralizzarle, offrendo un ottimo strumento sinergico di controllo anche delle situazioni impiantistiche. Quindi, il sistema è dotato di controlli locali e remoti ridondanti che azzerano le incertezze di qualsiasi situazione dubbia, fonte di ben noti contenziosi fra le parti in causa. La cassaforte si autocontrolla e controlla le operazioni, rendendo evidenti queste attività anche localmente a chi esegue le operazioni in quel momento. Questa caratteristica ha un'enorme efficacia sulla regolarità degli usi, in quanto aiuta l'utente a svolgere regolarmente le operazioni e, nel contempo, gli rende noto che tutto quello che fa è controllato, con un importantissimo effetto deterrente per eventuali malpensanti. Per arrivare a ciò, ovviamente, non può essere sufficiente una serratura elettronica a sé stante, ma occorre un sistema integrato. Infatti, la sola serratura elettronica, per quanto evoluta, potrà gestire sé stessa e fornire la memoria delle operazioni eseguite su essa stessa. Se la cassaforte è accessibile a più persone o addirittura a servizi terzi, è evidente che in caso di contradditorio la disponibilità delle informazioni di quanto accaduto rivesta importanza primaria. In sintesi, tutto questo noi lo chiamiamo Fisitronica® e la nostra offerta viene facilmente "confezionata" sulle esigenze del cliente a partire dal dimensionamento della sicurezza fisica, alla dotazione dei contenuti tecnologici per le funzionalità operative con la personalizzazione dei software, ai controlli con la progettazione dei sistemi di allarme e TVCC fino al servizio di monitoraggio remoto sia degli stati tecnici, funzionali e di sicurezza. Siamo convinti che lo scopo principale della sicurezza sia la prevenzione: ridurre cioè il rischio che i pericoli si traducano in danno e la dissuasione è un sistema formidabile.

In uno scenario in cui tipicamente i devices sono funzionali al cash-management, le vostre soluzioni vengono proposte al gestore del servizio (Banca o CIT) o all'utente finale? In cosa possono differenziarsi i due diversi approcci?

Proponendoci come "progettisti" della sicurezza, quindi anche di impianti di allarme, videosorveglianza e servizi tecnici su tutto il territorio nazionale, la nostra offerta si rivolge a tutti i settori del mercato. E' importante comprendere come l'approccio unico permetta soluzioni sinergiche in quanto armonicamente progettate, realizzate e mantenute in efficienza. In particolare, per le proposte di sistemi di gestione del denaro, ci rivolgiamo indistintamente all'utente finale come al CIT o alla banca. Al momento stiamo incontrando più interesse da parte dell'utente finale che, al di là delle performance specifiche delle apparecchiature "conta banconote", percepisce il vantaggio di avere un unico partner professionale esperto di tutte le tecnologie della sicurezza.

CONTATTI - CONFORTI SPA
Tel. +39 045 8878328
www.conforti.it

L’evoluzione verso la sicurezza fisica informatizzata in architettura aperta: l’approccio sistemico di Citel

di Nils Fredrik Fazzini, general manager Citel spa

La gestione informatizzata della sicurezza fisica

Nell’esperienza ormai ventennale di Citel nel mercato italiano, è ormai incontrovertibile il fatto che il professionista della sicurezza aziendale è sempre più orientato:

• a trattare **la sicurezza fisica come un’applicazione di processo informatizzabile** secondo criteri moderni, cominciando a considerare anche quelli che possono puntare eventualmente anche al *Cloud e all’Internet Of Things;*

• ad adottare le **innovazioni di sistema e di processo già sperimentate diffuse e consolidate**;

• a considerare la **convergenza con le istanze e le implicazioni più generali della compliance alla normativa sulla Continuità Operativa**.

Chi tende a questo approccio è semplicemente al passo con i tempi e potrà eventualmente scoprire che la sicurezza fisica professionale è da tempo allineata ai criteri attualmente popolari, anche se in passato era confinata alle Control Room della sicurezza di banche e grandi imprese industriali.

La vera novità degli anni recenti è che quel tipo di sicurezza, fatta di telegestione e interoperabilità, è diventata nel frattempo **accessibile alle dimensioni minori, con la tendenza a saldarsi con l’informatica venuta dal basso**: quella personale, anche indossabile, in attesa che il mondo della security proponga servizi di security innovativi ma efficaci e sostenibili.

Sono movimenti di fondo che sono maturati progressivamente e che soltanto negli ultimi anni hanno trovato una identità condivisa grazie all’acronimo **PSIM** segnalato da Citel nel 2012 sulla stampa di settore ma anticipato nella propria definizione italiana nel 2009.

Il PSIM e l’evoluzione settoriale

Il rischio di confusione

Il **PSIM** – Physical Security Information Management, si traduce letteralmente in ***gestione informatizzata*** **della sicurezza fisica**... La precisazione non è superflua, perché sta accadendo che la popolarità del paradigma presso l’utenza porta al fatto che “PSIM” venga usato anche per semplici supervisori di gestione centralizzata degli allarmi e uno degli scopi di questo documento è appunto quello di evitare che cadano nell’equivoco coloro che si avvicinano per la prima volta alla sicurezza fisica vista in chiave di informatizzazione.

Cosa è realmente il PSIM

Il PSIM - come un ERP *sui generis* - è un ***paradigma tecnico-funzionale***, basato sul presupposto elementare che anche la sicurezza fisica, come altre funzioni aziendali, va affrontata secondo modelli di articolazione funzionale e requisiti strutturali e di compliance strutturabili in un sistema informatico dipartimentale.

Come ogni paradigma oggetto di informatizzazione, il **PSIM incorpora processi, metodi, buone pratiche**, non

solo per ottenere scopi diretti e concreti, ma anche per conformarsi a disposizioni normative specifiche del settore di appartenenza. Da qui l’importanza dell’esistenza in Italia di un vero *Ecosistema, a supporto dell’evoluzione e della crescita di Centrax, il PSIM* di Citel: una comunità di utenti e di fornitori specializzati che negli anni contribuiscono costantemente all’accumulo selettivo di esperienza funzionale destinata a tradursi in nuovi moduli applicativi organici al progetto permanente Centrax-PSIM.

Il sistema informatico dipartimentale e le economie di scopo

Il PSIM appartiene a tutti gli effetti alla categoria dei sistemi informatici dipartimentali, ed è finalizzato ad attenuare il più possibile i rischi potenziali dell’organizzazione con misure progettate in funzione degli obiettivi sociali per il rispetto della normativa applicabile, a partire da quella sulla sicurezza e sulla safety fino a considerare l’intero ambito della ***business continuity***.

La *sicurezza* è un concetto ampio e multiforme: i processi per la sicurezza fisica in senso stretto e quelli pertinenti alla sicurezza in senso lato, possono essere impostati in funzione delle convergenze degli scopi e la condivisione delle risorse, per ottenere **buone pratiche finalizzate a *economie non più solo di scala ma anche di scopo*.** È sufficiente mettere a fattor comune il sistema informatizzato di gestione della sicurezza fisica anche per processi che possono sfruttarne l’infrastruttura, cosa tanto più possibile quando più esso è aperto, flessibile, versatile e intenzionalmente orientato alle economie di scopo. In definitiva, quanto più esso risponde ai criteri del PSIM – Physical Security Information Management.

Il focus sul TCO e la svolta del mercato

In passato la spinta a minimizzare il TCO nella sicurezza fisica era depotenziata già in fase di progetto dalla diffusa pratica di affidarsi – ad esempio nel caso di un progetto di Building Automation – ad una piattaforma unica: chiusa, e tuttavia comoda per tutti gli appartenenti a una filiera di cui facevano parte: il produttore di un intero sistema completo di catalogo, di un canale commerciale unico, di professionisti della progettazione ben supportati, di cosiddetti *system integrator*s o installatori esclusivisti.

Si trattava di un Ecosistema a tutti gli effetti, ma di tipo proprietario e tendenzialmente chiuso, accettabile per l’utente quando non esistevano alternative, ma con la tendenza ad essere **sempre meno accettato dopo che l’informatica personale ha introdotto paradigmi irreversibili di *open architecture*.**

E così oggi, oltre alle banche (le prime a liberarsi dei sistemi chiusi), anche altre categorie di utenza hanno sposato la pratica di mettere in concorrenza terze parti di installazione non più vincolate dal produttore o addirittura legate a patti di non concorrenza: distorsioni che erano rese possibili dalla chiusura architetturale della sistemistica del passato;

La progettazione della sistemistica di sicurezza che si ispira ai principi PSIM si trova in definitiva ad aver adottato implicitamente i criteri dell'informatica aperta, e con questo un indotto potenziale di benefici effetti sulla professionalità delle figure coinvolte:

- **favorisce la crescita professionale degli uffici tecnici dell'utente,** visto che potranno esercitare una indipendenza di giudizio che nei contesti chiusi tenderebbe ad essere invece sacrificata o distorta.
- **premia – tra i fornitori di servizi – quelli più dotati e capaci** e non quelli più dipendenti dal costruttore; quelli che riescono a combinare efficienza e capacità tecniche, organizzazione e flessibilità.
- non può che stimolare anche **l'evoluzione professionale dei progettisti e degli studi di progettazione,** con il possibile allargamento del campo d'azione, sul terreno informatico e probabilmente con l'allargamento delle relazioni a un ventaglio più esteso di discipline e di operatori nel mercato.

Quanto appena postulato è dimostrabilmente supportato dalla storia di Citel e dei suoi utenti e partner; una storia tutta in chiave PSIM è stata iniziata da Citel accompagnando nel percorso evolutivo grandi utenti nazionali (Poste e grandi banche, i gruppi dell'Oil&Gas), dimostrando nel tempo che il cambiamento di paradigma era non solo possibile ma inevitabile, non solo per i grandi utenti ma anche per le fasce di utenza dimensionalmente minori. E ottenendo – quanto al *PSIM come servizio* – anche l'adesione delle società di servizi di security, fino a quel momento storicamente vincolate alla una sistemistica chiusa e bloccata della vigilanza tradizionale.

Il PSIM si è diffuso tra i grandi ma anche tra i medi utenti con una rapidità inattesa, merito del paradigma positivo in chiave informatica: **finalmente riferimenti tecnici oggettivi, diffusi, normalizzati e aperti con ricadute benefiche sul TCO assolutamente evidenti** grazie allo smantellamento progressivo dei modelli commerciali che limitavano la libertà di giudizio e di scelta riguardo alla propria sistemistica, in particolare ai potenziali fornitori per la sua evoluzione e manutenzione.

L'Ecosistema alla base del Progetto Permanente

La dinamica di un Ecosistema di tipo PSIM è dovuta innanzitutto alla presenza di utenti innovativi, che però resta sterile senza l'azione specifica del produttore del sistema, che deve essere altrettanto motivato a trasformare idee e intenzioni in soluzioni di mercato attivando progetti e investendo su di essi.

La comunità degli utenti è la principale fonte di idee per l'innovazione dei processi e quindi il motore dell'evoluzione delle funzionalità, comprese quelle che implicano l'interazione tra dispositivi e tra sistemi, anche di produttori e tecnologie differenti.

Per raggiungere la massa critica che stabilizza nel tempo le sinergie, un Ecosistema ha poi bisogno dell'interesse ad aderire di terze parti: costruttori di prodotti complementari, fornitori di servizi, main contractors. Ma non basta, perché va aggiunto il ruolo di chi investe per realizzare integrazioni per un eventuale ritorno negli anni. In assenza dell'investitore nella sistemistica aperta, infatti, l'Ecosistema non si attiva.

Citel ha sbloccato questo freno all'innovazione accollandosi gli investimenti in nuovi sviluppi, sia di funzionalità che di integrazioni, con il risultato di rendere finalmente concreto il concetto astratto di architettura di sistema aperta. L'Ecosistema Centrax si è infatti materializzato in pochi anni e si è sviluppato con una progressione insolita per un mercato dominato da importanti gruppi internazionali.

Un risultato possibile soltanto con la convergenza di spinte naturali per l'utente, come la libertà di scelta e la sostenibilità dei costi, non solo al momento dell'acquisto ma per l'intero ciclo di vita del sistema. Una tendenza peraltro coerente con la spinta contemporanea alla riduzione dei costi fissi/ricorrenti, al perseguimento delle migliori pratiche e infine alla compliance alla normativa. Una convergenza inconciliabile se non affrontata utilizzando un sistema informatizzato professionale, in grado di abbattere i costi di gestione dei processi, ed esso stesso soggetto alle regole della gestione del ciclo di vita dell'infrastruttura, e in particolare di *quelle che puntano a considerarlo indefinito sfruttando la possibilità di un adeguamento progressivo delle prestazioni, l'aggiunta di nuove funzionalità, e non da ultima la possibilità di scelta competitiva delle terze parti di installazione e di manutenzione senza condizionamenti del costruttore.*

L'ECOSISTEMA CENTRAX – LA COMUNITA' DEGLI UTENTI

BANCHE e POSTE	INDUSTRIA, GDO, RETAIL. LOGISTICA	MUSEI e BENI ARTISTICI
Banca Popolare Valsabbina	Acciai Speciali di Terni (Gruppo ThyssenKrupp)	Palazzo Sangiacomo
Banca Marche	Alstom	Fondazione Villa Zito
Banca Popolare dell'Emilia Romagna	Berco (Gruppo ThyssenKrupp)	Museo del 900
Banca Popolare di Milano	Ceva Logistics	Punta Dogana - Palazzo Grassi
Banca Popolare di Vicenza	Conbipel	Palazzo Leone Montanari
Banco di Desio e della Brianza	Coop (Gruppo)	Palazzo Zevailos
Banco di Sardegna	Ducati	SOCIETA' DI SECURITY
Barclays Bank Italia	ENEL (Gruppo)	Axitea
BCC di Cantù	ENI (Gruppo)	Bassilichi
Cariparma (Gruppo)	Selex-ES Finmeccanica (Gruppo)	CIVIS (Gruppo)
Deutsche Bank Italia	Gruppo Richemont	Coopservice
Intesa Sanpaolo (Gruppo)	Mediaset	Gruppo Vision
Monte dei Paschi di Siena (Gruppo)	SAIPEM	IVRI
Poste Italiane (Gruppo)	SNAM	Rangers - Battistolli
UBI Banca (Gruppo)	SNATT Logistics	Securiy Trust
	TNT (Sicuritalia)	SecurSat
	GLS (Sicuritalia)	Sicuritalia
PUBBLICA AMMINISTRAZIONE		Stanley Security
Comune di Roma		

L'ECOSISTEMA CENTRAX – LA COMUNITA' DEI COSTRUTTORI DI APPARATI E SISTEMI INTEGRATI

(a ciascun costruttore possono corrispondere uno o più moduli di integrazione per vari apparati o sistemi)

videosorveglianza	video analisi	controllo accessi	intrusione e trasm. allarmi
Axis	Aitek	Axis Comunications	Saet
Bettini Video	Cognimatics	Iseo	Axel
Bosch - Divar	Technoaware	Kaba Axessor	Cias
D-Link		Nedap Retail	Elmo
Dahua	sistemi video	Salto	Guardall
Dallmeier (DLS, DMS)	3M (già PIPS)	Selesta	HESA
Dynacolor	Avigilon (V. 4 e 5)	Simons Voss	Honeywell
Elmo	Cisco VSOM Camera	Zucchetti Axess TMC	Inim
Euklis	Eptascape		Paradox DIAS
Everfocus	Genetec - Omnicast	aree self & safe, interblocchi	PB Elettronica
Ganz	Honeywell	Cometa	Securiton
GeoVision	Milestone	Saima	Teledata
Hikvision	Mirasys		UTC
Honeywell	Selea (Targha504)	sistemi di gestione contante	
March Network	Tattile	Cespro	ricevitori teleallarmi
Mesa	TKH aasset	Sitrade Italia	AMA
Mobotix	Visy (XML Gate)		Urmet
Samsung		bancomat - ATM	
Sight Logix	tecnologici - PLC - scada	Diebold	incendio
Sony	Adam 6052	Wincor Nixdorf	Notifier - AM
Syac TB	Andover	NCR	DEF
Teledata	Barionet 50		
UTC	Dali	Serrature elettrom. ritardat.	sistemi perimetrali
Vicon	Lovato	ZTF	DEA
Visimetrics	Moxa switch EDSP-510	Tecnosicurezza	Cias
	Perle I/O LAN DS1	Parma	Sight-Logix
citofonia - videocitofonia	Riello	m.i.b.	
2N Italia	Siemens-Omron	LEM	
Axis Communications			
Commend			

Le tendenze sinergiche verso la compliance: Safety, Energy Saving, Business Continuity

Negli ultimi anni l'utenza dotata di un PSIM ha iniziato a utilizzare l'infrastruttura anche per il rispetto della normativa sulla safety del lavoratore isolato, con processi intelligenti di monitoraggio interattivo mediante dispositivi indossabili combinati con l'impiantistica di protezione fisica locale; e sfruttando la rete dati protetta del PSIM per interagire con il centro di supervisione, dotato di procedure guidate e tracciate di gestione professionale di eventi ed emergenze a qualsiasi campo funzionale appartengano.

Il monitoraggio del malore o dell'aggressione del lavoratore isolato è stata sempre praticata presso i grandi utenti con molte piccole sedi, tipicamente banche, a rischio rapina, oppure imprese con attività a rischio infortunio. Ma di norma ciò è avvenuto separatamente dalle infrastrutture informatizzate per la sicurezza o, comunque, è stato realizzato con tecnologie analogiche piuttosto che digitali e con trasmissione su reti non particolarmente affidabili e non interoperanti con un sistema complessivo di gestione.

I primi casi di sinergia sono da considerare esemplari non solo per i risultati concreti ed evidenti di compliance ottenuta con forti economie di scopo, ma anche per gli effetti sinergici indotti, ad esempio ai fini della business continuity; casi di scuola settoriali sono certamente due progetti recenti di UBI Banca e di ENEL, che in centinaia di uffici mono-operatore sfruttano il PSIM e l'infrastruttura di rete per proteggere allo stesso tempo la salute del lavoratore e l'operatività dell'ufficio, utilizzando funzioni prevalentemente software.

Altro caso esemplare di sinergia, stavolta sul terreno del risparmio dei consumi energetici combinato con il comfort dell'ambiente lavorativo, è quello di Poste Italiane che ha sfruttato l'infrastruttura centralizzata della sicurezza fisica per un primo intervento a economia di scopo che ha coinvolto migliaia di uffici postali; un risultato che è valso a Poste il primo posto in un contest internazionale di settore.

Gli *stakeholder* e le motivazioni all'adozione di soluzioni in chiave PSIM

In quanto sistema informatizzato, un PSIM ha una componente prevalente software che, per sua natura, una volta raggiunta una certa diffusione può essere proposto a utenti grandi e meno grandi a prezzi modulati

sulle dimensioni del campo di impiego (numero di punti / impianti) e moduli funzionali (applicazioni, integrazioni, ecc.). Nel caso di Citel il PSIM Centrax segue da tempo un percorso di questo tipo: partito dalle grandi banche e dai grandi gruppi industriali, si è progressivamente allargato alle medie aziende diventando scalabile per prestazioni e prezzo fino alla gestione di un singolo impianto, con un catalogo sostenibile e accessibile anche per le terze parti che operano nel territorio a diretto contatto con l'utenza periferica e/o di dimensioni minori.

L'utilizzatore tipo di un PSIM è un'organizzazione all'interno della quale diversi settori hanno incarichi e responsabilità rispetto alla sicurezza fisica e alle sue attinenze: *stakeholders* con la tendenza sempre più marcata a svincolarsi dagli schemi e dalle pratiche del passato, basate sulla dipendenza dai costruttori e dalle loro reti di progettisti e terze parti di servizi:

- il **Security Manager**

• che vuole gestire la sicurezza secondo processi dimostrabilmente adeguati alla missione e alla responsabilità; finalizzati alla gestione efficiente e affidabile in quanto generata dall'intelligenza della progettazione e non dipendente dalla diligenza dell'operatore;

• che deve poter adeguare rapidamente le misure di attenuazione del rischio all'andamento della casistica delle minacce;

• che deve poter provare, adottare e integrare nuove soluzioni tecniche senza essere frenato dal fornitore del sistema chiuso;

• che deve avere in tempo reale notifiche di alert per carenze di gestione;

• che è responsabilizzato e valutato anche per risultati di compliance alla *business continuity.*

- l'**Ufficio Acquisti** che con l'apertura architetturale può mettere in competizione sia i fornitori di sistemi e prodotti, che quelli di servizi di installazione e di manutenzione; con la garanzia di poter puntare su una concorrenza meritocratica non viziata da legami particolari degli operatori con il fornitore della sistemistica e degli apparati;

- l'**ICT Manager**, che deve mettere a disposizione la rete dati LAN / WAN, eventualmente piattaforme server; che è responsabile della loro continuità operativa e che deve validare le qualità di resistenza ai penetration test degli apparati di sicurezza connessi alla rete aziendale;

- la **Direzione Generale**, che può decidere:

• di gestire le proprie varie responsabilità direzionali e di compliance in base a strumenti e processi professionali, automatizzati e autocontrollati che minimizzino omissioni, errori operativi e gestionali;

• che il sistema gestionale della sicurezza fisica possa e debba puntare a ogni possibile economia di scala e di scopo una volta accertato che esso può incorporare anche funzioni specializzate per processi di gestione della safety, la gestione delle emergenze, il monitoraggio dei consumi, per la *business continuity.*

Per un'organizzazione che sta ripensando la propria sicurezza fisica e la materia della ***business continuity,*** **l'approccio PSIM presenta in definitiva solo vantaggi e nessuna controindicazione,** sia per la società nel suo insieme che per le responsabilità dei vari stakeholder, come appena visto.

Il solo ostacolo al sistema unico e integrato in chiave PSIM è stata la naturale tendenza degli utenti a salvaguardare gli investimenti fatti nei sistemi di sicurezza preesistenti; ma si è trattato di un freno che si è limitato alla fase di decollo dell'architettura aperta, finché l'Ecosistema Centrax-open PSIM – una volta raggiunta la massa critica – ha messo a disposizione una gamma completa di moduli di integrazione per gli apparati e sottosistemi più diffusi nel mercato. **Da quel momento, per gli utenti orientati al PSIM il vincolo costituito dalle scelte del passato è saltato, e con esso il rischio di dover scegliere tra il rimanere vincolati alle tecnologie chiuse rinunciando al PSIM aperto oppure affrontare i costi del rifacimento degli impianti esistenti.**

La società

CITEL è una società per azioni italiana, indipendente, con una storia di 20 anni e una specializzazione nella sistemistica per la gestione della sicurezza fisica basata sulle tecniche informatiche e sulle reti dati, di cui è oggi il principale produttore nazionale.

Citel Spa
Milano
info@citel.it
www.citel.it

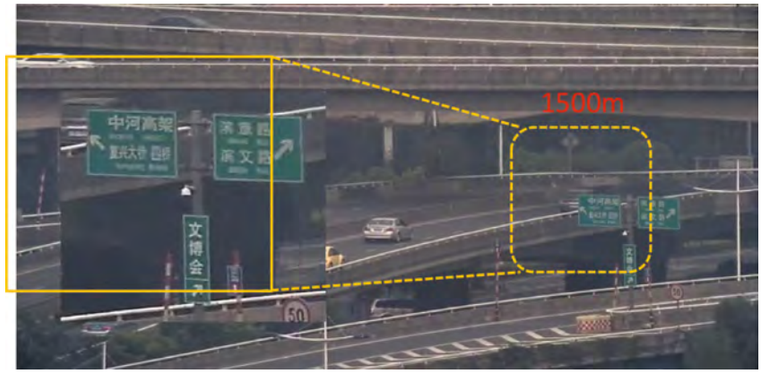
Dahua presenta una serie di termocamere intelligenti in rete

a cura della Redazione

HANGZHOU, CHINA — **Dahua Technology**, un costruttore leader mondiale di prodotti di videosorveglianza con sede a Huangzhou, presenta una serie di termocamere intelligenti in rete che offrono qualità superiore delle immagini e caratteristiche avanzate per applicazioni di sicurezza per perimetri, reti elettriche e industrie. La serie è progettata per trovare fonti di calore ed è in grado di fornire immagini altamente dettagliate, con caratteristiche molto ampie.

Network camera & thermal camera side by side

40x optical zoom lens



IVS and auto-tracking

Hot resource detects & alarm

La nuova famiglia di termocamere intelligenti in rete di Dahua include: termocamere ibride PTZ, camere ibride Speed Dome, termocamere bullet e termocamere Dome, tutte dotate di una vasta gamma di funzioni intelligenti. Le termocamere intelligenti adottano un sensore di alta qualità in grado di rilevare le minime differenze di temperatura. Questa serie di camere può raggiungere la massima accuratezza di rilevamento ed è in grado di lavorare nel buio completo e in condizioni meteorologiche avverse. Inoltre, le camere uniscono intelligenza, efficienza e alte prestazioni così come smart detection, smart analyze, smart perception, smart tracking e smart control.

Le termocamere intelligenti in rete possono determinare con esattezza sia la temperatura dell'oggetto che la distribuzione della temperatura anche in oggetti piccoli o in rapido movimento. Queste camere sono perfette per individuare infiltrazioni d'acqua attraverso muri, una persona nascosta nei cespugli di notte o identificare passeggeri con la febbre attraverso un checkpoint.

La termocamera PTZ ibirida in rete di Dahua è una combinazione professionale di una videocamera che integra uno zoom ottico max 40x e una termocamera, perfettamente sincronizzate nei movimenti di inclinazione e rotazione. La camera in rete può catturare immagini su vasta scala senza dover indietreggiare per inquadrare l'oggetto. La termocamera è adatta a funzionare nell'oscurità o per specifici controlli termografici. La lente speciale mette a fuoco la luce infrarossa emessa da tutti gli oggetti ripresi e può rilasciare simultaneamente diversi streams indipendenti H.264 per esigenze diversificate di qualità e senza limiti di larghezza di banda.

Dahua fornisce anche il software e gli accessori, compreso lo smart PSS, NVR e DMSS per lavorare insieme e rispondere alle specifiche richieste del trasporto, dell'energia, della sorveglianza dei confini e delle coste e ogni altra applicazione speciale.

La famiglia di termocamere in rete intelligenti di Dahua:

Thermal Hybrid PTZ Camera PT8320/8620(-T)

- Thermal resolution:640*512 or 336*256
- Lens optional:35/60/100mm
- Visible camera support 40X optical zoom
- Support IVS
- IP66-rated

Thermal Hybrid Dome Camera SD8320/8620(-T)

- Thermal resolution:640*512 or 336*256
- Lens optional:25/35/50mm
- Visible camera support 30X optical zoom
- Support IVS
- IP66-rated

Thermal Bullet Camera BF5300/5600(-T)

- Thermal resolution:640*512 or 336*256
- Lens optional:7/13/19/35mm
- Tri-mode output:IP/HDCVI/Analog
- Support IVS
- IP67-rated

Thermal Dome Camera SD5300/SD5600(-T)

- Thermal resolution:640*512 or 336*256
- Lens optional:13/19mm
- Tri-mode output:IP/HDCVI/Analog
- Support IVS
- IP66-rated

A proposito di Dahua Technology:

Dahua Technology Co, Ltd è un costruttore leader a livello mondiale di componenti professionali per la sicurezza e la sorveglianza. Negli ultimi 15 anni, Dahua ha investito fortemente in Ricerca e Sviluppo di soluzioni innovative per migliorare la sicurezza pubblica. Le soluzioni Dahua sono progettate per essere scalabili e modulari e offrire opzioni flessibili di configurazione. La società è collocata al 5° posto nel Security 50 Rankings 2015 di A&S International. Dahua si compiace del secondo posto come quota di mercato mondiale, secondo il report 2015 di IHS. Per maggiori informazioni visita **http://www.dahuasecurity.com**

CONTATTI: DAHUA TECHNOLOGY CO.
Tel. +86 571 87688883
overseas@dahuatech.com

Sistema di Sicurezza Integrata Avanzata realizzato da DAB Sistemi Integrati Srl per il Comune di Castellammare di Stabia

a cura di Matteo Canzonetti, Ingegneria di offerta DAB Sistemi Integrati

Il Comune di **Castellammare di Stabia** sorge nella parte sud della città metropolitana di Napoli, nel territorio compreso tra la fine della zona vesuviana e l'inizio della penisola sorrentina.

Il Comune, impegnato a garantire ai propri abitanti e ai numerosi turisti servizi efficienti in termini di sicurezza, ha valutato l'esigenza di realizzare un sistema di videosorveglianza per consentire alla Polizia Locale di monitorare la viabilità urbana, gli edifici pubblici e storici, rispettando la tutela della privacy dei cittadini.

La realizzazione del sistema di videosorveglianza è stato affidata, tramite una procedura di gara, all'azienda **DAB Sistemi Integrati Srl**. L'Azienda ha proposto e realizzato una soluzione di **Sicurezza Integrata Avanzata e personalizzata** che, a tutti gli effetti, può essere considerata come un esempio significativo e vincente di sviluppo di un progetto di **Smart City**.

Non si tratta di un semplice sistema di videosorveglianza, ma di una piattaforma complessa in grado di gestire la sicurezza del territorio da tutti i punti di vista. Un **sistema capace di aumentare l'efficienza e l'efficacia del processo di controllo del territorio e ottimizzare la gestione delle Forze di Polizia Locale, rendendo la Centrale Operativa il "cervello" della gestione della Città**. Una proposta innovativa e un sistema integrato che non ha trascurato gli investimenti effettuati integrando, all'interno della soluzione, anche le telecamere preesistenti sul campo. In particolare, sono state installate nuove telecamere per il monitoraggio dei punti "sensibili" come piazze, scuole, parchi pubblici e per il controllo delle principali strade d'accesso al Comune.

La soluzione realizzata permette di registrare le targhe dei veicoli che transitano e fornire informazioni utili alle Forze dell'Ordine per soddisfare ogni esigenza di sicurezza e di indagine. Per quanto riguarda la sicurezza stradale, il posizionamento delle telecamere in alcuni incroci particolarmente pericolosi ha permesso di chiarire le dinamiche degli incidenti, anche in assenza di testimoni oculari.

All'interno del progetto, è stata realizzata anche una rete a banda larga mista in Fibra Ottica e Ponti Radio Hiperlan per connettere i diversi punti sul territorio come solida base di comunicazione non solo del sistema di sicurezza, ma anche e soprattutto per futuri servizi e ampliamenti del sistema.

Tutela del patrimonio urbano, sicurezza per i cittadini e viabilità cittadina

L'architettura del sistema installato presso il Comune di Castellammare di Stabia è composto in totale di n. **138 telecamere**:

- n. 62 telecamere periferiche "Speed Dome" per il monitoraggio continuo e in tempo reale delle immagini

Telecamera fissa per il controllo stradale

Colonnina SOS Cometa

delle aree di interesse. Grazie alle loro funzionalità PTZ avanzate, permettono di inquadrare vaste aree con controllo del brandeggio e dello zoom ottico 28x, consentendo un'inquadratura sufficientemente dettagliata per le principali aree da monitorare

- n. 40 telecamere fisse dotate di sensore da 2 Megapixel, per la registrazione delle targhe dei veicoli in transito negli incroci o nelle vie di accesso o in itinere;
- infine, sono state integrate le 36 telecamere preesistenti.

Le 138 telecamere costituiscono un unico evoluto sistema di videosorveglianza territoriale interconnesso su una nuova Rete MAN a banda larga costituita da circa 4,5 Km di Fibra Ottica, 108 apparati Radio Hiperlan, 4 postazioni Hot Spot Wi-Fi e 90 apparati di Switching sul campo e nelle centrali.

Per il controllo, la gestione e il telemonitoraggio dell'intero sistema di videosorveglianza, sono state inoltre predisposte tre Sale Controllo all'interno delle Centrali Operative del Comando della Polizia Municipale, del Commissariato di Polizia di Stato e del Comando dei Carabinieri, ciascuna con postazione operatore e Videowall. Il sistema prevede una capacità di archiviazione e registrazione delle immagini provenienti da tutte telecamere per un periodo massimo di 7 giorni H24 nel rispetto delle regole del Garante della Privacy in materia di tutela dei cittadini nei confronti della videosorveglianza.

Il sistema di gestione e controllo implementato presenta alcune funzionalità a valore aggiunto per l'integrazione e l'amministrazione delle Colonnine SOS Cometa, dei Pannelli a Messaggio Variabile, Indirizzamento ai Parcheggi, Analisi Traffico e sistemi AVL (Rilevazione automatica di posizione dei veicoli della flotta Municipale). Sono state installate nello specifico, n. 9 Colonnine SOS Cometa equipaggiate per le richieste di soccorso dei cittadini, con comunicazione audio bidirezionale, visione della persona chiamante (telecamera frontale), videosorveglianza delle aree intorno alla colonnina tramite una Telecamere Speed Dome aggiuntiva posta sulla colonnina. Per dare informazioni utili alla cittadinanza a Viale Europa, a Piazza Unità d'Italia e sulla S145 Terrazza Panoramica, sono stati installati 3 Pannelli a Messaggio Variabile telegestiti dalla Centrale Operativa della Polizia Municipale.

Presso la Centrale Operativa della Polizia Municipale è stato attivato anche un software (validato C.N.I.P.A) per la gestione elettronica del Brogliaccio (consente la pianificazione e la registrazione delle richieste e degli interventi, supporta le funzioni di report di attività), dei Turni / Personale / Mezzi, degli eventi e registrazione schede di intervento, della posizione delle pattuglie della Polizia Locale su sistema cartografico, delle segnalazioni a mezzo e-mail e fax ad altri Enti.

Oltre alle tre Sale Controllo, sono state predisposte

Telecamera fissa per il controllo stradale

Pannello a Messaggio Variabile

cinque Centrali Operative Mobili installate su altrettanti veicoli della Polizia Locale per la visualizzazione delle immagini delle telecamere, costituite da Tablet con connettività Wi-Fi e 3G e applicativo di gestione della videosorveglianza.

Per combattere il fenomeno di abbandono dei rifiuti e sorvegliare situazioni critiche anche temporanee, il Comune è stato inoltre dotato di una Postazione Mimetizzata di Videosorveglianza. La tecnologia è costituita da un unico armadietto che contiene tutta la strumentazione (telecamera, illuminatore infrarosso per visione notturna, sistema di registrazione e sistema di alimentazione con gruppo batteria), di dimensioni e peso contenuto, autonomo dal punto di vista elettrico e completo di accessori per un veloce e facile fissaggio.

Inoltre, su un automezzo della Polizia Municipale è stata installata un Postazione Mobile di Videosorveglianza con telecamere brandeggiabile, sistema di videoregistrazione e sistema GPS per la geo localizzazione del mezzo).

Infine, per compensare i consumi energetici dell'intero sistema, in tre Istituti scolastici di competenza del Comune sono stati installati altrettanti impianti fotovoltaici da 6 KWp ciascuno per una potenza complessiva prodotta di 18 KWp.

Obiettivi raggiunti

La realizzazione del progetto di videosorveglianza si è rivelata valida per il Comune perché, oltre a rilevare gravi minacce, le postazioni installate in aree pubbliche rappresentano un deterrente contro attacchi alle persone, furti e atti vandalici. L'ottima qualità delle immagini ottenute, anche in condizioni di luce estreme, hanno permesso di monitorare senza interruzioni le aree a rischio, garantendo la sicurezza e la tranquillità dei cittadini.

Il sistema è in grado di aumentare l'efficienza e l'efficacia del processo di controllo del territorio, e ottimizzare la gestione delle Forze di Polizia Locale, rendendo la Centrale Operativa il "cervello" della gestione della Città. La flessibilità della soluzione realizzata, oltre ad integrare nel nuovo sistema delle telecamere già esistenti, ha offerto la possibilità di poter ampliare ed implementare nuove applicazioni future.

CONTATTI: GRUPPO DAB SPA
Tel. +39 06 412121
www.gruppodab.it

*Immagini fornite dal comune di Castellammare di Stabia

ANDI OTG, il sistema di identificazione biometrico contactless per luoghi ad alta frequentazione

a colloquio con Dario La Ferla, amministratore unico Securmatica
a cura della Redazione

La spinta degli ultimi gravi attentati di Parigi, sta crescendo la necessità di controllare l'identità delle persone nella fase di accesso in luoghi ad alta frequentazione – come stadi, teatri, ma anche stazioni ferroviarie, aeroporti, centri commerciali ecc. Quali sono le soluzioni rese possibili dalle tecnologie attuali?

In quest'epoca di globalizzazione e di cambiamento degli equilibri geopolitici, la gestione delle masse incontrollate di migranti che premono ai confini del Sud e dell'Est dell'Europa in cerca di migliori condizioni di vita, rappresenta uno sforzo insostenibile. La Crisi economica mondiale, le guerre civili e la propaganda politico-religiosa hanno recentemente dimostrato che un attacco terroristico può essere consumato ovunque. Inoltre un flusso migratorio non gestito favorisce anche il propagarsi di possibili focolai di malattie contagiose ormai debellate o nuove per i Paesi sviluppati.

Ciò premesso prendendo spunto dall'ultimo tragico evento accaduto a Parigi, ove gli obiettivi presi di mira erano luoghi di assembramento abituali per tutti i Paesi Civili, come lo stadio, il teatro ed i ristoranti (senza escludere la probabilità di altri attacchi anche in aeroporti, stazioni ferroviarie, ospedali, porti, centri commerciali, palestre, biblioteche, aree riservate all'interno delle sedi governative, luoghi di alta frequentazione, ecc.), e a fronte di una maggiore necessità di sicurezza discendente dalla situazione oggi vissuta, viene ritenuto quanto mai indispensabile poter procedere al controllo biometrico, in ambiti ove l'afflusso delle persone in via stanziale e/o straordinario è notevole, dell'identità in modo sistematico/fluido e veloce delle persone nella fase di accesso agli stessi (di fatto un solo sistema OTG è in grado di "leggere" circa 3000 persone all'ora); così facendo si avrebbe la possibilità di avere un controllo "accessi" regolamentato, inequivocabile e sicuro.

La biometria, soprattutto quella che rileva il dispositivo

prodotto da AOS (riscontro biometrico dell'identità tramite lettura a distanza delle impronte digitali anche senza fermate il flusso di persone), oggi, è l'unico sistema idoneo per ottenere un'identificazione certa delle persone perché basata su caratteristiche fisiche distintive, inequivocabili, individuali ed immutabili nel tempo e fornisce pertanto un accertamento assoluto, a differenza di altri strumenti identificativi fisici utilizzati (es. documenti di identità, tessere di riconoscimento, badge, key cards, i o password). Si pensi se questo sistema fosse stato installato presso il Tribunale di Milano, la dematerializzazione del tesserino di riconoscimento, avrebbe impedito l'accesso all'autore della strage. La credenziale di accesso non risiede più tra le mani dell'utilizzatore, ma nelle mani dell'utilizzatore.

Quali sono le caratteristiche e le prestazioni di un sistema OTG?

Riprendendo quanto sopra descritto e con particolare riferimento al propagarsi di possibili focolai di malattie contagiose ormai debellate nei Paesi sviluppati, il dispositivo concepito dalla AOS, peraltro certificata dalla US Federal Bureau of Investigation (FBI - il dispositivo è stato aggiunto nell'elenco dei prodotti certificati – CPL - il 27 novembre 2015) e nominato dalla Popular Science alla fine una delle 100 migliori innovazioni, prodotto negli USA ed unico nel suo genere in fatto di metodologia di rilevamento dato biometrico, permette l'acquisizione delle impronte in modo contactless/ touchless = senza alcun tipo di contatto fisico con il dispositivo (il tutto sia nella fase di acquisizione del dato che nella fase di utilizzo del dato stesso). Contactless/ touchless presenta diversi vantaggi, come ad esempio il fatto che offra una interazione molto più veloce rispetto ai sistemi attualmente presenti sul mercato, il fatto che sia un sistema anti contagio perfetto, vale a dire che nessuno entra in contatto fisco con il dispositivo (non ci sono superfici alle quali "appoggiarsi") né nella fase di enrollment (iscrizione/accreditamento) né tantomeno nella fase di utilizzo. Pertanto nessuna propagazione di malattie da contatto, ed infine proprio perché contactless – assenza di impronte latenti - il dispositivo non ha bisogno di alcuna manutenzione.
Che cosa significa senza contatto fisico? Significa che nessun soggetto o operatore viene in contatto con il dispositivo. Significa anche che nessun operatore ha bisogno di avere contatti con un soggetto.
Nessuna superficie da pulire, senza immagini fantasma e nessuna impronta digitale latente da eliminare; il funzionamento senza contatto cambia l'equazione dei costi facendo sì che la rilevazione delle impronte digitali divenga una semplice e veloce operazione.
OTG, uno dei dispositivi prodotti, è l'acronimo di "on the go" - "in movimento": nessun altro dispositivo è stato in grado di surclassare la velocità/facilità di rilevazione d'identità. Il dispositivo è in grado di registrare, previo enrollment, l'impronta digitale di quasi 3000 utenti all'ora. AOS ha investito un notevole sforzo al fine di assicurare che l'esperienza umana con il dispositivo ANDI® OTG fosse fluida e intuitiva e di agevole utilizzo per chiunque entrasse in contatto con il dispositivo, sia che fosse di statura bassa, alta oppure diversamente abile. È un sistema che permette: velocità nella registrazione/raccolta dei dati, risultati eccellenti con le impronte digitali usurate (usurate per l'età e per eventi di altra natura), migliore interoperabilità fornita rispetto ai dispositivi "tradizionali" basati sul contatto, qualità di rilevazione impronta che è indipendente dall'operatore, touchless/badge-less sinonimo d'igiene, ridotti costi di manutenzione, facilità d'uso per le persone e nessuna superficie calda o fredda al tatto (nessun shock statico!), raccoglie 4 impronte digitali per mano - quasi istantaneamente!
Rilevazione impronte a passo d'uomo "on the go" significa nessuna coda. I confini possono diventare più accessibili, mentre la vigilanza diventa più efficace. Il dispositivo può essere impiegato anche in coppia per catturare tutte le otto le impronte digitali da soggetti a tassi di clock alto come 54 persone al minuto. Un sistema che consente regimi di verifica dell'identità, di sicurezza, d'ingresso e uscita che prima erano irraggiungibili. OTG è l'unico dispositivo contactless/ touchless rilevatore di impronta con funzionalità multimodale presente sul mercato oggi.

Quali sono le categorie di utilizzatori di questi sistemi? Quali sono i costi di acquisto e di gestione?

Premesso che il dispositivo è stato presentato sul mercato agli inizi del 2015 motivo per cui la sua distribuzione ad oggi non è molto diffusa e da novembre del 2015 grazie ad un Distribution Agreement sottoscritto con Securmatica Security Management Srl, è divenuto distributore esclusivo per l'Italia, Il Vaticano, San Marino e Il Canton Ticino (CH) è presente sul mercato Italiano, possiamo confermare che lo stesso oggi è installato presso alcune aree del Dipartimento della Difesa US, è altresì installato presso un gestore – in fase di test – dell'agenzia US Dogana e Protezione Confini. Segnaliamo, infine, che il dispositivo ANDI ONEprint è installato presso "The Southern Poverty Law Center" che è Ente senza scopo di lucro per l'organizzazione di difesa legale americano specializzato in diritti civili e interessi dei contenziosi in ambito pubblico.
È giusto il caso di far menzione al fatto che il dispositivo, con discreto successo, è stato utilizzato in un programma PILOTA dell'Unione Europea sperimentazione di nuove tecnologie per la sicurezza delle frontiere presso l'aeroporto di Amsterdam's Schiphol per conto della eu-LISA ed in questi giorni viene testato presso l'aeroporto di Francoforte per conto di Lufthansa. Ad oggi non sono ancora stati pubblicati i risultati ma AOS sta partecipando con successo all'integrazione dei propri sistemi con uno o più aeroporti degli Stati Uniti e una serie di altri aeroporti a livello mondiale avranno presto Zero-Contact sensori di rilevazione impronte digitali installato.
Il sistema può essere utilizzato in innumerevoli "ambienti": Gestione dei flussi presso: stadi, tribunali, aeroporti, stazioni ferroviarie, ospedali, centrali elettriche, centri di ricerca, accesso a navi di crociera o aeromobili, porti, centri commerciali, palestre, biblioteche, aree riservate all'interno delle sedi governative, luoghi di alta frequentazione, scuole, amministrazione pubblica, piscine, centri direzionali, uffici, turismo, trasporti, banche, assicurazioni, hi-tech, telecomunicazioni, industria, eventi ticketless… etc.
Per quanto attiene i costi relativi al dispositivo stand alone oscillano tra eur. 22.500 ai 27.000 per OTG, tra eur. 1.500 a 2.000 per onePrint. Si prevedono bassissimi costi di gestione post installazione, perché essendo un prodotto contactless non necessita di alcuna manutenzione/pulizia programmata, Inoltre è assicurato un notevolissimo risparmio in costi di impegno del personale fisico che può essere sollevato dall'attività di controllo delle credenziali di accesso per essere dedicato all'attività di intercettazione delle persone non autorizzate per i quali OTG ha impedito l'accesso.

In che modo Securmatica organizza l'azione commerciale, la distribuzione, l'installazione e l'assistenza post-vendita dei sistemi OTG nel mercato italiano e della Svizzera italiana?

Securmatica è impegnata nell'integrazione con aziende specializzate nella installazione, produzione e programmazione di sistemi di controllo accessi. Inoltre l'azione commerciale è diretta alla realizzazione di progetti specifici per amministrazioni pubbliche e grandi aziende.

SECURMATICA security management

CONTATTI: SECURMATICA SECURITY MANAGEMENT SRL
info@securmatica.it
www.securmatica.it

Il Gruppo EGGER è la prima azienda al mondo ad aver installato la nuova soluzione Kaba EACM

a cura della Redazione

Nel nuovo edificio amministrativo presso la sede di St. Johann, il Gruppo EGGER ha deciso di affidarsi alla nuova soluzione di controllo accessi Kaba integrata direttamente in SAP.

Il Gruppo **EGGER** è un'impresa familiare che opera a livello globale. Dal 1961, gli oltre 7.200 collaboratori che nel frattempo hanno trovato impiego nel gruppo sono in grado di ottenere il meglio da un materiale prezioso come il legno. Nel giro di un anno è stato costruito il nuovo edificio amministrativo presso la sede di St. Johann, caratterizzato da un design ricercato e dall'utilizzo dei prodotti EGGER. Dal suo completamento nel marzo 2015, il moderno edificio offre 276 postazioni di lavoro e 48 di formazione professionale, una mensa per i collaboratori e un parcheggio interrato, su una superficie totale di quasi 9.000 m^2.

In un nuovo building innovativo, come la sede del Gruppo EGGER appunto, anche un controllo degli accessi funzionale e al passo con i tempi svolge un ruolo importante. Non a caso EGGER è la prima azienda al mondo ad aver installato la nuova soluzione di controllo accessi **Kaba EACM**. Il progetto pilota comprende lettori di controllo accessi online e varie access manager distribuiti nell'edificio. In questo caso non è stato solamente il carattere innovativo della soluzione a convincere, ma anche il design moderno dei componenti di controllo accessi.

La soluzione Kaba EACM garantisce all'azienda il massimo della sicurezza e contemporaneamente riduce al minimo i costi di gestione amministrativa. Tutte le autorizzazioni di accesso vengono gestite direttamente nel modulo SAP Organization Management e sono quindi parte integrante dei processi operativi. Per esempio, l'assegnazione delle autorizzazioni di accesso si svolge in modo molto semplice e automatizzato, a seconda della posizione di un collaboratore nell'azienda. Dalla definizione dei profili di accesso, all'assegnazione dei diritti, fino alla consegna o al ritiro dei supporti di accesso, l'intero processo di gestione degli accessi online viene effettuato tramite SAP. In questo modo l'utente si muove nell'ambiente SAP a cui è abituato, e non deve imparare a utilizzare un nuovo sistema.

"Con Kaba all'interno della nostra sede siamo riusciti a implementare in breve tempo un sistema innovativo e affidabile per la gestione degli accessi. L'eccellente preparazione e il sostegno nel progetto hanno permesso una messa in servizio del nuovo edificio senza alcuna difficoltà" afferma l'Ing. **Josef Schreder, Direttore SAP CC HR, Fritz Egger Gmbh & Co. OG**, a conferma della coesione di sicurezza e semplicità della nuova soluzione.

Per la realizzazione del concetto di sicurezza, il Gruppo EGGER beneficia inoltre dell'ampia gamma di prodotti Kaba, costituita da sistemi di chiusura meccanici ed elettronici, lettori di controllo accessi e sistemi di accesso singolo. Inoltre sono state già installate 110 maniglie elettroniche c-lever compact, gestite dai supporti Mifare esistenti. Nelle fasi successive del progetto è prevista l'integrazione delle maniglie elettroniche e i dispositivi di rilevazione presenze in Kaba EACM.

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

Dahua presenta una serie di telecamere in rete 4K ultra-HD

a cura della Redazione

Dahua Technology, costruttore leader a livello mondiale di prodotti di videosorveglianza con sede a Hangzhou, Cina, ha presentato **DH-IPC-81200**, l'ultima serie di telecamere in rete 4K ultra-HD. Questa nuova serie è l'offerta più elevata di Dahua, con una risoluzione di 12 Megapixel (4K UHD), è dotata di un codec 4K ultra-HD e del sistema di rilevamento intelligente.

Tutti i modelli di telecamere in rete della sere **DH-IPC 81200** sono dotati di una risoluzione totale di 3830 x 2160 alla massima velocità per offrire immagini spettacolari. Questa serie impiega l'elevato standard del sensore di colore **Sony Exmor R 1/1.7" CMOS** con 12 Megapixel di risoluzione effettiva e il DSP dual core **Ambarella Cortex-A9 1GHz** che genera immagini più luminose a maggiore sensibilità con minori disturbi. Con la straordinaria qualità video nella risoluzione 4K ultra HD, la nuova serie di telecamere in rete Dahua 4K ultra-HD è adatta per installazioni interne ed esterne per rendere piena fedeltà di scena e immagini nitide.

Dahua **HFW81200E-Z** e **HDBW81200E-Z** sono entrambe in grado di abilitare uno zoom ottico 4times con focalizzazione sincronizzata e possono zoomare con messa a fuoco rapida in 5 secondi. La potente lente offre un ampio angolo di visuale (106°-32°). La serie 4K ultra-HD adotta la nuova funzione E-PTZ che offre il tracciamento automatico degli oggetti che hanno generato un allarme. L'hardware di fascia alta è completato da un firmware altrettanto potente e da un software in grado di gestire una varietà di funzioni intelligenti compresi IVS, riconoscimento facciale, conta persone e mappe di calore. La nuova serie di telecamere in rete Dahua 4K ultra-HD offre una nuova esperienza di visione agli utilizzatori, è facile da usare, garantendo massima sicurezza e, nel contempo, efficienza operativa.

Modelli

12 Megapixel Ultra HD Network Bullet Camera (HFW81200E-Z)

12 Megapixel Ultra HD Network IR Dome Camera (HDBW81200E-Z)

Principali caratteristiche di prodotto

Hardware:

- 1/1.7" Sony Exmor sensor IMX226
- 4x optical zoom lens
- -30°C ~60°C working temperature
- IR LED Array, max 50 meters function

Software:

- Max Resolution: 4000x3000@15fps
- 4K (3840x2160)@30fps
- E-PTZ Function

A proposito di Dahua Technology:

Dahua Technology Co, Ltd è un costruttore leader a livello mondiale di componenti professionali per la sicurezza e la sorveglianza. Negli ultimi 15 anni, Dahua ha investito fortemente in Ricerca e Sviluppo di soluzioni innovative per migliorare la sicurezza pubblica. Le soluzioni Dahua sono progettate per essere scalabili e modulari e offrire opzioni flessibili di configurazione. La società è collocata al 5° posto nel Security 50 Rankings 2015 di A&S International. Dahua si compiace del secondo posto come quota di mercato mondiale, secondo il report 2015 di IHS. Per maggiori informazioni visita **http://www.dahuasecurity.com**

dahua TECHNOLOGY

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

CONTATTI: DAHUA TECHNOLOGY CO.
Tel. +86 571 87688883
overseas@dahuatech.com

Antieffrazione: certificare la sicurezza

a colloquio con Rocco Fusillo, Presidente di ERSI - Esperti Riferme e Serrature Italia
a cura della Redazione

La sicurezza, com'è noto, comprende ambiti diversi e legati tra loro dal filo rosso della tutela costante delle persone e delle cose. Dopo aver analizzato il settore dell'antincendio e della vigilanza, parliamo oggi di sicurezza antieffrazione con **Rocco Fusillo**, Presidente di **ERSI** (Esperti Riferme e Serrature Italia).

Presidente Fusillo, ricerche recenti affermano che la sicurezza è oggi un problema molto sentito, subito dopo le preoccupazioni dovute alla crisi economica e addirittura prioritario rispetto alle preoccupazioni sul proprio stato di salute. Allo stesso tempo, i dati relativi al possesso di sistemi di sicurezza domestici confermano l'aumentata propensione a proteggersi, anche in risposta alle percentuali relative ai furti in casa, cresciuti, secondo le ultime rilevazioni disponibili, di poco meno del 15% in un solo anno. ERSI, che raggruppa i maggiori esperti del settore sicurezza passiva, è l'Associazione di riferimento per il settore: qual è la vostra visione dell'attuale scenario?

Posso confermare che il lavoro del serraturiere è quanto mai in auge. Assistiamo, è vero, a un aumento dei furti, per certi versi fisiologicamente legato alla situazione odierna che, al di là di ogni retorica, presenta complessità sociali importanti. Non solo i furti, ma la necessità di "sentirsi al sicuro" nella propria casa spinge i cittadini a richiedere maggiori garanzie, per le serrature strettamente intese come per inferriate, finestre e serramenti blindati: cresce, infatti, la domanda per specialisti della sicurezza che possano mettere in evidenza i "punti deboli" delle case e degli stabili e prevedere anche sistemi di sorveglianza e monitoraggio a distanza. Tuttavia, è soprattutto l'upgrade tecnologico, negli ultimi anni molto rapido, a motivare un intervento degli specialisti in serrature. Molti cominciano solo ora a comprendere quanto una chiusura non adeguata possa vanificare un'ottima porta blindata: se solo dovessimo sostituire, senza nulla aggiungere, le chiusure esistenti ormai superate, avremmo un orizzonte di lavoro molto importante.

La professionalità e la qualificazione professionale dei serraturieri sono valori fondamentali e integranti per ERSI, tanto da avere già da tempo messo a punto con ICIM uno schema di certificazione volontario: è un tema alquanto d'attualità, visto che nell'ultimo anno è stata pubblicata in Italia una norma specifica per la certificazione delle figure professionali dei serraturieri e dei tecnici di casseforti.

Dal 1985 la qualifica professionale è uno dei temi fondamentali dell'Associazione. La Legge 4 del 2013 (*nata per disciplinare le figure professionali non regolamentate che non hanno albi, collegi e riconoscimenti legislativi e per le quali la UE sta sviluppando un sistema condiviso di riconoscimento delle competenze e delle professionalità che consenta la libera circolazione tra gli stati membri N.d.R.*) dà valore alla figura del serraturiere e agli sforzi fatti sin qui dall'Associazione. In particolare, la norma UNI 11557 tutela il riconoscimento delle competenze dei serraturieri e – grazie a un ente terzo come ICIM, primo organismo di certificazione italiano accreditato da Accredia secondo la UNI 11557 – offre garanzie ai clienti che possono così rivolgersi a esperti competenti e preparati nell'applicazione civile e industriale di serrature, nel rispetto del codice etico e del principio di riservatezza. In base alla sua esigenza di sicurezza, il cliente può scegliere il serraturiere più adatto: La certificazione è, infatti, articolata su tre livelli: junior, senior e maestro, oltre che a due livelli per i tecnici di casseforti domestiche e professionali.

ERSI fa corsi di formazione ed è la prima sede di esami in Italia qualificata da ICIM secondo la UNI 11557. Come sta andando, che grado di interesse e di risposta avete dai vostri associati? Quanti si sono già certificati?

L'opportunità della certificazione, al momento non cogente, è stata accolta molto bene dai nostri associati: in pochi mesi se ne sono certificati oltre la metà. Posso dire che la certificazione è stata in questi mesi un elemento attrattivo per l'Associazione, abbiamo avuto molte richieste anche da non iscritti, i corsi di formazione e le sessioni d'esame sono affollate. La formazione per noi è sempre stata importante ma ora molti, più facilmente, ne ravvedono la "finalità". In fondo la certificazione è anche un modo di cambiare la visione del serraturiere che "sale di grado" rispetto alla figura di fabbro. Certo, l'esame non è una formalità e leggere una norma non sempre è semplice per persone che magari hanno venti o trent'anni di esperienza sulle spalle, ma insieme a ICIM abbiamo messo a punto un protocollo vincente e la nostra formazione è strutturata in modo da accompagnare i serraturieri gradualmente, sino alla certificazione desiderata.

In un momento in cui sembra prevalgano liberalizzazioni di ogni tipo e i confini tra le professioni si fanno talvolta labili, qual è la vostra posizione? Auspicate la creazione di un nuovo albo dei serraturieri?

La nostra Associazione è già iscritta nell'elenco delle associazioni che rilasciano la qualifica professionale

presso il Ministero per lo Sviluppo Economico, dunque i serraturieri ERSI rappresentano professionisti che offrono garanzie di professionalità a privati e aziende. Al momento, però, manca una legislazione che possa sottendere alla creazione di un vero e proprio “albo”. Negli ultimi anni vediamo sempre più spesso enti e aziende rivolgersi a general contractor che non sempre, al loro interno, possiedono le competenze necessarie. Spesso questi soggetti si rivolgono a noi per integrare la loro attività con serraturieri esperti e professionali.

Come membro di ELF, la federazione europea dei serraturieri, ERSI ha una visione anche dello scenario internazionale?

Lavoriamo con tutti i paesi membri ELF soprattutto per armonizzare le varie normative e smussare le differenze tra le organizzazioni nazionali. Con la norma UNI 11557 abbiamo un formidabile strumento per portare la qualificazione professionale in tutti i paesi membri e uniformare la certificazione. I paesi del Nord Europa sono, in generale, più avanti perché possedevano una legislazione specifica, ma l’Italia non è da meno. ERSI già da anni lavora con ICIM per uniformare la qualificazione dei serraturieri su tutto il territorio nazionale. Siamo presenti in tutto il Paese, ma sicuramente in modo più capillare nelle regioni del Nord Italia e in particolare in Lombardia – dov’è la sede ERSI - Piemonte, Veneto, Emilia. Tra i nostri iscritti sono in aumento i giovani che, spesso, hanno ereditato la ferramenta di famiglia e cercano ora nuovi stimoli. Stimoli che vengono anche dal mercato, ad esempio

dal settore automotive che già da anni ha infuso al nostro comparto nuove sfide e nuove opportunità.

Per informazioni:
> sul calendario dei corsi di formazione dei serraturieri e sulle sessioni di esame:
www.ersi.it
info@ersi.it
> sulla certificazione professionale secondo la UNI 11557:
www.icim.it
info@icim.it

Premio H d’oro 2015 Categoria Beni Culturali Museali

a cura della Redazione

Categoria: **BENI CULTURALI MUSEALI**
Azienda installatrice: **MASSIMILIANO BASSANO - Napoli**
Denominazione e località dell’impianto: **MUSEO CIVICO “GAETANO FILANGERI” - Napoli**
Tipologia di Impianto realizzato: *Sistema di sicurezza integrato antintrusione, antieffrazione, di videosorveglianza e rilevazione incendi*

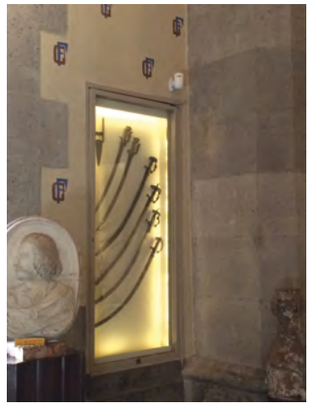
Lo scorso 23 ottobre, nel Cenacolo Palladiano della Fondazione Cini sull’Isola di San Giorgio Maggiore a Venezia si è svolta la cerimonia di premiazione dei vincitori e dei finalisti della decima edizione del **Premio H d’oro**, il concorso organizzato dalla **Fondazione Enzo Hruby** per premiare le migliori realizzazioni di sicurezza. Nella categoria *Beni Culturali Museali* ha vinto il prestigioso riconoscimento la società **Massimiliano Bassano di Napoli** per il progetto dedicato al Museo Civico “Gaetano Filangeri”, nella propria città.

Descrizione dell’impianto
La società Massimiliano Bassano è intervenuta per la protezione del Museo Civico Gaetano Filangieri andando a sostituire un impianto esistente ormai obsoleto con un nuovo sistema in grado di offrire un alto livello di protezione alla struttura museale e ai capolavori in essa custoditi. Tra questi si annoverano dipinti dello Spagnoletto, sculture di Luca della Robbia e altre importanti opere frutto di donazione da parte della nobiltà napoletana e

del Principe di Satriano Gaetano Filangieri, fondatore del Museo. La sfida è stata quella di conciliare efficienza, affidabilità e costi contenuti in un progetto che risultasse congruo alle indicazioni del Nucleo Carabinieri Tutela Patrimonio Culturale e della Sovrintendenza del Polo Museale di Napoli. La società Massimiliano Bassano ha progettato e realizzato un sistema integrato in grado di offrire in un'unica soluzione la gestione dei sistemi antifurto/antieffrazione, di videosorveglianza e di rilevazione incendi.

Il progetto è stato realizzato con tecnologie all'avanguardia quali centrali di allarme espandibili su Linea Bus, telecamere IP Megapixel connesse attraverso Switch POE e un sistema di rilevazione incendi indirizzato composto anche da rilevatori lineari.
La apparecchiature di sicurezza sono state installate nel massimo rispetto delle strutture e dei manufatti esistenti - quali importanti mosaici – senza intaccare minimamente con i cablaggi l'estetica delle sale espositive e dei vari ambienti, sviluppati su quattro livelli.
In considerazione della diversa tipologia di destinazione d'uso degli ambienti, il sistema è stato suddiviso in più aree, singolarmente ed autonomamente gestibili attraverso le tastiere installate nei locali ed interconnesse alla centrale di gestione di tutto il sistema.

In particolare sono state realizzate le seguenti aree:
- Volumetrico interno eseguito con rivelatori a doppia tecnologia a protezione delle aree museali;
- Volumetrico esterno eseguito con rivelatori digitali a doppia tecnologia;
- Perimetrale, attivo 24 ore su 24, realizzato con l'installazione di rivelatori di impatto antisfondamento e di contatti magnetici a triplo bilanciamento a protezione di porte, finestre e balconi;
- Antieffrazione vetrine espositive, per una protezione costante delle opere, realizzato con l'installazione di contatti magnetici a triplo bilanciamento e di speciali rivelatori acustici di rottura vetri;
- Antieffrazione e antisabotaggio degli armadi rack contenenti le apparecchiature di gestione e comando dei sistemi di sicurezza.



Tali aree interagiscono mediante una minuziosa programmazione con gli impianti di videosorveglianza e rilevazione incendi e consentono di mettere in evidenza i singoli eventi grazie alle telecamere di pertinenza associate ai vari allarmi (antifurto, antieffrazione, antiaggressione e rilevazione incendi).
Una scrupolosa programmazione tesa ad assecondare l'andamento dell'attività museale unita alla scelta di codici tracciabili e multilivello consentono una gestione sicura e indipendente degli impianti. Oltre alle normali funzioni di gestione del sistema, il personale autorizzato ha anche la possibilità di effettuare una supervisione da remoto sulle telecamere e sul resto degli impianti di sicurezza mediante software e app proprietaria.
In caso di allarme gli impianti inviano le segnalazioni alla centrale operativa dell'istituto di vigilanza. Quest'ultimo verifica anche il regolare inserimento e disinserimento del sistema nelle fasce orarie prestabilite e interviene in caso di allarme generale o aggressione.
Tramite i software di gestione e manutenzione, l'azienda installatrice è in grado di monitorare costantemente il buon funzionamento di tutti gli impianti, con il vantaggio di un intervento tempestivo in caso di segnalazione di guasti o anomalie.

Grado di difficoltà, problemi e soluzioni:
La progettazione e la realizzazione del sistema di sicurezza integrato hanno avuto un grado di difficoltà elevato. Nella fase di progettazione si è dovuto scegliere materiali economicamente vantaggiosi ma nello stesso tempo di alta tecnologia e qualità, vista l'importanza del sito da proteggere. Considerando le notevoli difficoltà che si sarebbero incontrate nella stesura dei cavi e nei cablaggi, e soprattutto il fatto di non poter minimamente modificare l'estetica delle sale con cavi o tubazioni a vista, ci si è dovuti adattare a percorsi esistenti, al passaggio nel sottotetto e in alcuni cavedi che hanno consentito il transito delle tubazioni e dei cavi forando la parete e il solaio soltanto nel punto oggetto di installazione dell'apparecchiatura prevista.
Durante la fase di esecuzione, non potendo eseguire le lavorazioni durante la normale attività del Museo, ci si è dovuti adeguare agli orari e ai giorni di chiusura organizzando anche lavorazioni notturne e nei giorni festivi, avendo l'impegno di dover rispettare i tempi di consegna molto stretti.

Caratteristiche particolari dell'opera:
Nonostante la complessità dei sistemi installati, per garantire un elevato livello di sicurezza la gestione degli stessi è stata resa particolarmente semplice per gli operatori.
La suddivisione in più aree consente facilmente di interagire con gli impianti per le varie funzioni di utilizzo. Inoltre, mediante le memorie eventi e le e-mail di alert programmate, la Direzione può controllare gli orari di inserimento e disinserimento degli impianti e delle video ronde eseguite dalla vigilanza.

Staff e tempo impiegati per la realizzazione:
Per la realizzazione dei lavori sono state impiegate sei unità lavorative e i lavori sono stati eseguiti in trenta giorni.

Dichiarazione del committente sull'impianto
L'intervento è stato preceduto da una serie di contatti con il Nucleo di Tutela del Patrimonio Storico dell'Arma dei Carabinieri al fine di concordare le tipologie e le protezioni necessarie per un museo che, benché privato, è sottoposto ai vincoli imposti dalla Soprintendenza. Nell'esecuzione del progetto si sono costantemente resi partecipi tali organi, per cui attualmente il Museo Civico Gaetano Filangieri dispone di un sistema ai massimi livelli di sicurezza. Una delle caratteristiche che hanno fatto selezionare l'azienda installatrice è stata la garanzia triennale fornita e il costante monitoraggio, rendicontato su base mensile, della videosorveglianza affidata ad una ditta privata.

I racconti della Sicurezza - 5

Al di sopra di ogni sospetto

Racconto di Claudia Bulow Boje Ferrentino, tratto dalla rivista "EHF-Sicurezza per la cultura", organo ufficiale della Fondazione Enzo Hruby, anno XXIV, n. 2 – Giugno 2015

Questo racconto di fantasia si basa sulla notizia diramata nella primavera 2015 della scomparsa di due incisioni dalla prestigiosa collezione della Biblioteca Pubblica di Boston: un autoritratto di Rembrandt, del 1634, e *Adamo ed Eva* di Dürer, del 1504. Dopo indagini dell'FBI e un nuovo inventario le opere sono state ritrovate all'interno della Biblioteca, nella mensola sbagliata.

La copertina del *Boston Herald* è dominata dal titolo *Errore di catalogazione o furto*?
Susan compra una copia del quotidiano all'edicola sotto casa e scoppia a ridere fragorosamente leggendo l'articolo sulla Biblioteca pubblica di Boston, lancia d'impulso il giornale sul sedile del passeggero e mette in moto l'auto. Si immette a gran velocità nel traffico in direzione di Jacksonville, in Florida, dove ha affittato un appartamento per qualche settimana. Abbassa i finestrini e lascia che il vento le scompigli i lunghi capelli mori, sente improvvisamente un senso di leggerezza e libertà. Erano anni che Susan desiderava spostarsi al caldo, non vede l'ora di lasciare la valigia in camera e correre in spiaggia.
In quelle circostanze altre persone sarebbero state come minimo in panico o si sarebbero costituite alla Polizia, ma non Susan, quell'improvviso senso di pericolo le piace e si sente più viva che mai. Non avrebbe mai pensato di essere "protagonista" di una vicenda simile, mite e tranquilla come è sempre stata. Tutte le persone che la conoscono la descriverebbero come una ragazza minuta e timida, che tende a nascondersi dietro quella grossa montatura per occhiali da cui non si separa mai, insomma una ragazza semplice senza grilli per la testa che non ha mai spiccato molto né in campo scolastico né in quello lavorativo. Rispetto a queste apparenze, Susan è forse molto altro.
Ora si sente più in viaggio che in fuga, non ha infatti organizzato meticolosamente la sua partenza. Quando ha percepito che la situazione sarebbe potuta diventare pericolosa, ha lasciato il suo appartamento in condivisione con Yena, un'infermiera di origine thailandese, con la scusa di far visita ad una vecchia zia a Philadelphia. Ha raccolto tutti i suoi risparmi, qualche vestito e si è lanciata in un'avventura on the road.
I suoi tesori li tiene custoditi in un'agenda di pelle marrone che tiene attentamente nella sua borsa. Li guarda spesso con occhi orgogliosi. Non ha alcuna intenzione di restituirli o rivenderli, li vuole tenere tutti per sé, sono per lei il simbolo di una rivincita personale, di una svolta. Non sono dei cimeli di famiglia o qualche oggetto personale denso di ricordi, si tratta di due incisioni: un autoritratto di Rembrandt e una stampa che raffigura Adamo ed Eva di Dürer.
Susan pensa spesso a quel furto e si compiace. Si giustifica, pensando che quelle stampe conservate nella Biblioteca di Boston non erano affatto valorizzate prima della loro sparizione, grazie al suo "intervento" sono invece salite alla ribalta, finendo su tutti i giornali nazionali e internazionali. Non si tratta di opere di poco conto ma di due incisioni firmate, una dal maestro olandese, l'altra dal più grande esponente del rinascimento tedesco, valutate rispettivamente 30 mila e 600 mila dollari.
Eppure non erano ben protette, anzi per niente, rubarle è stato per Susan un gioco da ragazzi. Quando ha

avuto l'occasione di entrare nel Dipartimento Libri Rari ha "lasciato cadere" nel suo zaino quelle stampe così preziose senza escogitare alcun piano particolare. La volontà della Biblioteca di rendere l'arte accessibile e fruibile al pubblico senza però prevedere un necessario adeguamento dei sistemi di sicurezza ha reso ogni giorno migliaia di opere vulnerabili.
Inoltre, Susan, per quello stage in Biblioteca, come altri giovani appassionati d'arte, non aveva ricevuto alcun compenso. Pensava quindi di essersi meritata qualche ricompensa.
È passato già un anno dal furto, solo ora è diramata la notizia della scomparsa delle incisioni. Il Boston Herald rivela che secondo il primo rapporto della Polizia le due opere erano assenti dall'inventario dai primi giorni di aprile, mentre altre fonti fanno sapere che non si trovano da almeno un anno. "Errore di catalogazione o furto?" è questo il titolo in copertina, la Polizia sta dunque vagliando tutte le ipotesi ma sembra brancolare nel buio.
Susan si sente tranquilla e speranzosa di potersi godere quelle settimane di sole e di iniziare una nuova vita in Florida mantenendo quel grande e prezioso segreto per sé.

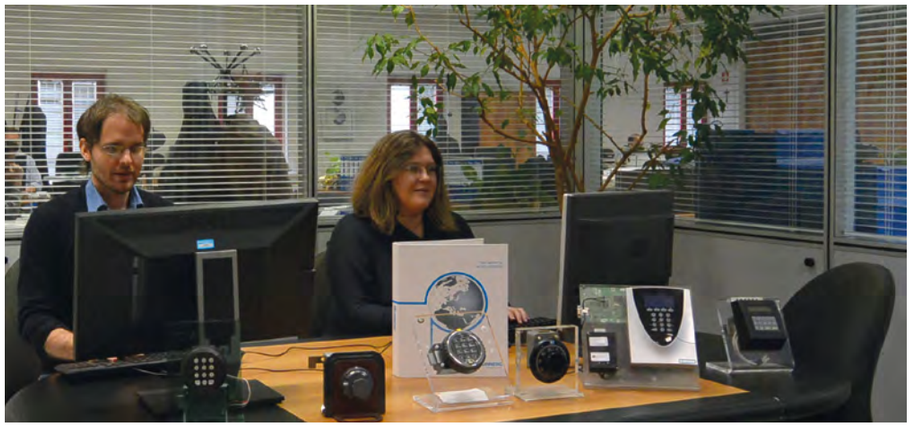
After-sales service, fiore all'occhiello dell'offerta Gunnebo per i mezzi forti

a colloquio con Luca Paloro, after sales service Gunnebo Italia spa
a cura della Redazione

Con una vasta gamma che comprende i marchi più conosciuti della sicurezza fisica (da **Chubbsafes** a **Lips Vago**, da **Fichet-Bauch**e a **Rosengrens**), Gunnebo è sicuramente uno dei principali operatori nel settore dei mezzi forti. Si tratta di prodotti altamente affidabili, ma nel caso si presenti la necessità di un intervento, la qualità del servizio è fondamentale: nessuno vuole rimanere a lungo con la cassaforte bloccata, né chiusa (impedendo l'accesso ai valori) né aperta (privando i beni della protezione che richiedono). Non è quindi un caso che Gunnebo dedichi ingenti risorse all'aspetto dell'*after sales service*, con personale altamente qualificato in grado di fornire un'assistenza eccellente. Come funziona in concreto il service Gunnebo? Lo abbiamo chiesto a Luca Paioro che, all'interno dell'azienda e con la collaborazione di Fabio, si occupa di questo importante servizio.

Cosa deve fare chi abbia un problema con il funzionamento della sua cassaforte?
La prima cosa da fare è chiamare il nostro numero verde 800 252 398: non si tratta di un tipico call center asettico - men che meno di un erogatore di messaggi automatizzati - ma di una vera e propria accoglienza telefonica al cliente dove i validi operatori Valeria e Enrico forniscono un contributo fondamentale all'attività di service. Con grande impegno, velocità e professionalità, raccolgono le necessità dei Clienti facendo domande specifiche per individuare al meglio il problema, la cui soluzione è a cura degli specialisti interni all'azienda che coordinano l'intervento dell' operatore più idoneo on site . Si tratta sempre di un tecnico qualificato e autorizzato da Gunnebo, che conosce perfettamente il prodotto ed è in grado di fornire il suo supporto in tempi rapidi in tutta Italia.

Oltre alla gestione dei malfunzionamenti segnalati dai clienti, offrite anche contratti di manutenzione programmata?
Naturalmente: la prevenzione è sempre la miglior strategia! Un controllo periodico è un ottimo sistema per minimizzare i rischi di dover intervenire d'urgenza, con conseguenti inevitabili disagi; inoltre gli eventuali interventi su mezzi forti sottoposti a regolari verifiche sono solitamente più rapidi e meno costosi rispetto alle riparazioni di casseforti che non hanno mai visto un tecnico dal giorno dell'installazione. La nostra rete di vendita propone programmi di manutenzione periodica a chi acquista mezzi forti, soprattutto se collocati in esercizi commerciali dove la costante affidabilità del servizio di custodia è fondamentale, e raccomanda di eseguire i controlli prescritti con regolarità.



Quali sono i punti di forza del servizio di assistenza Gunnebo?
Innanzitutto le tempistiche: riusciamo a concludere gli interventi in tempi che sono del tutto in linea con le aspettative e le esigenze dei clienti. Simili risultati sono resi possibili dalla capillare presenza sul territorio, che consente di garantire un rapido intervento al domicilio del cliente.
Oltre alla diffusione geografica, l'efficienza del nostro service deve molto anche alle caratteristiche professionali del team di tecnici qualificati e autorizzati Gunnebo: esperienza, competenza e forte orientamento alle necessità del cliente permettono di dare il meglio per risolvere il malfunzionamento in tempi rapidi.
L'assistenza per Gunnebo non si limita alla mera risoluzione del problema contingente ma la competenza del personale è a disposizione dei clienti anche per individuare soluzioni che garantiscano la soddisfazione del cliente nel lungo termine.

Evoluta, ergonomica, elegante: la nuova cassaforte Evolve

Evolve è una cassaforte evoluta, intelligente, elegante e sicura, con caratteristiche eccezionali: ergonomica, certificata EN 1143-1, apertura autom. motorizzata e battente senza maniglia nè fori.
Evolve è studiata per un utilizzo quotidiano, con accesso facilitato al contenuto dalla tastiera nella parte alta del battente.
Evolve ha un 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 è più alta che profonda per agevolare lo spostamento anche di oggetti piccoli e consentirle di adattarsi a spazi diversi, nelle abitazioni, uffici o negozi.
Certificata per il grado 1 da ECB.S, **Evolve** ha una serratura elettronica di sicurezza (EN 1300 classe B) con 1 codice master, 1 supervisore, 7 operatori, un ritardo di apertura programmabile da 0 a 99 minuti con possibilità di modifica e segnale di apert/chius..
Info su Evolve: http://www.cassefortilipsvago.it/casseforti-certificate/evolve-grado-i-size-1

Per ogni richiesta di informazioni relative ai mezzi forti si può contattare l'azienda:
All'indirizzo di posta elettronica numeroverde@gunnebo.com
All'indirizzo di posta elettronica lipsvago@gunnebo.com
Al numero verde **800 252398** oppure al numero **02 26710.1**
E infine tramite il nuovo sito dedicato interamente ai mezzi forti: www.cassefortilipsvago.it

Sistemi di sorveglianza discreti con la tecnologia kinsei di Xetal

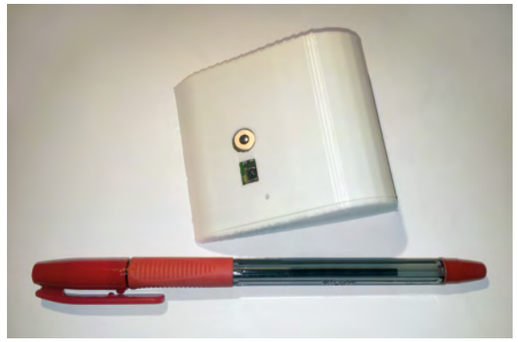
a colloquio con Mauro Maggiolini, CIO di Seeingsmart srl
a cura della Redazione

Sorveglianza discreta è un termine nuovo, quale è esattamente il suo significato?
Il termine "discreto" in italiano ha molti significati in questo caso lo utilizziamo nella accezione di "non invadente", "non importuno". Quindi intendiamo per *Sistemi di sorveglianza discreti* quei sistemi capaci di analizzare uno scenario per capire cosa stia succedendo ed individuare il verificarsi di particolari eventi, senza violare la privacy delle persone in esso coinvolte.

Perché pensate che ci sia bisogno di tali sistemi e perché le aziende dovrebbero adottarli?
Perché la sorveglianza, pur dovendo soddisfare le esigenze di sicurezza oggi tanto sentite, dovrebbe contemperarle meglio con le esigenze di privacy degli individui, che sono anche esse tanto sentite da poter condizionare il comportamento delle persone. Al momento, invece, la tecnologia utilizzata universalmente nell'automazione della vigilanza è la videosorveglianza che oggi domina incontrastata il mercato, raccogliendo miliardi di immagini di persone ignare, anche nei momenti e nei luoghi in cui non sussistono pericoli o sospetti di pericolo.
I sistemi da noi proposti tendono, invece, ad un migliore equilibrio tra le due esigenze, spostando le soluzioni verso un maggiore rispetto della privacy, senza tuttavia ridurre in modo significativo i livelli di sicurezza raggiungibili.

Quali sono i principi di funzionamento di questi sistemi?
Utilizzano una tecnologia innovativa, chiamata *kinsei*, sviluppata in **Xetal,** che assicura, per costruzione, la privacy delle persone coinvolte nello scenario sotto controllo, in quanto non utilizza immagini che ne consentano l'identificazione, come sono quelle che, invece, vengono fornite dalle telecamere.
Al loro posto si usano speciali sensori sviluppati da Xetal posti sulle pareti per controllare la posizione di una o più persone, con una precisione di circa 30 cm. Quando questa informazione viene associata alla conoscenza di uno spazio predefinito, *kinse*i può essere utilizzato per il rilevamento di una vasta gamma di eventi e situazioni, compresi gli incidenti probabili e altri rischi, in tempo reale, di giorno e di notte. *Kinsei* è affidabile, rispetta la privacy, può distinguere le persone dagli animali domestici, è estremamente facile da installare (non è necessario alcun cablaggio) e opera in modo indipendente dalle condizioni di illuminazione.

Quali sono le differenze o le analogie con telecamere e rilevatori di movimento, di cui questo sistema appare come un ibrido?
E' vero che assicurano funzioni di analisi dello scenario analoghe a quelle delle telecamere, ma lo fanno tutelando la privacy e lo fanno in modo completamente



automatico. Sono invece assolutamente diversi dai rilevatori di movimento a raggi infrarossi, che possono solo segnalare lo spostamento di persone. La tecnologia *kinsei*, anche grazie ad un sofisticato complesso di software, fornisce con estrema precisione il numero dei presenti anche se restano immobili, la loro posizione, i loro spostamenti, e può individuare situazioni di rischio, anche complesse, assicurando in ogni caso flessibilità di utilizzo, attendibilità dei risultati, affidabilità del funzionamento, interconnessione con altri sistemi elaborativi.

Come si integrano in un ambiente esistente?
In fase di installazione, apposite funzioni consentono di indicare al sistema la geometria del locale da controllare, le zone sensibili esistenti al suo interno e le condizioni da considerare sospette in base al numero di presenti, alla loro posizione ed ai loro percorsi all'interno del locale e nelle zone sensibili.
Durante l'esercizio, quando si verificherà una condizione per la quale è previsto che scatti un allarme, l'Hub farà squillare un dispositivo di allarme esterno come un campanello o un telefono fisso o mobile.
Per soluzioni più sofisticate, inoltre, l'Hub è in grado di segnalare le situazioni sospette, mediante il protocollo TCP/IP, ad un eventuale sistema di centralizzazione degli allarmi già in essere, per integrare e gestire segnali provenienti da sistemi di rilevazione basati su tecnologie diverse.

In quali forme pratiche questa tecnologia viene commercializzata attualmente?
Al momento vengono venduti due prodotti:
- **MoCa** che è un sistema finalizzato al controllo di ciò che avviene all'interno di un locale.
- **@Bed** che consente di controllare se una persona sta alzandosi o sta per cadere dal letto, quando nessuno gli è vicino.
E' inoltre stato annunciato un prodotto @Door che è in grado di gestire una porta automatica in base alla presenza di una o più persone, alla loro posizione rispetto alla porta da governare, il loro movimento e la loro direzione.
Tutti i prodotti Xetal sono commercializzati in Italia da Seeingsmart s.r.l..

Parlando di "riduzione delle immagini" si intende che le telecamere non siano dunque completamente eliminate?
In molti casi i sistemi di sorveglianza discreti possono essere considerati come una vantaggiosa alternativa ai sistemi di videosorveglianza sostituendoli completamente.
In altri casi, tuttavia, può essere più opportuno considerare i due impianti come due componenti che cooperano nei sistemi di allarme più complessi e sofisticati, per apportare ciascuno i vantaggi derivanti dalla caratteristiche fisiche della loro tecnologia di base.
La soluzione da noi proposta in questi casi si basa sulla scomposizione dell'attività di sorveglianza in due componenti:
- l'analisi proattiva che analizza nel continuo lo scenario per individuare situazioni sospette,
- la gestione delle situazioni sospette individuate dall'analisi proattiva.
La prima viene assegnata a sistemi di sorveglianza discreti, mentre le telecamere entrano in funzione solo quando sono effettivamente necessarie le immagini per dare supporto alla gestione delle situazioni sospette. Ne consegue una drastica riduzione del volume di immagini utilizzate a vantaggio della privacy.
Il vantaggio, inoltre, non è legato al solo aspetto quantitativo, infatti i video eliminati sono quelli ripresi in situazioni di non pericolo cioè quelli in cui le persone danno più valore alla privacy che alla sicurezza. Al solo sospetto di un pericolo, invece, il bisogno di sicurezza prevale e riprendere con le telecamere ciò che sta succedendo, diventa, per gli individui coinvolti,

una esigenza che mette in secondo piano i problemi di privacy.
L'uso promiscuo delle due tecnologie non aumenta il TCO perché il costo d'impianto dei sistemi discreti, di per sé contenuto, viene compensato dalla semplificazione dell'impianto di videosorveglianza (apparecchiature di ripresa, stoccaggio e trasmissione delle immagini) e dalla riduzione dei costi e delle complessità per l'installazione e la gestione.

In quali campi di applicazione ritenete che possano essere utilizzati ?
La tecnologia proposta è stata originariamente sviluppata per risolvere i problemi di sorveglianza di quelle persone malate che hanno bisogno di una assistenza continua, come ad esempio i pazienti affetti dal morbo di Alzheimer, dalla demenza senile, o quelli a cui è stato prescritto il divieto di abbandonare il letto da soli. In questi casi, infatti, l'esigenza di privacy è massima ed essere soggetto ad una videosorveglianza continua peggiorerebbe le condizioni di vita del paziente.
L'utilizzo della sorveglianza discreta in questi casi consente di migliorare le condizioni di vita dei pazienti riducendo il ricorso a sistemi di contenzione fisica.
D'altro canto, le strutture che li ospitano e che sono responsabili della loro salute, grazie a questa forma di automazione, possono ridurre il numero di addetti alla sorveglianza, senza accrescere il rischio di incidenti del paziente.
Dopo una lunga fase di sperimentazione presso strutture che operano in Belgio, abbiamo avviato nel 2015 la commercializzazione dei prodotti per la sanità anche in Italia, completando la prima fornitura ad un importane ospedale del prodotto @Bed specializzato per il controllo del paziente nel suo letto.
Contemporaneamente sono in corso diverse riflessioni e sperimentazioni in altri comparti applicativi quali ad esempio:
- controllo delle presenze
- prevenzione incidenti domestici
- gestione emergenze
Anche in ambito bancario, i sistemi di sorveglianza discreti offrono soluzioni ottimali per numerosi problemi come, ad esempio, la protezione degli ATM da attacchi fisici mediante la cooperazione con l'ATM in un sistema di "monitoraggio attività correlato".
Di recente, inoltre, abbiamo concluso una sperimentazione che ha dato esiti estremamente incoraggianti per la segnalazione di situazioni critiche nei locali di una agenzia bancaria quali, ad esempio:
- eventuale malore occorso ad un cliente presente nell'Area self quando è unattended;
- eventuale occupazione indebita della Area self, ad esempio quando è presente un numero di persone maggiore del massimo prefissato;
- determinare il numero di clienti presenti nel salone o area destinata al pubblico e correlare a tale numero la gestione automatica delle porte interblocco di accesso all'agenzia.

seeingsmart

La società Seeingsmart srl è stata costituita nel gennaio 2014 con l'obiettivo di sostenere la diffusione di sistemi di **sorveglianza discreti**, sistemi cioè capaci di analizzare uno scenario per capire cosa stia succedendo ed individuare il verificarsi di particolari eventi, senza violare la privacy delle persone in esso coinvolte.
L'idea è nata dalla collaborazione con **Xetal**, una società fiamminga, fondata e gestita da ricercatori italiani, che ha messo a punto una specifica tecnologia che consente di offrire sul mercato prodotti innovativi.
Le attività di **Seeingsmart** sono concentrate sulla diffusione in Italia sistemi di sorveglianza discreti. E' stato stipulato un accordo di distribuzione esclusiva per l'Italia dei prodotti di Xetal, della quale vengono venduti i prodotti ed i servizi di istallazione e manutenzione ad essi correlati. Viene studiata la domanda potenziale di prodotti Xetal nei vari comparti del mercato Italiano: sanità, banche, grande distribuzione, alberghi, farmacie, tabaccherie, ecc., ricercando nuove possibili applicazioni della tecnologia Xetal. E' in fase di sviluppo una rete di distribuzione per coprire l'intero territorio nazionale.
Mauro Maggiolini è il CIO di Seeingsmart srl che ha fondato insieme a Roberto Camilli (Presidente) ed Alberto Stefanecchia (Amministratore Delegato); collabora, inoltre, con Tecnologie Informatiche srl in veste di Consulente.
Ha lavorato nel settore ICT sin dal 1965 con ruoli e responsabilità sempre crescenti prima, per 9 anni, presso le Ferrovie dello Stato e successivamente, per 33 anni, presso la Banca D'Italia.

La Fondazione Hruby sostiene la protezione del Teatro Niccolini di Firenze

a cura della Redazione

Le più avanzate tecnologie di sicurezza vanno in scena nel tempio italiano della prosa. Carmelo Bene, Carlo Cecchi e Vittorio Gassman sono solo alcuni dei nomi illustri che hanno calcato le scene del **Teatro Niccolini**, il più antico di Firenze. La sua origine risale al 1650, quando un gruppo di nobili prese in affitto alcune stanze di palazzo Ughi in via del Cocomero costruendovi il teatro, che negli anni Settanta e Ottanta del Novecento fu un centro privilegiato per la prosa, tra i più importanti in Italia. Inutilizzato dal 1995 e pesantemente danneggiato dall'incuria, viene acquistato nel 2006 dall'imprenditore fiorentino Mauro Pagliai che avvia un'importante ristrutturazione, grazie alla quale oggi il teatro viene restituito alla città nel suo splendore originale. Nell'ambito di questa riqualificazione, la **Fondazione Enzo Hruby** ha sostenuto un importante intervento di protezione che ha permesso il rinnovo di tutti gli impianti di sicurezza, coinvolgendo la società **Inim Electronics** che ha offerto un contributo concreto al progetto per la parte riguardante il sistema antincendio.

Per una corretta protezione antintrusione, è stato realizzato un sistema di sicurezza all'avanguardia che permette il controllo di tutti i varchi e delle sale. Eleganti tastiere touchscreen consentono una gestione facile e intuitiva, che può avvenire anche attraverso app da smartphone. Per le comunicazioni di allarme vengono impiegati i vettori GSM/GPRS ed IP. La protezione antincendio, di fondamentale importanza

in un edificio di questo tipo, destinato ad ospitare oltre 400 spettatori ad ogni rappresentazione, è stata realizzata attraverso l'impiego di una centrale e di rivelatori di fumo di ultima generazione. Il sistema di videosorveglianza, che permette di controllare i locali ed i flussi delle persone avvalendosi di decine di telecamere megapixel su rete IP con funzione motion detection, è in grado di offrire, in caso di necessità, un valido supporto alle indagini delle Forze dell'Ordine. Tutte le immagini riprese sono registrate in modalità digitale ad alta definizione 24 ore su 24 e possono essere visualizzate in modo efficace ed in tempo reale su monitor da diverse postazioni di controllo. Trattandosi di un contesto di importante valore storico e artistico, è stata prestata la massima attenzione a mimetizzare le apparecchiature di sicurezza nel rispetto dell'estetica degli ambienti.

"Ognuno dei quarantanove progetti che abbiamo sostenuto fino a oggi – dichiara **Carlo Hruby**, Vice Presidente della Fondazione Enzo Hruby – *riveste un'importanza particolare: per alcuni è il prestigio del monumento, per altri la soddisfazione di offrire sicurezza ad un bene del patrimonio minore, che in Italia ha una diffusione straordinaria su tutto il territorio. Ma a rendere ogni volta speciale l'intervento è soprattutto il valore della condivisione con quanti hanno come noi a cuore la protezione del patrimonio storico e artistico italiano. E il progetto per la protezione del Teatro Niccolini di Firenze è per questo davvero straordinario, essendo realizzato grazie a tutti coloro che hanno sostenuto la Fondazione Enzo Hruby con il contributo del 5x1000 devoluto nel 2013. A ciò si aggiunge il valore del contributo offerto dalla società Inim Electronics che, coinvolta dalla nostra Fondazione, ha sostenuto questo importante progetto al nostro fianco".*

"Condividiamo la visione della Fondazione Enzo Hruby e la sensibilità per la salvaguardia del patrimonio storico-artistico italiano" – conclude **Elisabetta Saini**, Direttore Commerciale di Inim Electronics. *"Il Teatro Niccolini è stato il primo progetto portato avanti in collaborazione con la Fondazione, ma non l'unico di Inim: la protezione di cose e persone, unita all'attenzione per il sociale fanno parte della nostra mission e cercheremo sempre risorse per sostenere questo tipo di iniziative. Ringraziamo la Fondazione Hruby per la possibilità che ci ha offerto e per aver scelto la nostra tecnologia per proteggere una struttura di tale valore culturale, che auspichiamo possa offrire ai giovani talenti che calcheranno questo palcoscenico le stesse opportunità dei loro illustri predecessori."*

CONTATTI: FONDAZIONE HRUBY
info@fondazionehruby.org
www.fondazionehruby.org

La security nei luoghi di spettacolo, questa sconosciuta

di Valerio Weinberger

Il dibattito organizzato da **essecome** durante Sicurezza 2015 di Milano dedicato al tema Safety e Security in palcoscenico e nei luoghi di **spettacolo** ha attirato l'attenzione di alcuni professionisti sul tema della sicurezza nei luoghi di spettacolo: teatri, auditori, sale da concerto, cinematografi.

Era ora.

Per macabra coincidenza, ciò avveniva pochi giorni prima del feroce attentato terroristico messo in atto da criminali di matrice fanatico-islamista al teatro Bataclan di Parigi. E durante la discussione a Milano lo spettro di un atto terroristico in un luogo di spettacolo era stato evocato…

Gli esperti sanno che un grado di sicurezza assoluta in un luogo pubblico frequentato da molte persone è pressoché impossibile; stessa cosa, a maggior ragione, in un luogo di spettacolo frequentato ogni giorno da centinaia o migliaia di addetti e spettatori.

Gli spettatori vengono per assistere alla proiezione di un film, a un'opera, un concerto, una pièce teatrale, un balletto, in ogni caso a un momento di bellezza e di emozione, di concentrazione o di spensieratezza, d'intrattenimento o di riflessione, secondo i casi. Sono quindi forse poco indotti ad usare alcune elementari misure di accortezza, vigilanza e prudenza, analoghe a quelle che invece, come cittadini, probabilmente mettono in atto in altri contesti, ad esempio per prevenire scippi, furti, rapine, che so?, al supermercato, al ristorante, in un parcheggio, o semplicemente per strada…

Anche sul versante di quanti hanno varie responsabilità su teatri, auditori e cinematografi (organizzatori, gestori, pubblici amministratori, forze di sicurezza) si deve constatare come tutt'ora non abbondi fra gli addetti la consapevolezza di quale crescente importanza e rilevanza abbiano le pratiche legate alla prevenzione e alla sicurezza, a trecentosessanta gradi. Le misure legate alla sicurezza in teatri, auditori e cinematografi sono perlopiù ancora riferite, come in una sorta di automatismo mentale derivante forse dal dover applicare normative cogenti, agli aspetti dell'antincendio e alle vie di fuga in caso di evacuazione e panico.

Purtroppo, invece, l'evoluzione più recente della situazione internazionale, con le sue drammatiche accelerazioni, dovrebbe indurci a tener presente che teatri e sale da concerto, al pari di scuole, università o edifici di culto, sono luoghi esposti alle peggiori intenzioni, potenziali obiettivi di fanatismi religiosi e politici di varia natura, non solo jihadista. E dovrebbe portarci a osservare che spesso questi luoghi sono vigilati e difesi in maniera insufficiente. Forse fino ad ora i luoghi di spettacolo sono stati intesi, da quanti vi operano professionalmente o li frequentano da spettatori, come contesti ove è consentito un certo grado di "guardia bassa". Ebbene, è vero il contrario: i fatti di Parigi sono lì a mostrarcelo, con la cruda e concreta evidenza dei fatti tragici.

Dossiamo poi ammettere che le chiare avvisaglie giunte dal Teatro Dubrovka di Mosca, nell'ormai lontano 2002, sono state rapidamente e sostanzialmente ignorate o "rimosse", per varie ragioni. La distanza: nel mondo occidentale Mosca è, nella nozione dei più, una città di un altro continente, quasi di un altro mondo. L'epoca: nel 2002 la diffusione delle informazioni via internet, specie dalla Russia, non aveva certo la penetrazione capillare e la velocità che ha oggi. La sottovalutazione: in occidente era diffusa la sensazione che i conflitti legati al radicalismo terrorista di matrice fanatico-islamista potessero restare circoscritti e confinati in alcune situazioni "calde". Tutto ciò non è più così.

Che fare quindi?

La prima necessità è favorire l'acquisizione di una piena, matura e compiuta coscienza di quali siano oggi i livelli di rischio, e di quale debba essere di conseguenza l'attenzione da dedicare ad essi. Ciò può essere reso possibile solo iniziando con un attento, puntuale, non rituale o "chiacchierato" confronto fra esperienze, competenze, conoscenze, con una documentata riflessione su tecniche e pratiche.

A questo proposito i luoghi, virtuali o fisici, dove i professionisti e gli esperti s'incontrano con regolarità, nonché le loro associazioni di categoria, i loro consessi industriali, dovrebbero essere il punto naturale di partenza per questo processo.

Insomma, si moltiplichino e si allarghino le occasioni nelle quali chiamare a confronto gli addetti e gli "specialisti".

In secondo luogo, una maggiore attenzione da parte dei media potrebbe giovare all'allargamento di una consapevolezza diffusa da parte dei cittadini, che il godimento di un film o di un concerto può non essere disgiunto da una consapevole attenzione.

Inoltre momenti introduttivi e didattici nelle scuole potrebbero contribuire ad elevare il grado di diffusione di tale consapevolezza.

Senza militarizzare teatri, auditori o grandi arene usate per concerti, alcune misure possono essere attuate gradualmente, senza troppi sforzi, e con costi tutto sommato contenuti.

Qualche utile spunto può venire da un confronto con pratiche in uso nel trasporto aereo.

Alcuni esempi:

- l'adozione generalizzata della nominatività di biglietti e titoli d'ingresso, con controlli almeno casuali e occasionali della coincidenza, cui si può legare l'accelerazione del processo di crescente virtualizzazione dei biglietti (in alcuni teatri, per ora pochi, già si può entrare con un codice QR sullo smartphone, letto da una maschera mediante uno strumento mobile, o da un dispositivo fisso connesso a un varco per controllo accessi);
- la tracciabilità costante delle forme di pagamento (già di fatto favorita dalla crescente diffusione dell'acquisto di biglietti via internet), incentivando l'uso di carte di credito o bancomat;
- una moltiplicata installazione di telecamere a circuito chiuso per controllare non solo gli accessi e i perimetri esterni dei luoghi di spettacolo (talora già avviene), ma anche atrii, foyer, sale;
- brevi e chiare indicazioni date agli spettatori prima dell'inizio dello spettacolo sull'ubicazione delle uscite di sicurezza e sui percorsi di evacuazione;
- appositi corsi di formazione per maschere e personale di sala in genere che, purtroppo, quasi mai è formato per mettere in atto forme di controllo che vadano oltre i biglietti e una generica sorveglianza antincendio;
- obbligatoria presenza deterrente e vigilante di addetti alla sicurezza specificamente addestrati (perché ciò che è considerato normale in discoteche, stadi, aeroporti, stazioni ferroviarie o di metropolitana, non lo è altrettanto in teatri e cinematografi…?).

E l'elenco potrebbe allungarsi, con suggerimenti puntuali formulati da persone più esperte di chi scrive. Prima che un paio di prossimi attentati costringano le autorità competenti a considerare l'adozione di misure molto più restrittive (i metal detectors agli ingressi dei teatri…?), sarà forse opportuno che teatri, auditori, sale da concerto e cinematografi diano inizio a un processo di attenta riflessione su questi aspetti.

Nel 2016 ritorna Security & Counter Terror Expo

traduzione a cura di Federica Guizzo

L'evento, destinato a tutti gli operatori del settore della sicurezza nazionale e di beni e attività commerciali, si terrà a Londra il 19 e il 20 aprile.

I recenti sviluppi del terrorismo internazionale sono stati consistenti, con molteplici attacchi che hanno colpito su scala globale. La minaccia è in costante evoluzione ed è attualmente a un livello significativamente elevato in tutto il mondo. In Europa, a seguito degli ultimi avvenimenti, la questione della sicurezza nazionale e della lotta al terrorismo è in cima all'agenda dei governi. *Security & Counter Terror Expo* rifletterà tutti questi sviluppi e sarà l'occasione per presentare le tecnologie di avanguardia e valutare le ultimissime strategie. L'evento riunirà fondamentalmente i professionisti locali e internazionali, e prevedrà una serie di attività destinate a coloro che operano sia nel settore pubblico che in quello privato.

L'esposizione, che si terrà sempre all'Olympia di Londra, il 19 e il 20 aprile 2016, è il principale evento dedicato a tutti i professionisti che si occupano di preservare la sicurezza a livello nazionale, proteggere beni e persone contro gli atti di terrorismo e offrire le strategie di sicurezza più efficaci.

Nei due giorni di evento, in linea con le sette funzioni di sicurezza del Ministero dell'Interno del Regno Unito, saranno illustrate le ultime innovazioni in termini di tecnologia, di attrezzature e di servizi progettati al fine di agevolare i controlli alle frontiere, la protezione delle infrastrutture nazionali critiche, la sicurezza informatica, i grandi eventi, la gestione dei detenuti, le attività antiterrorismo e i servizi di pronto intervento.

David Thompson, Event Manager, ha dichiarato:

"I recenti avvenimenti che hanno interessato tutta l'Europa ci ricordano che la questione della sicurezza non è mai stata così importante. I bersagli sono sempre più disparati, così come i metodi utilizzati da coloro che cercano di farci del male."

"I terroristi continueranno ad adottare tattiche volte a evitare le intercettazioni, pertanto, l'intero settore della sicurezza dovrà essere sempre un passo avanti investendo nelle nuove tecnologie e nelle soluzioni di intelligence necessarie per far fronte alle minacce attuali e future."

Security & Counter Terror Expo svolge un ruolo fondamentale nel fornire un ambiente unico in cui i professionisti della sicurezza globale possono scoprire le soluzioni più innovative per combattere il terrorismo. Geoquip, NEC, Aselsan e Jackson's Fencing sono alcune delle più importanti multinazionali ad aver già confermato la loro presenza all'evento del 2016 e si uniranno a una serie di nuovi espositori.

Durante l'esposizione la sicurezza informatica rivestirà un'importanza fondamentale: la conferenza *The Cyber Threat Intelligence* vedrà le figure principali di questo

ambito discutere degli ultimi sviluppi. A cura di techUK, l'organo rappresentativo del settore tecnologico nel Regno Unito, riunirà tutti coloro che si occupano di combattere il terrorismo e la criminalità a livello informatico. Tra gli argomenti all'ordine del giorno, una panoramica delle minacce globali alla sicurezza informatica e le modalità con cui ridurle.

Talal Rajab, Programme Manager dei programmi *Cyber, National Security and Criminal Justice* (sicurezza informatica, sicurezza nazionale e giustizia penale) di techUK, ha aggiunto: *"Quello che un tempo, nel più ampio dibattito nazionale sulla sicurezza, era considerato un settore di nicchia è oggi la priorità di molti governi. Security & Counter Terror Expo è la piattaforma ideale per apprendere dalle figure più eminenti e restare in contatto con i principali e influenti responsabili del settore."*

Le infrastrutture nazionali critiche rappresenteranno sempre l'obiettivo primario dei terroristi e difenderle è un compito arduo e impegnativo. La conferenza *Critical National Infrastructure* (infrastrutture nazionali critiche) affronterà questa problematica illustrando le modalità per garantire la sicurezza e la resilienza dei beni e delle reti critiche.

L'esposizione del 2016 prevede inoltre una *Policing and Special Ops Zone* (area operazioni di polizia e operazioni speciali) dove saranno presentati gli ultimi prodotti, le strategie, le squadre speciali, e dove si rifletterà sull'applicazione della legge a livello mondiale.

In programma anche il popolarissimo *Hosted Buyer*, che offre agli operatori alla ricerca delle apparecchiature o della tecnologia di nuova generazione l'opportunità di organizzare preventivamente gli incontri con i fornitori interessati.

World Counter Terror Congress è stato invece ideato per offrire idee, analisi e prospettive contro le minacce attuali. Si tratta di un programma esteso e altamente specializzato di workshop, dibattiti e sessioni plenarie sviluppate per analizzare nel dettaglio le singole questioni, con un forum incentrato sulla discussione.

La parte centrale del programma è il *World Counter Terror Congress*, a pagamento, che presenterà alcune delle figure di spicco nel settore della sicurezza. Mark Rowley, Vicecommissario *Specialist Operations* presso il *Metropolitan Police Service*; Dottor Jamie Shea, Vice sottosegretario generale *Emerging Security Challenges* (sfide emergenti in materia di sicurezza) presso la NATO; e Sir Malcolm Rifkind QC, ex Presidente dell'*Intelligence and Security Committee* britannico, sono solo alcuni degli oratori confermati.

Si terrà inoltre una serie di conferenze gratuite dedicate agli specialisti e incentrate sulla sicurezza dei trasporti e sulle tecnologie avanzate.

La sede dell'evento è la stessa di *Ambition – EPRR Expo* – e di *Forensics Europe Expo*.

Per partecipare in qualità di auditori o di espositori al *Security & Counter Terror Expo 2016*, o per ulteriori informazioni, si prega di visitare il sito web http://www.counterterrorexpo.com

SECURITY & COUNTER TERROR EXPO
19-20 APRIL 2016 | OLYMPIA LONDON

DIGITAL WORLD, una nuova fiera per innovazione, tecnologia e mondo del digitale a Rimini dal 29 aprile al 1 maggio

a cura della Redazione

Digital World, una nuova Fiera di portata internazionale dedicata all' innovazione, alla tecnologia e al mondo del digitale in tutte le sue forme, si svolgerà presso la Fiera di Rimini dal 29 Aprile al 1 Maggio 2016.
La Fiera, organizzata dalla società Valorexpo di San Marino, rappresenta una piattaforma espositiva e di informazione che mira allo scambio e al collegamento tra le aziende del settore e a opportunità per il business, ma è orientata anche ad attrarre e coinvolgere un pubblico ancor più ampio. È' infatti un'occasione unica per gli espositori, per un incremento di contatti business e miglioramento dell'efficacia commerciale, ma anche un evento per i visitatori interessati alla scoperta delle nuove tendenze e tecnologie, con un'ampia offerta merceologica. **Digital World** è pensata sia per le aziende e professionisti ma anche per l'appassionato e per il semplice curioso, per chi è attratto dalla tecnologia e dal suo utilizzo nella vita di tutti i giorni.
Una Fiera per presentare le ultime novità in ambito tecnologico innovativo, promuovere nuove tecnologie ICT, conoscenza, formazione e imprenditorialità, ricca di contenuti, attività, strumenti e progetti che mettono in risalto l'evoluzione digitale e delle nuove tecnologie della comunicazione, dei servizi operativi dedicati alle aziende e delle applicazioni. **Digital World** si sviluppa su tematiche quali:

- **ICT:** Telecomunicazioni, radio, tv streaming, video, mobile e tablet, blog e social network;
- **IT:** servizi hardware e software, servizi cloud, hybrid e virtual, app development, e-commerce, mobile payment;
- **Smart Technology:** dal confort alle innovazioni nel campo della domotica, robotica, sistemi di sicurezza e video-sorveglianza, impianti di illuminazione e automazioni;
- **Soluzioni tecnologiche per Aziende:** strumenti professionali per video riprese come Droni, Rov, Uav e dirigibili per riprese aeree, telecamere per ispezione ad immersione, termo-camere, fotografia digitale;
- **Green Digital:** tecnologie ecologiche applicate all'efficienza energetica.

In un'epoca in cui la tecnologia è sempre più diffusa ed utilizzata in ogni ambito del sociale, gli oggetti e i macchinari diventano sempre più intelligenti, dinamici e interattivi. La tecnologia smart applicata a questi oggetti, consente "alle macchine" di interagire con gli esseri umani a vari livelli ed imporsi con maggior forza nel mercato dei dispositivi dedicati alla salute, allo sport e al tempo libero. Grazie alla possibilità di poter ricevere e trasmettere dati attraverso la connessione internet, prende sempre più piede la categoria di quei dispositivi da portare sempre con sé, facili da indossare e con un'attenzione particolare al gusto estetico, al quale va ad aggiungersi la capacità di controllare e gestire le funzioni vitali. Sono gli innovativi werables, come gli orologi intelligenti che monitorano e stimolano a migliorare lo stile di vita. Altri ancora sono quei dispositivi che ci accompagnano in un viaggio o in un attività sportiva, come le telecamere ad alta risoluzione dinamica che consentono di riprendere le immagini di una giornata dedicata al nostro sport

preferito o ad una vacanza e di geolocalizzare la nostra posizione trasmettendo dati in tempo reale. Scopri le ultime tendenze ideate per aumentare le prestazioni connettendoti a dispositivi e macchinari pensati per la salute, lo sport e il tempo libero che rendono la vita più semplice liberando dai piccoli impegni quotidiani.
Digital World, quando l'innovazione si fonde con la salubrità degli ambienti in cui si vive e la vita migliora grazie alla tecnologia intelligente a portata di mano, programmando la sicurezza e la manutenzione della casa grazie alla "domotica" e alle sue molteplici applicazioni e innovazioni per l'efficienza Energetica (tecnologia per l'industria, sistemi di illuminazione, climatizzazione, monitoraggio, robotica).
Nell'ottica di rispondere alle esigenze di risparmio energetico e rispetto per ambiente, dettate anche dalle nuove normative per la sostenibilità e l'efficienza energetica, **Digital World** sarà un'occasione di approfondimento riguardo le agevolazioni 2016 per famiglie e imprese. **Seminari e conferenze** su agevolazioni per riqualificazione di case, alberghi ed edifici, detrazioni fiscali, prestiti agevolati per avviare investimenti per il miglioramento dell'efficienza energetica e l'energia rinnovabile.

Quando il Digitale incontra il mondo dell'immobiliare.
Sempre più realtà del settore usufruiscono della tecnologia digitale per la presentazione dei propri servizi e delle proprie offerte.
Nella stessa location sarà presentata "Real Estate Expo & Networking", fiera internazionale dedicata all'immobiliare e ai servizi ad esso congiunti, in Italia e all'estero; in esposizione il mondo dell'immobiliare con le offerte e opportunità d'investimento. La presenza di questo settore sarà un'occasione in più per creare reti di relazioni, sinergie e sviluppare rapporti B2B.
Quando il Digitale incontra il mondo finanziario-bancario.
Un aspetto unico di questa fiera è il format innovativo proposto, la concomitanza del Forum d'Investimenti Internazionale in ambito immobiliare, di innovazione, di sviluppo territoriale e di collaborazioni internazionali "INVEST WORLD". Un'opportunità per presentare e conoscere le tecnologie digitali al servizio del settore finanziario-bancario.
"Invest World" in programma il 29 e 30 Aprile a RiminiFiera presenterà al grande pubblico e alla comunità imprenditoriale internazionale le opportunità d'investimento in Italia e all'estero in ambito finanziario, industriale, territoriale, d'innovazione e tecnologia, turistico, culturale e di attività per collaborazioni internazionali. Questo importante appuntamento segnerà un punto di riferimento per la consulenza finanziaria e sarà una piattaforma di incontro fra imprenditori, consulenti e investitori dove proporre il Know How italiano come core business del Paese.
Digital World dal 29 Aprile al 1 Maggio 2016 a RiminiFiera aperta al pubblico dalle 10.00 alle 20.00.
Tutte le informazioni relative a Digital Word ed eventi correlati si possono trovare sul sito internet della società Valorexpo www.valorexpo.com e nelle pagine Facebook degli eventi. Infoline: (0039) 0549-909067, e-mail: digitalworld@valorexpo.com.

NVX80: la tecnologia più avanzata per la massima affidabilità.

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

Il rivelatore di movimento **NVX80** di **PARADOX** distribuito da DIAS stabilisce il nuovo standard dei rivelatori per esterno, offre la massima affidabilità in ogni condizione climatica e ambientale, con la funzione "SeeTrue" per identificare i tentativi di mimetizzazione degli intrusi. NVX80 unisce tecnologie a infrarossi passivi e a microonde e delle funzioni antimascheramento e antistrisciamento. L'antimascheramento a infrarossi attivi riconosce il degrado nella trasparenza della lente e gli oggetti che bloccano la lente principale entro 30 cm dal rivelatore; l'antimascheramento a microonde consente la rilevazione di movimenti a breve distanza (m 0.75 –m 2.00). NVX80 assicura un'alta immunità agli animali domestici e ai falsi allarmi, è protetto contro la rimozione e l'apertura ed è facile da installare e da regolare. A corredo del rivelatore viene inoltre fornito un kit comprendente un tettuccio protettivo per l'utilizzo in esterno e una squadretta con snodo che consente di ottenere la copertura ottimale in ogni tipo di installazione.

ELAN presenta le nuove Batterie al Litio BIGBAT.

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

ELAN arricchisce il suo portafoglio prodotti con novità interessanti. Il marchio storico **BIGBAT**, già produttore delle Batterie al piombo STANDARD e LONG LIFE, ha da poco lanciato sul mercato otto nuovi modelli di **Batterie al Litio**.
Queste batterie vengono utilizzate per il funzionamento di una vasta gamma di apparecchi elettronici quali sistemi di sicurezza, sensori, telecomandi, telecamere e fotocamere, elettrodomestici a bassa potenza ed altro ancora.
ELAN e **BIGBAT** offrono al cliente modelli da 3V (CR) e 3.6V (ER) con diverse tipologie di amperaggio e in grado di operare ad una temperatura che normalmente oscilla tra i -55°C e i +85°C.
L'affidabilità e l'esperienza dell'azienda fanno di queste batterie un prodotto estremamente sicuro e di elevata efficienza. I test hanno dimostrato infatti che lo stoccaggio per 10 anni delle batterie al Litio BIGBAT, a temperatura ambiente, porta ad una dispersione di capacità inferiore all'1% l'anno.
Non a caso BIGBAT è da anni garanzia di qualità nel settore delle batterie ricaricabili.

Mai più chiavi… Cilindro wireless ekey lock.

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

Grazie alla combinazione tra cilindro wireless e lettore d'impronte digitali, il retrofit di una soluzione ekey nella porta di casa diventa molto facile. Il lettore d'impronte vi dà una sicurezza in più rispetto alla chiave che può essere persa, dimenticata o rubata.

Vantaggi di ekey lock

- Per porte interne, esterne e in vetro
- Nessun cavo all'interno della porta
- Montaggio semplice
- Facilmente smontabile in caso di trasloco
- Senza modifica dei serramenti e infissi
- Transponder attivo come "seconda chiave per gli ospiti"
- Elevato standard di qualità e sicurezza a costi accessibili
- ekey lock è indicato per abitazioni private, aziende e immobili in affitto

Al riconoscimento di un dito memorizzato, il lettore d'impronte invia un segnale cifrato al cilindro wireless nella porta. Il pomello sul lato esterno della porta si accoppia e il cilindro può essere "sbloccato" come se ci fosse una chiave – girando il pomello. Il cilindro wireless è alimentato con una batteria.

HESA presenta la nuova centrale ZeroWire di UTC.

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

La nuova centrale **ZeroWire** di UTC distribuita da HESA si distingue per alta affidabilità, semplicità di installazione, manutenzione e gestione ed elevate prestazioni.
Con 64 zone e 4 aree, offre le funzioni più innovative, come l'integrazione con telecamere IP per video verifica, il collegamento e la gestione del sistema tramite app e l'automazione domotica tramite il protocollo Zwave. La programmazione è semplice e veloce e può essere eseguita anche da remoto tramite app su smartphone.
ZeroWire è dotata di tastiera a bordo e sirena interna e può essere collegata alla rete Internet tramite cavo IP o wi-fi, o ancora acquistando una scheda 3G da inserire nella centrale. La nuova centrale ZeroWire è compatibile con tutti i sensori via radio appartenenti alla gamma di UTC a 433 MHz, oltre che ad alcuni tra i dispositivi più affidabili oggi presenti sul mercato resi disponibili da HESA già assemblati con i trasmettitori. ZeroWire saprà farsi apprezzare anche dagli utenti più esigenti, andando incontro a tutte le necessità di sicurezza e confort.

Nuova centrale Laser Unit.

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

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

Datix Wi-Track Pro, il lettore ronda evoluto.

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

Datix Wi-Trak Pro è il lettore portatile per il controllo in tempo reale di ronde e servizi di vigilanza con specifiche funzionalità per la sicurezza degli Operatori. Il terminale legge tag RFID ed integra ricevitore GPS per localizzazione all'aperto. Il lettore permette chiamate rapide a 2 numeri e la trasmissione di dati di timbratura ed allarmi in tempo reale al centro di monitoraggio via connessione dati bidirezionale. Per la sicurezza dell'Operatore, il dispositivo è dotato di allarme panico attivabile da tastiera e sistema di allarme automatico "uomo a terra".
Datix Wi-Trak è compatibile sia con software presso datacenter delle Società di Vigilanza sia con **Datix2Cloud**, il nuovo servizio cloud SaaS per la gestione di picchi di lavoro e commesse temporanee senza investimento in PC dedicati.
Datix Wi-Trak Pro è la soluzione per le Società di Vigilanza moderne per le quali è irrinunciabile semplificare le procedure, razionalizzare le risorse, garantendo la sicurezza degli Operatori e la erogazione ai Clienti di servizi sempre più puntuali.

VUpoint per verifiche video live inHD.

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

VUpoint è la rivoluzionaria soluzione di RISCO per realizzare la verifica video live in HD, integrando perfettamente i sistemi di sicurezza professionali RISCO con Telecamere IP.
VUPoint integra la Videosorveglianza in modo semplice, senza la necessità di installare e programmare altre apparecchiature relativamente complesse oltre alle sole telecamere.
Una delle principali innovazioni di VUpoint consiste nel fatto di essere un sistema basato sul cloud che, con un semplice PC connesso ad internet, può essere configurato e gestito.
VUpoint offre un livello di sicurezza senza precedenti e la possibilità di visualizzare immagini video dal vivo attraverso l'App per Smartphone iRisco o tramite l'applicazione web.
Con VUpoint gli utenti possono "vedere" all'interno delle loro proprietà, visualizzando qualsiasi evento: Allarme, Guasto, Panico, Disinserimento.
VUpoint è compatibile con tutti i sistemi antintrusione cloud compatibili di RISCO Group.

Vi invitiamo a visualizzare il video di VUPoint, scansionando il QRCode di seguito:

CST-03 Contatti codificati per cancelli e portoni industriali.

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

TSec presenta una nuova linea di sensori codificati ad alta tolleranza. Sono costruiti sull'ossatura tecnologica della Coded Sensor Technology, un brevetto TSec, che consente di realizzare coppie di sensori e magneti codificate. In pratica il sensore passivo è in grado di riconoscere il proprio magnete. Usando un magnete diverso da quello codificato, causano l'apertura di un circuito di tamper 24h indipendente dal contatto primario.
I sensori CST, nonostante la loro tecnologia avanzata, si presentano alle centrali come comuni contatti passivi, con completa compatibilità con ogni marca di centrale. I modelli CST-03 aggiungono alla codifica una grande tolleranza, adatti per portoni industriali e cancelli. Sono completamente resinati, garantendo installazioni in esterno sicure nel tempo.
Disponibili nella versione CST-03 con cavetto da 3 mt oppure CST-03-M con terminali a morsetto.
Possono essere montati in linea o ad angolo retto senza necessità di staffe accessorie
Sono garantiti 10 anni e sono prodotti interamente in Italia.

Calendario Fiere

TB FORUM powered by Intersec 2016
09.02.16 - 11.02.16
Moscow, Russia

SECURITY & COUNTER TERROR EXPO 2016
19.04.16 - 20.04.16
Olympia, Londra

DIGITAL WORLD
29.04.16 - 01.05.16
Rimini Fiera

INTERNATIONAL OIL & GAS SECURITY EVENT 2016
11.05.16 - 12.05.16
London

CHINA (Guangzhou) INTERN.SAFETY AND HEALTH EXPO
13.06.16 - 15.07.16
China (Guangzhou) Poly World Trade Center Expo

IFSEC INTERNATIONAL 2016
21.06.16 - 23.06.16
Excel London

SECURITY ESSEN 2016
27.09.16 - 30.09.16
Essen, Germania

SECUREXPO EAST AFRICA
08.11.16 - 10.11.16
Nairobi, Kenya

ALL OVER IP
23.11.16 - 24.11.16
Moscow, Russia

essecome security&safety

n. 01 gennaio-febbraio 2016 | ISSN: 2384-9282 | Anno XXXIX
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Claudia Bulow Boje Ferrentino, Nils Fredrik Fazzini, Matteo Canzonetti, Valerio Weinberger.
Traduzioni a cura di Federica Guizzo

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

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

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

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

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
contatto@lilastudio.it

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

Partner essecome 1/2016

CNI PROTECTION | CYBER SECURITY | POLICING AND LAW ENFORCEMENT
MAJOR EVENT SECURITY | BORDER SECURITY | OFFENDER MANAGEMENT | SERVICES

SECURITY & COUNTER TERROR EXPO

19-20 APRIL 2016 | OLYMPIA LONDON

Supported by Home Office

The leading event for public and private sector security and counter terror professionals

3,000+
products and services on display

100+
free conference and seminar sessions

10,000+
private & public sector visitors

200+
expert speakers from the private sector, police, government, military and intelligence services

#SCTX16

Register as a free visitor online and save £50

www.counterterrorexpo.com/secureindex

Co-located with: FORENSICS EUROPE EXPO; Ambition The EPRR Expo

Sponsored by: MEESONS SAFE SECURE ACCESS; xtralis The sooner you know; sodexo QUALITY OF LIFE SERVICES

Follow us on

Organised by: CLARION EVENTS

GALASSIA 3.0

Global PSIM Solution

ONE*to*ONE - Interactive LAB

INVITO

presso il nuovo **R&D Lab** di **DAB Sistemi Integrati**, sede di Roma e Milano per una **Demo** della Piattaforma **Galassia 3.0** - Global PSIM Solution.

COS'È GALASSIA 3.0?

La nostra piattaforma di *Physical Security Information Management.*

PERCHÈ GALASSIA 3.0?

E' una soluzione multi brand, multi sito, scalabile, interoperabile, flessibile e aperta.

COME OPERA?

Galassia 3.0 è in grado di centralizzare sistemi di Security, Safety e Controllo Tecnologico esistenti, integrando diverse tipologie di sensori, apparati e sistemi di diversi produttori.

QUALI VANTAGGI?

La piattaforma è in grado di incrementare il livello di Sicurezza, ottimizzando i costi totali e salvaguardando gli investimenti pregressi in impianti esistenti.

Per valutare la soluzione Galassia 3.0 e verificarne le potenzialità in termini di efficacia, efficienza ed economicità, La invitiamo a partecipare ad una Interactive Demo a Lei dedicata.

Di seguito i riferimenti per concordare un incontro:

e-mail: demogalassia@dabsi.it
tel. +39 06 4121 2020

ROMA: Via Tiburtina 1135 – 00156 RM
MILANO: Viale Sarca 336 F – 20126 MI
BOLOGNA: Via N. Dall'Arca 58 C – 40129 BO

DAB Sistemi Integrati Srl
www.gruppodab.it