essecome ONLINE 01/18

Periodico digitale di informazione di security & safety

2018 · ANNO XXXVIII · ISSN 2384-9282

SECURITY FOR RETAIL 2018: LA SICUREZZA NELL'ERA DELL'OMNICANALITÀ

LE NUOVE COMPETENZE DEL RISK MANAGEMENT DEL RETAIL A CONGRESSO

Roma, 18 aprile 2018 – Confindustria, Sala Pininfarina

Le nuove modalità di acquisto online interessano tutte le tipologie di operatori, dalle grandi catene internazionali ai negozi di prossimità, senza distinzione di settore merceologico. Modalità che impongono radicali adeguamenti organizzativi in ogni passaggio della catena distributiva e in ogni funzione aziendale, a partire da quelle interessate alla sicurezza dei beni e dei profitti.
Gli operatori sono oggi esposti a reati fisici, informatici e combinati che riguardano tanto le merci trattate quanto i dati dei clienti, mentre la minaccia terroristica ha posto al centro dell'attenzione la protezione fisica delle persone che frequentano i punti vendita - dai centri commerciali ai mercati rionali - con l'inevitabile cambio di paradigma da "sicurezza privata" a "sicurezza partecipata" tra pubblico e privato.
In che modo devono rispondere le funzioni aziendali della sicurezza a queste sfide? Quali sono i modelli di riferimento da adottare? E quali sono gli errori da evitare?
A queste domande verrà data risposta nelle sessioni di **SECURITY FOR RETAIL 2018** dal confronto tra responsabili della sicurezza del Retail, esperti internazionali nelle diverse discipline e operatori della sicurezza specializzati.

PROGRAMMA

ore 11 - Condividere le informazioni, la risposta alle nuove minacce
- Un esempio concreto: il Rapporto sui furti nel Retail 2017 (Crime&Tech e Laboratorio per la Sicurezza)
- La partecipazione tra pubblico e privato per la sicurezza nelle aree commerciali
- DL 25/2017: committenti e fornitori di servizi, l'importanza di essere partner

ore 13 - Networking lunch

ore 14 - Cyber security e GDPR
- Cos'è la cyber security per il retailer
- GDPR a -37 giorni: il punto della situazione

ore 15.30 - Coffee break

ore 16 - L'evoluzione del rischio in un mondo social
- Etica e sicurezza delle tecnologie
- La gestione delle crisi nell'era dei social – cause ed impatti del rischio reputazionale

SFR SECURITY FOR RETAIL 2018 è organizzato da essecome editore con il Laboratorio per la Sicurezza

INIM IN TOUR CON PRIME

Inim organizza, in collaborazione con i propri distributori ufficiali, meeting formativi per presentare la centrale Prime agli installatori di tutta Italia.
Personale Inim qualificato illustra le novità di casa Inim davanti ad una platea di installatori professionali.

Inim investe sulla propria filiera distributiva in formazione e strumenti di vendita idonei ad essere performanti sul mercato e ad offrire un servizio ottimo ai propri clienti.

Prime: un solo prodotto per ogni tipo e grandezza di installazione.

Con Prime, Inim Electronics introduce sul mercato una centrale antintrusione e domotica per installazioni professionali "top di gamma" e all'avanguardia.

Residenze di prestigio, banche, industrie, centri commerciali possono beneficiare delle enormi potenzialità della piattaforma Prime. Quando anche piccole applicazioni residenziali e commerciali abbiano bisogno di funzionalità all'avanguardia, Prime è la scelta migliore anche per questo tipo di applicazioni.

Prime è quindi nativamente connessa ad **Inim Cloud** e alle sue potenzialità ed è quindi la scelta di elezione per tutte le installazioni che richiedono connettività IP ed in particolare connettività Cloud. La connetività IP a bordo della scheda principale garantisce grande rapidità di risposta nell'uso dell'**App AlienMobile** e nell'uso dell'interfaccia web di Inim Cloud. Tempi di risposta estremamente rapidi per una esperienza d'uso davvero gratificante.

Tramite l'App AlienMobile, tramite l'interfaccia web del Cloud o tramite il web-server disponibile sulla scheda PrimeLAN, l'utente ha tutto sotto controllo. Inserimenti e disinserimenti, accensioni e spegnimenti, gestione dell'illuminazione, gestione degli scenari domotici, gestione dei cronotermostati ambientali e notifiche in tempo reale di tutto quanto accade. Tutto in punta di dita sullo schermo touch del dispositivo mobile o del PC.

La gestione del sistema in modalità locale può essere effettuata attraverso interfacce utente alfanumeriche tradizionali, utili soprattutto in ambito industriale, o per mezzo delle interfacce touchscreen Alien da 4,3 o 7" perfette per le applicazioni residenziali. L'utente può inoltre interagire con il sistema grazie a tag e lettori di prossimità e telecomandi.

La piattaforma Prime è in grado di gestire i protocolli KNX e ONVIF che consentono al sistema Prime di interagire con i più diffusi sistemi domotici e con ogni sistema di videosorveglianza IP che sia ONVIF compatibile.

Un sistema che è allo stato dell'arte dal punto di vista tecnologico non poteva che essere allo stato dell'arte anche dal punto di vista normativo e delle certificazioni. Prime è certificata, in tutti i suoi modelli, al Grado 3 delle normative europee **EN50131** ed è anche certificata al massimo livello, ATS6, come sistema di comunicazione secondo la norma **EN50136**.

Sommario Interattivo

CLICCA SULL'ICONA PER SCARICARE L'ARTICOLO CHE TI INTERESSA

L'editoriale

Innovazione digitale e omnicanalità, banche e retailer verso una stessa sicurezza?

In un convegno all'inizio di febbraio sugli effetti dell'innovazione digitale sulle piccole banche, è stato spiegato che, in base alle esperienze internazionali di settore, il divario tra le competenze richieste dai nuovi modelli organizzativi e di business e quelli precedenti non si può colmare adeguando per gradi le strutture preesistenti, ma è necessario crearne di totalmente nuove, dove concentrare le figure professionali alle quali è affidata l'innovazione.

Le strutture "old economy" andranno quindi gradatamente smantellate, in parallelo allo spostamento delle attività della banca verso la "new economy".

Uno schema tanto facile da comprendere quanto difficile da applicare, in particolare se le banche sono piccole e legate al territorio: *"Il nostro scopo è sostenere l'economia della zona, è più semplice per una grande banca tagliare diecimila posti di lavoro che a una cassa rurale tagliarne dieci"*, ha commentato uno dei presenti.

Problema insuperabile, considerando che la digitalizzazione è un percorso obbligato per tutto il sistema bancario, comprese le piccole banche locali.

Lo è anche per i retailer, alle prese con il passaggio alla cosiddetta "omnicanalità", la moltiplicazione delle modalità di acquisto al dettaglio - store, mobile, web, social, phone – che sta demolendo i modelli organizzativi precedenti, basati invece sulla moltiplicazione dei negozi fisici sul territorio.

In entrambi i casi, non essendo nemmeno confrontabile il rapporto costi/ricavi tra la vecchia modalità (analogica, fisica) con la nuova (digitale, dematerializzata), non c'è storia: migliaia di agenzie bancarie e di negozi sono stati già chiusi e forse ancora di più dovranno chiudere nei prossimi anni, con decine di migliaia di posti di lavoro letteralmente evaporati.

Cosa c'entra tutto questo con la sicurezza? Moltissimo, come si può intravvedere dalla convergenza in corso delle competenze necessarie per la sicurezza delle banche e dei retailer. Se nella modalità "fisica" saper proteggere il denaro contante allo sportello dai rapinatori a mano armata era molto diverso dal saper difendere mutande e bottiglie di vino dai taccheggiatori di borgata, nella modalità "digitale" la protezione dei dati dei clienti da attacchi cyber o le contromisure ad una crisi di reputazione sui social sono perfettamente identiche, per la banca e per il retailer.

E' ragionevole pensare che ci saranno interessanti effetti sullo scambio di competenze (e forse anche di posti di lavoro) tra i responsabili della sicurezza dei due settori che, in fondo, si assomigliano sempre di più sotto il sole digitale della globalità.

securindex formazione

securindex formazione è una sezione della piattaforma integrata **securindex**, dedicata all'organizzazione di **Corsi di Formazione Professionale e di Aggiornamento per Operatori della Sicurezza**.

securindex formazione si avvale della collaborazione di docenti di comprovata conoscenza delle materie previste nei Corsi.

I Corsi di **securindex formazione** sono di tre livelli:

- **Corsi Introduttivi**
- **Corsi Avanzati**
- **Corsi per la Certificazione delle Figure Professionali**

IL PROGRAMMA DEL II BIMESTRE 2018 PREVEDE I SEGUENTI CORSI OPEN:

Corso Reti IP per sistemi videosorveglianza nell'ambito del GDPR 679/2016
16 ore
8-9 marzo
Milano c/o Camplus Turro

Corso di vendita di sistemi di sicurezza - Professional Base
8+8 ore
6 aprile + 20 aprile
Milano c/o Camplus Turro

Corso per Progettisti e Installatori di sistemi di sicurezza propedeutico alla certificazione IMQ AIR
20 ore
18-20 aprile
Milano c/o IMQ

Ai partecipanti verrà rilasciato l'**Attestato di Partecipazione** che, nei casi in cui è previsto, consente di accedere all'esame di Certificazione anche in sessioni diverse dal Corso frequentato.

Per informazioni ed iscrizioni: segreteria@securindex.com | tel. 02.36757931
Per la certificazione IMQ – AIR: scarica, compila e invia la domanda di ammissione all'esame di certificazione

Caro onorevole, cosa promette per la sicurezza?

di Raffaello Juvara

La sicurezza è al centro del dibattito pre-elettorale di queste settimane per tutti gli schieramenti politici, avendo scoperto che è un tema che, per svariati motivi, tocca in questo momento "la pancia della gente" più di altri. D'altra parte, è anche uno dei temi politici più diretti, che porta gli esponenti dei vari partiti a confrontarsi senza veli sul piano ideologico e misurare, di conseguenza, la capacità di attrarre il consenso degli elettori.
Elettori tra i quali ci sono anche gli operatori della sicurezza, pubblica e privata.

Come abbiamo fatto notare agli onorevoli **Emanuele Fiano (PD), Giorgia Meloni (FdI) e Angelo Tofalo (M5S)**, ponendo a loro le stesse tre domande, solo gli operatori privati sono oltre 200.000, tra installatori, guardie giurate e incaricati fiduciari. Un bacino di votanti che non sempre ha trovato nei parlamenti e nei governi delle passate legislature l'attenzione dovuta al ruolo ricoperto per assicurare ai cittadini il diritto alla sicurezza garantito dalla Costituzione, partecipando fattivamente all'azione dello Stato da molto tempo prima che si maturasse la stessa concezione di "sicurezza partecipata", oggi perfino abusata.

Queste le domande:

1. Secondo i dati Istat, i reati denunciati sono in calo, in particolare gli omicidi e i reati predatori, ma l'insicurezza percepita dei cittadini risulta invece stabile. Da cosa dipende secondo lei questo fenomeno?

2. Il fenomeno dei reati non denunciati evidenzia una sostanziale sfiducia nelle istituzioni da parte dei cittadini e degli operatori economici. Come può essere risolto questo problema?

3. "Sicurezza partecipata" significa collaborazione tra pubblico e privato per garantire la sicurezza dei cittadini. In che modo il suo partito si propone di incentivare privati – aziende e famiglie – che partecipano alla sicurezza pubblica investendo denaro per mettere in sicurezza se stessi?

Qui di seguito, le risposte di Emanuele Fiano, Giorgia Meloni, e Angelo Tofalo.

EMANUELE FIANO – PARTITO DEMOCRATICO

Secondo i dati Istat, i reati denunciati sono in calo, in particolare gli omicidi e i reati predatori, ma l'insicurezza percepita dei cittadini risulta invece stabile. Da cosa dipende secondo lei questo fenomeno?
Noi stiamo parlando di un miglioramento dei fattori di sicurezza misurabili quantitativamente a fronte di una stabilità, e non di un aumento della percezione di insicurezza. La differenza tra questi due andamenti del problema ha origini varie.
Innanzitutto, un miglioramento dei dati che misurano la sicurezza non vuol certo dire che i questi problemi siano stati risolti in modo totale.
In secondo luogo, la situazione sociale produce oggi molti fattori di insicurezza: sul lavoro, sulla pensione, sulla casa e, più in generale, sul futuro. Fattori che non solo aumentano la percezione soggettiva di insicurezza, ma sono prodotti da condizioni sociali reali, che determinano oggettivamente percezione di insicurezza. Possiamo citarne tanti, dall'insufficienza di edilizia residenziale pubblica ai valori ancora alti di disoccupazione, ricordando comunque che il fenomeno globale ed epocale dell'immigrazione è oggi il principale fattore di percezione di insicurezza.
Questo quadro, per quanto dal mio punto di vista abbia avuto un sensibile miglioramento nel corso di questa legislatura, ha prodotto e produce condizioni che alimentano la sensazione di non essere sicuri o di non essere protetti a sufficienza. Anche per questo, noi abbiamo dedicato uno sforzo cospicuo agli investimenti sia in sicurezza (7 miliardi di euro in 5 anni) sia per il recupero e la riqualificazione dei territori più esposti a problemi sociali, come i quartieri periferici delle città per i quali sono stati investiti 2 miliardi di euro.
Aggiungerei per ultimo, come fattore che produce insicurezza, la questione della comunicazione pubblica e della propaganda politica. Lo spazio destinato a questi aspetti, lo sfruttamento a fini elettorali della paura, sono per alcuni partiti il motore essenziale della loro stessa ragion d'essere. Senza l'esaltazione della paura, non ci si può presentare come gli sceriffi migliori e non si può raccogliere consenso. Ma la soluzione non è l'esaltazione della paura. La soluzione sta nel far rispettare la legge anche nei quartieri di edilizia residenziale pubblica impedendo, ad esempio, le occupazioni abusive, nel combattere la disoccupazione, nel governare e ridurre i flussi di immigrazione: quello che abbiamo fatto e che bisogna continuare a fare.

Il fenomeno dei reati non denunciati evidenzia una sostanziale sfiducia nelle istituzioni da parte dei cittadini e degli operatori economici. Come può essere risolto questo problema?
Il problema della mancata denuncia deve trovare una risposta nella certezza della risposta dello Stato, sia nell'intervento delle forze dell'ordine che nell'opera della magistratura. Per questo motivo, in questi anni, oltre all'investimento in sicurezza (assunzioni, riordino, stipendi, investimenti), siamo intervenuti sulla certezza della pena, aumentando i minimi di pena per i reati cosiddetti "predatori" per permettere che il giudice cautelare possa trattenere in carcere le persone arrestate anche prima della condanna, in virtù di una previsione minima di pena superiore a qualsiasi sconto di pena previsto per questi reati.

"Sicurezza partecipata" significa collaborazione tra pubblico e privato per garantire la sicurezza dei cittadini. In che modo il Partito Democratico si propone di incentivare privati – aziende e famiglie – che partecipano alla sicurezza pubblica investendo denaro per mettere in sicurezza se stessi?
Noi abbiamo già fatto passi in questa direzione come, ad esempio, gli incentivi previsti nel decreto sicurezza urbana per i Comuni che installano sistemi di telecamere intelligenti e altrettanto è stato fatto, con modalità diverse, per i privati. La politica di incentivo all'investimento privato nei sistemi passivi deve essere ampliata, è un aiuto tangibile all'azione delle forze dell'ordine.

GIORGIA MELONI – FRATELLI L'ITALIA

Secondo i dati Istat, i reati denunciati sono in calo, in particolare gli omicidi e i reati predatori, ma l'insicurezza percepita dei cittadini risulta invece stabile. Da cosa dipende secondo lei questo fenomeno?
Chiariamo una cosa: non è che ci siano meno reati, anzi. È la gente che non va più a denunciare furti e reati predatori. Oggi, purtroppo, l'insicurezza è un sentimento diffuso, dovuto alle politiche messe in campo dalla Sinistra: svuota carceri, indulti mascherati, depenalizzazioni. L'Italia è l'unica Nazione che pretende, siccome ha un problema di sovraffollamento delle carceri, di adeguare il sistema penale alla capienza delle carceri. Non si può fare. E visto che non si va in carcere, il sentimento di insicurezza delle persone aumenta.
Ma c'è anche un altro paradosso: i carnefici diventano vittime e le vittime vengono processate. Guardate il caso del capotreno condannato per violenza privata e per abuso d'ufficio perché ha fatto scendere un nigeriano privo di biglietto. Follie simili le abbiamo purtroppo viste anche nei confronti delle Forze dell'ordine colpevoli di fare il loro lavoro. Perché nell'Italia devastata dal buonismo di Sinistra è proibito far rispettare le regole.

Questo fenomeno evidenzia una sostanziale sfiducia nelle istituzioni da parte dei cittadini e degli operatori economici. Come può essere risolto questo problema?
Il problema sarà risolto da Fratelli d'Italia al governo quando tornerà la certezza della pena e la sicurezza degli italiani sarà nuovamente al centro dell'azione dello Stato. Nel nostro programma c'è l'impegno a costruire nuove carceri; diremo basta agli sconti di pena automatici e faremo in modo che gli immigrati scontino le pene a casa loro. Per noi, la difesa è sempre legittima e, se lo Stato non è in grado di difendere i cittadini, deve consentirti di difenderti da solo.
Sono convinta che la sfiducia nelle istituzioni si combatta anche con la valorizzazione delle nostre Forze dell'ordine il cui compenso dovrebbe essere parametrato a quello che avviene nelle grandi democrazie occidentali. È paradossale che, nell'Italia di oggi, un poliziotto al primo incarico prenda meno di 1200 euro per rischiare la vita ogni giorno, nella stessa Italia nella quale c'è gente che prende in considerazione l'idea di darti 800 euro per stare a casa.
Quando Fratelli d'Italia sarà al governo, porremo rimedio a una delle ultime trovate dei Governi Pd nella riforma dell'ordinamento penitenziario voluta dal Ministro Orlando: chi commette reati con pena fino a 4 anni non va in carcere ma viene affidato ai servizi sociali. Cioè niente carcere per furti, scippi, truffe agli anziani, intrusione in casa e molti altri reati che affliggono gli italiani onesti. È naturale quindi la sfiducia nelle istituzioni da parte dei cittadini onesti.

"Sicurezza partecipata" significa collaborazione tra pubblico e privato per garantire la sicurezza dei cittadini. In che modo Fratelli d'Italia si propone di incentivare privati – aziende e famiglie – che partecipano alla sicurezza pubblica investendo denaro per mettere in sicurezza se stessi?
La sicurezza partecipata è fondamentale per garantire la tranquillità dei cittadini. Quando Fratelli d'Italia sarà alla guida della Nazione, stabiliremo degli incentivi per le istallazioni delle telecamere, sia per le famiglie che per le imprese. Naturalmente, dovranno essere delle telecamere che abbiano una utilità anche per la collettività, dovranno cioè essere posizionate in modo tale da inquadrare anche parti di strade, creando così un vero e proprio sistema di raccordo tra i privati e il pubblico.
Un altro aspetto di cui terremo conto per favorire i privati che partecipano alla sicurezza pubblica riguarda le forme di incentivo e sostegno all'illuminazione privata che abbia una ricaduta positiva sul territorio, tipo l'illuminazione di abitazioni o capannoni fronte strada. Favoriremo poi forme di incentivo ad attività commerciali aperte di notte in zone decentrate, periferiche, e degradate. Infine, stabiliremo delle agevolazioni per la possibilità di accesso gratuito al trasporto pubblico e a determinati eventi a pagamento per la vigilanza armata riconoscibile in divisa. Per capirci, due guardie private in divisa se hanno la possibilità di andare gratis in metro sono sicuramente un deterrente al crimine. Sono convinta che la divisa a prescindere sia un deterrente alla criminalità.

ANGELO TOFALO – MOVIMENTO 5 STELLE

Secondo i dati Istat, i reati denunciati sono in calo, in particolare gli omicidi e i reati predatori, ma l'insicurezza percepita dei cittadini risulta invece stabile. Da cosa dipende secondo lei questo fenomeno?
In effetti, dalla lettura dei dati Istat risulta che i reati denunciati siano in calo, in particolare gli omicidi e alcuni tipi di reati predatori. Resta però il fatto che l'insicurezza percepita dei cittadini non diminuisca, anzi.
Con ogni evidenza, ci troviamo ormai a vivere nella "società del rischio", dove bisogna saper distinguere tra sicurezza oggettiva e quella percepita, dovendo tuttavia tenere ben presente che la Sicurezza è un bene di fondamentale importanza, una necessità per tutti i cittadini.
Desidero sottolineare che, in base ai nostri principi, le persone devono essere libere di vivere la quotidianità senza sentirsi minacciati nella loro incolumità ed anche le proprietà dei singoli devono essere protette da ingiusti danneggiamenti.
Esiste poi una dimensione collettiva della sicurezza, che si realizza nella tutela dell'ordine pubblico. Non basta, infatti, garantire la protezione dei singoli, se non vengono garantiti interessi collettivi fondamentali, come la legalità e l'ordine sociale.
Il programma Sicurezza del Movimento Cinque Stelle rappresenta un percorso di comprensione e condivisione di tematiche molto delicate, uno strumento importante in un mondo in cui le minacce sono in continua evoluzione e non sempre visibili come, ad esempio, la minaccia cyber.

Il fenomeno dei reati non denunciati evidenzia una sostanziale sfiducia nelle istituzioni da parte dei cittadini e degli operatori economici. Come può essere risolto questo problema?
L'unico modo per invertire questa sostanziale sfiducia dei cittadini verso le istituzioni, evidenziata proprio dal fenomeno dei reati non denunciati, è diffondere una cultura della sicurezza sviluppando, appunto, modelli di "sicurezza partecipata".
Il Movimento 5 Stelle reputa meno efficiente un sistema di sicurezza organizzato secondo una struttura piramidale, in cui lo Stato sia l'unico soggetto preposto a garantire la prevenzione e la repressione dei crimini; un sistema in cui il cittadino sia dunque semplice destinatario delle politiche elaborate a livello governativo e realizzate per mezzo delle forze di Polizia.
Per questo motivo, il Movimento si impegnerà perché siano disciplinate forme di sicurezza partecipata, in cui il bene in questione sia prodotto da una molteplicità di attori, posti tra loro in una relazione di natura paritaria. La sicurezza non può essere imposta dall'alto ma è un bene di tutta la collettività e ognuno, nell'ambito del ruolo sociale ricoperto, può concorrere al suo mantenimento.
Si suole parlare, a questo riguardo, di "sicurezza integrata" quale strumento attuativo di politiche che vedono integrarsi le competenze esclusive dello Stato in materia di ordine e sicurezza pubblica con quelle riconducibili agli enti locali ed ai privati operanti sul piano della prevenzione quali, ad esempio, dei "governi territoriali di prossimità".
Va ricordato che nell'attuale assetto costituzionale, il riconoscimento delle prerogative esclusive statali in materia di «ordine pubblico e sicurezza» non esclude affatto l'importanza di stabilire per legge statale forme di coordinamento tra centro e periferia; anzi, se pur prima del 2001 si sono avute forme di collaborazione, da allora è la stessa Costituzione (art. 118, comma 3) a prevederne la necessità.

"Sicurezza partecipata" significa collaborazione tra pubblico e privato per garantire la sicurezza dei cittadini. In che modo il Movimento 5 Stelle si propone di incentivare privati – aziende e famiglie – che partecipano alla sicurezza pubblica investendo denaro per mettere in sicurezza se stessi?
Parliamo di una stretta collaborazione tra pubblico e privato per garantire la sicurezza dei cittadini. Su questo abbiamo proposto una reale partnership tra le due parti con formazione ed informazione costante per la PA e la defiscalizzazione dei costi della sicurezza aziendale che deve, quindi, trasformarsi culturalmente in un investimento per tutta la Comunità, tenendo saldo il principio che la Sicurezza non viene imposta dall'alto ma è un bene di tutta la collettività per la quale ognuno può concorrere al mantenimento, nell'ambito del ruolo sociale rivestito.

Servirà “un’etica dell’algoritmo”, parola del Garante

di Maria Cupolo, avvocato Privacy Officer e Consulente della Privacy Certificato ISO 17024:2012 TUV Italia

Il Garante Privacy **Antonello Soro**, lo scorso 30 gennaio , in occasione della Giornata Europea per la protezione dei dati personali, ed in apertura del convegno “Uomini e macchine. Protezione dati per un’etica del digitale”, si è soffermato su temi quanto mai importanti, fotografando l’era in cui viviamo, un’era dove in un mondo iperconnesso siamo guidati dalla scia dei dati che tracciamo e dove, proprio alla luce del sempre maggiore progresso tecnologico, è sempre più necessaria “un’etica dell’algoritmo”.

Il Garante ha sottolineato, infatti, come ***“ogni cosa sarà “smart”: non solo i telefoni, ma anche le nostre auto, le nostre case, le nostre città; l’internet degli oggetti e l’analisi dei big data convergeranno con l’intelligenza artificiale e i sistemi biometrici: in definitiva vivremo in un pianeta “intelligente”.”***

Il processo di connessione e, dunque, le ricadute, tutte, che ognuno avrà nella propria vita, per quanto riguarda le proprie decisioni o, ancora, per le scelte e gli orientamenti che saranno sempre più determinanti in ogni ambito dell’ economia se solo pensiamo allo sviluppo delle tecnologie ed al loro impiego, ebbene ogni passaggio richiederà maggiore responsanbilizzazione da parte di tutti i soggetti coinvolti affinchè i rischi connessi al progresso vengano il più possibile minimizzati.

Ecco allora che ***“la normativa di protezione dati rappresenta un fondamentale presidio di garanzia tanto in termini di diritti esercitabili dall’utente quanto in termini di complessiva responsabilizzazione dei titolari, a vario titolo coinvolti, nella sempre più articolata filiera in cui si snodano questi trattamenti”.***

E infatti, non possiamo non pensare al coinvolgimento davvero di tutti, ovvero di coloro che utilizzano i tanti dispositivi tra loro connessi o si imbattono nell’utilizzo di tecnologie che pongono alla base algoritmi sempre più in grado di rivelare ***“stili di vita, capacità economica, preferenze, addirittura patologie o dipendenze”*** nonché di coloro che in quella filiera sempre più articolata come appunto definita dal Garante stesso, dovranno assumere un atteggiamento sempre più etico e consapevole perché ***“la tecnica dev’essere progresso, in primo luogo umano e sociale, non cieco positivismo, pena la negazione delle essenziali conquiste di civiltà raggiunte nel corso della storia. In questo senso è necessaria un’etica dell’algoritmo, da strutturarsi nel rispetto dei principi in particolare di dignità e non discriminazione fondativi dello stato di diritto”.***

Le riflessioni svolte hanno, pertanto, richiamato l’attenzione sul Regolamento Europeo 679/16 che sancisce alcune ***“garanzie essenziali”*** che costituiscono in ogni ambito e per tutti i soggetti coinvolti, un momento di consapevolezza e di opportunità perché ***“in un mondo iperconnesso e in un’economia fondata sui dati se il diritto in generale svolge, oggi, sempre più, una funzione di umanizzazione della tecnica – soprattutto quando il soggetto di diritti rischia di divenire mero oggetto di calcoli predittivi e tecniche manipolative- il diritto alla protezione dei dati rappresenta una straordinaria risorsa per mantenere la persona, nella sua libertà e nella sua responsabilità, al centro della società digitale”.***

Convegno
“UOMINI E MACCHINE. PROTEZIONE DATI PER UN’ETICA DEL DIGITALE”
30 gennaio 2018

Intervento Antonello Soro
Presidente del Garante per la protezione dei dati personali

“Dio è il primo tecnico. La tecnica è l’ultimo dio”. Così Emanuele Severino descrive “la tendenza fondamentale del nostro tempo”, ovvero l’abbandono, da parte della tecnica, del suo carattere strumentale, per assurgere a fine in sé, esponendo l’uomo al rischio di divenire, paradossalmente, egli stesso strumento della tecnica anziché suo signore.

E se già nel primo novecento il “dominio della tecnica” fu considerato tratto distintivo del post-moderno, esso caratterizza ancor più marcatamente il nostro tempo, profondamente mutato dalle nuove tecnologie e dalle loro implicazioni sociali, economiche, persino politiche ed esistenziali.

Il 27 dicembre 1982 la rivista “Time” dedicava al computer – per la sua “grande influenza nella nostra vita quotidiana” - la propria copertina, assegnando per la prima volta la qualifica di soggetto dell’anno a una “macchina” anziché a una persona.

La pubblicazione – che sembrò quasi suggerire la fine della centralità culturale e sociale dell’uomo – precedeva di poco più di un anno quel 1984 in cui George Orwell prefigurava, già settant’anni fa, la riduzione dell’uomo a codice e l’affermazione della sorveglianza totale quale tecnica di governo della complessità sociale.

Non si trattava, del resto, di una preoccupazione isolata se pochi anni dopo Erich Fromm avrebbe osservato come “la civiltà sta producendo macchine che si comportano come uomini e uomini che si comportano come macchine. Il pericolo del passato era che gli uomini diventassero schiavi. Il pericolo del futuro è che gli uomini diventino robot”.

Il progresso tecnologico appariva pertanto- già prima dell’avvento di internet- come talmente capace di sconvolgere i parametri del vissuto individuale e collettivo, da rovesciare l’interrogativo su cosa l’uomo possa fare delle macchine nel suo inverso: cosa le macchine possano fare dell’uomo.

Se, dunque, il mero calcolatore suggeriva l’idea di un potere smisurato della tecnica e del costo umano del progresso, la rivoluzione -cognitiva, simbolica, antropologica- determinata da internet (of things, of toys, of beings) e dall’intelligenza artificiale, dovrebbe oggi indurci ad un supplemento di riflessione.

Essenzialmente perché il digitale è divenuto la trama stessa delle nostre vite, agente potentissimo di trasformazione sociale, struttura e sovrastruttura insieme, testo e contesto: la cornice entro cui si svolge ogni espressione dell’uomo, che condiziona secondo i soli parametri della funzionalità e dell’efficienza.

Con internet, la tecnologia da strumento si è fatta dimensione, ecosistema in cui siamo così profondamente immersi da non renderci conto, fino in fondo, delle sue implicazioni.

Che si estendono dal lavoro (con inquietanti interrogativi sulle prospettive di occupazione) alla salute e alla ricerca scientifica ma anche alla giustizia, che finisce con il divenire “predittiva”, affidando agli algoritmi persino quelle decisioni dirimenti sull’uomo -colpevolezza, libertà, punibilità-che sembravano l’ultimo baluardo della sovranità e, quindi, della razionalità umana.

L’impatto sull’esistenza individuale e collettiva non è, del resto, meno rilevante.

La genomica infrange il dogma dell’immutabilità del testo del nostro futuro, così come scritto nei cromosomi.

Con le tecnologie indossabili la persona è modificata nella sua stessa fisicità: incorpora la tecnica e, quindi, la predisposizione al controllo. Il corpo diviene una password che rende accessibile a chiunque la nostra identità più remota; la fisicità è ridotta a superficie di scrittura di un’identità indifesa.

Del resto, affidare a un algoritmo impronte digitali, reticolo venoso, iridi, può sottrarci quanto di più intimo custodiamo come riferimento ultimo del nostro essere.
Gli algoritmi determinano, infatti, non soltanto la nostra percezione del mondo, ma la nostra stessa identità, che con internet diviene necessariamente plurale, affiancandosi a quella fisica anche un caleidoscopio di identità digitali che concorrono, fin quasi a prevalere, sulla prima.
E finiremo con l'essere sconosciuti a noi stessi ma trasparenti a chiunque sia capace di estrarre frammenti di noi dalla galassia delle nostre tracce on-line. E' quello che Derrick de Kerckhove chiama inconscio digitale: ciò che ancora non sappiamo di noi ma che la rete sa, per effetto del pedinamento dello sciame informativo prodotto dal nostro comportamento on-line.
Nel 2016 abbiamo generato tanti dati quanti ne ha prodotti l'intera storia dell'umanità sino al 2015.
Tra dieci anni questa quantità raddoppierà ogni 12 ore.
Attualmente il 70 % delle transazioni finanziarie è realizzato mediante algoritmi e il valore dei dati personali cresce progressivamente. L'innovazione digitale nel sistema finanziario darà un forte impulso alla crescita dell'economia globale.
Le grandi compagnie tecnologiche sono impegnate a tradurre i big data in megaprofitti.
Scienziati e ingegneri in tutto il mondo puntano al prossimo salto nella capacità di elaborazione, ai cosiddetti supercomputer alla esascala, con capacità di calcolo fino a mille volte quelle dei migliori supercomputer attuali: macchine in grado di risolvere problemi che oggi non è possibile affrontare in campi diversi come la climatologia, le energie rinnovabili, la genomica, la geofisica.
L'intelligenza artificiale, dal canto suo, diviene sempre più capace di auto-apprendimento e, quindi, di autonomia. Evieneusatasemprepiùspessoafinididifesa,conilricorsoadispositivi lacuiintrinsecapredisposizionealdualusefasfumareilconfine tra civile e militare.
Il passaggio dalla "guerra ibrida all'iperguerra informatica" si annuncia come tutt'altro che irrilevante.
E' significativo che personalità come Elon Musk, Bill Gates o Stephen Hawking manifestino forti preoccupazioni sui rischi legati agli sviluppi dell'intelligenza artificiale.
Per altro verso, è convincimento diffuso tra gli esperti che nei prossimi dieci o al massimo vent'anni, circa la metà dei lavori attuali saranno realizzati da macchine dotate di intelligenza artificiale.
E non solo lavori manuali, ma soprattutto lavori che comportano lo sviluppo di processi intelligenti. Molti osservatori prevedono una grande crisi occupazionale, non delle tute blu ma dei colletti bianchi, e non è infondato il rischio di una stagione di grandi tensioni sociali a livello globale.
Pur non accedendo alla teoria del pendio scivoloso e dunque al netto di ogni visione apocalittica, ciò che è certo è che stiamo vivendo la più radicale trasformazione sociale, economica, antropologica, persino politica, dalla fine della seconda guerra mondiale.
L'assunzione di lavoratori, la determinazione dell'affidabilità per un prestito, la valutazione della capacità di un insegnante, persino il rating di legalità ai fini dell'aggiudicazione degli appalti sono sempre meno il frutto di una scelta umana e sempre più l'esito di selezioni algoritmiche, alle quali deleghiamo, quasi fideisticamente, il compito di decidere aspetti determinanti della vita delle persone.
Presto ogni oggetto attorno a noi, persino il nostro abbigliamento, sarà connesso: si stima che in 10 anni vi saranno 150 miliardi di sensori in rete, 20 volte di più della popolazione mondiale.
Ogni cosa, dunque, sarà "smart": non solo i telefoni ma anche le nostre auto, le nostre case, le nostre città; l'internet degli oggetti e l'analisi dei big data convergeranno con l'intelligenza artificiale e i sistemi biometrici: in definitiva vivremo in un pianeta "intelligente".
Tutto ciò favorirà certamente, per un verso, un netto miglioramento della qualità della vita, liberandoci – come già oggi è evidente- del peso di molte incombenze quotidiane e dischiudendo possibilità prima precluse.

Ma il processo di connessione di tutte le cose deve essere governato con lungimiranza, per minimizzare i rischi cui già oggi questi fenomeni ci espongono.
L'apparente "innocuità" di oggetti di uso quotidiano (si pensi alle bambole-robot o alla domotica) ci induce, infatti, a sottovalutare in primo luogo la probabilità che essi rappresentino il canale di accesso elettivo per attacchi informatici e hacker capaci di sfruttarne le vulnerabilità. In secondo luogo, di questi dispositivi sottovalutiamo la capacità di rivelare, mediante l'uso secondario dei dati raccolti, stili di vita, capacità economica, persino patologie o dipendenze.
La normativa di protezione dati, sotto questo profilo, rappresenta un fondamentale presidio di garanzia, tanto in termini di diritti esercitabili dall'utente quanto in termini di complessiva responsabilizzazione dei titolari, a vario titolo coinvolti, nella sempre più articolata filiera in cui si snodano questi trattamenti.
E dovrebbe servire per minimizzare il rischio, inaccettabile anzitutto sul piano culturale, di intendere la cessione dei propri dati, quale tributo necessario alla fruizione dei vantaggi offerti dal pianeta connesso.
Numerose applicazioni hanno dimostrato che gli algoritmi non sono matematica pura -infallibile e neutra- ma piuttosto opinioni umane strutturate in forma matematica e riflettono quindi spesso, in misura più o meno rilevante, le precomprensioni di chi li progetta o le serie storiche assunte a riferimento.
Con il rischio, dunque, non soltanto di cristallizzare il futuro nel passato, leggendo sempre il primo con gli schemi del secondo, ma anche di assumere le correlazioni (quasi sempre contingenti) delle serie storiche considerate, come relazioni necessariamente causali.
Un algoritmo utilizzato negli Usa per il calcolo del rischio di recidiva penale si è dimostrato, ad esempio, incline ad assegnare – in assenza di ragioni criminologiche -un tasso maggiore ai neri rispetto ai bianchi, solo sulla base delle correlazioni desunte da una determinata serie storica assunta a riferimento.
Il risultato che si trae dall'impiego di tecnologie che dovrebbero assicurare la massima terzietà rischia dunque di essere, paradossalmente, più razzista, lombrosiano o anche solo antistorico di quanto possa essere la pur fallibile razionalità dell'uomo.
Eppure la giustizia predittiva continua a esercitare un fascino particolare, assecondando l'antica idea di un diritto talmente positivo da essere capace di autoapplicazione senza l'intermediazione umana, legittimato non dalla sovranità ma dalla sua stessa, sola, infallibilità.
E' lecito chiedersi se questa giustizia, paradossalmente così performativa, sarà ancora umana e se, quando ad emettere le sentenze sarà un algoritmo anziché un uomo, saranno garantite davvero la giustizia e l'equità.
La discriminazione algoritmica rischia pertanto, se non sapientemente governata, di approfondire le iniquità alle quali vorrebbe ovviare, senza che ne siamo neppure consapevoli perché la precomprensione coperta da veste statistica non ci appare più tale e perché le modalità di decisione algoritmica non sono sindacabili perché neppure conoscibili.
Non va poi sottovaluto l'impatto degli algoritmi sulla formazione dell'opinione e della stessa coscienza individuale.
Secondo Dominique Cardon, il 95% degli internauti si concentra sullo 0,03% dei contenuti potenzialmente disponibili on-line, per effetto della gerarchizzazione delle notizie determinata dai motori di ricerca, in base a criteri tutt'altro che neutri perché desunti anche dal nostro comportamento on-line.
Con una sorta di cornice cognitiva basata non sul riconoscimento dell'altro ma sul rispecchiamento del sé, ci viene dunque proposto ciò che assomiglia di più all'immagine di noi che si è costruito il motore di ricerca.
Traendo informazioni dal nostro comportamento passato, l'algoritmo rafforza e conferma le nostre opinioni, indebolendo quell'etica del dubbio che è il presupposto necessario del rispetto della differenza e di ogni altra attitudine democratica.
Come schiavi digitali, siamo così prigionieri di una bolla di filtri autoreferenziale, capace di renderci sempre più intolleranti verso le differenze e di negare il pluralismo informativo e le stesse straordinarie opportunità di

arricchimento cognitivo che pur la rete potrebbe offrire.
Sul piano politico, la possibilità offerta dagli algoritmi di “informatica persuasiva” di personalizzare i contenuti proposti agli utenti per renderli maggiormente appetibili e appunto persuasivi, ha sancito l’affermazione del “big nudging”. Ovvero dell’uso dei big data e di metodi profilativi per esercitare quel tipo di intervento pubblico di stampo paternalistico, fondato appunto sul “nudge” (pungolo), che consente di “guidare” la condotta dei cittadini persuadendoli all’adozione di comportamenti socialmente desiderabili.
Come dimostrano questi sommari esempi, dunque, il tema della neutralità dell’algoritmo, dell’equità delle sue soluzioni e, più in generale, della sostenibilità etica e giuridica della tecnologia diviene, oggi, una questione democratica cruciale.
Per scongiurare - o quantomeno minimizzare - i rischi connessi al digitale, valorizzando peraltro le sue straordinarie opportunità, è necessaria un’assunzione di responsabilità da parte di ciascun soggetto coinvolto nel governo della tecnologia, che per restare “umano” deve incentrarsi su irrinunciabili principi etici e giuridici.
La tecnica dev’essere progresso, in primo luogo umano e sociale, non cieco positivismo, pena la negazione delle essenziali conquiste di civiltà raggiunte nel corso della storia. In questo senso è necessaria un’etica per l’algoritmo, da strutturarsi nel rispetto dei principi, in particolare di dignità e non discriminazione, fondativi dello Stato di diritto.
Vi è in gioco, del resto, anche una sfida culturale: non cedere all’idea che la nostra persona sia definita dal punteggio attribuitogli da un sistema di classificazione e valutazione computerizzata, irresponsabile e dal funzionamento opaco.
Di qui l’importanza delle norme del Regolamento generale sulla protezione dei dati sulla contestabilità e la trasparenza del processo decisionale automatizzato, dei suoi criteri e delle sue conseguenze, esigendo la possibilità di un intervento umano, contrastando la delega assoluta al cieco e neppure neutro determinismo dell’algoritmo.
Del resto, la disciplina sulla protezione dati delinea una cornice generale al cui interno possono ricondursi i più complessi fenomeni con i quali dobbiamo oggi confrontarci.
Così per l’iperconnettività favorita dall’internet degli oggetti, il nuovo quadro giuridico europeo sancisce alcune garanzie essenziali per impedire che in questo flusso ininterrotto di dati l’uomo, da sua fonte, divenga oggetto di un potere che lo trascende.
La salvaguardia dell’autodeterminazione informativa, dell’autonomia e della responsabilità delle scelte - articolata non soltanto nei vari istituti del consenso informato, ma anche nella valutazione di impatto privacy, della minimizzazione del trattamento, della protezione sin dalla progettazione e per impostazione predefinita - è in questo senso presidio essenziale per mantenere il governo sulle nostre tracce digitali, che più di ogni altro aspetto concorrono oggi a definire la nostra identità e, con essa, la nostra libertà.
Tutto questo diverrà ancor più importante con l’avvento dell’internet of beings e, dunque, l’incorporazione delle nuove tecnologie all’interno della nostra stessa fisicità, che determineranno mutamenti radicali nell’antropologia, nel rapporto tra natura e cultura, biologia e biografia, perdendo la prima la funzione di limite della seconda.
In tale contesto, noi pensiamo che nella dignità e non nella materialità del dato biologico vada ricercato il limite oltre cui la tecnica non può e non deve spingersi.
E in un mondo iperconnesso e in un’economia fondata sui dati e alimentata dall’intelligenza artificiale, presupposto per la dignità e quindi anche per la libertà dell’uomo è la protezione di ciò che, come i suoi dati personali, lo caratterizza più emblematicamente.
E se il diritto in generale svolge oggi, sempre più, una funzione di umanizzazione della tecnica- soprattutto quando il soggetto di diritti rischia di divenire mero oggetto di calcoli predittivi e tecniche manipolative – il diritto alla protezione dei dati rappresenta una straordinaria risorsa per mantenere la persona, nella sua libertà e nella sua responsabilità, al centro della società digitale.

Citel, dopo un 2017 in crescita, annuncia l'ERP della sicurezza fisica e della compliance

a colloquio con Nils Fredik Fazzini, amministratore delegato di Citel Spa
a cura della Redazione

Citel Spa, nome storico nel settore **PSIM**, ovvero dei sistemi informatici e delle soluzioni per la gestione della sicurezza fisica, della safety e della compliance in genere, comunica di avere chiuso il 2017 con un bilancio ancora in formazione ma che fa emergere un risultato in positivo con una crescita dei ricavi intorno al 10% e un portafoglio ordini record, superiore al 30% dei ricavi dell'anno appena chiuso.
Abbiamo chiesto all'AD di Citel, **Nils Fredrik Fazzini**, le sue valutazioni sull'anno appena trascorso e sugli indirizzi tecnici e commerciali che la società intende attuare nel 2018 in continuità o meno con gli anni recenti.

I ricavi nel 2017 sono in linea con le aspettative? E quali sono le particolarità nella composizione?
È un risultato con ricavi in crescita di circa il 10% - interamente basato su sistemistica e piattaforme PSIM - e lo stesso vale per il risultato finale, che è positivo e in linea con l'andamento negli anni recenti. I numeri saranno rilasciati a bilancio approvato. Alla crescita dei ricavi ha contribuito in misura significativa l'acquisizione di nuovi utenti e commesse di peso in ogni settore, dal credito alla manifattura, dalla GDO alle Infrastrutture Critiche, che sono andati ad aggiungersi agli utenti attuali, che comprendono già i più grandi nomi in quei comparti.

Quali sono i nuovi nomi tra gli utenti che hanno aderito al modello PSIM?
L'Ecosistema dell'utenza del Centrax-open-PSIM di Citel continua ad essere senza confronti nel mercato italiano, visto che comprende le principali banche italiane e Poste, grandi nomi come Amiacque, Enel, ENI, IKEA, Fastweb, Italgas, Ducati, Lamborghini, Leonardo, Mediaset, Snam, Saipem; ed inoltre grandi musei, il Comune di Roma, i principali nomi della Logistica e dei Servizi di Security per un totale di oltre 100 PSIM in esercizio di ogni dimensione: dal più esteso in assoluto, Poste Italiane con 12.000 uffici collegati, a quelli dedicati ad una Infrastruttura Critica o a una impresa industriale come la Ducati o la Lamborghini.
100 utenti di peso sono un numero elevato, se si considera che si tratta di società ai vertici di classifica dei rispettivi settori, una fascia dove gli interlocutori sono particolarmente sensibilizzati al tema della sicurezza anche per motivi di compliance, e dove l'informatizzazione della soluzione non è un'opzione ma, ormai, una strada obbligata.
Sono utenti necessariamente esigenti e che, in tutta una serie di casi, per la prima volta hanno fatto un progetto di rottura con un passato in cui ci si poteva soltanto adattare ad un catalogo unico. Ed è interessante collaborare in casi come questi, dove si tocca con mano una particolare motivazione ad innovare e migliorare i processi gestionali e le soluzioni tecniche una volta recuperata la libertà progettuale.

Quali pensa siano le linee di tendenza del mercato PSIM nel 2018 e oltre?
L'espansione continuerà nella fascia alta, dove vi sono ancora molti grandi utenti non ancora toccati dall'evoluzione PSIM, ma anche in fascia media, dove la flessibilità della nostra sistemistica permette soluzioni sostenibili. D'altra parte, non vedo alternative al modello di informatizzazione sottintesa nel PSIM anche nelle fasce inferiori. Si tratterà soltanto di creare un modello per il coinvolgimento delle Terze Parti incaricate di sostituirsi a Citel avendone comunque tutto il supporto formativo e operativo necessario.

Che tipo di concorrenza pensate di incontrare in fascia da media a medio-bassa? Non pensate di scontrarvi con i produttori di sistemi di supervisione della sicurezza, tipicamente desk-top mono-operatore e mono-applicazione?
In realtà questa competizione è già in corso in qualche misura ma in forma anomala, anche se non è detto che vi sia della malafede. Ci sono stati casi in cui è stato proposto come PSIM un puro software di supervisione di allarmi, con una grafica curata e alcune funzioni appropriate; mentre tutti gli addetti ai lavori sanno che quella *"workstation"* con a bordo un *"Application Software"* non è un *Sistema Informatico*: ergo, non è un PSIM.
Una soluzione di tipo workstation potrà essere chiamata al massimo *"postazione di supervisione allarmi"* ed è evidente, per chi si informa, che un PSIM è su un altro pianeta. In molti casi è solo un equivoco, che nasce dal fatto che nel settore della sicurezza fisica gli specialisti in informatica con una specializzazione sistemistica non sono molto diffusi. Quanto prima sarà quindi necessario arrivare ad un chiarimento, di cui non ci siamo mai preoccupati perché il nostro utente-tipo in fascia alta e medio alta è già attrezzato per non prendere in considerazione sistemi che non siano chiaramente un PSIM nella sostanza tecnico applicativa e nella struttura che lo propone e supporta.

Ci può anticipare quali politiche ed iniziative avete in preparazione per la condivisione con il mercato potenziale PSIM per consolidare una cultura del PSIM professionale e per supportare gli indirizzi evolutivi di questo segmento di mercato? Ed anche per contenere l'estensione di quelle zone grigie che si generano dalla rincorsa al PSIM?
Innanzitutto siamo quasi pronti con un e-book, che stiamo integrando appunto con delle classificazioni mirate ad evitare le ambiguità e le scorciatoie suscettibili di pregiudicare il buon esito di un progetto che poi è l'utente a pagare.
Ma, soprattutto, lavoreremo sull'organizzazione del nostro Ecosistema di utenti e partner in ottica ERP. Ed è naturale che ciò venga fatto da noi per primi, per la nostra completa aderenza al paradigma del sistema informatico, e che l'Ecosistema di utenti, partners, terze parti, non vada soltanto identificato e informato ma vada anche attivato e stimolato per produrre valore aggiunto da far ricadere sulla comunità.
Potrei concludere affermando che, fino ad oggi, Citel è riuscita a gestire questi processi sinergici facendo da perno dell'ecosistema di utenti, terze parti, fornitori complementari sulla base di rapporti soprattutto individuali; mentre ora riteniamo giunto il momento per stimolare e alimentare con apposite iniziative i processi collaborativi che un modello di tipo ERP punta ad organizzare, alimentare e valorizzare.

Il paradigma e il modello collaborativo riconducibile all'ERP sono i più appropriati e attuali per qualificare un PSIM professionale, evolutivo, aperto

Questa è la conclusione cui è arrivata Citel di recente. Il modello **ERP** (Enterprise Resource Planning), nato nel mondo dell'informatica gestionale, porta a costituire la cinghia di trasmissione di un sistema complessivo che fa convergere processi informatizzati di gestione su una base dati che coinvolge software *dipartimentali* specializzati, forniti insieme al sistema principale di governo, oppure da partner o da altri fornitori selezionati dall'utente, preesistenti o di nuova adozione.
Condizione irrinunciabile per l'appartenenza all'ERP: l'**impegno dei fornitori complementari a collaborare all'integrazione per l'interoperabilità**, dei propri prodotti e piattaforme secondo un accordo normalizzato nell'interesse dell'utente finale.
In realtà tutto questo è già in atto, se si considerano le tre comunità che costituiscono l'Ecosistema Centrax-open-PSIM: quella degli utenti, quella delle terze parti di integrazione e quella dei produttori complementari integrati; con numeri tali che ormai richiedono una forma di organizzazione e di procedimenti che renda fluidi i processi sinergici e che li canalizzi a fini di efficienza e fruibilità.
Per il Security Manager utente di un PSIM di Citel, l'approccio e il contesto ERP, una volta a regime, potrà permettere la condivisione di problematiche, soluzioni e valutazioni, compresa la qualificazione delle terze parti di servizio. E faciliterà tra l'altro la messa a fuoco dei valori di sistema e di processo, sia nell'immediato che in chiave di assicurazione dei requisiti di qualità del *Progetto Permanente* o, se si preferisce, di *Life-cycle Project*.

CONTATTI: CITEL SPA
info@citel.it
www.citel.it

Axis Communications, i molti significati di un miliardo di dollari di fatturato

a colloquio con Andrea Monteleone, National Sales Manager Italy presso Axis Communications
a cura di Raffaello Juvara

Nel 2017 Axis ha raggiunto l'importo non solo simbolico di un miliardo di dollari di fatturato. Cosa comporta questo traguardo, in termini di quote di mercato globale e di influenza sui comportamenti degli utilizzatori, in considerazione della corsa al ribasso dei prezzi che si è vista negli ultimi anni?
In un contesto di mercato globale così complesso ed articolato, quel numero assume molti più significati rispetto alle sole quote di mercato e all'influenzamento degli utilizzatori. E' vero che il mercato è stato spesso guidato dal prezzo più conveniente, ma prima o poi ci si trova a fare i conti con la qualità dei prodotti installati, con le garanzie offerte in termini di supporto long-term ai firmware, alla cybersecurity, alla possibilità di aggiornare i sistemi e alla continuità di funzionamento che si può garantire. Axis, da questo punto di vista, ha sempre adottato politiche molto chiare, e sempre di più lo farà. Il mercato, evidentemente, apprezza questi sforzi, scegliendo di investire sulle nostre soluzioni per poter beneficiare del valore aggiunto che siamo in grado di creare.

Alla fine del 2017 IPVM aveva considerato concluso il corso ribassista (vedi). Quali sono le vostre valutazioni in merito?
La corsa al ribasso della componente hardware è, dal mio punto di vista, parte integrante dell'evoluzione di un qualsiasi mercato che si stia avvicinando alla maturità. Guardando al recente passato, abbondano gli esempi di questo genere, basti pensare ai PC piuttosto che alla telefonia cellulare. Sempre prendendo spunto dagli stessi esempi, si evince anche come i player di mercato che assumano il ruolo di innovatori, introducendo nuove tecnologie, nuove modalità di utilizzo di tecnologie esistenti e che si orientino alla creazione di valore aggiunto acquisiscano e mantengano nel tempo una posizione di vantaggio. Da qui i nostri risultati. La lettura della situazione attuale data da IPVM è sicuramente interessante e aderente alla realtà, aggiungo che sia i produttori che il canale non possano, né vogliano, proseguire in questa corsa perché un'ulteriore compressione delle marginalità porterebbe ad azzerare il profitto che, a conti fatti, è il fine ultimo a cui tutti gli attori coinvolti puntano.

Il CAGR molto elevato del vostro fatturato negli ultimi 5 anni quanto è dovuto alla linea di prodotti tipici di videosorveglianza (telecamere e recorder) e quanto alle altre linee di prodotto?
La risposta non è così immediata, poiché vanno considerati sia fattori esterni che interni. Innanzitutto, nel periodo considerato è cambiato il perimetro aziendale, per via dell'acquisizione di Citilog, Cognimatics e 2N, e questo ha comportato, oltre all'aumento delle dimensioni aziendali in numero di dipendenti, anche un aumento di fatturato. Dall'altra parte, le strategie di Axis in termini di differenziazione e ampliamento della proposta - controllo accessi, soluzioni per il retail, soluzioni per l'audio - hanno contribuito non poco al raggiungimento di questo risultato. Certo è che il peso della parte legata più squisitamente alla videosorveglianza la faccia ancora da padrone.

Quali sono secondo voi le linee con maggiori potenzialità di crescita nei prossimi anni, nelle diverse aree geografiche?
Ragionando in termini globali, risulta sempre molto difficile tratteggiare la situazione, in quanto le dinamiche delle varie regioni sono profondamente diverse e anche il product mix varia notevolmente. Riducendo la portata del ragionamento al sud Europa, anche gli analisti sembrano convergere su una crescita CAGR del comparto TVCC abbastanza contenuta, in media, ma comunque con volumi e fatturati importanti per quanto concerne le soluzioni basate su tecnologia termica – tipicamente impiegate in ambiti critici e industriali – e multisensor, sempre più utilizzate al posto delle PTZ in ambito di sorveglianza cittadina. Per tutto quanto invece sia riconducibile alle analitiche, negli ambiti più disparati, le stime sono decisamente più positive, sia in termini di volumi che di fatturato. Il vero game-changer, infine, sembra essere il controllo accessi, dove sono attese le crescite più importanti.

E quali saranno i mercati verticali di maggior interesse in Emea ed in Italia?
A livello EMEA e Italiano, il mondo delle infrastrutture critiche sta vivendo una stagione di importanti investimenti in generale e, vista la particolare situazione geopolitica, la quota parte di questi investimenti destinata alla sicurezza sta diventando molto importante. Per quanto riguarda Axis, e questo è vero anche a livello globale, l'altro mercato verticale di riferimento è quello del retail, dove le richieste della clientela e le possibili applicazioni sono in continua crescita ed evoluzione.

Parliamo del mercato italiano. Come viene apprezzata la qualità dei prodotti rispetto al prezzo?
Dipende molto dal segmento di mercato considerato. Sulla fascia enterprise con clientela privata, la maturità e l'approccio metodologico della clientela spesso portano a ragionare in termini di ROI (Return on investment) e quindi il solo parametro del prezzo di acquisto (CAPEX) non è decisivo. Al contrario, in ambiti pubblici la sensibilità al prezzo è molto maggiore. Se ci riferiamo al mercato di medio e piccolo cabotaggio, la sensibilità al prezzo è molto più alta, principalmente perché c'è meno attenzione alle potenziali applicazioni di un sistema di sicurezza e le esigenze applicative sono molto meno complesse ed articolate.

Infine, i vostri partner di canale. Quali sono le vostre linee guida nel prossimo futuro, con catene di distribuzione sempre più accorciate e utenti finali sempre più informati?
Il tema del canale non è in alcun modo in discussione: Axis ha fatto della correttezza e trasparenza nei confronti dei partner di canale una bandiera. Che il cliente finale sia sempre più consapevole e informato per noi diventa un vantaggio competitivo, perché sarà ancora più facile veicolare certi messaggi di qualità, ma sempre e comunque al fianco dei nostri partner, che sono e saranno elementi chiave della nostra strategia

AXIS COMMUNICATIONS

CONTATTI: AXIS COMMUNICATIONS
Tel. +39 02 8424 5762
www.axis.com

CEDISS, una realtà della distribuzione che punta alla crescita professionale del partner installatore

a colloquio con Laura Rossi, titolare e amministratore unico dell'azienda Cediss srl
a cura della Redazione

Ci parli di Cediss, una delle più consolidate e storiche realtà operanti nella security e nella safety in Italia
Cediss nasce nel 1981 come centro specializzato nella distribuzione di apparecchiature elettroniche per la sicurezza, mettendo a frutto tutte le precedenti esperienze nel settore dell'impiantistica. Da sempre l'obiettivo di Cediss è di proporre prodotti innovativi ed affidabili. Le necessità di sicurezza, in casa, sui mezzi di trasporto o negli ambienti di lavoro, hanno peculiarità specifiche diverse da caso a caso. Per questa ragione, diamo al nostro rapporto col cliente un taglio sartoriale: prendiamo in esame ogni richiesta ed operiamo un'analisi attenta ed approfondita, che ci permette di proporre la soluzione migliore alla problematica presentata. Un progetto su misura è un progetto efficace.

I settori nostri core business sono:
• Sicurezza Building: antintrusione, antincendio, rilevazione gas tossici – esplosivi, EVAC, TVCC controllo accessi domestico;
• Sicurezza Automotive: controlli video, videosorveglianza, antincendio e rilevazione gas, cartelli indicatori, conta passeggeri e gestione flotte;
• Sicurezza Kitchen: antincendio.

Qual è la concezione di sicurezza che trasferite ai vostri clienti clienti ed ai partner di canale?
Attribuiamo a tutti i nostri clienti grande importanza ed il nostro obiettivo primario è la loro soddisfazione, che ci imponiamo di raggiungere offrendo assistenza nella realizzazione dell'intervento dalle fasi di progettazione fino alla messa in opera. Il nostro obiettivo è di offrire risposte duttili e sempre all'avanguardia alle esigenze di sicurezza, in ogni settore. Per questo non ci accontentiamo di proporre semplici prodotti, vogliamo bensì offrire soluzioni tecnicamente affidabili e personalizzate su misura per ogni singolo cliente. Portiamo a termine commesse complesse seguendo progetto, realizzazione, collaudo e garantendo il nostro supporto e la nostra consulenza in ogni passaggio. Per i nostri clienti è anche prevista una formazione sugli aspetti normativi, sulla manutenzione più appropriata e sulle caratteristiche distintive dei nuovi prodotti.

Quali sono i vendor ai quali vi appoggiate per avere riscontri sul campo della vostra impostazione?
Attraverso un catalogo ricco ed un assortimento completo di prodotti disponibili nel nostro magazzino, siamo in grado di soddisfare con rapidità le richieste più eterogenee. Con noi, è possibile contare su un servizio di vendita calibrato sulle caratteristiche del singolo intervento, per una soluzione su misura, efficace ed efficiente.

I nostri partner sono:

Fire: Bosch, EL.MO., Ksenia, Amerex, Dafo
TVCC: Bosch, TKH Group, EL.MO., TVT, Huawei, Streamax
Intrusione: Bosch, EL.MO., AVS, CIAS, DAITEM, Ksenia, Crow
Audio: Bosch
Intercom: Commend
Accessori: TSEC, Cooper Safety, Avotec, Wolf Safety, Teltonika, E.Lan, MARSS, Peplink
Controllo Accessi: EL.MO., Simons Voss
Automazione: Cardin
Rivelazione Gas: Sensitron, Amerex

Il vostro programma di incontri con la cittadinanza di comuni della provincia di Bologna è un modo concreto per divulgare la cultura della sicurezza tra gli utilizzatori finali. In che cosa consiste e in che modo si articola?
L'obiettivo di questi incontri è di divulgare ai privati cittadini e alle aziende la cultura della sicurezza. I relatori di questi incontri sono professionisti selezionati con larga esperienza nel settore, la collaborazione con i comuni ci consente di raggiungere la cittadinanza in veste istituzionale. Gli incontri si articolano in sessioni differenziate per le aziende e per i privati rispondendo alle diverse esigenze.

Quali sono i vostri progetti per il futuro?
Cediss è alla continua ricerca di soluzioni tecnologicamente avanzate che rispondano alle esigenze di sicurezza e che garantiscano affidabilità e prestazioni nel tempo. Allo stesso tempo uno dei nostri obiettivi è la crescita continua insieme ai nostri clienti con percorsi formativi e sessioni didattiche organizzate con la collaborazione dei nostri partner

CONTATTI: CEDISS SRL
www.cediss.com

ERMES: la comunicazione Over IP in ambito sanitario

di Filippo Gambino, CEO di Ermes Elettronica srl

Introduzione
Grandi strutture come i moderni ospedali necessitano di sistemi di comunicazione affidabili e di flessibile impiego da utilizzare per le comunicazioni all'interno dei reparti, la diffusione degli annunci al pubblico, la gestione delle comunicazioni tra il pubblico stesso e gli addetti al primo intervento in concomitanza con la gestione delle emergenze.

Ottimizzando le comunicazione tra gli operatori e quelle tra questi ed il pubblico si rendono più efficienti i processi consentendo di migliorare i servizi all'utenza e di realizzare consistenti risparmi in termini di ore/lavoro e quindi di costi.

I sistemi di comunicazione si possono raggruppare in tre principali famiglie:

1. sistemi di interfonia destinati principalmente all'utilizzo da parte del personale per le comunicazioni di servizio;
2. sistemi di diffusione sonora utilizzati dal personale per effettuare comunicazioni ed annunci agli utenti;
3. sistemi di chiamata di emergenza a disposizione del pubblico per richiedere assistenza in particolari situazioni di difficoltà sia per motivi di safety sia per motivi di security.

Oltre che per le comunicazioni di servizio all'interno dei reparti o tra reparti diversi gli apparati di interfonia e diffusione sonora trovano utilizzo ad integrazione della funzionalità di altri sistemi come il controllo accessi, la videosorveglianza, la rilevazione incendi.

Particolare rilevanza, in quanto prescritti da precise norme di legge, rivestono gli impianti audio di evacuazione asserviti ai sistemi di rilevazione incendi, i sistemi di chiamate di emergenza a servizio degli "spazi calmi" lungo le vie di fuga ed i sistemi di richiesta di soccorso da installare negli ascensori.

La tecnologia Over IP
Nel progettare i sistemi di comunicazione in strutture di vaste dimensioni come gli ospedali, riveste particolare importanza la scelta della tecnologia da adottare.

I vantaggi offerti dall'adozione di impianti in tecnologia Over IP rispetto ai tradizionali sistemi analogici sono evidenti. In primo luogo, perché il trasferimento dei segnali sotto forma numerica elimina del tutto la possibilità di accoppiamento di disturbi all'audio; in secondo luogo, la capillare diffusione della rete dati nelle strutture di nuova concezione consente di eliminare quasi del tutto la necessità di stendere una rete cavi destinata all'esclusivo utilizzo per questi servizi, con la conseguente riduzione dei costi di installazione.

Inoltre l'utilizzo di una rete dati esistente e condivisa con altri sistemi riduce notevolmente i tempi di progettazione e consente di modificare ed espandere il sistema con semplicità adattandolo ad ogni futura esigenza.

In generale, dove sia già disponibile una LAN utilizzata per gestire una rete di computer, l'automazione di una linea di produzione o un impianto di videosorveglianza, è semplice, rapido ed economico realizzare impianti di interfonia, citofonia, videocitofonia, diffusione sonora o di chiamata di emergenza condividendo la rete con i servizi preesistenti.

ERMES ha messo a punto una serie di apparati Over IP in grado di soddisfare tutte le necessità basati su di un'unica piattaforma software, quindi facilmente integrabili tra loro, che utilizzano esclusivamente una rete LAN realizzata con qualsiasi tipo di tecnologia (rame, fibra wireless, …), purché conforme allo standard ETHERNET.

Questi apparati utilizzano un protocollo di comunicazione Peer-To-Peer (P2P) grazie al quale gli apparati (Peer) scambiano i dati audio e di controllo direttamente tra loro senza la necessità di passare attraverso una unità centrale (server) il cui disservizio può pregiudicare la funzionalità dell'intero sistema: ERMES ritiene di fondamentale importanza utilizzare il protocollo P2P per i sistemi dove è richiesto un elevato grado di affidabilità.

Apparati per uso ospedaliero
Per l'uso negli ospedali e in genere per le strutture destinate all'erogazione di servizi sanitari, ERMES dispone di una gamma di apparati per interfonia, diffusione sonora e chiamata di emergenza particolarmente vasta ed in grado di soddisfare le esigenze di qualsiasi tipo di ambiente: sale operatorie, laboratori diagnostici, uffici, locali classificati ATEX.

In particolare, ERMES dispone di una famiglia di apparati appositamente studiati per i locali medici, ove si svolgono attività diagnostiche, terapeutiche, riabilitative e chirurgiche; tali apparati sono anche idonei ad essere installati nella "zona paziente", il volume in cui un paziente può venire in contatto con altri apparecchi elettromedicali o con masse estranee sia direttamente sia per mezzo di altre persone in contatto con tali elementi.

Tali interfoni sono particolarmente adatti all'installazione nelle sale operatorie e nelle camere bianche, in quanto l'interfono ha grado di protezione IP66 ed è quindi protetto da polvere, sporcizia e getti di liquidi come è possibile avvenga in tali ambienti; inoltre, la speciale pellicola di protezione del pannello frontale assicura un effetto repellente allo sporco e si presta ad una facile pulizia con i detergenti e disinfettanti solitamente utilizzati.

Gli interfoni per camere sterili si integrano con tutti gli altri interfoni della gamma ERMES, come le consolle interfoniche da ufficio, gli interfoni per montaggio a parete, sia da interno sia da esterno, o gli interfoni per ambienti classificati ATEX che a volte sono richiesti nei locali tecnologici.

ermes
freedom to communicate

CONTATTI: ERMES ELETTRONICA SRL
Tel. +39 0438 308470
www.ermes-cctv.com

Da TSec nasce Inxpect MSK-101, la rivoluzione della protezione volumetrica per l'antintrusione

a cura della Redazione

TSec è una realtà in forte crescita che ha saputo rispondere alle esigenze del mercato fin dai suoi primi prodotti, diventando rapidamente un simbolo dell'alta sicurezza.
L'azienda progetta e produce dispositivi per impianti di rilevazione antintrusione ad alto contenuto tecnologico. Dopo quattro anni di ricerca e sviluppo, nasce **Inxpect MSK-101**. Questo prodotto rivoluziona il mondo della protezione volumetrica partendo dalla tecnologia di rilevazione.
I sensori di movimento intelligenti della serie MSK sono basati su tecnologia radar **FMCW**, la stessa tecnologia presente nei radar utilizzati sulle navi e sugli aerei, di recente impiegata anche nel settore automobilistico. Quella stessa classe di tecnologia è stata concentrata in un dispositivo per la sicurezza, un sensore che può essere usato sia all'interno sia all'esterno degli edifici e che rivela il movimento in maniera estremamente puntuale. L'algoritmo di elaborazione del segnale di cui è dotato, è inoltre "intelligente" al punto da essere in grado di riconoscere se il movimento è di un essere umano, di un volatile o di altro piccolo animale. Ne capisce la direzione, la velocità ed è in grado di discriminarne il movimento, riducendo quindi i rischi di falsi allarmi. Si comporta come una telecamera, ma senza usare la visione ottica.

Il sensore dispone di quattro uscite a relè, preconfigurate nel seguente modo:
relè 1: allarme;
relè 2: preallarme;
relè 3: manomissione per spostamento o per estrazione del sensore;
relè 4: guasto.

Lo stato dei relè è riportato nella pagina principale dell'applicazione mobile Inxpect, disponibile gratuitamente per Android e iOS, con la quale si programma il sensore da smartphone o tablet, per facilitare le verifiche sul campo in fase di installazione.
Per quanto riguarda la **Pet Immunity Protection**, il sensore è in grado di discriminare il movimento di un essere umano da quello di un animale domestico. Il livello di Pet Protection del sensore è facilmente gestibile tramite la stessa app di configurazione.
Un livello di Pet Protection basso garantisce un maggior livello di sicurezza ma, contemporaneamente, espone a un maggior rischio di falsi allarmi. È adatto a scenari dove non è ammesso alcun movimento nell'area monitorata (es.: in un museo). Un livello di tolleranza alto è adatto a installazioni esterne, dove la probabilità di falsi allarmi per animali o altri oggetti in movimento è molto alta.
Un livello di tolleranza intermedio permette, ad esempio, di ignorare i movimenti in un'abitazione di un animale domestico, ma di segnalare correttamente i movimenti di persone che camminano o si avvicinano carponi.
All'interno del campo visivo del sensore, la zona di allarme e l'eventuale zona di preallarme definiscono l'area effettivamente monitorata dal sensore. Se non è definita una zona di preallarme, la zona di allarme corrisponde all'intera area monitorata.

L'applicazione permette di impostare facilmente le zone di allarme e preallarme, trascinando il cursore relativo fino alla distanza desiderata. L'algoritmo di elaborazione del movimento Inxpect fornisce all'istallatore una completa flessibilità con la possibilità di configurare aree di allarme e pre-allarme fino ad un massimo di 20m con accuratezza centimetrica, sensibilità e modalità di segnalazione alla centrale di allarme, pre-allarme, manomissione e guasto.
Un altro aspetto unico dell'MSK-101 è relativo alla sua capacità di comprendere dinamicamente quando un oggetto si muove, ma non si avvicina o allontana dal sensore stesso: questo concetto di "oggetto semi-statico", rilevato in tempo reale dal sensore, permette di ridurre drasticamente la possibilità di falsi allarmi in presenza di tende, porte o finestre rimaste aperte, cespugli, ecc.
Grazie alla scocca meccanica dal design unico, MSK-101 può essere installato a muro o a soffitto, senza bisogno di accessori aggiuntivi. La contro-piastra posteriore agisce come adattatore multi-standard per le principali scatole elettriche da incasso, per standard Italia, UK, Francia, Germania e USA.
A seconda dell'orientamento, il sensore può essere utilizzato per monitorare un'area ampia (orientamento orizzontale o "volumetrico") oppure per monitorare un'area perimetrale, creando una sorta di barriera di protezione per gli accessi lungo un muro o un cancello (orientamento verticale, o "a barriera").
L'ampiezza del campo coperto con orientamento orizzontale del sensore (volumetrico) è di circa 90° massimo sul piano orizzontale e di 30° sul piano verticale. Nel caso di orientamento verticale (a barriera) il campo coperto diviene una barriera larga, nel suo punto più ampio, circa 2m, e che si estende per 20m.
Grazie alla sua capacità di fornire a qualsiasi centrale di allarme segnali relativi al movimento che avvenga nel range di differenti aree completamente configurabili, l'MSK-101 è in grado di aumentare sensibilmente il livello di sicurezza di tutti i sistemi anti-intrusione.
Il montaggio e la programmazione del sensore richiedono pochi minuti, in qualsiasi configurazione installativa.
Grazie alla produzione e ingegnerizzazione rigorosamente Made in Italy con controllo qualità su ogni singolo pezzo, MSK-101 e tutte le soluzioni di TSec si pongono ai vertici del mercato per sicurezza e contenuto tecnologico e soddisfano pienamente tutte le moderne esigenze installative diminuendo sensibilmente i costi di installazione e manutenzione di qualunque impianto.

Caratteristiche principali del Mod. MSK-101

- Modalità d'impiego: Sensore di movimento con involucro stagno
- Modalità di rilevazione: Algoritmo di elaborazione del movimento basato su tecnologia radar FMCW a 24GHz
- FOV: 90° orizzontale / 30° verticale
- Distanza massima (rilevazione persona): 20 metri
- Altezza di montaggio: da 1,5 a 3,0 metri
- Velocità di rilevazione: >0,05 m/sec
- Uscite: 4 relè stato solido programmabili N.C. o N.O.\ Configurazioni di default: tamper, guasto, pre-allarme, allarme (N.C.)
- Periodo di riscaldamento: Meno di 1 secondo
- Caratteristiche elettriche: 12VDC +/- 25%, 100mA (max) a 12VDC
- Peso: 150 g
- Temperatura di esercizio: -40/+60 °C
- Materiale dell'involucro: Polimero tecnico
- Certificazioni: CE, include ID FCC: UXS-SMR-3X4, compatibile EN-50131-2-3 Grado 3, Classe ambientale IV
- Grado di protezione IP: IP67

TSec TECHNOLOGY FOR SECURITY

CONTATTI: TSec SpA
Tel. +39 030 5785302
www.tsec.it

Il collasso mediatico sociale e la pelliccetta scagnata

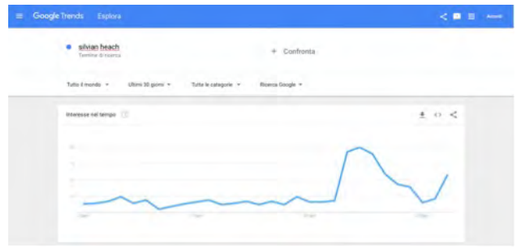
di Giuseppe Mastromattei, presidente del Laboratorio per la Sicurezza

L'ultima volta che avevo parlato di "collasso mediatico sociale" è stata in occasione delle elezioni presidenziali negli Stati Uniti, quando mi sono imbattuto in una foto che ritraeva Hillary Clinton di fronte ad una folla di ammiratori, i quali però davano le spalle alla candidata per farsi dei selfie.

Niente in confronto a quello che è successo in un centro commerciale di Caserta recentemente.
Chiunque abbia avuto una minima esperienza nel Retail avrà sicuramente avuto modo di imbattersi con clienti che presentavano dei reclami per problemi avuti con dei prodotti.
In ogni situazione del genere, sempre molto delicata, è compito dell'addetto alle vendite o del responsabile del punto vendita gestire la situazione al meglio, con l'unico obiettivo di far contento il cliente ed ovviamente tutelare il profitto dell'azienda. Ma in questo caso qualcosa è andato storto. In questa situazione, oltre ad una cliente che si è scatenata all'interno del negozio inveendo contro la commessa e lamentandosi che l'abito acquistato poco tempo prima avesse perso colore macchiando una pelliccia che stava indossando durante un matrimonio, sempre all'interno del negozio, un altro cliente ha ripreso tutto e pubblicato immediatamente il video sui social.
E da quel momento, un semplice e comune episodio di reclamo, sebbene un po' colorito nella gestione della comunicazione da parte della cliente, è diventato un vero e proprio caso mediatico, il video è diventato in poche ore un cosiddetto "video virale".

Quale dei due clienti ha arrecato il maggior danno all'azienda?
Mettiamoci però nei panni dell'azienda che si è vista, in un attimo, balzare agli onori della cronaca e costretta a gestire una crisi, anzi una "nuova" crisi.
Ma non dimentichiamoci che spesso le crisi si trasformano in opportunità, se ben gestite. E questo è stato il caso Silvian Heach.
Siamo tutti d'accordo che l'azienda non abbia fatto una bellissima figura in questa circostanza e sicuramente sarebbe stato possibile evitare tutto ciò. Ma ecco che cosa è successo nel web nei giorni successivi: Il marchio ha avuto un'impennata impressionante e, analizzando la funzione pubblica di Google Trends, sono stati raggiunti valori mai registrati prima.

Gestire "social media crisis", non è semplice, ma è importante essere preparati e soprattutto consapevoli di quello che è l'ambiente in cui ci si muove. Nel caso specifico, la reazione dell'azienda è stata molto particolare e, forse, molto efficace. Silvian Heach infatti ha deciso di riprendere l'episodio con molta ironia e leggerezza ma, soprattutto, con estrema velocità, pubblicando immediatamente un video in risposta a quanto accaduto di assoluto effetto e sdrammatizzante (qualche testata giornalistica ha definito questa reazione addirittura "geniale").



#PELLICCETTE IN PROMOZIONE FINO AD ESAURIMENTO — VIENE DA SILVIAN HEACH — IN OMAGGIO VITAMINA C PER 150 INVITATI

La cliente, dal suo canto avrà sicuramente ricevuto un adeguato risarcimento al danno subito, ed un'inaspettata (e sicuramente piacevole) visibilità mediatica.

E tutti vissero felici e contenti…

Ma non sempre queste storie hanno tutte un lieto fine, perché casi del genere sono oggi dietro l'angolo e il rischio di trovarsi impreparati è estremamente alto. Il danno e la perdita di profitto che potrebbero generare questo tipo di crisi, ai tempi dei social media, potrebbe avere un effetto devastante sull'azienda.
Dobbiamo evolverci e farci trovare pronti, ma siamo solo all'inizio. Temo che assisteremo ancora ad episodi del genere, siamo nell'era della omnicanalità!

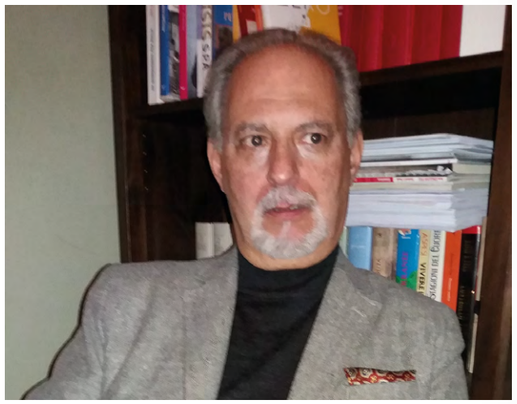
LABORATORIO PER LA SICUREZZA

CONTATTI: LABORATORIO PER LA SICUREZZA
segreteria@laboratorio-sicurezza.org

La sicurezza dei centri commerciali: è necessaria una progettazione integrata

di Eduardo Parisi - avvocato, senior consultant in Sicurezza

La costruzione di un centro commerciale consiste, principalmente nella realizzazione di una piattaforma commerciale e di gallerie di negozi di grandi dimensioni che, solitamente, comportano un radicale cambio di abitudini per gli abitanti dell'area dove si ubicano questi complessi. Assistiamo alla realizzazione di veri e propri "epicentri", che offrono prodotti e servizi concentrati in un unico punto, in grado di soddisfare i bisogni dei nuclei famigliari che li visitano e li utilizzano.



Quando entriamo in un centro commerciale, non abbiamo una percezione di insicurezza, anzi riteniamo che le telecamere installate, le colonnine antitaccheggio ed il personale addetto alla sicurezza ci possano tutelare e che la nostra sicurezza sia salva. Ma ricordiamoci che si tratta di misure di sicurezza normalmente finalizzate a contrastare i furti!

Condividiamo con i nostri figli, consorti, amici, momenti conviviali all'interno dei centri commerciali usufruendo dei ristoranti, bar e cinema presenti all'interno di tali aree. Riteniamo che essi siano stati concepiti e costruiti contemplando tutte le misure necessarie per essere conformi alle normative vigenti in materia.

Ma non dobbiamo dimenticare che la chiave della sicurezza in un centro commerciale dev'essere la capacità di garantire la protezione e l'incolumità delle persone che lo visitano oltre ad evitare i furti dei prodotti presenti nei negozi, non dimenticando comunque che sono la causa principale di perdita economica nel settore della grande distribuzione.

La problematica della sicurezza nei centri commerciali è, di conseguenza, molto delicata per il solo fatto che si debba gestire l'incolumità di una grande concentrazione di persone all'interno di una superficie circoscritta. Pertanto, è necessario effettuare un'analisi del rischio specifica che, pur comprendendo la sicurezza dei beni e delle infrastrutture, vada a focalizzarsi sulla protezione delle persone. Per questo, è fondamentale che tutto il sistema sia omogeneo. Purtroppo non sempre siamo in grado di ragionare in termini di prevenzione dato che, per molti, la prevenzione viene vista come un costo, serve poco e costituisce una perdita di tempo…

Analizziamo il concetto di "sicurezza":

"La sicurezza si definisce come uno stato psicologico che, per mezzo di misure circoscritte, atte a proteggerci sia dal punto di vista di incolumità fisica, sia dal punto di vista materiale, ci permette di svolgere i compiti a cui siamo preposti, o che riteniamo necessari, al fine di conseguire uno sviluppo ed il raggiungimento di uno stato di benessere".

Ricordiamoci che ogni centro commerciale è una realtà autonoma, ognuna delle quali deve avere un proprio "Sistema di Sicurezza" gestito in modo puntuale dai preposti che rispondono direttamente al top management, dal momento che questa responsabilità non può essere delegata.

Le persone che visitano e usufruiscono di un centro comerciale sono i destinatari prioritari del Sistema di Sicurezza. Dobbiamo pertanto concentrarci sempre più nella realizzazione di un sistema che contempli le misure atte a limitare o, meglio, impedire atti terroristici o criminali di ogni genere, per tutelare le persone che visitano i nostri centri commerciali. In questo modo concepiamo la **sicurezza come un servizio che, come tale, dev'essere utile ed efficiente.**

Dobbiamo insistere sul concetto di "Sistema di Sicurezza" che viene spesso confuso con quello di "misure di sicurezza" ovvero l'insieme delle soluzioni applicative che, solitamente, è molto complesso integrare in modo funzionale in una struttura coerente e logica.

In genere, siamo portati a ritenere che le criticità in termini di sicurezza in un centro commerciale possano derivare dal malfunzionamento delle telecamere o dalle inadempienze da parte del personale di vigilanza. Personalmente, ritengo invece che le cause siano ben altre, da ricercare all'origine.

Il problema, a volte, è di natura strutturale o, meglio, progettuale, in quanto nella fase di progettazione di un centro commerciale vengono considerate due fasi:

1. L'ingegnere consegna il progetto integrato del sistema di sicurezza da lui valutato, progettato e raccomandato.

2. L'architetto consegna il proprio progetto che contempla anche gli aspetti specifici tecnici relativi alle vie di accesso e di uscita.

A volte, può accadere l'errore che la progettazione degli impianti di sicurezza attiva (antintrusione, videosorveglianza, rilevamento incendio ecc) venga assegnata ad una società di consulenza o ad uno studio di ingegneria, mentre la realizzazione del sistema venga affidato ad uno dei vari fornitori di attrezzature di sicurezza passiva (porte, casseforti, sistemi di blindatura, serrature di sicurezza ecc). A mio avviso, quest'approccio è sbagliato, in quanto il Sistema di Sicurezza deve essere il risultato di un progetto integrato in ogni sua fase, dalla progettazione fino alle procedure di manutenzione durante l'esercizio.

Analizziamo l'attentato al centro commerciale "Centro Andino" di Bogotà (Colombia) avvenuto nel 2017: un terrorista era penetrato nelle toilette delle donne e si era fatto esplodere in una fascia oraria di grande affluenza, uccidendo tre donne e provocando numerosi feriti. La perizia effettuata a posteriori ha evidenziato che all'interno del bagno non era stato utilizzato "materiale a norma" che, probabilmente, avrebbe potuto consentire la fuga alle persone intrappolate. Un altro aspetto importante da sottolineare è che la polizia non è riuscita a ricostruire i fatti a causa della mancanza di immagini dettagliate, per quanto sul luogo fossero installate oltre 250 telecamere!

Riporto qui di seguito un elenco degli errori più ricorrenti in termini di progettazione di un Sistema di Sicurezza all'interno dei centri commerciali:

1. Mancata individuazione di un responsabile della revisione e

della verifica della coerenza di progettazione delle componenti di security e safety dell'edificio;

2. Mancanza di un piano dettagliato del progetto dell'edificio e della sua sicurezza. Partendo dal presupposto che la fase di progettazione dell'edificio sia la parte più importante per il successo o l'insuccesso del progetto stesso, più è dettagliato il progetto, minori saranno le variazioni. L'assenza di un'analisi del rischio, la mancanza della redazione di piani di evacuazione, la mancanza di misure antintrusione, i capitolati di carpenteria incompleti sono fattori che influiscono negativamente sull'economicità complessiva del progetto e, quindi, sul ritorno dell'investimento;

3. Assegnazione di appalti al massimo ribasso, con offerte poco "trasparenti";

4. Autorizzazione di varianti al progetto in fase di realizzazione. Tali variazioni solitamente vengono richieste da chi si è aggiudicato la gara per ottenere maggiori margini economici. Qualora si rendesse necessario approvare variazioni, bisogna verificare che esse siano coerenti e integrate nel progetto globale, per non trovarsi di fronte a situazioni difficili da gestire;

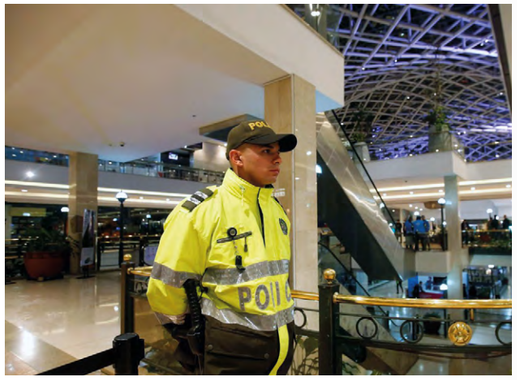
5. Mancanza di una visione globale del Sistema di Sicurezza da parte degli investitori, che si riflette sugli studi di architettura e di ingegneria. Se i progetti non sono integrati tra loro, ci ritroviamo da un lato il progetto di sicurezza e dall'altro il progetto di architettura, ovvero progetti a sé stanti che non "parlano" tra di loro, che a posteriori possono risultare ridondanti o perfino produrre effetti contrapposti;

6. Supremazia del paradigma *"vince il progetto più veloce da realizzare"* ed *"al minor costo"*;

7. Mancanza di esperti di settore certificati in grado di effettuare audit specifici in termini di sicurezza sulla base di una pianificazione strutturale.

I Sistemi di Sicurezza devono essere efficienti ed in sinergia tra le parti *Engeenering* e *Human Resource,* per garantire che le diverse attività vengano svolte in modo automatico e coordinato.

Mentre scrivo quest'articolo, il ricordo va a quanto si è verificato qualche tempo fa al Centro Commerciale "Il Globo" a Busnago (MB) : alcune persone hanno avvertito improvvisamente un persistente bruciore alla gola ed agli occhi, ripetuti attacchi di tosse e sensazione di soffocamento. E' scattato l'allarme, sono arrivate quattro ambulanze ed un'auto medica. Risultato: una ventina di persone, tra adulti e bambini, risultavano intossicati



Centro commerciale Andino

e sono stati portati all'ospedale. Sono intervenuti i carabinieri e anche un nucleo NBCR dei vigili del Fuoco a scopo di precauzione. Non essendo la prima volta che si verifica un episodio simile in questo centro, significa che le misure di sicurezza devono forse venire rielaborate per evitare che si ripetano tali episodi.

Per fortuna, l'episodio è successo alla sera di un giorno settimanale, ma è inevitabile domandarsi quali conseguenze avrebbero potuto esserci se si fosse verificato nei giorni di maggior affluenza, durante il fine settimana o nel periodo natalizio.

Nei momenti di punta, la gestione delle emergenze risulta molto più complessa in quanto, nella maggioranza dei centri commerciali, le zone di passaggio sono state progressivamente ridotte, per ospitare aree di ristoro ed attività promozionali di ogni genere. La presenza di display, stand, tavoli e sedie posizionati nelle aree di transito per accogliere il maggior numero di clienti rendono più difficoltoso il raggiungimento delle vie di uscita di caso di evacuazione, che non sempre sono rese facilmente individuabili dall'illuminazione e dalla segnaletica d'emergenza.

Se i clienti che transitano nel centro commerciale sono la componente più preziosa da salvaguardare, queste anomalie devono essere assolutamente evitate.

L'unica risposta è un approccio coordinato, con l'individuazione di figure competenti in grado di "far parlare" tra di loro i diversi soggetti e tecnologie che concorrono alla sicurezza di un centro commerciale, sulla base di procedure condivise.

Premio H d'oro 2017
Categoria BENI CULTURALI MUSEALI

a cura della Redazione

Categoria: **BENI CULTURALI MUSEALI**

Azienda installatrice: **Dome Security Technologies Srl**

Denominazione e località dell'impianto: **Fondazione Palazzo Grassi - Punta della Dogana - Venezia**

Impianto realizzato: *Sistema di monitoraggio di due opere d'arte (sculture poste in esterno) attraverso un impianto di videosorveglianza IP con encoder di video-analisi e sistema di sensori sismici*

Lo scorso 27 novembre al Museo Egizio di Torino si è svolta la premiazione dei vincitori e dei finalisti della dodicesima edizione del Premio H d'oro, il concorso organizzato dalla **Fondazione Enzo Hruby** per premiare le migliori realizzazioni di sicurezza e con esse la professionalità dei più qualificati operatori del settore. Nella categoria Beni Culturali Museali ha vinto il Premio H d'oro 2017 la società **Dome Security Technologies** di Udine con un progetto di videosorveglianza, video analisi e antintrusione a protezione di due opere d'arte poste all'esterno della Fondazione Palazzo Grassi – Punta della Dogana a Venezia.

Descrizione dell'impianto

L'impianto di protezione delle opere d'arte è formato da due sistemi distinti consistenti in:

- un sistema di videosorveglianza su rete IP abbinato ad un encoder video per video-analisi.

Le telecamere scelte garantiscono un'elevata qualità delle immagini grazie all'alta risoluzione e consentono di adattare l'inquadratura della scena tramite software, senza la necessità di manovrare direttamente a bordo telecamera. Permettono quindi non solo un'analisi video accurata e precisa dell'area allarmata, ma anche il monitoraggio ambientale del contesto di installazione, garantendo immagini ricchissime di dettagli.

- un sistema di rilevazione delle vibrazioni mediante sensori sismici posizionati all'interno del basamento delle sculture, pertanto non visibili dall'esterno.

I sensori rilevano le vibrazioni meccaniche provenienti da tentativi di scavalcamento, taglio recinzioni oppure dal calpestamento dell'area protetta. Sono cablati e collegati con apposito cavo; l'unità di controllo consente la taratura e regolazione dei sensori per meglio adattare il sistema alle condizioni ambientali nelle quali deve operare.

Entrambi i sistemi sono interfacciati e gestiti da una centrale antintrusione a 50 zone.

Per la segnalazione acustica degli allarmi sono state installate **due sirene con scheda di sintesi vocale a bordo e con messaggio personalizzato.**

Tipologia dei materiali utilizzati

Telecamere IP 4 megapixel ottica varifocale 2,8-12mm - Illuminatore IR portata 30 mt. - Encoder Video da 4 canali per video analisi - Illuminatori ad infrarosso con portata fino a 50mt e apertura O/V di 60° - Illuminatori ad infrarosso con portata fino a 20mt e apertura O/V di 50° - Centrale antintrusione con 10 terminali a bordo ed espandibile fino a 50 terminali - Espansioni 5 terminali configurabili come ingressi o uscite - Tastiera di gestione con monitor LCD - Stazioni di alimentazione supplementare con alimentatore da 3A - Sirene da esterno autoalimentate con batteria tampone e scheda di sintesi vocale incorporata - Centrali di gestione dei sensori sismici - Sensori sismici.

Grado di difficoltà, problemi e soluzioni

Difficoltà medio-alta.

Principali problemi affrontati e soluzioni

- Presenza di costante afflusso di turisti attorno a opere prive di una protezione fisica perimetrale permanente

La soluzione prospettata è stata la creazione di un sistema di protezione basato sull'interfacciamento di due diverse tipologie di rilevazione.

In particolare, il sistema di video analisi è stato studiato per entrare in funzione per un'opera H24 e per l'altra con modalità diversa tra giorno e notte. Durante il giorno il sistema attiva il messaggio vocale qualora le persone si avvicinino al basamento e/o lo tocchino. Mentre è stata pensata un'area virtuale intorno ai basamenti stessi, entrando nella quale durante le ore notturne, il sistema entra in funzione. In questo modo è stata garantita la sicurezza dell'area destinata ad ospitare le statue.

In entrambi i casi la video analisi mette in funzione la sirena con scheda di sintesi vocale e messaggio personalizzato: "Attenzione, area videosorvegliata. Si prega di non toccare la scultura. - Area under video surveillance. Please do not touch the artworks."

- Condizioni del contesto ambientale critiche e gestione dei falsi allarmi

La presenza dei canali circostanti in cui transitano natanti (vaporetti) che generano onde e urti di natura sismica ai basamenti delle statue ha evidenziato la problematica della frequente generazione di falsi allarmi e/o allarmi impropri provenienti dai sensori.

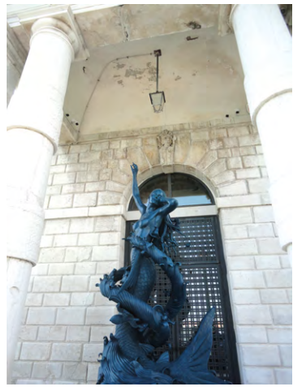
La soluzione da noi prospettata è stata quella di procedere ad una taratura il più precisa possibile e coerente con le peculiarità del sito, in modo da contrastare le condizioni ambientali sfavorevoli. Anche questo aspetto è stato risolto grazie al sistema di video analisi interfacciato con i sensori sismici integrati nelle basi.

Caratteristiche particolari dell'opera

Integrazione di due sistemi di rilevazione differenti, al fine di garantire il maggior livello di monitoraggio e protezione di sculture poste all'aperto e senza alcun tipo di protezione o eliminazione perimetrale.

Staff e tempo impiegati per la realizzazione

Direzione Tecnica e Commerciale per progettazione e pianificazione lavori, più due tecnici specializzati per un mese di lavoro.



Novità nella gamma PARADOX: il modulo di espansione ZX82

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

La gamma **PARADOX** distribuita da **DIAS** offre le soluzioni più complete per la sicurezza antintrusione, in grado di coniugare le più alte prestazioni con una particolare attenzione al design. Una linea in continua evoluzione che spesso si arricchisce di nuovi prodotti dalle caratteristiche sempre più avanzate.

E' il caso del nuovo modulo di espansione a 8 zone ZX82, che fornisce fino a otto ingressi di zona cablati aggiuntivi e l'interruttore antimanomissione a bordo.

Il modulo ZX82 fornisce indicazioni visive per le zone, collegato alla linea seriale delle centrali; è dotato di una scatola ABS semplice da installare, con un meccanismo di blocco integrato che protegge da manomissioni.

Compatibile con le centrali **SPECTRA SP, MG5000/MG5050 e DIGIPLEX EVO di PARADOX, è conforme EN50131** Grado 3.

CARATTERISTICHE:
• Contatto antimanomissione
• Conforme EN50131 Grado 3
• Firmware aggiornabile

Rivelatori perimetrali BXS Shield di OPTEX

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

HESA presenta i rivelatori perimetrali da esterno serie **BXS Shield** di **OPTEX**, disponibili sia in versione cablata sia in versione senza fili nei colori bianco e nero o interamente bianco.

Il design incontra le più elevate prestazioni in un sensore che ha una doppia rilevazione laterale fino a 12+12m con antimascheramento. BXS Shield è altamente affidabile grazie alla funzione logica AND che riduce i falsi allarmi e all'area di rilevazione individuale che permette al lato destro e a quello sinistro del sensore di avere un'uscita indipendente, oltre alla possibilità di essere regolata singolarmente. La facilità di installazione e l'alta affidabilità completano le prestazioni di questo rivelatore che dispone di grado di protezione IP55 e di una custodia resistente ai raggi UV.

PRESTAZIONI
- Portata m 24 (12 su ciascun lato) angolo 180° con fasci di rilevazione regolabili nella portata
- Logica SMDA per compensazione avanzata della temperatura e immunità ai disturbi ambientali
- Uscite individuali del segnale (destra e sinistra)
- Antimascheramento ad infrarossi attivi per rilevare il mascheramento con oggetti coprenti
- Protezione antistacco posteriore

Prime e la connettività nativa

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

Prime è nativamente connessa ad **Inim Cloud** e alle sue potenzialità ed è quindi la scelta migliore per tutte le installazioni che richiedono connettività IP ed in particolare connettività Cloud.

La connettività IP a bordo della scheda principale garantisce grande rapidità di risposta nell'uso dell'**App AlienMobile** e nell'uso dell'interfaccia web di Inim Cloud. Tempi di risposta estremamente rapidi per una esperienza d'uso davvero gratificante.

Tramite l'App AlienMobile, tramite l'interfaccia web del Cloud o tramite il web-server disponibile sulla scheda PrimeLAN, l'utente ha tutto sotto controllo. Inserimenti e disinserimenti, accensioni e spegnimenti, gestione dell'illuminazione, gestione degli scenari domotici, gestione dei cronotermostati ambientali e notifiche in tempo reale di tutto quanto accade.

Tramite l'**App InimTech Security** l'installatore può gestire gli impianti installati e connessi al Cloud, ricevere notifiche, contattare i clienti ed avviare il navigatore direttamente dal suo smartphone. Tutto in punta di dita sullo schermo touch del dispositivo mobile o del PC.

La piattaforma Prime, grazie alla scheda **PrimeLAN**, è in grado di gestire i protocolli KNX e ONVIF che consentono al sistema Prime di interagire con i più diffusi sistemi domotici e con ogni sistema di videosorveglianza IP che sia ONVIF compatibile. Prime è un sistema ibrido (cablato + via radio bidirezionale). La centrale nasce cablata ma la semplice aggiunta del ricetrasmettitore bidirezionale **BS200** la trasforma in una potente centrale via radio ai massimi livelli di prestazione ed affidabilità.

Beyond: il sensore intelligente da esterno di RISCO Group

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

Beyond è il sensore intelligente da esterno di **RISCO Group** rinnovato nella flessibilità di installazione e di portata. Infatti, Beyond può essere ora installato da 1,8 m a 2,7 m di altezza e regolato da un minimo di 5 m a un massimo di 12 m.

Grazie alla doppia tecnologia (DT) e combinando due canali a microonda in banda K e due canali PIR, Beyond garantisce prestazioni superiori riducendo i falsi allarmi, attraverso le esclusive e innovative tecnologie di rivelazione progettate da RISCO per l'ambiente esterno. In particolare, grazie alle due microonde, **Sway Recognition Technology (SRT)** riconosce e ignora gli oggetti che oscillano senza spostarsi, come rami e arbusti; **Digital Correlation Technology (DCT)**, invece, considera minacce solo quei soggetti che causano segnali simili e correlati in entrambi i canali PIR; mentre **Direct Sunlight Immunity** garantisce immunità alla luce solare, ignorando gli improvvisi sbalzi di intensità luminosa sulla base di un esclusivo algoritmo.

Beyond – disponibile oggi in versione cablata – è in grado di indirizzare le esigenze e soddisfare i requisiti di case private, siti industriali e remoti grazie alla capacità di effettuare una rilevazione degli intrusi affidabile in condizioni ambientali avverse con il minor numero di falsi allarmi. Inoltre, garantisce protezione 24 ore su 24 da atti di vandalismo e supporta l'ultima generazione di verifica visuale ad alta definizione, attivabile tramite l'app per smartphone **iRISCO**, web browser o vigilanza.

Contatti CLH-300/ 301

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

I nuovi contatti magnetici passivi firmati **TSec** offrono la sicurezza della tecnologia antimascheramento brevettata **Magnasphere** in un robusto involucro in tecnopolimero rinforzato con fibra di vetro.
I contatti **CLH-300** sono pensati e ideati per offrire la massima sicurezza garantendo una flessibilità di installazione senza uguali.
Il contatto è formato da una base universale, che contiene i componenti del sensore, e da una cover disponibile nei colori marrone, bianco e grigio.
Inoltre, per garantire il massimo della personalizzazione, con un ordine minimo di 100 pezzi è possibile richiedere altri colori RAL.
Grazie all' antimascheramento magnetico, non è possibile inibire l'apertura del contatto mediante influenzamento magnetico dall'esterno del perimetro protetto.
La versione **CLH-301** offre in aggiunta un microswitch anti-rimozione per garantire i massimi livelli di sicurezza.
I CLH-300 e 301 sono disponibili nelle versioni con morsetti o con cavo, questi ultimi con resinatura completa ed adatti per uso in esterno.
Il sistema modulare per il cablaggio consente di utilizzarli con uscita diretta del cavo, con la guaina armata inox e con qualunque altra guaina con diametro interno di 8mm.
I nuovi sensori permettono la fuoriuscita del cavo dal retro del sensore che lo rende completamente invisibile e non attaccabile.

Come tutta la serie H di TSec, i contatti magnetici CLH-300 e 301 sono interamente prodotti in Italia e garantiti 10 anni.

essecome ONLINE

n. 01 gennaio 2018
ISSN: 2384-9282
Anno XXXVIII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Maria Cupolo,
Giuseppe Mastromattei,
Eduardo Parisi.

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

EDITORE
Secman srl
Verona - Via Del Fabbro, 2
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

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

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

GRAFICA/IMPAGINAZIONE
contatto@lilastudio.it