essecome ONLINE 07/20

Periodico digitale di informazione di security & safety

2020 · ANNO XXXX

## NORMATIVA CPR: ELAN ACQUISISCE LA CLASSE CCA – S1A – D0, A1


Malgrado le difficoltà per tutto il settore industriale, sin dall'inizio dell'emergenza **ELAN**, azienda marchigiana di Camerano (AN) sta portando avanti l'attività nel rispetto dei decreti emanati dal Governo e delle norme di sicurezza per clienti, fornitori e dipendenti. L'azienda, riconosciuta come uno dei principali fornitori sul mercato internazionale per la produzione di cavi e batterie, è noto con i marchi **ELAN** (cavi) e **BIGBAT** (batterie) e viene scelta ormai da anni da una vasta schiera di installatori e distributori del settore della Sicurezza.

Sotto il marchio ELAN, l'azienda produce e distribuisce un vasto assortimento di cavi a bassa tensione. Nel portafoglio aziendale troviamo **cavi allarme in PVC e in LSZH, cavi antincendio** con il prodotto più conosciuto sul mercato, l'**Elanfire**, **cavi di rete** (UTP, FTP,...) e una vasta gamma di **cavi coassiali** e **cavi segnale**.

Già da alcuni mesi la Elan stava lavorando per aggiornare ed implementare alcune certificazioni in ambito CPR ed oggi è possibile comunicare importanti novità.

Come noto, da luglio 2017 tutti i cavi allarme e i cavi sicurezza immessi sul mercato devono rispondere alla normativa **EN 50575** che specifica *"i requisiti di prestazione alla reazione al fuoco, alle prove e i metodi di valutazione dei cavi elettrici utilizzati per l'alimentazione elettrica, il controllo e la comunicazione utilizzati nei lavori di costruzione soggetti a prescrizioni di resistenza all'incendio".*

L'obiettivo della CPR è quello di garantire la libera circolazione dei prodotti da costruzione all'interno dell'UE, adottando un linguaggio tecnico armonizzato che definisca le prestazioni e le caratteristiche dei prodotti. Naturalmente, fanno parte dei materiali da costruzione anche i cavi elettrici per energia, controllo e telecomunicazione di qualsiasi tensione e tipo di conduttore. In questo caso specifico, l'obiettivo è di limitare la generazione, la propagazione dell'incendio e l'emissione di fumo, valutando la loro reazione e il loro comportamento in caso di incendio.

Perché i cavi allarme, i cavi dati, e qualsiasi altro tipo di cavo siano rispondenti alla CPR, devono disporre di una D.O.P. *(Declaration of Performance)* redatta dal produttore. Per emettere la D.O.P. il produttore deve fare in modo che i prodotti rispondano ai requisiti per la marcatura CE. La D.O.P. dovrà accompagnare ogni cavo immesso sul mercato fino all'utilizzatore finale, il quale dovrà esibirla alle autorità competenti, qualora esse la richiedano.

Oltre che dalla D.O.P., i cavi conformi alla CPR possono essere riconosciuti dalla loro marcatura o etichettatura. Le informazioni necessarie da apporre sulla marcatura sono (EN 50575 art.7): *Nome del produttore o marchio di fabbrica - Descrizione del prodotto o codice - Classe di reazione al fuoco.*

E' compito del singolo Stato membro definire le classi nazionali di reazione al fuoco opportune, per le proprie tipologie di installazione. Le classi di reazione al fuoco devono essere scelte tra quelle definite dalla norma EN 13501-6. ELAN da dopo avere lavorato internamente sulle prove di resistenza al fuoco, ha ottenuto la **Classe Cca – S1a – d0, a1** per specifici cavi allarme LSZH schermati, cavi allarme LSZH twistati, cavi antincendio Elanfire e cavi Konnex.

**Per chi fosse interessato, sul sito Elan sono disponibili tutte le dichiarazioni di conformità e le classi per cui i cavi sono certificati.**



# Sommario Interattivo

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

# Vigilanza privata e Ministero dell'Interno, "vorrei ma non vorrei" la libertà


Non è necessaria un'esegesi troppo approfondita della comunicazione che proviene dal mondo della vigilanza privata per cogliere il senso di esasperazione e di frustrazione degli operatori per l'attuale pessima qualità delle relazioni con il Ministero dell'Interno, l'autorità alla quale il settore è assoggettato dal TULPS del 1931.
I suoi rappresentanti lamentano che il dialogo tra l'amministrazione e le parti sociali, che in passato aveva consentito di concertare positivamente i termini della riforma imposta dalla sentenza di Strasburgo del 2007, sia stato interrotto **(leggi)** in modo unilaterale dal Viminale proprio quando i suoi uffici periferici (prefetture e questure), le imprese (istituti di vigilanza) ed i lavoratori (guardie giurate) avevano maggior bisogno di direttive chiare e condivise per gestire una transizione tutt'altro che semplice dal vecchio al nuovo modello.
Alcuni pensano che l'interruzione sia stata provocata dai ricorrenti ricambi di funzionari delle PA che, talvolta, possono portare ai vertici degli uffici persone inesperte della materia di cui si devono occupare e, magari, poco propense al confronto; altri sostengono invece che al ministero ci sia stata una decisione consapevole di trasformare il dialogo, giudicato ormai inutile con soggetti che non possono più venire gestiti e controllati come prima, in un flusso di direttive calate dall'alto sugli aspetti ancora sottoposti a regime autorizzatorio.
Un osservatore esterno potrebbe domandarsi perché gli imprenditori non traggano lo spunto da questa situazione per richiedere formalmente una più ampia "laicizzazione" del settore per affrancarsi finalmente dal giogo degli **anacronismi del TULPS** ed alleggerire l'amministrazione, afflitta dai tagli degli organici e dall'endemico deficit digitale della PA, da un fardello di incombenze burocratiche che poco o nulla contribuiscono alle funzioni di controllo che competono all'Autorità di P.S.
Sempre guardando da fuori, si allineerebbe una volta per tutte il sistema italiano ai modelli internazionali che hanno consentito altrove lo sviluppo di "imprese di sicurezza" **(leggi)** del tutto incomparabili con i nostri bonsai di provincia, rimasti tali proprio a causa di quell'anomalo rapporto di "subalternità concessoria" nei confronti dello Stato.

In realtà, la sensazione è che gli operatori nostrani siano sempre più infastiditi dai lacci della burocrazia ma, in fondo, non vogliano perdere del tutto l'ombrello protettivo del regime autorizzatorio temendo la concorrenza delle imprese di sicurezza non regolamentate, avvezze a combattere sul mercato senza esclusione di colpi.
E sull'altro fronte non si può escludere che, mentre gli impiegati degli uffici territoriali di Polizia Amministrativa gioirebbero per il minor carico di lavoro, non tutti i dirigenti degli stessi uffici sarebbero felici di rinunciare al piccolo potere, dall'antico sapore borbonico, che possono ancora esercitare nei confronti dei titolari di autorizzazioni di PS.
Insomma, un "vorrei ma non vorrei" la libertà da entrambe le parti che, purtroppo, sta ritardando la realizzazione di un modello di partenariato autentico e compiuto tra pubblico e privato, che consenta di utilizzare proficuamente uomini, competenze e mezzi della vigilanza privata per la sicurezza del Sistema Paese.

# Vigilanza privata, dove sta l'anacronismo

*intervista a Marco Stratta, Segretario Generale di A.N.I.V.P.*

**Marco Stratta**, Segretario Generale di **ANIVP**, analizza la situazione della vigilanza privata nella "nuova normalità" tracciando un quadro molto preoccupante, al punto da lanciare un appello ai colleghi delle altre associazioni per un'azione congiunta più forte utile a migliorare la vita della categoria e salvaguardare l'occupazione.

**Cosa sta succedendo alla vigilanza privata in questo particolarissimo autunno 2020?**
Da buon piemontese, non è mia abitudine esternare comportamenti troppo evidenti o che possano creare disturbo agli altri. Mia nonna diceva: *"ma poi cosa pensa la gente?"* Forse abbiamo paura di venire giudicati e di dover gestire le conseguenze di un proprio agire. Esprimersi in Italia non è facile, per cultura e tradizione nessuno come l'italiano sa esaltare o stroncare una posizione. Roberto Saviano definiva quest'ultima attività come "la macchina del fango". E' per me dunque un grande sforzo rendere pubbliche alcune considerazioni su una domanda molto specifica ma anche importante, non solo per me: cosa è veramente superato nel settore della vigilanza privata?
Per cercare delle risposte costruttive alla domanda, è utile che faccia una premessa.
Esattamente dieci anni fa è uscito il DM 269/2010 che doveva riformare il settore aprendolo al mercato e trasformando gli *"istituti di vigilanza"* disegnati dal Titolo IV del Regio Decreto 18 giugno 1931 n. 773 (TULPS) in moderne *"imprese di sicurezza"* attraverso la rimozione di due cardini fondamentali dell'impianto normativo originario: i limiti territoriali e i tariffari, a cui si doveva affiancare la professionalizzazione degli operatori. La riforma è rimasta invece parzialmente incompiuta a causa della volontà dell'Amministrazione di mantenere il controllo sulle attività delle imprese e degli operatori, le guardie particolari giurate, impedendo che venisse rimosso anche il terzo cardine della *"totale dipendenza autorizzatoria"*. Un vincolo fortissimo, comprensibile alla luce del DM 154/2009 sulla sicurezza partecipata, ma che, nei fatti, impedisce alle aziende di rispondere in modo puntuale alle richieste del mercato, dovendo rispettare procedure *"pre-riforma"* e sottostare ai tempi operativi delle strutture territoriali preposte. Il problema diventa paradossale quando riguarda l'impossibilità di rispondere alle richieste proprio di servizi di sicurezza partecipata provenienti da gestori pubblici di obiettivi sensibili (porti, aeroporti, ecc).

**Cosa è quindi superato?**
Non credo proprio lo siano gli istituti di vigilanza, almeno la maggioranza. La posizione è ampiamente motivata.
In un settore dove le aziende medie non superano i 50 dipendenti, le imprese di vigilanza hanno fatto passi da gigante dalla sentenza della Corte Europea del 2007, quasi una mutazione genetica. Sono passate da strutture che sopperivano a gravi carenze manageriali, tecnologiche ed organizzative solo grazie ad un collante di impronta quasi militaresca, ad organizzazioni societarie mediamente di maggiori dimensioni, con un apporto tecnologico, manageriale ed organizzativo molto più elevato, evolvendo perfino la vision aziendale e affacciandosi in alcuni casi nel mondo della *"security system integration"* con sempre più frequenti partnership con player di settori complementari. Già solo la terminologia aiuta a capire l'evoluzione.
In questo scenario non considero poi superato il ruolo della guardia giurata, semmai è poco difeso. La riforma normativa del 2010 ha voluto riconoscere delle prerogative che erano corrette e sensate nell'ambito di un contesto pubblicistico che non poteva cedere troppo al privato ma necessitava, almeno come utente, di figure di riferimento comunque maggiormente qualificate. Oggi è lo stesso contesto pubblico a derogare agli obblighi sia per ignoranza delle leggi che per mera necessità di risparmio (gli Uffizi di Firenze sono solo un esempio). Di conseguenza, le aziende sopportano obblighi e impegni cogenti in materia di formazione e qualificazione del personale, senza poterli scontare adeguatamente sul mercato.

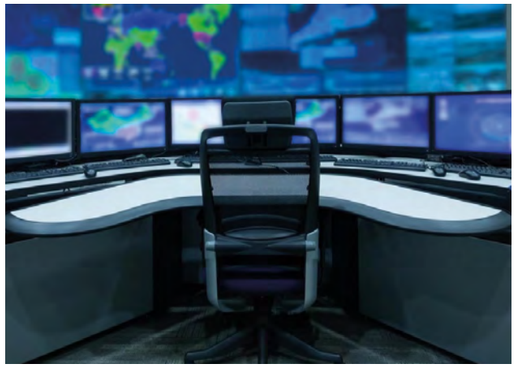
**Si parla da tempo dei problemi di dialogo con le autorità tutorie. Qual è la situazione ad oggi?**
Elencando le cose desuete per il nostro settore, si dovrebbe parlare delle autorità tutorie ma, sinceramente, ha poco senso. Le autorità semplicemente esistono e cercano di fare il loro dovere nell'alveo degli strumenti in dotazione. Semmai, gli operatori sono troppo spesso in balia della linea politica del momento o della sensibilità personali del funzionario-dirigente preposto.

**Come conciliate i ritmi imposti dal mercato con i tempi e i modi dello schema autorizzatorio originario?**
Questo è il punto nodale, la cosa veramente-assurdamente-drammaticamente "vecchia": le procedure che regolano la vita quotidiana del settore, ovvero le dinamiche autorizzatorie. Alcuni esempi per capirci meglio:

**1.** Come può un settore totalmente esposto alle regole del mercato, assolutamente immerso nel contesto privatistico, poter competere decorosamente se impiega mediamente 3 mesi per autorizzare un operatore come "guardia particolare giurata"?

**2.** Perché dobbiamo mandare i documenti per il rinnovo dei titoli mediamente 60-90 giorni prima della scadenza, e talvolta non basta nemmeno questo termine?

**3.** Perché alla fine del lock-down tutti i settori produttivi non vedevano l'ora di ripartire mentre la vigilanza privata non poteva invece assumere nuovo personale in quanto le sedi del Tiro a Segno Nazionale restavano chiuse? Hanno riaperto solo in ordine sparso e molti non rilasciavano gli attestati,



con una situazione che ha cominciato a normalizzarsi solo dopo ferragosto

**4.** Perché se una impresa che decide di fare una operazione societaria, che magari salvaguarda parte dell'occupazione da un fallimento, deve impazzire tra mille differenti procedure-valutazioni-interpretazioni delle svariate Prefetture e Questure? E' forse troppo pretendere una linea di condotta univoca che non porti l'imprenditore a rischiare sanzioni, sospensioni, incameramenti di cauzioni?

Ecco cosa nel nostro settore è veramente "vecchio", "anacronistico", "superato". E non credo che questi problemi siano il prezzo da pagare per garantire il controllo e la tutela del sistema, penso piuttosto sia solo un problema organizzativo da superare al più presto.

**In che modo?**
Mi rivolgo ai colleghi delle altre associazioni che conoscono perfettamente i problemi descritti, e chiedo:
vogliamo fare qualcosa assieme, per cercare di dare una vita più decorosa a queste aziende che, che portano ancora il titolo di "istituti" di vigilanza?
Francamente, non credo che ci siano altri problemi più importanti da affrontare prima di questo.
Abbiamo la capacità, le competenze e le conoscenze per fare, e fare bene.

# Le linee guida della Norma CEI EN 62676-4: come progettare un impianto di videosorveglianza

*di Angelo Carpani - Libero professionista, laureato in Ingegneria elettronica presso il Politecnico di Milano, iscritto all'Ordine degli Ingegneri della Provincia di Como (n.2368 sez.A), esperto nella progettazione di impianti di videosorveglianza in ambito comunale.*

**Introduzione**

Le norme tecniche di riferimento per gli impianti di videosorveglianza appartengono alla serie **CEI EN 62676**, le quali affrontano otto temi di standardizzazione, dai requisiti generali di sistema fino ai protocolli e metodi di misurazione delle performance delle telecamere.

Affrontiamo questo argomento in quanto è fondamentale avere la disponibilità di un riferimento tecnico: il rispetto delle prescrizioni in esso contenute costituisce presunzione di regola dell'arte.

La Norma **CEI EN 62676-4**[1], in particolare, fornisce i requisiti e le raccomandazioni per la scelta, la *progettazione*, l'*installazione*, la *messa in servizio* e la *manutenzione* dei sistemi di videosorveglianza per applicazioni di sicurezza.

In queste poche righe non si ha certo la pretesa di illustrare tutti i contenuti della Norma; vorrei quindi soffermarmi su alcuni aspetti tecnici particolari da tenere in considerazione nella progettazione di un impianto di videosorveglianza.

In premessa è utile richiamare gli *scopi funzionali* di una telecamera che sono definiti nella Norma:

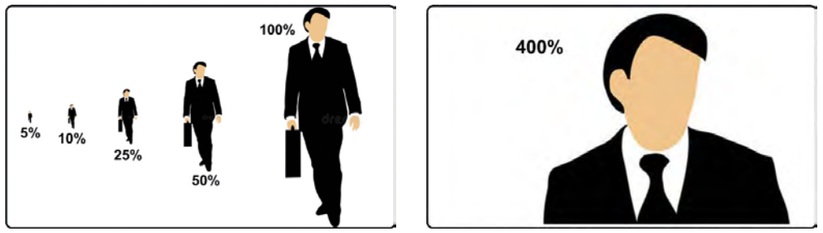
- **Verifica:** la telecamera deve consentire all'operatore di ottenere informazioni dagli oggetti (un esempio di oggetto può includere un testo o un logo su un indumento).
- **Identificazione:** la telecamera deve consentire l'identificazione di un individuo oltre ogni ragionevole dubbio.
- **Riconoscimento:** la telecamera deve consentire all'operatore di ottenere il riconoscimento di un individuo.
- **Osservazione:** la telecamera deve consentire la visualizzazione di dettagli caratterizzanti un individuo, quali un particolare abbigliamento, permettendo al contempo la visione delle attività che si svolgono intorno a un incidente.
- **Rilevamento:** la telecamera deve consentire all'operatore di determinare con affidabilità e semplicità se un obiettivo, quale ad esempio una persona, sia presente.
- **Monitoraggio:** la telecamera deve consentire la visualizzazione di un numero, la direzione e la velocità di movimento di individui in un'ampia area, affinché la loro presenza sia nota all'operatore.

La norma definisce anche la dimensione con cui deve essere ad es. inquadrata una persona (bersaglio) in termini di altezza in percentuale (%) rispetto all'altezza dello schermo per ottenere i diversi scopi funzionali.

[1] *Questa Norma supera la Norma CEI EN 50132-7.*



L'altezza percentuale con cui deve essere inquadrata una persona (bersaglio), rispetto all'altezza percentuale dello schermo dipende ovviamente dalla risoluzione della telecamera:




| Scopo funzionale della telecamera | Risoluzione Full HD (1080p ~ 2 Megapixel) | Risoluzione HD (720p ~ 1 Megapixel) |
|---|---|---|
| **Verifica** | 150% | 250% |
| **Identificazione** | 40% | 60% |
| **Riconoscimento** | 20% | 30% |
| **Osservazione** | 10% | 15% |
| **Rilevamento** | 10% | 10% |
| **Monitoraggio** | 5% | 5% |

**Tutti vogliono le Ferrari, ma poi si accorgono di non avere le strade per viaggiare a 300Km/h.**

Negli impianti di videosorveglianza è sempre più frequente la richiesta e l'impiego di telecamere ad altissima risoluzione come ad esempio le **Ultra HD – 4K (~ 8 Megapixel)**.

Mi capita spesso, nella mia attività professionale in cui seguo quasi esclusivamente Enti Locali (Comuni), di progettare impianti di videosorveglianza per finalità di ordine pubblico e, quindi, essendo di competenza delle Questure e delle Forze dell'Ordine, di dovermi attenere alla ormai "famosa" **Circolare del Ministero dell'Interno N.558/ SICPART/421.2/270 del 2 marzo 2012**, avente per oggetto i sistemi di videosorveglianza in ambito comunale. Nel *Documento Tecnico* allegato, vengono descritte le caratteristiche tecniche delle *telecamere di contesto* (fisse), per le quali viene richiesta una risoluzione minima del sensore Full HD (1920x1080p), e delle *telecamere di osservazione* (brandeggiate), per le quali viene richiesta una matrice attiva del sensore con un numero di pixel non inferiore a 4CIF (704x576p). Se la gara d'appalto viene aggiudicata con il criterio dell'offerta economicamente più vantaggiosa, anziché con il criterio del prezzo più basso, le ditte partecipanti hanno buon gioco ad offrire, pur di aggiudicarsi la gara, quale miglioria tecnica, telecamere con risoluzione più alta, come ad es. le telecamere 4K; salvo poi dimenticarsi di dimensionare conseguentemente la rete di comunicazione, allo scopo di garantire la trasmissione dei flussi video alla massima risoluzione e al massimo frame rate (fps - fotogrammi per secondo) consentito dalle telecamere stesse, e di dimensionare lo storage server allo scopo di mantenere la conservazione delle immagini per i famosi 7 giorni dettati dal Garante della Privacy.

Ad oggi non mi è ancora capitato di collaudare un impianto di videosorveglianza in cui le telecamere 4K erano configurate come tali: tutte erano configurate ad una risoluzione nettamente inferiore (mediamente Full HD ~2 Megapixel) e ad un frame rate pari nettamente più basso dei 25fps (mediamente 6fps) e la giustificazione che viene addotta è sempre la stessa: non c'è banda! In qualche caso, non avendo dimensionato adeguatamente lo storage server, il periodo di conservazione delle immagini veniva fortemente ridotto a 2/3 giorni, anziché i classici 7 giorni consentiti dalla normativa sulla privacy.

In qualche caso ho riscontrato delle incongruenze del tipo: erano state installate telecamere 4K quando in Centrale Operativa erano ancora presenti monitor con risoluzione Full HD. É evidente che, come dice la Norma CEI EN 62676-4, *“se la risoluzione della telecamera non è uguale a quella del dispositivo di visualizzazione, la scena rappresentata potrebbe non mostrare la quantità dei dettagli prevista”.*
Si consideri poi che le telecamere 4K, proprio per la “pesantezza” degli *streaming video* che devono trasmettere, impiegano un algoritmo di compressione video noto come H.265. Ebbene, il problema è che diverse piattaforme software VMS (Video Management System) ancora oggi non supportano la compressione video H.265 e sono ancora ferme a H.264.
Da ultimo, occorre anche tenere in considerazione le capacità computazionali che devono avere i sistemi di gestione e di registrazione delle immagini che devono essere molto elevate. I server quindi, non solo devono avere una adeguata capacità di storage per l’archiviazione delle immagini, ma devono essere anche dotati di processori *CPU multi core* con prestazioni elevate, in grado di elaborare immagini ad altissima risoluzione.
Da qui la metafora provocatoria: a cosa serve acquistare le Ferrari, se poi non si costruiscono le strade per viaggiare a 300Km/h?
Va bene impiegare le telecamere 4K (cioè le Ferrari), ma poi bisogna pensare alle strade per farle viaggiare a 300Km/h (cioè dimensionare in modo adeguato la rete di comunicazione, che sia wireless o in fibra ottica) ed a sfruttarne tutte le potenzialità (adottando un SW in grado di supportare lo standard di compressione video H.265 e un HW con server aventi una capacità computazionale adeguata e storage di archiviazione in grado di conservare le immagini 7 giorni) stando attenti a non mettere dei limiti di velocità (monitor di visualizzazione con una risoluzione inferiore a quella delle telecamere).
Il problema è che vengono realizzati progetti e vengono aggiudicate gare d’appalto senza prestare la dovuta attenzione agli aspetti di cui sopra. Le stazioni appaltanti a volte si fregiano di avere installato telecamere 4K salvo poi accorgersi, in fase di collaudo, che sono configurate come delle normalissime Full HD e ad un frame rate basso.

**Ma veniamo alla domanda: è sempre necessario l’impiego di telecamere ad altissima risoluzione configurate al massimo frame rate?**
La norma ci dice che dipende dai livelli di rischio delle aree/obiettivi che si vogliono controllare.
Nell’*Allegato D* della Norma CEI EN 62676-4 viene riportata una tabella molto interessante che contiene esempi di tali elementi basilari con qualità dell’immagine e frequenza dei fotogrammi minimi in funzione del livello di rischio percepito. Riportiamo di seguito uno stralcio della tabella:

| Località | Attività | Qualità dell’immagine in funzione del livello di rischio | | |
|---|---|---|---|---|
| | | Alta | Media | Bassa |
| Parcheggio | Furto, aggressione | Osservazione + PTZ – 6fps | Rilevamento + PTZ – 6fps | Osservazione – 6fps |
| Rastrelliere per biciclette | Furti, vandalismo | Riconoscimento – 6fps | Osservazione – 6fps | Osservazione – 6fps |
| Sportelli automatici | Furto, aggressione, frode | Identificazione – 12,5fps | Identificazione – 6fps | Identificazione – 6fps |
| Perimetro | Attività | Rilevamento – 2fps | Rilevamento – 2fps | (*) Rilevamento – 6fps |
| Magazzino | Furto | Riconoscimento – 12,5fps | Osservazione – 6fps | (*) Osservazione – 6fps |

*(*) è accettabile una riduzione della frequenza predefinita dei fotogrammi se è presente un meccanismo di attivazione allarmi tale da causare l’aumento della frequenza dei fotogrammi se attivato.*



Dalle tabelle sopra richiamate si evince che se si vuole “riconoscere” l’autore di un furto di una bicicletta parcheggiata presso una rastrelliera, è sufficiente adottare una delle due tipologie di telecamere:

- telecamera Full HD (1080p ~ 2 Megapixel) posizionata in modo tale da riprendere l’autore del furto con un’altezza pari al 20% dello schermo e configurata con almeno 6fps:
- telecamera HD (720p ~ 1 Megapixel) posizionata in modo tale da riprendere l’autore del furto con un’altezza pari al 30% dello schermo e configurata con almeno 6fps.

Ci sarebbero molti altri aspetti interessanti della Norma sui quali soffermarsi, quali ad es. l’*installazione*, la *messa in servizio*, la *manutenzione*, ma ho voluto adesso concentrami su questi aspetti tecnici particolari in quanto la Norma offre dei criteri interessanti, oserei dire “originali”, che ci possono guidare nelle scelte progettuali.
Il problema di fondo, come dice la Norma, rimane però sempre uno: *“la mancanza di un’idea chiara da parte di proprietari e/o installatori sullo scopo di ogni telecamera e sul livello di dettaglio necessario per conseguire tale scopo. Le telecamere che tentano di svolgere troppe funzioni o sono prive di uno scopo chiaro costituiscono uno spreco di risorse poiché difficilmente producono immagini utilizzabili”.*

# Il processo di integrazione tra installazione della sicurezza e building automation

*di Maurizio Callegari, consulente e formatore*

L'Italia ha una grande domanda potenziale di building automation, sia per il mondo industriale che, non da meno, per quello residenziale.
La tecnologia ha oggi raggiunto dei livelli veramente ragguardevoli, almeno per alcuni produttori, però rimane confinata a relativamente pochi utilizzatori e la sua conoscenza si diffonde piuttosto lentamente.
Questa è la situazione in cui si vengono a trovare numerosi installatori di sicurezza quando, sempre più spesso, viene loro chiesto di integrare il sistema di sicurezza con un'automazione più ampia che riguardi tutto l'edificio, soprattutto per ottenere miglior comfort e maggior risparmio energetico.
La building automation è quindi un settore dove la domanda sembra precedere e trainare l'offerta, perché gli utenti sembrano essere spesso più sensibili dei costruttori e degli integratori a questi temi.

***"Il settore della building automation si trova quindi sottoposto a spinte contrapposte, dove la domanda tende a svilupparlo, mentre l'offerta tende spesso a rallentarlo"***

Il settore della building automation si trova quindi sottoposto a spinte contrapposte, dove la domanda tende a svilupparlo, mentre l'offerta tende spesso a rallentarlo. Ma quali sono i nodi che attanagliano l'offerta?

**1. Nodi istituzionali**

a) Non esiste un Albo di installatori che ne certifichi la preparazione.
b) Non esiste un processo di qualifica che li porti a differenziarsi da altri operatori improvvisati.
c) Non esiste un processo di qualifica dei sistemi: nella sicurezza, i precedenti "livelli IMQ" sono oggi trasformati in gradi (1,2,3 o 4) dalle norme EN. Nella building automation questo manca, per cui spesso prodotti costruiti nelle famose "cantine italiche" con processori e logiche ultradatate, sono paragonati e parificati, agli occhi degli utenti ad altri prodotti modernissimi ed iperperformanti, costruiti magari sempre in Italia, nelle numerose Silicon Valley nazionali.

**2. Nodi di conoscenza tecnica.**

In particolare si osservano:
a) Carenze conoscitive da parte degli installatori, che si legano a sistemi a loro familiari e difficilmente si spostano o aprono l'orizzonte ad altri sistemi.
b) Carenze conoscitive da parte dei progettisti che, al pari degli installatori, si legano alle tecnologie che conoscono e tendono ad utilizzarle ad ampio spettro, a volte anche in maniera impropria ed inefficiente. Solo in rari casi e per grandi sistemi vengono fatte gare aperte e pubbliche con la comparazione di più soluzioni, mentre spesso scatta invece il binomio tecnologia/operatore, rendendo così l'offerta ancora più rigida, più ingessata e meno trasparente e competitiva.

**3. Nodi di comunicazione**

A fronte dell'enorme potenzialità di questi sistemi, la comunicazione sui loro vantaggi è assolutamente troppo scarsa. Comunicano poco:
a) I costruttori, rivolti soprattutto a sensibilizzare la filiera, ma con effetto limitato sui progettisti e quasi inesistente sui clienti finali.
b) Comunicano poco anche gli integratori, che hanno spesso potenzialità e capacità enormi ma, tuttavia, espongono e mettono in luce molto timidamente, sotto l'incalzare delle richieste degli utenti finali, che si trovano spesso, come detto, a richiedere soluzioni al mondo tecnico per avere risposte alle loro necessità.
c) Comunicano infine poco anche i progettisti, spesso anche comprensibilmente travolti dalla rapidità dell'evoluzione tecnologica, che li costringe ad aggiornamenti costanti e li vede a volte dover rincorrere le soluzioni per affrontare una domanda sempre più esigente, articolata ed evoluta.

**4. Nodi commerciali e propositivi**

Questo mondo altamente tecnologico è sostanzialmente attanagliato dal principio che il prodotto è il centro di tutto, scordandosi troppo spesso che esso necessita di essere venduto con un'opportuna azione commerciale, tanto vituperata e denigrata quanto indispensabile, per coniugare le necessità dei clienti con le potenzialità delle soluzioni.
Si rileva quindi una carenza abissale nelle capacità di vendita degli integratori così come dei costruttori, tutti volti ad agire all'interno della filiera ma pochissimo a dialogare con i clienti finali, che sono così in balia di confusione, poca trasparenza ed operatori scaltri e scorretti.

***"La soluzione: è necessario aumentare nettamente il livello di preparazione degli operatori"***

La soluzione: è necessario aumentare nettamente il livello di preparazione degli operatori, soprattutto con:

**1. Formazione tecnica ulteriore:**

a) per aumentare le competenze realmente di tutta la filiera,
b) per saper scegliere di volta in volta le soluzioni migliori,
c) per poter offrire proprio le soluzioni più efficienti per soddisfare tutti i bisogni dei clienti.

**2. Formazione commerciale:**

a) Per imparare ad approcciare correttamente i clienti
b) Per imparare ad evidenziare efficacemente i vantaggi delle proprie soluzioni
c) Per imparare a differenziarsi da operatori meno capaci e performanti, ma spesso più scaltri
d) Per imparare a condurre con efficacia le trattative sino al successo finale.

Solo in questo modo il settore della building automation potrà diventare realmente maturo, in grado di conseguire quei traguardi di crescita che potenzialmente gli spettano e contribuire quindi al miglioramento del benessere sociale complessivo che le sue soluzioni sono senz'altro in grado di offrire molto efficacemente e largamente.

# Quanto e come l'emergenza sanitaria ha modificato l'approccio alla difesa della filiera agroalimentare?

*a cura della Redazione*

Tra gli effetti collaterali della pandemia Covid-19, si sono delineate a livello globale nuove minacce per la filiera agroalimentare che vanno a sommarsi a quelle preesistenti, innalzando il livello di allerta degli stake-holders.
Aumenta di conseguenza l'importanza e la consapevolezza del ruolo della **Food Defence**, la disciplina che comprende norme, competenze, tecnologie e servizi preposti alla tutela complessiva del cibo.
**essecome** apre una sezione tematica permanente dedicata alla Food Defence per approfondire e divulgare gli argomenti relativi ad uno dei più rilevanti mercati verticali per l'industria della sicurezza, iniziando con un'intervista a **Francesco Rana**, corporate security manager di un primario gruppo agroalimentare italiano.

**Tutela del cibo nella "nuova normalità": quali sono le principali minacce per la filiera agroalimentare percepite in questa fase, dalla produzione alla trasformazione fino al consumatore?**
In un clima decisamente critico, il settore agroalimentare ha tenuto il colpo. Anzi, come noto i consumi nell'ambito food & beverage sono stati tra i pochi ad aver segnato delle variazioni positive durante il lockdown ma anche dopo, confermandosi anticiclici rispetto alle altre filiere.
Ovviamente, questo trend positivo ha determinato l'aumento di esposizione al rischio di natura fraudolenta, inducendoci ad innalzare il livello, già elevato, di attenzione e sensibilità per quella che è denominata "Food Defence".
Le attività di mitigazione del rischio, concentrate sulle alterazioni indotte da manipolazioni non autorizzate delle derrate, sul tampering degli imballi e delle confezioni lungo tutta la filiera, si sono pienamente integrate con tutte le prescrizioni governative emanate per contrastare l'emergenza sanitaria.
Questa "nuova normalità" ha indotto una maggiore e più efficace comprensione dell'utilità di procedure e sistemi a protezione del processo produttivo.
Non trascuriamo comunque il fatto che, nella crisi sanitaria che stiamo vivendo, si insinua inevitabilmente ogni forma di frode. La frode alimentare trova terreno fertile poiché la crisi induce a concedere deroghe per garantire la continuità operativa.
In questo contesto c'è stato inevitabilmente un incremento di casi di frode segnalati.
D'obbligo, pertanto, è aggiornare le valutazioni dei rischi facendo attenzione a tali vulnerabilità collegate alla crisi acuta e di medio termine ormai profilata.

**Come si manifestano nel comparto gli attacchi cyber che stanno imperversando a livello goblale?**
La pandemia Covid 19 ha accelerato la trasformazione digitale in tutti i comparti industriali, incluso quello agroalimentare, tuttavia qualche ambito ha riscontrato difficoltà, peraltro scontare, ad inseguire questa trasformazione.
Forse perché il successo della trasformazione digitale sta non solo nell'adozione di tecnologie avanzate, ma anche nell'adattamento delle strutture organizzative: le iniziative digitali possono facilmente fallire se le strutture organizzative e i processi decisionali non si adattano al nuovo mandato.
Su questo terreno ancora incerto, la criminalità informatica si attiva con phishing multilivello, malware, attacchi informatici mirati proprio alle aziende agroalimentari che vedono il ritorno degli "hacktivisti", ossia gli attivisti della rete che usano le proprie competenze da hacker per mettere in atto forme di protesta o di disobbedienza civile.
Tutto ciò determina una ipersensibilità del comparto, in virtù della quasi completa automatizzazione dei processi e, soprattutto, dell'impegno continuo e costante alla qualità del prodotto nei confronti del consumatore finale.
Le aziende più lungimiranti, ipotizzando questi scenari di rischio, hanno implementato protezioni efficaci (ad esempio tramite la segmentazione delle reti), in modo da proteggere il business.
Non posso non fare un accenno allo smart working che in questo periodo ha visto un consistente aumento di utilizzo. Lavorare da casa per preservare la popolazione aziendale, continuando a garantire, per quanto possibile, l'operatività e la continuità dei servizi, è un cambio di rotta importante nelle modalità di intendere il lavoro.
Una nuova situazione che rientra nella trasformazione digitale che, se da una parte presenta effetti decisamente positivi, dall'altra comporta pericoli sulla sicurezza di aziende e individui in termini di cyber risk, in quanto hacker e criminali informatici sono ormai da mesi in agguato

approfittando della situazione emergenziale, per colpire tramite l'utilizzo di e-mail, siti web, telefonate e anche messaggi di testo, ed accedere a network privati e informazioni riservate.

**Ritiene che il quadro normativo sia in linea con la situazione attuale? Cosa si dovrebbe chiedere al legislatore nazionale e/o europeo?**
La domanda mi fa ritornare sull'argomento del riconoscimento alla filiera agroalimentare di Infrastruttura Critica, argomento affrontato in tempi non sospetti da autorevoli ricercatori alla luce della Direttiva Europea 2008/114/CE.
La Dir. 2008/114/CE all'Art. 2 punto a), definisce "Infrastruttura Critica" «*un elemento, un sistema o parte di questo ubicato negli Stati membri che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini ed il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni*»
La filiera agroalimentare per dimensione si attesta, in Italia, al secondo posto dopo il comparto metalmeccanico e si pone a livello europeo in 3° posizione per fatturato dopo Francia e Germania; dati importanti a cui si aggiunge il ruolo nevralgico che la stessa ha avuto e continua ad avere durante questa crisi sanitaria.
Con le sue tipicità, è un'infrastruttura che va protetta e difesa da attacchi intenzionali e da disastri naturali.
Sempre la stessa direttiva 2008/114/CE all'Art. 2, lettera b) definisce "Infrastruttura Critica Europea" «*un'infrastruttura critica ubicata negli Stati membri il cui danneggiamento o la*

*cui distruzione avrebbe un significativo impatto su almeno due Stati membri. La rilevanza dell'impatto è valutata in termini intersettoriali».*

La responsabilità della protezione delle infrastrutture critiche nazionali viene quindi demandata ai loro proprietari e agli Stati membri, considerando critiche solamente il comparto energia ed i trasporti ed escludendo evidentemente la filiera agroalimentare.

L'Italia nel 2011 ha recepito la Direttiva Europea con il Dlgs dell'11 Aprile n. 61 nelle quali designa, come infrastrutture critiche, solamente quelle indicate dalla Dir. 2008/114/CE.

L'auspicio è che, in virtù della strategicità che il settore riveste, oggi più che mai, dato che il paese sta attraversando un periodo storico critico ed in considerazione delle vulnerabilità connesse al settore stesso, l'esigenza di considerare il settore agroalimentare una infrastruttura critica è diventata una priorità.

**Le soluzioni oggi disponibili per mettere in sicurezza il cibo rispetto ai diversi rischi (sanitari, predatori ecc,) rispondono alle esigenze attuali? Dal vostro punto di vista cosa sarebbe necessario?**

Anche se il mondo del cyber crime ha catturato in maniera preponderante la nostra attenzione, non foss'altro perché il nemico attacca in maniera subdola, a volte per caso, scatenando i suoi effetti dirompenti spesso a distanza di tempo, nell'ambito della food defense abbiamo la necessità di proteggere l'infrastruttura alimentare anche e soprattutto fisicamente.

Il mercato offre una vasta gamma di soluzioni tecnologiche decisamente in linea con le esigenze del settore.

Nell'ottica della protezione concentrica degli obiettivi

sensibili è opportuno partire dalla protezione perimetrale con sistemi di video sorveglianza evoluti (telecamere termiche/video analisi) e sistemi antintrusione.

Anche il controllo accessi mediante l'utilizzo di teste di lettura dei classici badge o anche di apposite app scaricate sugli smartphone, riveste una fondamentale importanza.

Nelle fasi topiche della pandemia le autorità di controllo hanno valutato positivamente l'utilizzo di tali tecnologie a protezione delle infrastrutture e dei processi di lavorazione.

Resta inteso che la risorsa umana, debitamente formata, trova già ma, a mio avviso, dovrebbe trovare più spazio nel processo della security.

Ogni tipologia di strumento tecnologico deve consentire una difesa preventiva da ogni forma di attacco ma la gestione della situazione è in capo alla risorsa umana.

L'integrazione di sistemi, tecnologie e procedure non può prescindere dall'esistenza di un affidabile centro di controllo (Security Control Room) che può assolvere anche ad altre necessità come ad esempio. i controlli sull'automazione dei processi in fasce notturne.

# AXIS e la sicurezza delle Infrastrutture Critiche nella nuova normalità

*a cura della Redazione*

**AXIS Communications** ha organizzato il 27 ottobre la tavola rotonda digitale **“Sicurezza delle Infrastrutture Critiche, cosa cambia nella nuova normalità”** con la partecipazione di Corradino Corradi (AIPSA), Gabriele Faggioli (CLUSIT), Corrado Giustozzi (AGID) e Andrea Monteleone (AXIS Communications).

Nell’intervista che segue, **Andrea Monteleone**, National Sales Manager per l’Italia di AXIS Communications, riassume i contenuti della tavola rotonda e spiega la vision di AXIS.

**La sicurezza delle Infrastrutture Critiche nella nuova normalità: facendo una sintesi dei contenuti della tavola rotonda del 27 ottobre, quali sono i contenuti da appuntare?**

Nel corso del dibattito, partendo dal preoccupante trend di crescita dei cyber attacchi, sono emersi spunti molto interessanti relativi a nuove minacce ed esigenze di difesa, grazie alla competenza e all’esperienza dei partecipanti che rappresentavano tutti gli stakeholder della filiera coinvolti, ad oggi, dal punto di vista normativo: regolatore, vendor, system integrator e cliente finale.

Il primo semestre 2020 ha visto, infatti, un’escalation globale dovuta soprattutto al contesto pandemico nel quale attività come didattica a distanza e lavoro da remoto hanno reso ancora più vulnerabili e attaccabili aziende e istituzioni pubbliche. Preoccupano, in particolar modo gli attacchi diretti a realtà del comparto Difesa.

L’attuazione della Direttiva NIS e dell’italiano Perimetro di Sicurezza Cibernetica, attraverso una serie di decreti ministeriali, mirerà a offrire un organico e ambizioso quadro a tutela degli operatori di servizi essenziali: definizione che amplia il tradizionale concetto di “infrastrutture critiche” includendovi settori quali banche, sanità e molti altri, a conferma della mutata consapevolezza del legislatore sul tema. La normativa sconta, purtroppo, tempi inevitabilmente più lenti rispetto alla reale evoluzione delle minacce oltre a un’implementazione delle norme a due velocità tra livello europeo e locale.

Emerge quindi, dalla discussione, la necessità di acquisire, o immettere sul mercato a seconda dell’interlocutore, prodotti, soluzioni e sistemi facilmente adattabili e scalabili, per poter far fronte all’evoluzione delle minacce e garantire sempre un alto livello di sicurezza fisica e logica.

Un altro elemento interessante emerso durante il confronto, per certi versi ancora più critico, è che in Italia la maggior parte del tessuto imprenditoriale è costituito da PMI nelle quali le infrastrutture aziendali sono gestite, quasi sempre, da terze parti. In questo contesto, la consapevolezza del rischio è poca e la gestione della sicurezza viene percepita spesso come un costo. Per questo motivo, anziché investire oculatamente, le problematiche vengono risolte in modo approssimativo senza comprendere a fonde le possibili conseguenze. La conclusione, condivisa, è che accertarsi di poter mantenere i propri sistemi costantemente aggiornati, principalmente dal punto di vista delle patch software e firmware, sia uno, se non il primo, degli elementi da tenere in considerazione.

Il punto d’arrivo su cui tutti i relatori concordano, in vista anche di una rinnovata normalità, è l’urgenza di una massiccia alfabetizzazione digitale dei cittadini e di una sempre più forte attenzione, anche a livello mediatico, verso l’incentivazione delle nuove generazioni a scegliere


percorsi formativi e di carriera indirizzati al mondo della cybersecurity, senza dimenticare che gli utenti di oggi sono quelli da rendere immediatamente più edotti.

**Qual è la visione di AXIS in proposito e quali supporti offrite al sistema?**

La necessità da parte delle aziende di investire in campo security è sempre maggiore, la filiera della sicurezza dovrebbe infatti assumere un ruolo progressivamente sempre più importante.

Un vendor come Axis, che mette a disposizione la tecnologia e considerando che è responsabile in prima istanza della sicurezza, deve proporre al mercato soluzioni e prodotti che siano sicuri by design, in grado di poter dialogare secondo protocolli e modalità standard con tutti gli altri dispositivi, per poter installare quella soluzione ovunque e utilizzarla al massimo delle sue performance, senza inibire il funzionamento di tutto il resto.

L’hardware deve essere il primo baluardo di difesa per il cliente. L’impegno è di rendere le infrastrutture aziendali il più resilienti possibili. Si pone molta attenzione alla provenienza dei componenti, alla tecnologia utilizzata, alle modalità di rilascio e di aggiornamento del software e del firmware a bordo. Si parte da un assessment approfondito di tutta l’infrastruttura aziendale e, a valle di queste valutazioni, vengono poi definite le priorità e di conseguenza gli investimenti. Ma è qualcosa di difficilmente definibile perché tutto va valutato in funzione delle specifiche caratteristiche delle singole aziende.

Un vendor del settore sicurezza come Axis deve quindi dialogare con chi queste soluzioni le progetta, le installa e le gestisce e con chi le utilizza, in modo che tutti siano coinvolti e il feedback e le esigenze che arrivano dal mercato possano essere trasformati in tecnologia da utilizzare e installare. Allo stesso tempo ciò che siamo anche chiamati a fare è fornire al cliente finale ogni strumento possibile anche promuovendo l’educazione al buon uso delle tecnologie, condividendo best practices e informazioni per un utilizzo che sia sicuro - nel senso più ampio del termine - dei prodotti immessi sul mercato. La formazione, intesa come presa di consapevolezza di come si debba usare correttamente la tecnologia, è infatti frutto di un dialogo paritetico tra vendor, installatore, utente e ente di controllo.

Contatti:
Axis Communications
Tel. +39 02 8424 5762
www.axis.com

# L’integrazione tra sicurezza fisica e sicurezza ITC secondo Kaspersky

*intervista a Cesare D’Angelo, Head of Enterprise di Kaspersky*

**L’integrazione funzionale, tecnologica e organizzativa tra sicurezza fisica e sicurezza ITC è un’esigenza sempre più avvertita a causa dell’aumento a livello globale degli attacchi “combinati”. Quali sono le vostre valutazioni in merito?**

L’avvento di nuove tecnologie, come il 5G o l’IoT, sta cambiando radicalmente le connessioni e porterà ad una naturale espansione ed intensificazione delle cyber minacce correlate. Basta guardare alle nostre case oggi dove citofoni, lavatrici, sistemi di video sorveglianza, tutto è connesso alla rete e tutto è potenzialmente attaccabile. Secondo Gartner, entro il 2025 avremo circa 25 miliardi di connessioni IoT. Questo sicuramente incrementerà il livello di comfort delle nostre abitazioni e delle nostre città, aiutandoci a risolvere i problemi relativi alla disponibilità di risorse e consentendo alle organizzazioni di misurare le performance di produzione, introdurre l’automazione e aumentare l’efficienza.

Tutti questi benefici, però, rendono l’IoT un sistema critico che va assolutamente protetto, al fine di evitare che l’impatto positivo di questa grande opportunità su imprese e persone venga annullato. Anche perché si tratta di piattaforme utilizzate anche in tutti quei settori considerati critici come ad esempio l’healthcare, le smart cities o le reti elettriche.

I sistemi di automazione degli smart building, ad esempio, sono tipicamente costituiti da sensori e controller usati per monitorare e automatizzare il funzionamento di ascensori, impianti di vario genere come quello di ventilazione, di climatizzazione, elettrici, di fornitura idrica, di video sorveglianza, o allarmi anti-incendio e sistemi di controllo degli accessi e molte altre informazioni critiche e sistemi

di sicurezza. Questi sistemi sono solitamente gestiti e controllati da normali workstation che, spesso, sono connesse a Internet.

Un attacco riuscito contro una di queste workstation può facilmente concludersi con il mal funzionamento di uno o più sistemi critici dello smart building. Inoltre, le piattaforme IoT possono essere collegate a sistemi critici come quelli per il controllo del traffico, l’erogazione dell’energia e dei trasporti, quindi è fondamentale garantire la loro continuità e integrità. In definitiva l’Internet of Things è un potente strumento di business, ma per cogliere i suoi benefici le organizzazioni devono impegnarsi a fondo.

Per ottenere un’efficace implementazione, oltre a competenze specifiche, sono richiesti processi di business dedicati. Anche la sicurezza informatica è una questione che deve essere presa in considerazione sin dalle fasi iniziali dell’implementazione dell’IoT. Noi di Kaspersky vogliamo aiutare i nostri clienti ad affrontare questo compito sviluppando soluzioni di sicurezza IoT e sensibilizzandoli sui rischi e le problematiche.



Anche l’avvento dei droni ha dato nuovi accessi ai criminali informatici per minare la sicurezza e la privacy degli utenti. Nel 2018, il mercato globale dei droni ha raggiunto un valore di circa 14 miliardi di dollari; entro il 2024 dovrebbe arrivare a toccare i 43 miliardi di dollari. Questa crescita è determinata dalle potenziali opportunità e dai tanti cambiamenti positivi che l’utilizzo di veicoli volanti privi di equipaggio può portare con sé: consegna di merci, ispezione di siti minerari, costruzioni edilizie, ma anche puro divertimento. Nonostante questi aspetti positivi, l’uso popolare di questa tecnologia rivoluzionaria potrebbe essere influenzato da alcune connotazioni negative che spesso vengono associate al mondo dei droni. I droni possono essere utilizzati anche per fare spionaggio, possono ferire le persone in caso di incidenti, possono causare danni alle infrastrutture critiche, comprese le centrali nucleari, o anche perturbare il normale funzionamento di un aeroporto, come è accaduto all’aeroporto britannico di Londra Gatwick, quando la pista è stata chiusa proprio a causa di droni in volo.

Considerando tutti questi fattori, è chiaro come sia sempre più importante contribuire alla costruzione e al mantenimento di un approccio orientato alla fiducia verso la tecnologia, in modo da salvaguardare il suo apporto innovativo - per le imprese e per i privati - e, nello stesso tempo, assicurarsi che le nuove frontiere tecnologiche non determinino rischi per la privacy o per la sicurezza.

**È possibile delineare un confronto tra la situazione italiana e quella degli altri paesi dell’area EMEA e/o world in termini di attacchi conclamati?**

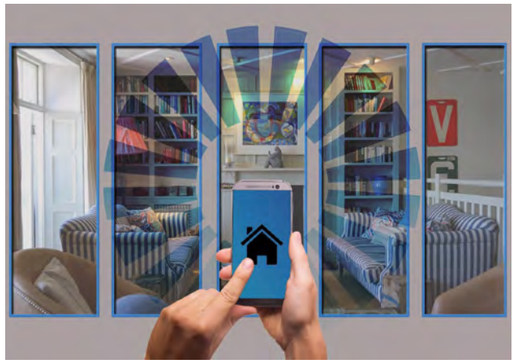
Recentemente abbiamo condotto un’indagine sulle minacce informatiche rivolte agli smart building dalla quale è emersa, in parte, la situazione a livello europeo degli attacchi rivolti ai sistemi di sicurezza di questi edifici. Secondo questa analisi, infatti, quattro computer su dieci (37.8%), usati per gestire i sistemi di automazione degli “edifici intelligenti”, sono stati oggetto di attacchi malevoli. Sebbene non sia del tutto chiaro se questi sistemi siano stati deliberatamente presi di mira, questa ricerca dimostra come gli smart building siano spesso oggetto di varie minacce generiche. Per quanto non si tratti di minacce sofisticate, molte di queste possono costituire un pericolo importante per le operazioni quotidiane degli smart building. La maggior parte degli attacchi arrivava dal web ed utilizzava diverse versioni di spyware, ovvero malware che hanno l’obiettivo di rubare le credenziali degli account e altre informazioni importanti. Dall’indagine è emerso, inoltre, che l’Italia è il Paese con il maggior numero di attacchi rivolti ai computer per gli smart building (48,5%), seguito da Spagna (47,6%), Regno Unito (44,4%), Repubblica Ceca (42,1%) e Romania (41,7%).

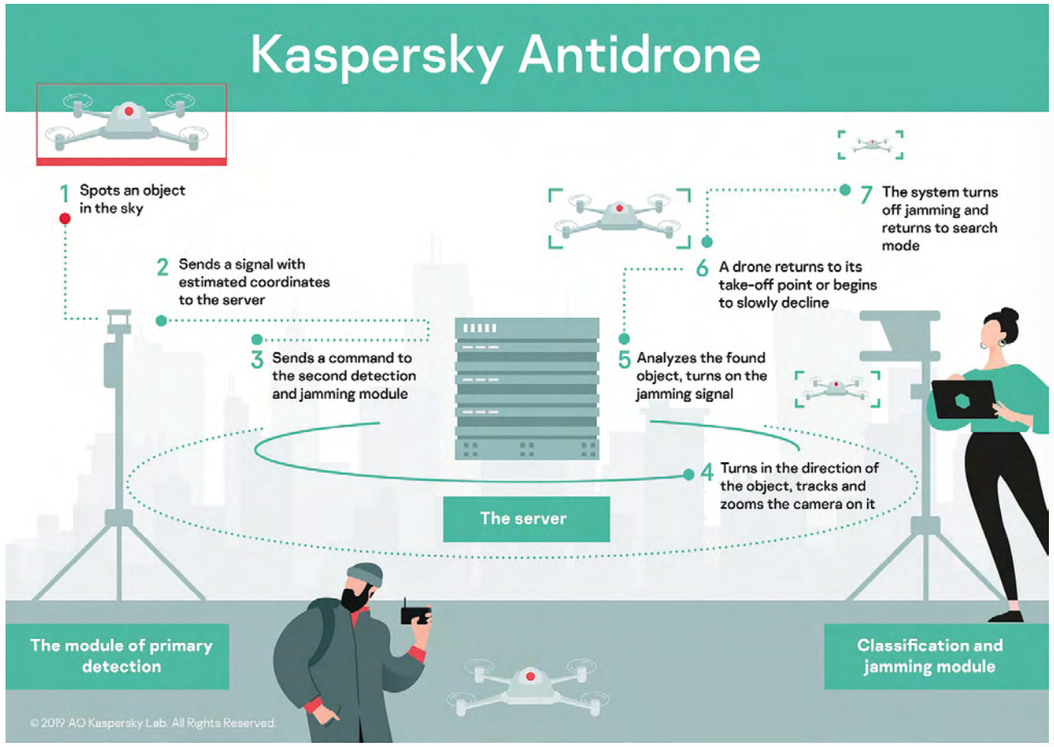
**Come valutate il livello di consapevolezza sul punto delle funzioni decisionali delle organizzazioni pubbliche e private?**

Quello che riscontriamo sul mercato è un livello di consapevolezza mediamente abbastanza alto, che però non corrisponde necessariamente a una prioritizzazione degli investimenti necessari a indirizzare il problema. La prima controparte con cui dialogare per condividere questa necessità sono i System Integrator e i Produttori di tecnologie, coi quali è fondamentale indirizzare il tema della vulnerabilità informatica dei prodotti fin dalla loro progettazione: lavoriamo da tempo con alcuni importanti player proprio per fare in modo che gli “oggetti” che comporranno una soluzione o che arriveranno dal cliente finale siano progettati e realizzati includendo componenti di sicurezza informatica, e che lo stesso processo di produzione di questi oggetti sia gestito da macchinari protetti anche in questo senso.

**Quali sono le proposte di Kaspersky per la sicurezza integrata?**

Per rispondere alle esigenze crescenti di sicurezza integrata, Kaspersky mette a disposizione Kaspersky IoT Secure






Gateway e KasperskyOS che, insieme, garantiscono il comportamento sicuro del gateway stesso, così come di tutti i dispositivi collegati e dell'intero sistema IoT.

Il mercato offre ora numerosi gateway e router descritti come "sicuri" o "affidabili". Questi dispositivi forniscono una vasta gamma di tecnologie per la protezione contro le minacce informatiche: scanner antivirus, controllo del traffico di rete, firewall, ecc. È importante capire, però, che queste tecnologie sono progettate per proteggere i dispositivi collegati al gateway, ma nessun produttore protegge effettivamente il gateway stesso.

Se è compromesso, tutte le tecnologie di sicurezza che lo accompagnano possono essere disattivate. **Kaspersky IoT Secure Gateway** contiene una gamma di tecnologie che consentono di adottare un approccio qualitativamente diverso per la sicurezza in ambito IoT e per quella relativa ai device presenti all'interno delle smart home. Oltre alle migliori tecnologie per la sicurezza dell'infrastruttura, questa soluzione implementa tecnologie affidabili che garantiscono il comportamento sicuro del gateway o del router stesso. Abbiamo progettato la nostra soluzione per incorporare moduli e tecnologie di sicurezza nel firmware del dispositivo, in modo da poter proteggere l'hardware con diversi gradi di personalizzazione.

**KasperskyOS**, invece, è un sistema operativo sicuro per dispositivi embedded connessi con requisiti specifici di sicurezza informatica, che crea un ambiente in cui vulnerabilità o codici malevoli non rappresentano più un problema. Il concetto alla base di KasperskyOS è di consentire ai programmi di eseguire solo attività documentate previste dalla policy, comprese, quindi, anche le stesse funzioni del sistema operativo.

Il vantaggio per i programmatori è di poter sviluppare una politica di sicurezza insieme alle funzionalità reali di un'applicazione riducendo drasticamente la possibilità di attacchi informatici.

Inoltre, per rendere più sicuro l'uso di dispositivi volanti senza piloti o equipaggio, ridurre i possibili rischi associati e attribuire maggiori responsabilità all'operatore, Kaspersky ha sviluppato una propria soluzione "antidrone". Il software



**Kaspersky Antidrone** coordina il lavoro di diversi moduli hardware forniti dai partner ed è in grado di distinguere i droni da altri dispositivi. Il modulo di rilevamento primario procede con la ricerca dei droni utilizzando videocamere combinate con sensori radar, LIDAR e audio, a seconda delle esigenze del cliente e delle condizioni ambientali. L'utilizzo di uno scanner laser per determinare la posizione del drone è un "unicum" della soluzione proposta da Kaspersky, che non ha precedenti applicativi in questo campo. Quando un oggetto in movimento viene rilevato nel cielo, le sue coordinate vengono trasmesse a un server dedicato, che le invia a un'unità speciale. In base ai dati provenienti dal modulo di rilevamento primario, questa unità ruota verso l'oggetto, lo segue e la telecamera zooma sull'oggetto stesso. Contemporaneamente, una rete neurale, progettata proprio per identificare i droni e distinguerli da altri oggetti in movimento, analizza l'oggetto dal video. Se il sistema lo riconosce come drone, il server invia un comando al modulo dedicato il quale disturba, tramite interferenze, le comunicazioni tra il dispositivo e il suo controllore. Come risultato, il drone torna al luogo di partenza o atterra nel punto in cui ha perso il segnale con il controller.

Se poi pensiamo a tutti quegli oggetti molto semplici che popolano le nostre abitazioni (bollitori elettrici, telecamere di video sorveglianza, frigoriferi intelligenti) e che possono essere connessi alla rete attraverso semplici app installate sui nostri cellulari, ci rendiamo conto che uno degli inconvenienti maggiori di questi dispositivi smart

è che solo le case produttrici possono risolvere i problemi di sicurezza che potrebbero insorgere. I proprietari di tali oggetti spesso non possono fare nulla. Affinché sia più facile per gli utenti individuare le vulnerabilità nei dispositivi smart connessi alla rete domestica, abbiamo creato un'app apposita: **Kaspersky IoT Scanner**. Questa app per Android analizza la vostra rete di casa, elabora un elenco di tutti i dispositivi che vi sono connessi e individua le vulnerabilità più comuni. Dopo essere stata installata, IoT Scanner analizza la rete domestica e localizza tutti i dispositivi collegati a essa. Successivamente, analizza alcune porte di rete specifiche dei dispositivi e verifica quali porte sono aperte e quali no. Se IoT Scanner individua alcune porte che potrebbero essere sfruttate per scopi dannosi, allora l'app invia una notifica e invita l'utente a chiudere tali porte, risolvendo così la vulnerabilità.

kaspersky

# NUOVO SISTEMA PRIME 3.0.
## LA DOMOTICA NON SARÀ PIÙ COME PRIMA.

**InimHome**

APP PER GESTIONE SICUREZZA, DOMOTICA E VIDEOVERIFICA CON CATEGORIZZAZIONE AUTOMATICA USCITE DOMOTICHE: ILLUMINAZIONE, TAPPARELLE, VARCHI ELETTRODOMESTICI.


**Flex2R/2T**

MODULO SU BUS CON 2 RELÈ 230V, 5A E 2 TERMINALI. GESTIONE NATIVA DI TAPPARELLE, VENEZIANE E PUNTI LUCE.

**PrimeLAN**

MODULO CON NUOVE FUNZIONALITÀ PER LA GESTIONE DI SISTEMI DI VIDEOSORVEGLIANZA ONVIF E KNX.

**Smarty/W**

SIRENA WIRELESS DA INTERNO.

**PrimeWiFi**

MODULO DI CONNETTIVITÀ WIFI.



**Flex/5R**

MODULO SU BUS. 5 RELÈ, 230V, 16A. ALLOGGIATA IN CONTENITORE PER BARRA DIN 5 MODULI.

**nBy/K**

LETTORE DA INCASSO SU BUS DOTATO DI 1 TERMINALE ED AGGANCIO UNIVERSALE KEYSTONE.


**Nexus/4GP**

MODULO GSM 2G E 4G (LTE) INTEGRATO SU I-BUS CON BATTERIA TAMPONE.

**Nexus/4GU**

MODULO GSM 2G E 4G (LTE) INTEGRATO SU I-BUS CON TERMINALI A VISTA.

Con Prime 3.0, Inim introduce non solo una centrale che arriva a supportare ben 500 terminali (oltre che 500 codici utenti e 500 chiavi), ma fa molto di più. Inim riscrive il futuro della domotica (e della sicurezza antintrusione), introducendo nuovi dispositivi con funzionalità ancora più avanzate. Per un sistema integrato di ultima generazione, con prestazioni mai viste prima.

inim.biz

inim ELECTRONICS

# Nuova normalità, le generazioni M e Z chiedono più sicurezza in store

*Intervista a di Erika Andreetta, partner di  PwC Italia, Consumer Markets Consulting Leader*

**PwC Italia** ha realizzato un paper a cura di **Erika Andreetta** sul rilancio dei consumi nella fase post COVID 19 **(leggi)**, che riporta i risultati di una ricerca sui cambiamenti comportamentali dei consumatori nella nuova normalità, focalizzata in particolare sulle richieste espresse dalle generazioni **M (1980 - 1995) e Z (1995 - 2005)**.

**Possiamo riassumere i risultati della ricerca, in particolare sulla richiesta di sicurezza dei giovani nella customer experience in store?**
La nostra ricerca ha fatto emergere tre aspetti chiave:
- necessità di customer experience sicure e accessibili
- domanda di tecnologie per la sicurezza in store
- preferenza di prodotti italiani perché ritenuti “più sicuri”

In merito alla necessità di customer experience sicure e accessibili, la prova che la salute e la sicurezza siano la priorità per i consumatori è ovunque. Ad esempio, nella nostra ricerca i tre principali motivi per vivere nelle città prima dell’epidemia erano:
- prospettive di occupazione (31%)
- sicurezza e protezione (27%)
- assistenza sanitaria (19%).

Dopo l’epidemia, la sicurezza e l’assistenza sanitaria sono diventate importanti tanto quanto le prospettive di occupazione, rispettivamente con il 49% e il 45% delle preferenze vs il 45% per l’occupazione.
Ci attendiamo, quindi, che i clienti avranno bisogno di maggior sicurezza nella propria shopping experience. I retailer si dovranno pertanto preoccupare della customer experience che sarà messa a dura prova dalle misure anti-Covid (sanificazione, distanziamento, DPI, ecc.).

Serviranno addetti con una professionalità sempre più alta per interagire nel modo corretto con le differenti sensibilità del pubblico. Sarà fondamentale avere la capacità di mantenere la distanza e sviluppare l’empatia tramite il servizio offerto.

**Per quanto riguarda la domanda di sicurezza in store, cosa avete rilevato?**
Di certo i retailer dovranno saper rispondere alle esigenze del “nuovo consumatore” che, adesso, è più consapevole dei vantaggi dello shopping mobile (come facilità e velocità) ma ha anche nuovi bisogni e priorità:
- In primis la sicurezza; per far sì che i consumatori si sentano sicuri di poter tornare ad avere interazioni fisiche in store, hotel e altre attività, la prima cosa di cui avranno bisogno è la garanzia che questi luoghi possano rendere la loro esperienza del cliente più sicura possibile.

Ad esempio, in un recente sondaggio PwC sui clienti del settore Hospitality negli Stati Uniti, gli intervistati hanno


affermato che la loro priorità al momento della prenotazione di voli e hotel era “la fiducia del brand, in particolare la sicurezza e la pulizia”.
- Ma non meno importante la tecnologia per garantire facilità e velocità nello shopping ed esperienza omnichannel.

Secondo la nostra indagine, le tecnologie più ricercate in negozio sono appunto legate ai bisogni di sicurezza/ facilità ed esperienza omnichannel:
- 38% sistemi di self check-out
- 26% app per la navigazione in-store (per cercare più velocemente i prodotti e forse anche per ridurre i tempi di permanenza in store)
- 26% esperienza di acquisto employee-free (preferita in particolare dagli Amazon addicted)

**Qual è l’atteggiamento dei giovani verso i prodotti italiani?**
Cresce il valore dei prodotti “Made in Italy” per i giovani consumatori italiani:
- l’83% dei millennials e il 71% dei gen Z ritiene che sia molto / abbastanza importante acquistare prodotti italiani. Il dato è in crescita rispetto al 2019 rispettivamente con il 67% e il 55%
- Solo il 2% dei giovani italiani non attribuisce importanza al Made in Italy nelle scelte di acquisto

Il motivo principale che spinge ad acquistare “Made in Italy” è la qualità e la “sicurezza dei prodotti” per il 78% dei millennials e gen Z, dato in crescita rispetto all’anno precedente, rispettivamente +19% M e +47% Z.

# I nuovi problemi di sicurezza per il mondo della Logistica a Supply Chain Edge 2020

*intervista a Pietro Pedone, membro di board di CSCMP – Italy Round Table*

**Quali sono i problemi di sicurezza maggiormente sentiti dal mondo della logistica in questo periodo?**
Nel passato si parlava soprattutto di **sicurezza fisica** per le persone (protezione da infortuni, al lavoro o in viaggio) e per le cose e i mezzi (incidenti, rotture, furti). Oggi sono diventate importanti anche "altre" sicurezze come la **cyber-security** (col crescere repentino dello smart working e dell'e-commerce) e la **sicurezza sanitaria** per contrastare la pandemia. La "distanza di sicurezza" non è più solo quella obbligatoria tra i veicoli nel traffico, ma è diventata anche la distanza di sicurezza tra le persone. Ecco il "salto di specie": prima controllavamo i movimenti delle **cose** e dei mezzi (camion, carrelli), oggi dobbiamo controllare anche i movimenti delle **persone**: distanze, percorsi differenziati, limiti agli assembramenti sui mezzi pubblici, al ristorante, oltre che all'interno di un magazzino o di una fabbrica.
Alla Logistica delle cose, si aggiunge la Logistica delle persone. Ad esempio, I sistemi RTLS (Real Time Location System) studiati sia per localizzare i carrelli (per ottimizzare i percorsi, ma anche per evitare collisioni) sia per ricercare i prodotti all'interno di un magazzino o di un piazzale, sono applicabili anche alle **persone** per evitare incontri ravvicinati o assembramenti eccessivi. Gli strumenti per ottimizzare la logistica diventano strumenti per garantire anche maggior sicurezza sanitaria.
Un discorso a parte vale per la cyber security: lasciando ad altri gli approfondimenti legati allo smart working e alla blockchain, sono molto legate alla logistica le estensioni dei collegamenti richiesti dall'e-commerce. Basti pensare alla tracciatura della spedizione e alla certificazione della consegna in tempo reale: la sicurezza della rete e la riservatezza dei dati sono fondamentali.

**Quali temi sono stati affrontati durante la sessione dedicata alla sicurezza fisica da lei coordinata durante Supply Chain Edge 2020?**
Sicurezza fisica, digitale e sanitaria sono state spesso collegate

tra loro. La logistica, per sua natura, integra la filiera, le funzioni e tutti gli attori coinvolti. Analogamente le varie esigenze di controllo si possono avvalere di dispositivi potenziati e arricchiti per più scopi e di sistemi per il controllo integrato. Alla torre di controllo per la filiera, si affianca la **torre di controllo** per la sicurezza: in tempo reale per prevenire e attivare gli interventi più appropriati e al più presto o, anche, individuare azioni criminali preparatorie, in tempo utile per prevenire e sventare l'atto predatorio. Come si parla di **logistica integrata** (se non è integrata, non è "Logistica"), così ormai si parla di **controllo integrato** multifunzionale e, il più possibile, automatico con sistemi "intelligenti" di allarme, che leggono le situazioni di rischio, individuano le reazioni e innescano gli interventi più opportuni.
Fondamentale nelle filiere del freddo (food, medicinali) è assicurare il mantenimento della temperatura: è sicurezza fisica? o digitale, o sanitaria?
Una sfida logistica da vincere in assoluta sicurezza sarà la distribuzione del **vaccino** (prossimamente, speriamo!): enormi unità di prodotto, provenienti da diverse parti del mondo, dovranno essere distribuite in modo capillare nel più breve tempo possibile. Fondamentale sarà la sicurezza della temperatura (si parla di decine di gradi sotto lo zero: proibitive per molte delle attuali strutture).



# L'integrazione di Security, Safety e Health: Vigilanza Group al Supply Chain Edge 2020

*a cura della Redazione*

Si è svolta il 16 ottobre l'edizione virtuale di **Supply Chain Edge**, il convegno annuale organizzato dall'Italy Roundtable di CSCMP (Council of Supply Chain Management Professional), nell'ambito del quale sono state illustrate le soluzioni integrate di sicurezza per il mondo della logistica sviluppate da **Vigilanza Group**.
Il key account manager **Lucio Piccinini** ha presentato due case history sviluppate in contesti diversi che hanno fatto comprendere l'efficacia dell'approccio e la validità delle soluzioni proposte dal security service provider di Brescia.

**Partecipando a Supply Chain Edge 2020 avete portato le testimonianze di due vostri importanti clienti nel settore della logistica e del retail, Tauro Autotrasporti e MD spa. Ci può riassumere i criteri con i quali avete affrontato queste due diverse situazioni?**
La progettazione della soluzione di sicurezza personalizzata parte sempre da un'attenta analisi delle esigenze del cliente. Seppur per utilizzi diversi, sia Tauro che MD sono stati dotati della piattaforma software proprietaria di Vigilanza Group.
Nel primo caso, la tecnologia ha permesso la completa esportazione di tutti i servizi di sicurezza e presidio svolti precedentemente da una persona fisica impiegata nell'arco notturno all'interno della guardiola del sito.
Le nostre tecnologie permettono di svolgere servizi in remoto come il controllo del sito in video analisi, la gestione del sistema antintrusione, la ricezione di segnali incendio nel rispetto della EN 54.21, la telegestione degli accessi fisici (porte, cancelli, ecc.), delle luci e dei segnali di diffusione sonora, oltre alla videocitofonia.
In sintesi, si tratta di un "piantonamento virtuale" a tutti gli effetti, come abbiamo definito questo specifico servizio. Nel caso di MD, abbiamo ottimizzato e razionalizzato i processi di acquisizione, analisi e coordinamento degli interventi fisici sul posto per tutti i punti vendita che ci sono stati affidati. Il software consente la centralizzazione in un'unica interfaccia delle segnalazioni provenienti dai sistemi di sicurezza attiva presenti nei negozi, in particolare il sistema antintrusione e il sistema di videosorveglianza, mentre gli algoritmi di analisi video, permettendo alle telecamere di divenire dei veri e propri sensori, consentono l'invio di alert al centro decisionale. Gli operatori della nostra centrale coordinano il pronto intervento delle pattuglie di vigilanza e delle forze dell'ordine fin dalla prima violazione da parte di intrusi del perimetro vigilato.

**Qual è stato il livello di soddisfazione dei vostri clienti?**
La soddisfazione clienti è misurata dall'analisi dei dati dei benefici offerti dalle soluzioni "taylor made" applicate. Gli aspetti migliorativi, direttamente proporzionali al grado di soddisfazione, si concretizzano in due principali aree: l'innalzamento degli standard di sicurezza e la riduzione dei costi di gestione.
Aziende come Tauro Autotrasporti, che utilizzano hub con superfici molto estese da sorvegliare, apprezzano l'efficienza di un centro remoto sempre connesso e a completa disposizione per ogni esigenza, mentre possono misurare una drastica riduzione dei costi rispetto alle soluzioni precedenti con l'impiego giornaliero di personale fisico. Grandi catene di retailer come Md gradiscono la possibilità di analisi a monte dei segnali ricevuti, con un efficace e concreto contrasto dei reati predatori che consente una sensibile riduzione delle differenze inventariali.

# Le case history di MD spa e Tauro Autotrasporti

*Le testimonianze di Pasquale Grottola (MD spa) e Giorgia Tauro (Tauro Autotrasporti)*

*Pasquale Grottola*

*Giorgia Tauro*

**Per quali problemi di sicurezza vi siete rivolti a Vigilanza Group?**

*Pasquale Grottola:* L'analisi della protezione dei siti durante gli orari di chiusura evidenzia una chiara vulnerabilità, riferita ai reati predatori che avvengono tramite la forzatura degli accessi o la demolizione di vetrate. L'adeguamento delle difese passive, ossi il rafforzamento delle vetrate e dei varchi di accesso, non garantisce comunque la completa protezione poiché l'irruenza degli attacchi si adegua a sua volta al tipo di protezione. La vulnerabilità, seppur in termini ridotti, continua a manifestarsi sia per le modalità di esecuzione sia per i brevissimi tempi entro i quali si consuma il reato. Lo studio dei processi, con i quali i malfattori operano, hanno rilevato la necessità, da parte di quest'ultimi, di una breve fase di preparazione che prevede l'organizzazione di mezzi e strumenti necessari per poter compiere il reato. Risulta pertanto facile dedurre dove e quando intervenire per garantire un'adeguata protezione da tali attività.

*Giorgia Tauro:* Nel 2017, durante la costruzione del nuovo stabile sito in Castellalto (TE), ci eravamo orientati verso una soluzione di vigilanza tradizionale, impiegando personale fisso in loco. Ma in realtà questa soluzione non si è dimostrata idonea per assicurare la sicurezza e la tranquillità del nostro personale e dei nostri clienti, che sono aspetti fondamentali per noi. Per questo abbiamo svolto un'attenta ricerca di mercato e abbiamo conosciuto questa azienda giovane e dinamica. Le esigenze della nostra struttura erano, e sono ancora più oggi, quelle relative alla possibilità di attacco esterno del nostro hub, sia durante le ore notturne che nell'orario delle partenze dei nostri vettori, quando i rimorchi sono carichi di merce pronti alla partenza. Infine la continua crescita della flotta aziendale ci impone di collaborare con personale sempre nuovo ed il turn-over degli autisti certamente non avvantaggia la sicurezza del sito.

**Quali soluzioni avete adottato?**

*Pasquale Grottola:* L'uso della tecnologia è sempre più determinante. Il supporto di piattaforme ed algoritmi sviluppati in maniera specifica permettono, tramite l'utilizzo degli impianti di videosorveglianza, di attivare gli stati di allarme proprio nella fase di avvicinamento al sito e, quindi, di preparazione del reato.
I software di videoanalisi permettono di anticipare l'attivazione degli allarmi e, di conseguenza, dell'intervento fisico da parte della vigilanza e/o delle forze dell'ordine. Considerata la psicologia di chi delinque, rappresenta un ottimo e funzionale deterrente.

*Giorgia Tauro:* Abbiamo progettato un nuovo modello di sicurezza, basato su un sistema centralizzato nelle centrali operative di Vigilanza Group con telecamere esterne ed interne nei magazzini e nella struttura, software di analisi video, centrali antintrusione e di rilevazione fuoco/fumo di ultima generazione, automazioni. Quando termina l'attività di magazzino, c'è un vero e proprio passaggio di consegne tra il nostro personale ed il "piantone virtuale" che prende in carico e gestisce il sito con procedure concordate fino al mattino, quando i nostri addetti rientrano in servizio.

**Sono stati raggiunti gli obiettivi che avevate previsto?**

*Pasquale Grottola:* Assolutamente sì. In alcuni casi abbiamo registrato "falsi allarmi" che, di fatto, rappresentavano dei veri e propri sopralluoghi da parte dei malfattori che hanno ben valutato le difese del sito desistendo dal loro intento. E' opportuno sottolineare che, oltre all'efficienza della tecnologia, c'è un importante contributo degli operatori che gestiscono la piattaforma. L'efficienza degli interventi dev'essere misurata in secondi e non in minuti e, nonostante l'automatismo delle piattaforme, è decisiva l'attenzione della sala operativa nel valutare e seguire parallelamente come e quando agire in circostanze simili.

*Giorgia Tauro:* Il riscontro è stato positivo e funzionale per il controllo del personale e delle merci. La reportistica real time ci relaziona ogni giorno quanto accade in nostra assenza. Gli autisti ed il personale autorizzato entrano ed escono dal sito in completa sicurezza potendo contare sul "piantone virtuale" che supervisiona ogni suo angolo. Inoltre, a dar ragione alla scelta fatta ci sono i dati: due attacchi predatori sventati ed un notevole risparmio economico ottenuto grazie alla fruizione di un servizio tecnologico in outsourcing.

**Dal suo punto di vista, cosa sta cambiando in questa fase per la sicurezza delle merci?**

*Pasquale Grottola:* I cambiamenti nelle abitudini dei consumatori in questo periodo hanno modificato il rapporto tra richiesta e fornitura, in particolare per l'aumento dell'utilizzo dell'e-commerce che comporta problematiche di sicurezza del tutto specifiche. L'analisi della sicurezza si è spostata, passando dalla quasi totale attenzione per i negozi alla garanzia di un iter di consegna che parte dai fornitori fino all'arrivo sugli scaffali, con l'esigenza di un adeguato sistema di prevenzione nella fasi di trasporto.

*Giorgia Tauro:* Le problematiche che accomunano il mondo del trasporto sono molteplici, tra le quali troviamo sicuramente intrusioni ed attacchi predatori, rapine, furti delle merci sia all'interno dell'hub che in fase di trasporto, attacchi alla flotta. Controllare tutto è davvero una sfida e devo dire che uno dei primi aspetti da prendere in considerazione è la scelta di collaboratori fidati per le mansioni più critiche per l'attività aziendale.

# Tendenze settoriali e convergenze con l'informatizzazione dipartimentale della sicurezza fisica – le nuove tecnologie e l'open-BMS di Citel

*di Nils Fredrik Fazzini, CEO di Citel spa*

Negli ultimi tempi, la stampa di settore negli USA ha pubblicato i risultati di due ricerche sulle tendenze di fondo nel settore della sicurezza fisica ad opera, rispettivamente, di **Stanley Security** (ricerca nei Paesi occidentali, commentata da Citel su **essecome n. 1/ 2020**) e di **SIA** - Associazione dell'Industria della Sicurezza - nell'ambito della comunità dei produttori USA.

La prima ricerca si è svolta tra gli **utilizzatori** di soluzioni per la sicurezza fisica in campo internazionale, la seconda tra **operatori e produttori**.

**Due indagini internazionali complementari e convergenti verso l'informatizzazione della sicurezza fisica**

La complementarietà delle due indagini, che hanno toccato buona parte del mercato aziendale della sicurezza fisica nel mondo occidentale, permette di comporre un quadro generale che si presta a delle interessanti considerazioni ed anche al consolidamento di una nomenclatura appropriata ed aggiornata in un contesto che a questo proposito è forse ancora troppo fluido.

Il prospetto che segue, ottenuto con l'abbinamento dei risultati delle due indagini, non è oggetto di commenti sui singoli valori e tecnologie ma si presta, data la vicinanza temporale delle due ricerche e l'ampiezza del campo osservato, a fornire un contributo al consolidamento di una classificazione aggiornata nella materia e per delle considerazioni sintetiche nel quadro sempre più complesso delle nuove tecnologie, quelle all'attuale stato dell'arte ed anche quelle emergenti in funzione della *Digital Transformation* in atto.

| **Quadro della diffusione di nuove tecnologie di due diverse indagini diffuse di recente dalla stampa specializzata nel 2019 e nel 2020, con l'abbinamento alle singole tendenze tecnico funzionali** | |
|---|---|
| **SIA** – rilevazione tra i **produttori** USA, previsione della diffusione delle **tecnologie** innovative (*in ordine di importanza decrescente*) | **Stanley** – indagine tra gli **utilizzatori** USA e Europa sui **fattori e processi funzionali** dell'innovazione settoriale *associati da Citel alle singole tecnologie SIA nella prima colonna (non in ordine di importanza)* |
| 1 - Artificial Intelligence | - Machine Learning<br>- Customer Experience Transformation |
| 2 - Predictive Data Analytics | - Monitoring Automation<br>- Big Data<br>- Programmatic Evolution |
| 3 - Connectivity and the IoT of Everything | - Cloud Technology<br>- Remote services<br>- SAAS – software as a service<br>- Network Security |
| 4 - Cloud Computing | |
| 5 - Cybersecurity of Physical Security | |
| 6 - Touchless & Frictionless Solutions | - Stricter Access Control Requirements |
| 7 - Facial Recognition | |
| 8 - Emphasis on Data Privacy | *non rilevato* |
| 9 - Responsive Environments & Intelligent Spaces | - Machine Learning |
| 10 - Move to Service Models | *indicato per tutte le tecnologie* |

**La sistemistica innovativa attuale e la nomenclatura**

Al di là di un eventuale contributo alla normalizzazione di una nomenclatura univoca e appropriata per le nuove tecnologie, auspicabile in una fase evolutiva come quella attuale, quello che emerge nettamente è il fatto che **tutte le innovazioni** indicate dagli utilizzatori, in corso o imminenti nel campo della **sicurezza fisica**, riguardano **tecnologie** e **processi *informatici*** applicati alle soluzioni in campo, alle comunicazioni, fino al governo dipartimentale della sicurezza nel suo insieme.

Coprendo un ambito dove i valori che si perseguono e si governano arrivano a coinvolgere scopi e responsabilità di un Security Manager che vanno dalla protezione di persone e beni al rispetto di *normative sempre più stringenti*, alla *tutela della continuità operativa fino* - addirittura - alla stessa *resilienza aziendale*.

E poiché **l'informatica applicata è una disciplina strettamente basata *sui sistemi***, ne consegue che: 1) tutte le tecnologie, attuali e tendenziali, applicate a quei processi **non possono essere – per definizione – operative, interattive e governabili se non sono parte integrante di uno specifico *sistema informatico***; 2) che nella fattispecie è necessariamente di tipo ***dipartimentale, specializzato e dedicato alla sicurezza fisica*** dell'impresa.

Ma anche un sistema **aperto e predisposto all'interazione con altri sistemi e processi**, viste le dinamiche attuali del settore e il corollario di servizi e tecnologie riassunte nel prospetto; interazioni che potranno essere efficaci e governabili solo se innestate organicamente in **una sistemistica informatizzata di gestione e supervisione progettata per quella visione e per quell'assetto** su due livelli applicativi: quello aziendale e quello dedicato all'edificio.

**Centrax open-PSIM** di Citel è nato partendo dalle competenze informatiche e di automazione di Citel applicate ad una visione di interattività anche orizzontale nell'ambito della sicurezza fisica telegestita in una chiave di sistema dipartimentale aziendale oppure dedicato alla sicurezza fisica di singoli edifici. Con una struttura che comprende funzionalità di governo e sottosistemi che riguardano intrusione – incendio – accessi – videosorveglianza.

**Centrax open-BMS** è invece il frutto di un recente accordo di Citel con un produttore specializzato – che ha permesso di adottare e integrare alle applicazioni PSIM una sistemistica specializzata per la gestione integrata degli impianti tecnologici di un *building*, inteso sia come un qualsiasi edificio fino al grattacielo per uffici oppure al complesso industriale.

E con questo è stato istituito il modello Centrax-open BMS, dove "open-BMS" è probabilmente un neologismo, necessario per riferirsi ad un BMS che – rompendo con una storia pluridecennale di settore dominata dai sistemi chiusi mono-fornitore – è finalmente aperto all'integrazione di un numero e una varietà estesa di apparati, sottosistemi e sistemi nell'ambito delle applicazioni BMS con un probabile primato non solo nell'ambito della sicurezza, del controllo accessi e della videosorveglianza, ma anche degli impianti tecnici di alimentazione elettrica, di climatizzazione, di spostamento delle persone, e relativi protocolli specializzati, pubblici o meno.

Con Centrax open-BMS, quindi, Citel specializza il modello Centrax open-PSIM che si è affermato nel settore della sicurezza fisica per l'ampiezza del catalogo delle funzioni e delle integrazioni, per le varianti sistemistiche e per la scalabilità, dalla workstation al centro servizi in chiave as-a-service, fino all'infrastruttura corporate multisito.

CITEL

Contatti:
Citel spa
marketing@citel.it
www.citel.it





# Secursat: data analysis, connettività, digitalizzazione, remote maintenance

*intervista a Alessandro Visconti, Sales and Customer Account Manager di Secursat*

**La security, grazie alla digitalizzazione, si trova davanti a grandi opportunità ma anche sfide complesse. Ci può riassumere vision e mission di Secursat, una realtà fortemente innovativa nel panorama nazionale della sicurezza?**
Secursat considera la sicurezza come un ombrello protettivo del business in generale, pertanto le nostre strategie di sviluppo di modelli e servizi di security si basano, continuamente, sullo studio approfondito delle evoluzioni nei mercati dei nostri clienti e, dunque, sui bisogni di crescita e sviluppo che le aziende manifestano.
L'emergenza sanitaria che abbiamo vissuto e stiamo ancora vivendo ha accelerato la strada del digitale, rendendo per i nostri clienti, a prescindere dai settori, i modelli di business digitali non solo uno strumento per contrastare la concorrenza, ma un vero e proprio tema di sopravvivenza. Mentre i nostri clienti, dunque, hanno lavorato per indirizzare la strategia aziendale verso le vendite digitali, noi abbiamo lavorato per modernizzare le capacità di gestione delle attività di sicurezza sfruttando la connettività ed utilizzando i dati per migliorarne l'efficacia e l'efficienza e proporre ottimizzazioni concrete e *saving* significativi basati, non come spesso avviene sull'abbassamento del prezzo, ma sulla razionalizzazione di costi ed investimenti.
Abbiamo capito di essere pronti ad accettare le evoluzioni in atto e dimostrarci sempre più agili nel cogliere i cambiamenti e, per questo, abbiamo implementato un modello di business basato anche sulla remotizzazione di tutte le attività che non è necessario svolgere on-site e sulla capacità di organizzare i dati e le informazioni in maniera standardizzata.
Indagando, infatti, le necessità dei nostri clienti ci siamo trovati di fronte l'evidenza che, nel settore della sicurezza, i prodotti sono oramai diventati delle commodities, con differenze spesso minime tra marche e modelli, e che sono la capacità di progettazione e la gestione delle attività di security a fare la differenza, spesso significativa, nella struttura dei costi aziendali.

***"la riduzione dei costi, necessaria in questa fase quanto più in quella di ripresa, può essere resa possibile dall'evoluzione delle attività attraverso approcci nuovi, digitali, remoti capaci di aiutare ad ottimizzare i processi e monitorare i risultati"***

La base dello sviluppo del nostro progetto è condividere con i nostri clienti che la riduzione dei costi, necessaria in questa fase quanto più in quella di ripresa, non dovrà necessariamente essere associata all'assottigliamento del prezzo del prodotto o del servizio, all'abbassamento della qualità, alla riduzione di ore o di competenze o alla rinuncia del servizio stesso, ma può essere resa possibile dall'evoluzione delle attività attraverso approcci nuovi, digitali, remoti capaci di aiutare ad ottimizzare i processi e monitorare i risultati.
Ci siamo così domandati se i nostri Security Operation Centers (SOC) non potessero diventare degli "hub di innovazione"; centri non solo di monitoraggio di eventi e situazioni di security, ma anche luoghi dove garantire il continuo corretto funzionamento degli impianti nonché la gestione complessiva di strutture ed infrastrutture. Una delle nostre risposte è stata la *Remote Maintenance*. Grazie alla ricerca e sviluppo effettuata negli ultimi anni, grazie al mix di competenze tecniche sui sistemi di security tradizionali, competenze IT e competenze di *data science*, nonché attraverso la costruzione nel tempo di una complessa infrastruttura di rete basata sul cloud e sui più moderni standard di sicurezza internazionale,

abbiamo realizzato un modello che consente di garantire lo svolgimento delle attività di manutenzione ordinaria dei sistemi di antintrusione e videosorveglianza anche da remoto attraverso i SOC.

**Cosa è la Remote Maintenance, come funziona?**

La RM *(Remote Maintenance)* è più comunemente conosciuta in campo software come RMM (Remote Maintenance Monitoring) o più recentemente *Smart Maintenance*, e consiste nella capacità di stabilire una connessione con apparati e sistemi, fornendo un servizio di assistenza diretto e veloce, risolvendo molti problemi facilmente, senza attese né spostamenti, tramite la connessione on-line. Attraverso operazioni studiate dal nostro team di tecnici, abbiamo creato un modello, costituito da una serie di test e operazioni, applicabile ad esempio agli impianti di anti-intrusione e videosorveglianza coerentemente con quanto stabilito dalle norme CEI 79-3 e CEI EN 62676, comportando benefici che spaziano dall'ottimizzazione degli investimenti, alla riduzione della mobilità, alla gestione più efficace delle attività. La *Remote Maintenance* è possibile grazie all'utilizzo presso i nostri SOC di piattaforme PSIM ed un mix di competenze tecniche evolute di security tradizionali e competenze IT, sfruttando i collegamenti dei sistemi utili per il monitoraggio dei siti anche per svolgere test e operazioni di ripristino sugli impianti, nonché tutte quelle operazioni necessarie per garantirne il corretto funzionamento nel tempo.

Questo modello ci consente, dunque, di razionalizzare la mobilità alle sole operazioni realmente necessarie, oltre che effettuare un più costante e continuo monitoraggio del funzionamento degli apparati, offrendo, secondo la nostra visione, un grande vantaggio potenziale alle aziende, estendibile a molte altre tecnologie, apparati e sistemi. Offre anche un primo importante passo verso la remotizzazione di attività spesso a basso valore aggiunto, valorizzando altresì nel contempo le competenze on-site dei tecnici sempre più qualificati e non schiacciati in una logica di costi ma di valore.

**Cosa serve per avviare un servizio di manutenzione remota?**

Chiaramente è sempre importante effettuare uno studio di fattibilità delle operazioni, nonché un'analisi sugli apparati di security in uso e sui modelli di connessione. Come anticipato, abbiamo sviluppato il modello a partire da competenze di security tradizionali che ci consentono di conoscere dettagliatamente le logiche alla base del funzionamento di impianti e sistemi. Per sviluppare questo percorso, inoltre

è sempre necessario partire dall'organizzazione dei dati e delle informazioni, non sempre agevole, dei clienti secondo un modello standardizzato. È importante sottolineare, infatti, che la *Remote Maintenance* non è un'idea replicabile tout court ma un modello che necessita di competenze, di data analysis preventive e di un percorso rivolto all'innovazione complessiva della gestione tradizionale della sicurezza che mette al centro della questione dati e connettività.

La *Remote Maintenance*, infatti, non dipende dalle tecnologie tanto quanto dalla loro conoscenza, dalla capacità di trasmissione di dati delle stesse nonché dalla capacità di organizzazione delle informazioni e gestione delle attività. Secursat ha implementato il proprio modello a partire da censimenti, anagrafiche e consistenze ordinate all'interno di un data-set digitale, sempre aggiornato, che consente di conoscere con precisione i dettagli degli impianti e delle tecnologie. In tal senso si è rivelato strategico l'utilizzo della nostra piattaforma di *ticketing in cloud* che ci consente di ordinare le attività, calendarizzare gli interventi necessari e di non lasciarli al caso, di monitorare l'andamento dei lavori, la tipologia di intervento, il rispetto di SLA e KPI contrattuali, nonché di accedere ad una dashboard real-time dove è possibile conoscere i dettagli relativi alle attività di manutenzione individuando situazioni critiche e casi che comportano costi significativi per garantire la sicurezza e la protezione delle persone e dei luoghi.

**Ritenete che questo servizio sia il più innovativo offerto da Secursat?**

Sicuramente la *Remote Maintenance* è una delle nostre risposte alla necessità di portare l'innovazione nel settore della sicurezza, ribaltando il tradizionale approccio che vede l'innovazione associata ad un prodotto nuovo, più performante, più personalizzato e così via, e sciogliendo, in parte, quel dualismo che vuole la sicurezza fisica e quella informatica due percorsi necessariamente distinti.

Non stiamo parlando di Cyber Security, che necessita di competenze dedicate, stiamo portando avanti l'idea che innovare per Secursat significa sfruttare le competenze IT per cambiare i processi e riuscire a fare cose tradizionali in modo del tutto nuovo e diverso. All'interno della nostra visione, dunque, non si tratta altro che di una naturale conseguenza del processo di digitalizzazione già in atto in tutti gli altri settori e scenari, creando valore nella security, non distruggendo mercato, competenze e professionalità.

**Dal vostro punto di vista, si tratta di una evoluzione necessaria nel settore della security?**

Il mercato odierno, ed ancora una volta ribadiamo nei diversi settori, è sempre più propenso a comprare servizi a prezzi più bassi, con la principale conseguenza della riduzione della qualità del servizio erogato e, talvolta, con la mancata erogazione.

La *Remote Maintenance* si propone dunque come risposta a questa tendenza distruttiva della qualità e del servizio, proponendo un'alternativa valida alle necessità di ottimizzare i costi ed indirizzare gli investimenti verso soluzioni utili al business in generale in un quadro evolutivo di perimetri di competenze e di scenari di crisi.

L'accelerazione dei processi digitali promossa dal Covid-19 nonché il generale cambiamento nelle aspettative e nelle richieste da parte dei clienti, inoltre, impone al settore della sicurezza in generale lo sviluppo di nuovi approcci e modelli basati su soluzioni digitali, cloud, algoritmi e modelli di Machine Learning, tutte soluzioni che comportano come condizione *sine qua non* dati ed informazioni puntuali, coerenti ed aggiornati.

Lo sviluppo di un modello basato sulla manutenzione remota consente di avviare un percorso verso la standardizzazione dei dati e delle informazioni e porre, dunque, le basi per lo sviluppo di nuovi modelli tecnologici, con l'unico obiettivo di creare valore in un difficile percorso identitario della security oggi minacciato da modelli di business quantitativi e non qualitativi.

SECURSAT
Build your security

Contatti:
Secursat
Tel. +39 0141 33000
www.secur-sat.com

# Da Alesys i software di centralizzazione user friendly

*Intervista a Alessandro Ferrari, CEO di Alesys*

**Ci può parlare di Alesys e della sua storia?**
Alesys nasce nel 2003 come società di consulenza per lo sviluppo di software personalizzati, che la portano a collaborare con alcune aziende del settore della sicurezza. Sono gli anni in cui si inizia a parlare, anche nel nostro settore, di IP e iniziano ad affermarsi i primi software per gestione video, tecnologia che si preannunciava pronta a soppiantare tutti gli altri dispositivi.
Nei primi due anni di attività, mi resi conto della necessità di trovare una soluzione semplice per la gestione unificata di tutti i sistemi di sicurezza e non solo per il video, che aveva raggiunto già importanti traguardi.
L'idea fu quella di virtualizzare i pannelli sinottici che, seppur ormai obsoleti, erano ancora molto utilizzati. Un software incentrato sulle mappe interattive era la soluzione.
Il nostro giovane team di sviluppo (all'epoca nessuno di noi aveva raggiunto i 30 anni) iniziò a lavorare all'idea, arrivando nel 2007 alla prima versione stabile del prodotto la cui compatibilità era ridotta però a pochi dispositivi. Inizialmente, la parte più complicata è stata proprio convincere i produttori a rilasciare gli strumenti per l'integrazione, che era vista con un po' di distacco. Per fortuna, oggi, la situazione è molto diversa e la collaborazione con i vari brand è fondamentale.
A distanza di tanti anni, la tecnologia e gli scenari sono molto cambiati e Alesys, attraverso continui investimenti in ricerca e sviluppo, non ha mai smesso di seguire l'innovazione e le sempre più crescenti esigenze del mercato.
Nell'ultimo anno, Alesys ha inoltre deciso di presentarsi con un look rinnovato e una nuova organizzazione per supportare al meglio il partner nelle fasi di analisi e proposizione.

**In che modo riportate nei vostri software l'idea "user friendly"?**
In tutti i progetti che seguiamo mettiamo sempre al primo posto l'utente che, nella maggior parte delle occasioni, non è una figura tecnica. Questo significa gestire un allarme in modo rapido e con una procedura omogenea per tutti i sottosistemi, in modo totalmente trasparente per l'operatore.
In secondo luogo, si cerca di agevolare il lavoro dell'installatore o del manutentore.
Interfacce semplici e guidate permettono di avere una maggiore produttività e una rapida curva di apprendimento dell'utilizzo del software. Questo significa che il partner può gestire in autonomia le soluzioni con un risparmio notevole a livello di "total cost of ownership".
Il punto chiave è di rendere l'utilizzo e l'aspetto del programma il più possibile simile a concetti ed esperienze note all'utente, risultando così ergonomico.

In un'ottica di miglioramento ed evoluzione degli sviluppi è estremamente importante il feedback dei clienti e dei partner perché l'operatività e le esigenze del campo sono diverse da quelle degli ambienti di test. Una cosa da evitare è proprio l'aggiunta di funzioni che appagano più il team di sviluppo rispetto all'utilizzatore. Spesso gli utenti subiscono strumenti non ottimali perché "se è così ci sarà un motivo a me sconosciuto".

**La "nuova normalità" attribuisce un ruolo determinante alle piattaforme di gestione di sistemi da remoto. Cosa proponete ai vostri mercati verticali di riferimento?**
La "nuova normalità" ha velocizzato un processo già iniziato grazie all'evoluzione delle tecnologie e della velocità delle reti. La supervisione remota multi-sito è sempre più richiesta in tutti gli scenari, non solo di vigilanza. La velocità delle reti geografiche permette ormai di avere un numero di flussi video consultabili dall'operatore come se fosse sul sito locale. Questa condizione permette un'operabilità con la stessa esperienza "utente locale".
La remotizzazione degli allarmi non è l'unico scenario in cui la supervisione può essere applicata. Le nostre soluzioni sono utilizzate, molto spesso, anche nella sicurezza di edifici o di campus dove la dimensione o la rapidità di intervento sono molto importanti.
Pensiamo, ad esempio, ad un centro commerciale o ad un campus industriale: l'identificazione di un allarme, magari incendio, deve permettere un intervento rapido e mirato per non creare panico o interruzioni importanti di servizio. Sia da remoto che in locale, una nuova tendenza è poi quella legata alle funzionalità di conteggio degli accessi: nato inizialmente per un utilizzo prettamente statistico in ambito marketing e commerciale, oggi è molto richiesto in ambito safety per la regolamentazione delle presenze attraverso semafori o pannello sinottico così come presente nel nostro software Enumero.

**Come interagite con i vostri partner nel percorso di integrazione sempre più spinta di questo periodo?**
L'integrazione ha raggiunto livelli inimmaginabili fino a qualche tempo fa, non solo in termine di prodotti e sistemi ma anche di procedure e sinergie tra le figure aziendali. La migrazione verso un mondo sempre più su IP impone la collaborazione tra le figure deputate alla security e gli IT manager. Questo scenario presenta nuove sfide per lo specialista di sicurezza come, ad esempio, la gestione della cyber security.
La sicurezza, l'integrità del dato e gli scenari di rete complessa sono ormai una richiesta ricorrente da parte degli utenti. Oltre ad un focus di sviluppo rispetto agli standard di sicurezza, è importante fornire un servizio di consulenza che possa aiutare l'interazione tra i dipartimenti.
La soluzione, quindi, per una reale e proficua collaborazione, è quella di supportare il partner in tutte le fasi di prevendita e progettazione, in modo da rispondere alle richieste e i desiderata del cliente finale. Un altro aspetto importante è la continua formazione dei nostri partner.
La formazione è fondamentale e viene erogata in diverse modalità: dai corsi alla fornitura licenze ad uso interno, che il partner può utilizzare per sperimentare o testare le funzionalità del sistema.
Dall'altro lato, la partnership con i produttori rappresenta un punto chiave per una soluzione di integrazione come la nostra. La conoscenza dei prodotti gestiti ci permette di aiutare l'installatore a risolvere le possibili problematiche attraverso un canale di supporto unico. All'interno del nostro laboratorio, infatti, testiamo ogni prodotto accuratamente prima di integrarlo per comprenderne i punti di forza e le possibilità. Così facendo siamo in grado di rispondere alle necessità del cliente in modo concreto ed esperienziale per accompagnarlo nell'intero processo.
Oltre a ciò, conoscere il prodotto, significa fornire la migliore integrazione in termini di funzionalità e ergonomicità, nostri focus principali da sempre.

ALESYS
SECURITY MADE SIMPLE

Contatti:
Alesys
Tel. +39 0331 219436
www.alesys.it

# La Fondazione Enzo Hruby protegge a Genova i capolavori di “Michelangelo. Divino artista” e gli accessi del Teatro della Gioventù

*a cura della Redazione*

Nell’ambito del proprio impegno per sostenere la protezione del patrimonio culturale italiano e per diffondere la cultura della sicurezza, la **Fondazione Enzo Hruby** interviene ogni anno in tutto il Paese con progetti destinati alla messa in sicurezza di importanti beni e monumenti - sia i più celebri al mondo, sia quelli destinati al patrimonio cosiddetto “minore” - per proteggerli contro furti, sottrazioni, vandalismi e danneggiamenti. Inoltre, è oggi attiva anche per rispondere alle nuove esigenze di sicurezza emerse durante l’emergenza sanitaria, ovvero la necessità di dotare i luoghi della cultura di sistemi che possano tutelare la salute dei visitatori e del personale, consentendo la continuità delle attività dei singoli enti.

Due importanti progetti ci portano a Genova, dove la Fondazione Enzo Hruby ha già sostenuto negli scorsi anni la protezione della Lanterna, dei Musei di Strada Nuova e del Museo Luxoro.

I nuovi progetti sono dedicati l’uno alla mostra ***Michelangelo. Divino artista*** al Palazzo Ducale e l’altro al **Teatro della Gioventù**, che è stato ad ottobre la sede principale del Paganini Genova Festival.

La mostra *Michelangelo. Divino artista* - realizzata dall’Associazione Culturale MetaMorfosi, con la quale la Fondazione Hruby prosegue una proficua collaborazione avviata ormai da molti anni – mette in scena nell’Appartamento del Doge e nella Cappella Dogale di Palazzo Ducale l’arte più grande di tutti i tempi e la coniuga alle moderne tecnologie di sicurezza utilizzate per la protezione puntuale di alcuni dei capolavori esposti. I sensori installati nell’ambito di questo progetto sono attivi durante le visite del pubblico, ma non solo. A mostra chiusa rappresentano un secondo livello di protezione specifico a implementazione di quello del Museo. Le teche espositive sono inoltre protette da rivelatori in grado di segnalare urti o aperture indesiderate, attraverso sensori a effetto tenda in grado di allertare il servizio di guardia in caso di avvicinamenti eccessivi all’opera. Questo progetto, oltre ad offrire adeguata protezione ai capolavori in mostra, rappresenta anche uno stimolo per comunicare le importanti possibilità che oggi la tecnologia offre per la sicurezza delle opere esposte nei musei, nelle chiese e ovunque sia richiesta una protezione costante e sempre attiva contro episodi criminosi e danni accidentali.

L’intervento destinato al Teatro della Gioventù ha anch’esso la finalità di offrire una protezione costante e sempre attiva, in questo caso destinata a tutelare non le opere d’arte ma la salute delle persone attraverso appositi termoscanner installati all’ingresso del Teatro. Questi dispositivi hanno permesso per tutta la durata del Paganini Genova Festival di rilevare la temperatura corporea, impedendo l’accesso in caso di temperatura superiore a 37.5 gradi e nel caso in cui la mascherina non fosse correttamente indossata dall’utente. Questi progetti mettono bene in evidenza che la tecnologia oggi offre risorse davvero importanti e facilmente accessibili che consentono di proteggere in maniera costante e sempre attiva i beni del nostro patrimonio culturale contro i principali rischi a cui sono quotidianamente esposti. Queste risorse consentono al tempo stesso di tutelare i luoghi della cultura.

FONDAZIONE ENZO HRUBY

Contatti:
Fondazione Enzo Hruby
info@fondazionehruby.org
www.fondazionehruby.org

# Iniziano i preparativi per SICUREZZA 2021, l'edizione della "nuova normalità"

*intervista a Paolo Pizzocaro, Fiera Milano - Exhibition Director SICUREZZA*

**Siamo ad un anno da SICUREZZA 2021, che potrebbe essere il primo evento settoriale di respiro internazionale in Europa dall'inizio della pandemia. Un'opportunità importante per Fiera Milano ma anche molte responsabilità in più. Come avete adeguato l'organizzazione delle manifestazioni in presenza del Quartiere per garantire la sicurezza del pubblico e degli espositori?**

Grazie alla collaborazione con un team di esperti e in sinergia con i principali players del settore, Fiera Milano si è dotata di un "Protocollo per il contenimento della diffusione del nuovo coronavirus" che traccia linee guida concrete che ritroveremo in occasione di SICUREZZA 2021, anche se, naturalmente, ogni decisione sarà subordinata alla curva della situazione pandemica e alle relative disposizioni governative di quel momento.

È previsto il controllo della temperatura all'ingresso, l'utilizzo obbligatorio delle mascherine e i gel igienizzanti saranno disponibili in tutto il quartiere, ma a garantire la sicurezza di espositori e visitatori saranno anche le tecnologie e la digitalizzazione.

In particolare, sarà ulteriormente incentivata la preregistrazione online, eliminando assembramenti alle casse e passaggio di biglietti cartacei. Grande supporto verrà poi dal digital signage: ledwall ad alta risoluzione consentiranno una informazione immediata in tutto il quartiere, indicando, per esempio, quali ingressi usare o quali padiglioni in un determinato momento sono troppo affollati. Una heatmap permetterà infatti la geolocalizzazione, monitorando flussi e percorsi e garantendo il distanziamento.

Infine, attraverso la nuova App di quartiere si potrà usufruire di nuovi servizi digitali, come la prenotazione online dei parcheggi o del pasto.

**In generale, quali sono le evoluzioni del modello delle fiere B2B, ora più che mai importanti per il rilancio dei settori rappresentati?**

Può sembrare strano, ma la situazione che stiamo vivendo ha in un certo senso aumentato, anche in ambito B2B, il desiderio di incontrarsi e confrontarsi "in presenza". In mercati in continua evoluzione, come è quello di SICUREZZA, emerge il bisogno di una piattaforma di confronto, soprattutto in questo momento in cui tutti cercano di capire dove sia meglio andare. Se è vero che abbiamo ormai capito la capacità abilitante del digitale, è anche vero che stiamo andando nella direzione di un approccio "Phygital", in cui fisico e digitale convivono. Ecco perché il contesto fieristico può rappresentare un valore aggiunto, che si tratti di confrontarsi sulle urgenze di un comparto o di lanciare un nuovo prodotto.

**La "nuova normalità" ha fatto comprendere al mercato come know-how, tecnologie e servizi, sviluppati in origine per la sicurezza da azioni dolose (security), siano in realtà determinanti anche per la tutela dell'integrità e la salute delle persone (safety e health). Come verrà affrontato a SICUREZZA 2021 questo tema, che apre scenari ancora più importanti per la filiera?**

In questi mesi diverse tecnologie di security hanno dimostrato il loro ruolo "abilitante". Penso ai termoscanner, ai sistemi di rilevazione della temperatura, ma anche al controllo accessi integrato con la video per la verifica del corretto utilizzo della mascherina o alle porte automatiche con ingresso touchless, che riducono il rischio di contaminazione delle superfici.

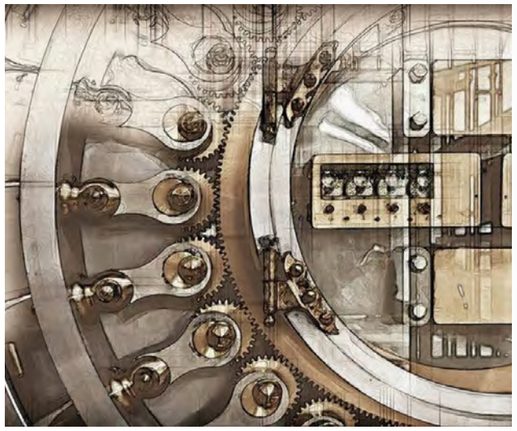
Una indubbia opportunità per il settore, che mi auguro possa anche oggi avvantaggiarsi di una maggiore consapevolezza dell'importanza della prevenzione e del costo della non sicurezza. Ma dobbiamo tener anche ben presente il monito di diverse associazioni di settore: là dove c'è tanta domanda, c'è il rischio di una moltiplicazione dell'offerta, che può purtroppo penalizzare la qualità e innescare una battaglia dei prezzi che non fa bene a nessuno.


Per questo, durante SICUREZZA ancora una volta daremo ampio spazio al tema della professionalità e della certificazione. Perché, se la moltiplicazione dei contesti di utilizzo è una occasione da cogliere, va regolamentata e vanno definiti gli standard che garantiscono l'affidabilità delle soluzioni applicate.

# Anima Sicurezza qualifica i Tecnici manutentori di casseforti

*a cura della Redazione*

**Anima Sicurezza**, l'associazione che rappresenta le aziende produttrici e manutentrici di sistemi di sicurezza passiva (casseforti, porte e camere corazzate, serrature meccaniche ed elettroniche, ecc), ha istituito un corso di formazione per manutentori sulle normative che regolamentano la sicurezza passiva. Il corso consente l'accesso all'esame tenuto da **ICIM** per la certificazione delle competenze. **Fabio Podda**, vice presidente di Anima Sicurezza, spiega per essecome i contenuti del progetto:



Le casseforti sono l'ultimo baluardo a difesa dei valori contro i furti o gli accessi indebiti a documenti riservati. La loro efficienza è parte integrante del rispettivo grado di sicurezza e, pertanto, deve essere mantenuta sempre al massimo livello anche a garanzia di una corretta interpretazione assicurativa.
Le manutenzioni periodiche e gli interventi tecnici devono essere condotti da personale qualificato che garantisca il mantenimento di tutte le caratteristiche fisiche e funzionali al livello originale.

Il **Tecnico di Casseforti** è la figura professionale che opera nel settore della sicurezza passiva. Svolge attività di installazione, attivazione e la manutenzione di casseforti sia domestiche che professionali.
Il tecnico abilitato è un professionista preparato sia sul piano tecnico sia sul piano degli aspetti relazionali, consapevole della delicatezza del suo ruolo, fatto di riservatezza, responsabilità e rispettosa comunicazione con il cliente.

**Anima Sicurezza**, tramite un forte impegno di tutti gli associati e con il contributo delle case costruttrici aderenti, ha dato vita ad un progetto per qualificare e certificare i tecnici di manutenzione casseforti e serrature a livello nazionale. Ha istituito pertanto un corso specifico di formazione e di aggiornamento tecnico e pratico dei manutentori, nonché sulle norme in vigore che regolamentano la sicurezza passiva. Il corso fornisce loro i requisiti per sottoporsi all'esame teorico e pratico redatto e tenuto da **ICIM** come prevede la normativa **UNI EN 11557:2014** per la qualifica e la certificazione.
Per conseguire la certificazione, il tecnico di casseforti professionali deve essere in grado eseguire le attività afferenti la sua professione. Deve dimostrare di avere una buona conoscenza ed esperienza riguardanti l'installazione, la progettazione e la risoluzione di anomalie complesse riguardanti i congegni del mezzoforte.
Il candidato sostiene un esame scritto preparato da ICIM nell'ambito del quale deve dimostrare di avere una buona conoscenza di programmazione di dispositivi elettronici, di avere nozioni di elettromeccanica applicate a mezziforti di custodia e versamento (tipo casse continue) e degli aspetti normativi.

Deve inoltre dimostrare di essere in grado di eseguire attività complesse legate a questa professione, dimostrando di avere esperienza maturata a seguito di prolungato esercizio delle funzioni, di essere preposto ad attività di alta specializzazione con particolare preparazione e capacità, di vantare capacità di coordinamento dell'attività ai fini dello sviluppo e della realizzazione degli obiettivi aziendali. E' prevista anche una prova pratica su casseforti professionali di vari gradi di sicurezza fornite dai costruttori. Nella prova viene richiesto di risolvere problematiche riguardanti serrature, riferme e relativi blocchi passivi.

Certificare i tecnici è un valore aggiunto, erano figure alle quali non veniva riconosciuta una competenza specifica, ma venivano identificate genericamente come "fabbri". Anima Sicurezza ha sempre creduto nella loro qualificazione. Molto utile ed importante è l'aspetto dell'etica professionale. Attraverso la qualificazione e la conseguente certificazione si instaura con il cliente un rapporto di fiducia. In questo senso occorre colmare il perdurare del vuoto di informazione. Il cliente non sa che ci sono aziende che gestiscono la manutenzione delle casseforti e serrature con tecnici qualificati e certificati.

Oggi, grazie al lavoro di Anima Sicurezza si è giunti con ICIM alla definizione di uno schema di certificazione in quanto si è finalmente ravvisata la necessità di far qualificare il servizio di "serraturiere" da un ente indipendente secondo standard elevati che tenessero conto delle procedure di lavoro, dell'adeguatezza delle attrezzature e della qualità dell'assistenza al cliente. Il lavoro mira a certificare le competenze dei professionisti (serraturieri e tecnici di casseforti), ai quali si richiede una qualifica certificata per garantire la sicurezza dei beni (security) e della persona (safety).
La richiesta di maggiore sicurezza arriva, oggi, dall'utenza domestica, dalle aziende, da Enti ed Istituzioni. Si allarga anche l'esigenza di competenze specifiche, ovvero di professionisti che siano in grado di consigliare, caso per caso, quali soluzioni adottare dal punto di vista tecnico ed economico.

ICIM, ha ottenuto l'accreditamento per la certificazione dei serraturieri e dei tecnici di casseforti. È il primo organismo di certificazione italiano accreditato da Accredia (Ente Italiano di Accreditamento) secondo la UNI 11557, una delle norme sviluppate in base alla legge 4/2013 per disciplinare le figure professionali non regolamentate, ovvero i moltissimi professionisti per i quali non esistono albi o collegi e che non hanno un riconoscimento a livello legislativo.

I nominativi dei Tecnici di Casseforti certificati sono presenti nelle liste presenti nei siti **ICIM, Anima Sicurezza** e **Accredia**.

Consultando e scegliendo nelle liste dei nominativi dei Tecnici di Casseforti certificati, il cliente ha la certezza di tutela, sicuro di poter rivolgersi a esperti competenti e preparati nell'applicazione civile e industriale di serrature e mezzi forti, nel rispetto del codice etico e del principio di riservatezza.

ANIMA sicurezza
SOLUZIONI E SERVIZI PER LA CUSTODIA DI BENI E VALORI

# Venitem Action, i professionisti della sicurezza incontrano l'eccellenza nel design e nella tecnologia

*intervista a Giuseppe Manente, General Manager di Venitem*

**Venitem Action** si è tenuta il 24-25 settembre scorsi presso la sede Venitem. Dalla presentazione della nuova sirena da incasso, ad un programma interamente dedicato al business degli installatori di sistemi di sicurezza, **Venitem Action** è stato un momento davvero memorabile per la storia del settore security. Il primo evento organizzato direttamente da Venitem per gli installatori, per proporre una soluzione che riesca a svoltare l'intera filiera in Italia. Venitem, da decenni protagonista nella produzione di sirene di allarme contraddistinte da design inimitabile e una tecnologia imbattibile, si è posta in prima persona per portare avanti un ambizioso programma, dapprima sposato da molti importanti distributori di sicurezza e ora da molti professionisti del settore.

**Possiamo introdurre Venitem parlando dei numeri di un'eccellenza italiana nel design e nella tecnologia?**
Alla fine del 2019 Venitem aveva venduto oltre 4 milioni di sirene d'allarme, tra furto e incendio, innumerevoli alimentatori e relè. Senza contare tutti i prodotti accessori al nostro core business, ma che da anni Venitem ha deciso di offrire ai propri clienti per dare una soluzione completa, "protetta" da un marchio riconosciuto e stimato nel mercato.
Abbiamo chiuso l'anno con grandi soddisfazioni, e con l'apertura di molti progetti interessanti, sia per nuovi design che per l'innovazione di prodotto, per rendere la sirena Venitem non solo la più venduta ma anche la più innovativa in Europa.

**Come sta reagendo il vostro mercato dopo il lock-down?**
In generale l'economia ha conosciuto una flessione importante negli ultimi mesi; aziende e attività di piccole dimensioni han chiuso, e in alcuni casi, anche realtà più strutturate hanno dovuto rivedere il loro business.
Il settore security, soprattutto per quelle aziende che hanno potuto continuare anche solo parzialmente la loro attività, non è stato tra i più colpiti da questa crisi. In alcuni casi, è stata un'occasione per studiare le reali necessità del mercato e convertire il proprio business per soddisfarle.
Nel caso di Venitem, abbiamo deciso  a ridosso della chiusura dello scorso marzo di analizzare quali reali soluzioni avremmo potuto offrire per la pandemia, pur continuando a servire al meglio la nostra abituale clientela diretta.



È così che sono nati **i DPA, i Dispositivi di Prevenzione Automatici**, una nuova categoria di prodotti realizzata ad hoc per ottemperare alle misure di protezione e rendere automatici i processi di prevenzione nelle attività commerciali, aziende e enti.
Si tratta di dispositivi ottici e vocali programmabili e attivi, in grado di interagire in maniera diretta con l'utenza per automatizzare le misure di prevenzione dettate dal Governo. Per questo progetto, abbiamo attivato i nostri ingegneri e il nostro comparto tecnico (che ancora una volta si è dimostrato all'altezza delle aspettative: reattivo e professionale) per portare a termine il progetto nel giro di poche settimane.


**Come è andato l'incontro con gli installatori dello scorso 24 e 25 Settembre?**
È stata un'esperienza davvero interessante, perché abbiamo avuto l'opportunità di incontrare personalmente molti professionisti che quotidianamente lavorano con i nostri prodotti. Un'occasione unica per aprire le porte della nostra azienda e aprire un dibattito sul miglioramento generale della filiera produttore - distributore - installatore - utente. Già da tempo abbiamo deciso di lavorare in prima persona per proporre delle attività (concernenti le vendite ed anche il processo di marketing, oltre che la specializzazione e la formazione) volte ad incentivare una crescita nel settore.
Un progetto ambizioso e che ci impegna davvero molto, ma che ci sta dando ottimi frutti e molte soddisfazioni. Il Venitem Action è stato un momento di formazione e informazione davvero importante, che ci ha consentito di presentare la nostra soluzione ed il nostro progetto di impegno attivo.


**Quali sono i progetti per il 2021?**
Dopo il successo di Giudecca (**www.sirenaincassata.it**), la sirena incassata lanciata quest'anno ma che ci apre già delle ottime prospettive per il futuro, per il 2021 abbiamo in serbo molti progetti riguardanti non solo nuove tecnologie e nuovi design, ma anche soluzioni per implementare alcuni processi che potrebbero agevolare gli acquisti e rendere più snelle le procedure.

Ricordo che Venitem è un'azienda che da anni lavora con prodotto pronto a magazzino, con tempi di consegna e di gestione davvero rapidi. Ci piacerebbe estendere questo modo di operare a tutti i livelli, aumentando anche la presenza con i nostri clienti diretti e non.
Ci auguriamo che le condizioni sanitarie del Paese migliorino per poter operare a 360 gradi nel mercato e con i nostri clienti.
Senza dubbio, visto il protrarsi della pandemia e vista l'efficacia di questo tipo di prodotti, continueremo ad essere presenti nel mercato con i DPA (**www.prevenzioneautomatica.it**), al fine di sostenere tutti quegli imprenditori e aziende che necessitano di un supporto pratico e accessibile per il rispetto delle normative in tema di prevenzione.

# ProSYS™ Plus: il nuovo sistema super ibrido di RISCO Group

*a cura della Redazione*

**RISCO Group** presenta la nuova versione super ibrida di **ProSYS™Plus**, il sistema di sicurezza con video verifica visiva, abilitata da sensori radio da interno e da esterno con fotocamera integrata, e tastiera touch screen.
La centrale ProSYS™Plus costituisce il cuore del sistema ed è ora ancora più potente e flessibile delle versioni precedenti grazie a un'avanzata capacità di soddisfare ogni esigenza installativa combinando sensori radio, cablati e accessoristica Bus. Le tre modalità di connessione, infatti, possono coesistere senza limiti offrendo la massima flessibilità per ogni tipo di configurazione.
Oltre al **nuovo contenitore in policarbonato** per installazioni Grado 3, ProSYS™Plus si contraddistingue per la **nuova tastiera touch screen RisControl** che abilita un'esperienza d'uso senza paragoni: grazie a un'interfaccia intuitiva, che utilizza icone simili a quelle di uno smartphone, l'utente ha la possibilità di controllare lo stato del sistema, inserire o disinserire l'allarme e accedere a video live o alle registrazioni delle telecamere IP VUpoint in tutta semplicità.
Inoltre, RisControl offre una visualizzazione personalizzabile con accesso rapido alle funzioni più utilizzate ed è integrata nel Cloud di RISCO.
A breve, la tastiera consentirà anche di includere il campanello elettronico con telecamera Doorbell, per permettere all'utente di beneficiare del pieno controllo della propria abitazione o del proprio ufficio, ovunque si trovi, e di interagire con l'ospite.
Progettata per grandi installazioni commerciali fino a 512 zone, ProSYS™Plus è una soluzione estremamente flessibile che ben si adatta anche a strutture residenziali, offrendo elevati livelli di sicurezza grazie alla conformità agli standard di Grado 3.
In aggiunta alla video verifica abilitata da VUpoint con telecamere IP, la nuova soluzione di RISCO offre anche **verifica visiva** dell'allarme in tempo reale, grazie a sensori radio da interno e da esterno con fotocamera integrata.


I sensori **eyeWAVE™** da interno e **Beyond DT** da esterno possono ora essere implementati anche su ProSYS™Plus grazie all'utilizzo della **nuova espansione radio dotata di canale video**: al momento del verificarsi di un evento, immagini in alta definizione e a colori o brevi clip video vengono trasmesse direttamente sullo smartphone dell'utente finale o alla vigilanza, insieme alla notifica push.
La funzionalità di video verifica, con fotocamere o telecamere, permette quindi di verificare in tempo reale la causa dell'allarme per poter agire di conseguenza e in modo tempestivo.
ProSYS™Plus è in grado di supportare le più avanzate tecnologie di comunicazione disponibili – tra cui multi-socket IP, 3G e WiFi – per poter configurare più canali contemporaneamente. Si tratta di un requisito fondamentale per assicurare la massima ridondanza e resilienza nel sistema di comunicazione.
ProSYS™Plus può essere controllata, configurata e gestita dal collaudato Software di Configurazione (CS). Questo consente agli installatori di configurare e gestire da remoto le installazioni di sistemi RISCO Group, compiere operazioni automatizzate su gruppi selezionabili di centrali e molto altro.

Contatti:
RISCO Group
Tel. +39 02 66590054
www.riscogroup.it

# Hanwha Techwin presenta le telecamere Wisenet X PTZ PLUS

*a cura della Redazione*

Tracking basato sull'intelligenza artificiale, controllo PTZ preciso, precisione preset migliorata, illuminazione IR adattiva e sicurezza informatica avanzata sono solo alcune delle molte innovazioni integrate nelle nuove telecamere **Wisenet X PTZ PLUS** lanciate da **Hanwha Techwin**.
Progettate per la protezione perimetrale e per applicazioni in grandi spazi aperti come aeroporti, parcheggi, aree industriali, stadi e centri cittadini, le nuove telecamere da 2 MP, 6 MP e 4 K Wisenet X PTZ PLUS sono in grado di catturare immagini a una distanza di 200 metri indipendentemente dalle condizioni di illuminazione, grazie anche alla tecnologia IR adattiva che regola l'angolo dei LED IR della telecamera in modo che corrisponda al livello di zoom.


**Il chipset Wisenet7**

Il cuore delle nuove telecamere Wisenet X PTZ PLUS è **Wisenet7**, l'innovativo chipset proprietario di Hanwha Techwin che offre un insieme di tecnologie che migliorano significativamente la sicurezza informatica delle telecamere. Le telecamere possono inoltre contare su di un sistema proprietario di emissione certificati per dispositivi Hanwha Techwin che memorizza certificati unici nei prodotti Wisenet sia durante la fase di sviluppo che durante il processo di produzione.
Wisenet7 permette inoltre di acquisire immagini di altissima qualità con una funzione WDR (Wide Dynamic Range) "avanzata" che utilizza le tecnologie Local Contrast Enhancement e Scene Analysis per catturare immagini ultra-nitide in scene che presentano livelli molto alti ed estremamente bassi di luminosità.

**Auto-tracking**

La funzione di tracking automatico basato su tecnologia AI permette agli operatori di monitorare i movimenti di persone o veicoli senza dover interagire con la telecamera stessa. In pochi click gli operatori possono programmare una telecamera in modo che segua automaticamente i movimenti di un oggetto specifico. Ciò è reso possibile dall'analisi video con deep learning che rileva e classifica persone e veicoli grazie agli algoritmi AI esclusivi di Hanwha Techwin.

**Preset precisi**

Durante il loro ciclo di vita, la maggior parte delle telecamere PTZ eseguiranno panoramiche e inclinazioni varie migliaia di volte e non è inusuale che si verifichino errori di posizionamento. Le telecamere Wisenet PTZ PLUS, che hanno una precisione di posizionamento preset di ± 0.1°, sono in grado di rilevare se non sono puntate esattamente sul campo visivo specificato correggendo di conseguenza la posizione.

**Altre caratteristiche importanti**

• I tergivetro incorporati rimuovono pioggia, nevischio o neve e attivano un riscaldatore sulla lente per asciugare l'acqua residua.
• Un angolo di inclinazione verticale esteso fino a 110° garantisce inoltre un campo di visione molto ampio.
• I miglioramenti nel controllo manuale della funzionalità PTZ rendono molto più semplice per gli operatori eseguire lo zoom manuale per osservare in dettaglio gli oggetti da monitorare e seguirne il movimento.
• Una funzione di salvataggio della messa a fuoco, che può essere applicata a 32 aree predefinite, permette ad una telecamera spostata in una nuova posizione di mettere rapidamente a fuoco l'immagine, indipendentemente dalle condizioni di illuminazione.

**Pensata per gli installatori**

Compatte e circa il 65% più leggere della maggior parte delle dome PTZ, le telecamere Wisenet X PTZ PLUS vengono installate su una piastra di montaggio e possono essere posizionate rapidamente e facilmente allineando i vari componenti sul supporto e fissandoli a incastro garantendo quindi un' elevata ottimizzazione delle attività di installazione.

**Qui sotto sono elencate le nuove telecamere Wisenet PTZ PLUS:**

- Wisenet XNP-9300RW: Telecamera PTZ con zoom ottico 30X 4K
- Wisenet XNP-8300RW: Telecamera PTZ con zoom ottico 30X 6 MP
- Wisenet XNP-6400RW: Telecamera PTZ con zoom ottico 40X 2 MP

*"Stabilire un nuovo standard è una frase piuttosto inflazionata per il lancio di nuovi prodotti, ma credo che la si possa utilizzare davvero parlando di queste nuove telecamere",* ha affermato **Uri Guterman**, Head of Product & Marketing di Hanwha Techwin Europe. *"I nostri eccellenti team di progettazione, sviluppo e produzione hanno messo in campo tutta la loro esperienza e sono riusciti a raggiungere risultati innovativi riguardo la capacità degli utenti di osservare in dettaglio e seguire qualsiasi attività o incidente sospetto con l'auto-tracking".*

Hanwha Techwin Europe

Contatti:
Hanwha Techwin Europe LTD
Tel. +39 02 36572 890
www.hanwha-security.eu/it

## DIAS presenta il nuovo modulo di comunicazione PCS265LTE di PARADOX

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

Il nuovo modulo di comunicazione PCS265LTE/4G/3G/2G di **PARADOX** offerto da **DIAS** consente l'invio dei dati di rapporto GSM e messaggi di testo SMS e, grazie alla connessione al server SWAN, tramite l'applicazione Insite GOLD permette il monitoraggio e il controllo della centrale, del controllo accesso e di automazione, e la ricezione delle notifiche push.
L'applicazione è disponibile per Android e iOS. PCS265LTE è equipaggiato con processore **Quectel EC21**, una serie di moduli LTE di categoria 1 ottimizzati appositamente per applicazioni M2M e IoT.
Questa tecnologia di connettività LTE è conveniente e a basso consumo e offre velocità di trasmissione dati massime fino a 10 Mbps in downlink e 5 Mbps in uplink. Queste caratteristiche rendono EC21 una soluzione ideale per numerose applicazioni IoT, che non dipendono dalla connettività ad alta velocità ma richiedono comunque la longevità e l'affidabilità delle reti LTE.

**Caratteristiche**

- Velocità di comunicazione LTE/4G (3.75G)/3G/2G
- Connessione automatica 3G/2G se 4G non è disponibile
- Due schede NanoSIM supportano la ridondanza del provider
- Connessione automatica a SWAN per l'utilizzo dell'app Insite GOLD
- Inserimento e disinserimento del sistema anche tramite SMS
- Notifica push dall'App Insite GOLD con gestione veloce e sicura della centrale
- La batteria agli ioni di litio (opzionale) consente il funzionamento in caso di mancanza dell'alimentazione
- Connessione RS-485 tramite il modulo CVT485 per l'installazione remota
- Segnalazione perdita connessione centrale
- Comunicazione crittografata (128 bit)
- Contatto anti-manomissione e anti-rimozione
- Compatibile con le serie EVO, Spectra SP, MG5000, MG5050 e MG5075

## Novità per il modulo telecamera VXI-CMOD di OPTEX

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


Tra i prodotti di punta del catalogo **HESA**, merita una menzione speciale **VXI-CMOD** di **OPTEX**, distribuito da HESA insieme a tutta la gamma del produttore leader mondiale nella sicurezza antintrusione.
**VXI-CMOD** è un modulo telecamera Wi-Fi facilmente integrabile con il sensore **VX Infinity (VXI)**, grazie al quale il rivelatore apprezzato per l'affidabilità e le eccezionali prestazioni può giovarsi della funzione di video verifica: con estrema facilità i professionisti della sicurezza possono così aggiornare tutti i rivelatori VXI cablati già installati, aggiungendogli un modulo telecamera con angolazione panoramica a 180 gradi e visione notturna HD 1080p.
Quando il sensore VXI rileva un intruso, viene attivato VXI-CMOD: quest'ultimo registra l'evento e manda un avviso a uno o più smartphone abbinati del proprietario (iOS o Android). L'avviso è prodotto tramite l'App OPTEX Vision e può essere ricevuto da più utenti in contemporanea. Attraverso l'app, gli utenti possono accedere in ogni momento alla visualizzazione e alla registrazione audio in diretta.
Un'interessante novità che da oggi arricchisce le prestazioni di VXI-CMOD è la possibilità di registrare il flusso video proveniente dal modulo telecamera su NVR e, dunque, di integrare il prodotto agli impianti TVCC.
Questo consente al modulo di operare non solo autonomamente ma anche nell'ambito di sistemi di sicurezza più ampi, offrendo grandi vantaggi nelle varie installazioni.





## Inim Home P2P rende disponibile su smartphone la gestione dei sistemi Inim

INIM ELECTRONICS S.R.L.
(+39) 0735 705007
www.inim.biz


Inim Home app


Inim home P2P app

Da oggi l'App **Inim Home** diventa anche P2P per la gestione remota dal tuo smartphone dei sistemi **SmartLiving, Prime e Sol di Inim**.
**Inim Home P2P** permette il collegamento alle centrali mediante connessione diretta Peer-To-Peer ed è anche disponibile la versione **Inim Home** che può interfacciarsi al **Cloud INIM** per un'esperienza utente più ampia e completa.
Puoi controllare a distanza casa e ufficio impartendo comandi antintrusione e domotici comodamente dal tuo dispositivo mobile, in qualsiasi momento e ovunque ti trovi. Con la sua grafica accattivante, Inim Home supporta tutte le dimensioni dei display ed ha un'interfaccia con icone, semplici ed intuitive.
Con pochi tocchi hai la possibilità di inserire, disinserire o parzializzare l'impianto antintrusione, accedere agli scenari, verificare lo stato di sensori, uscite ed eventuali guasti del sistema, leggere il registro eventi; puoi azionare condizionatori, irrigatori, luci, tapparelle e molto altro.
Inim Home offre anche la funzione cronotermostato per regolare il clima in diversi ambienti.
É disponibile anche l'interazione con telecamere per una videoverifica real-time: Inim Home permette di associare una o più telecamere ad una zona e mostrare sullo smartphone il video real-time delle telecamere attivate in caso di allarme di quella zona.
Se vengono impiegate telecamere con standard ONVIF, è possibile controllarne i movimenti e lo zoom ed è possibile la visione multipla e simultanea di più telecamere.

## MACS FENCES, la recinzione 4.0

NUOVA DEFIM S.P.A.
(+39) 031 33521
www.nuovadefim.com

L'intelligenza artificiale applicata ai sistemi di recinzione perimetrale è a portata di mano: la soluzione sviluppata da **Nuova Defim Orsogril**, insieme al partner tecnologico **TSec**, è innovativa e decisamente smart.
**MACS Fences** (MEMS-based anticlimbing system), integrato con le recinzioni prodotte da **Nuova Defim Orsogril**, rileva in maniera puntuale i tentativi di effrazione e scavalcamento, discriminando con grande precisione eventi naturali o accidentali.
Grazie alla facilità di installazione e alla possibilità di monitoraggio da remoto, è un importante passo avanti verso la ricerca di soluzioni efficaci per la sicurezza perimetrale.
MACS è una tecnologia unica che reinterpreta gli acceleratori MEMS già presenti negli smartphone, in chiave di sicurezza. Grazie a speciali algoritmi elaborati appositamente per i modelli della linea **Recintha** e per le recinzioni in grigliato, è un sistema affidabile perché identifica in modo univoco ciascun sensore, fornendo una precisa indicazione del punto in allarme.
Il sistema MACS è veloce e flessibile, due caratteristiche che lo rendono adatto all'integrazione con sistemi di allarme già presenti. Gli sviluppi futuri saranno garantiti da aggiornamenti firmware.
Il sistema si compone di una catena di sensori ed un master. La catena è precablata e composta da 120 sensori. L'installazione avviene lungo la recinzione, fino a coprire un perimetro massimo di 1,2 chilometri per singolo master.

essecome ONLINE

**n. 7/2020**
Anno XXXX
Periodico fondato da Paolo Tura

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

**HANNO COLLABORATO A QUESTO NUMERO**
Maurizio Callegari, Angelo Carpani,
Nils Friedrik Fazzini

**SEGRETERIA DI REDAZIONE**
redazione@securindex.com

**PUBBLICITÀ E ABBONAMENTI**
marketing@securindex.com

**EDITORE**
essecome editore srls
Milano - Via Montegani, 23
Tel. +39 02 3675 7931

**REGISTRAZIONE**
Tribunale di Milano n. 21 del 31 gennaio 2018

**GRAFICA/IMPAGINAZIONE**
Lilian Visintainer Pinheiro
lilian@lilastudio.it