

essecome

ONLINE
02/21



Periodico digitale di informazione di security & safety

2021 - ANNO XLI



securindex formazione



I CORSI DI SECURINDEX FORMAZIONE

securindex formazione si rivolge ai professionisti della sicurezza che operano nelle aree:

TECNICA



VIGILANZA PRIVATA



COMMERCIALE / DIREZIONALE



proponendo per ogni area percorsi a livello **BASE** e **AVANZATO** per lo sviluppo delle competenze professionali, con il contributo di docenti di comprovata conoscenza delle materie trattate.

- I corsi sono strutturati in lezioni erogate a distanza (FAD) in modalità sincrona e vengono organizzati in sessioni **OPEN** a calendario e in sessioni **RISERVATE** a richiesta.
- Ogni partecipante deve essere dotato di adeguata attrezzatura audio/video e di connessione ad Internet.
- I partecipanti possono scegliere se frequentare consecutivamente tutte le lezioni del corso prescelto nella stessa sessione, oppure se distribuirle su due o più sessioni **senza maggiorazione della quota di partecipazione**.
- Nei corsi di Area Tecnica è possibile partecipare a lezioni singole
- Ai partecipanti che hanno completato il corso prescelto o frequentato lezioni singole, viene rilasciato un **Attestato di Partecipazione** che consente, quando previsto, l'ammissione agli esami per l'ottenimento della certificazione delle competenze presso gli Enti di Certificazione che hanno qualificato il percorso formativo, ovvero per l'ottenimento di crediti formativi.
- **E' richiesta l'iscrizione entro 8 giorni dalla data di inizio del corso con versamento anticipato dell'intera quota del corso, comprensiva di IVA.**
- **securindex formazione** si riserva di confermare il corso entro 3 giorni dalla data di inizio. In caso di conferma emetterà fattura al soggetto fiscale indicato dal partecipante; in caso di annullamento restituirà l'intero importo ricevuto

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

- 05 Videosorveglianza, riconoscimento facciale e cybersecurity, che sia l'ora della consapevolezza?
- 06 SFR&L 2021, la sicurezza delle cose nella nuova normalità - Informazione e formazione per tutelare operatori e merci
- 08 SFR&L 2021, la sicurezza delle Cose nella nuova normalità - L'importanza strategica per il Paese della legalità nella logistica
- 10 SFR&L 2021, la sicurezza delle Cose nella nuova normalità - Autotrasporti, si devono combattere le tariffe criminogene
- 12 SFRL&L 2021, la sicurezza delle Cose nella nuova normalità - Le società di sicurezza a fianco degli operatori della logistica
- 14 SFR&L 2021, la sicurezza delle Cose nella nuova normalità - Come cambia la domanda di sicurezza nello store
- 16 Cashless e normativa antiriciclaggio: il trasporto valori ad un bivio epocale
- 17 Il nuovo ruolo del CIT - 1. Innovazione tecnologica e riorganizzazione aziendale per cogliere le nuove opportunità
- 19 Il nuovo ruolo del CIT - 2. Un futuro di compliance antiriciclaggio, riduzione delle imprese, evoluzione digitale
- 20 Ricerca accademica, relazioni istituzionali e formazione: i cardini della mission di GRALE per la compliance antiriciclaggio
- 22 Tutelare le imprese sane nei periodi di crisi. La collaborazione tra banche e trasporto valori
- 24 Antiriciclaggio, il ruolo centrale dei soggetti non finanziari gestori del contante
- 26 Riciclaggio, su 120 miliardi di operazioni illecite all'anno il 10% è in contanti
- 27 Compliance antiriciclaggio e riduzione del contante, sfide e opportunità per il sistema del trasporto valori
- 29 Business Unit Safe Storage di Gunnebo Italia: Una presenza attiva sul territorio nazionale per aggiungere valore al business dei clienti
- 32 RISCO GROUP, un partner di riferimento affidabile per le società di vigilanza
- 34 Arriva in Italia AddSecure, leader europeo nelle soluzioni IoT per la sicurezza delle comunicazioni e dei dati critici
- 36 DEKRA Italia entra nella security con la certificazione di aziende e figure professionali
- 38 Intelligenza artificiale per le smart city
- 40 La Guida ELAN ai cavi sicurezza e alla Normativa CPR
- 44 Hanwha Techwin lancia una nuova gamma di NVR per applicazioni con telecamere AI Deep Learning
- 46 Cybersecurity e privacy by design dei produttori, consapevolezza degli utenti finali: i punti chiave di Genetec contro le minacce informatiche
- Redazionali Tecnologie 48 - 49



Inim Online Training. Il tuo allenamento settimanale sui sistemi intrusione e incendio Inim.



Dai primi di marzo, parte Inim Online Training: la nuova sessione di webinar per scoprire tutto sui sistemi intrusione e incendio Inim. Con la possibilità di curiosare anche tra i reparti aziendali di produzione, ricerca e sviluppo. Tre livelli di preparazione differenti (base, intermedio, avanzato) per una palestra formativa gratuita, dedicata ad installatori e progettisti Inim. E a chi vuole diventarlo. Un appuntamento settimanale imperdibile, dalle ore 16.00 alle ore 18.00. Pronto alla sfida? Inquadra il QR code e iscriviti ai webinar.

L'editoriale del direttore



Videosorveglianza, riconoscimento facciale e cybersecurity, che sia l'ora della consapevolezza?

Fin dall'inizio della pandemia nel 2020, era stata prevista un'impennata degli attacchi ai sistemi informatici delle organizzazioni, costrette a far lavorare da casa i propri dipendenti con i dispositivi personali connessi alle reti aziendali.

Puntualmente, si sono spalancate praterie per tutti i corsari del web, dalle bande a caccia di riscatti agli hacker in cerca di scalpi illustri, dal momento che erano ben poche le strutture preparate ad affrontare una situazione simile

perché, come tutti sanno, la sicurezza costa, rallenta i processi, richiede impegno e "tanto, a noi non succede".

Tra quelli colpiti e chi ha visto colpire il vicino, il lato positivo di quest'altro genere di pandemia è stato l'aumento della consapevolezza di essere tutti esposti ai rischi cibernetici, anche perché il primo passo per proteggere le aziende è stata la formazione accelerata sulle cose da fare e da non fare quando si usano pc e tablet personali per lavorare da casa. Adesso, sarebbe utile che il secondo passo fosse una maggiore attenzione verso l'ambiente in cui viviamo, sempre più imbottito di oggetti connessi e, quindi, esposti alle minacce informatiche attraverso i rispettivi indirizzi IP.

Ad esempio, quanti sanno che i dispositivi domotici che rendono più comoda la vita in casa possono diventare altrettanti comodi "cavallini di troia" per spiare le nostre abitudini, per mettere fuori uso l'antifurto o, magari, per arrivare al tablet con il quale (anche) lavoriamo, se non sono stati progettati e messi in servizio in modo da offrire almeno un livello minimo di sicurezza?

E nel momento in cui anche l'opinione pubblica sembra stia comprendendo quanto siano pericolose per la privacy le tecnologie per il riconoscimento facciale, quanti sanno che, se i sistemi di videosorveglianza per il controllo degli spazi pubblici, delle infrastrutture critiche, degli obiettivi sensibili non sono sicuri, qualcuno potrebbe attaccarli per dirottare le immagini per cercare chi gli interessa con un bel software di analisi video, in diretta o in differita a proprio piacimento?

All'inizio del 2021, il Consiglio d'Europa ha (finalmente) adottato delle linee guida che dovrebbero regolamentare il riconoscimento facciale ([leggi la newsletter del Garante Privacy](#)), rivolte ai governi, alle amministrazioni pubbliche e private ed ai loro fornitori. Nelle intenzioni degli estensori, queste linee dovrebbero orientare l'utilizzo delle tecnologie nel rispetto dei diritti civili, regolandone l'impiego in base ai principi della necessità e della proporzionalità.

Questo è bene, ma si deve sperare che, quando si passerà dalle linee guida ai regolamenti attuativi, i normatori europei e nazionali si ricordino del problema della sicurezza delle telecamere, per evitare di rendere drammaticamente inutile tutto il lavoro fatto per tutelare la libertà delle persone.

In altre parole, sarebbe meglio accertarsi che la casa abbia il tetto prima di chiudere la porta.



SFR&L 2021, la sicurezza delle Cose nella nuova normalità - Informazione e formazione per tutelare operatori e merci

intervista a Franco Fantozzi, Responsabile del Gruppo di Lavoro per l'Italia di TAPA - Consulente senior di security - Professore associato Università Cattolica Sacro Cuore Milano

Durante il ciclo di tavole rotonde "SFR&L 2021" di cui lei è stato coordinatore scientifico, è emerso a più riprese il problema delle responsabilità dei committenti in relazione alle tariffe al massimo ribasso che, in determinate circostanze, possono risultare "criminogene" anche sul piano della sicurezza fisica dei lavoratori. Dal suo punto di osservazione di rappresentante di TAPA in Italia, come valuta la situazione?

Innanzitutto ringrazio per l'opportunità fornita dalle tavole rotonde di sollevare l'attenzione da parte dei principali attori della filiera della logistica su tematiche riguardanti la sicurezza fisica. Dal punto di vista dell'osservatorio qualificato fornito da TAPA mediante il ricorso ad una banca dati alimentata dai principali operatori, dalle imprese manifatturiere e dalle Forze dell'Ordine emerge, con evidenza, il continuo incremento di episodi criminosi in danno degli autotrasportatori e degli hub logistici che, anche recentemente, hanno mostrato carenze notevoli dal punto di vista dell'adeguata verifica dei fornitori.

Affidarsi a fornitori che, rinunciando talvolta al possesso di adeguate competenze e conoscenze, pur di ottenere il servizio ricorrono al massimo ribasso, si è rivelata quasi sempre una scelta inadeguata che ha posto il datore di lavoro ed il security manager in grandi difficoltà, senza escludere il fatto che spesso emergono vere e proprie mancanze di conformità rispetto alle normative, con conseguenze civili e penali.

Una inadeguata e incompleta verifica dei fornitori in fase pre-contrattuale risulta essere spesso l'ostacolo maggiore per il raggiungimento di una supply chain security efficiente e conforme a leggi e regolamenti.

Cosa si potrebbe fare per migliorare la situazione? E' possibile/auspicabile pensare ad interventi normativi da parte delle Autorità tutorie?

Sicuramente da parte del datore di lavoro - e del security manager che deve sostenerlo in questa opera - servirebbe maggiore senso di consapevolezza e maggiore senso di responsabilità per andare verso l'adozione di standard di sicurezza che contemperino misure di sicurezza attiva e passiva adeguate e soprattutto, un modello di governance e di compliance virtuoso ed efficiente.

Anche le Autorità competenti potrebbero certamente predisporre disposizioni e regolamenti che si affianchino agli standard che al momento, non essendo norme cogenti, lasciano al senso di responsabilità della committenza la decisione sul merito.

Qual è la situazione in termini di procedure e di formazione degli operatori?

A mio avviso, c'è ancora molto da fare in questo ambito. La formazione e l'informazione degli operatori deve essere sempre più dettagliata e non generalista e deve consentire agli operatori di avere un quadro il più possibile esaustivo in termini di norme, procedure e modalità operative.



Sicuramente, anche nel settore delle procedure si può intervenire al fine di essere sempre più conformi ed allineati per la tutela degli operatori.

Da questo punto di vista può essere certamente di aiuto il fare ricorso ad istituti di formazione qualificati e certificati.

Quale potrebbe essere il ruolo degli operatori della filiera della sicurezza, in uno scenario di partecipazione con gli operatori della supply chain?

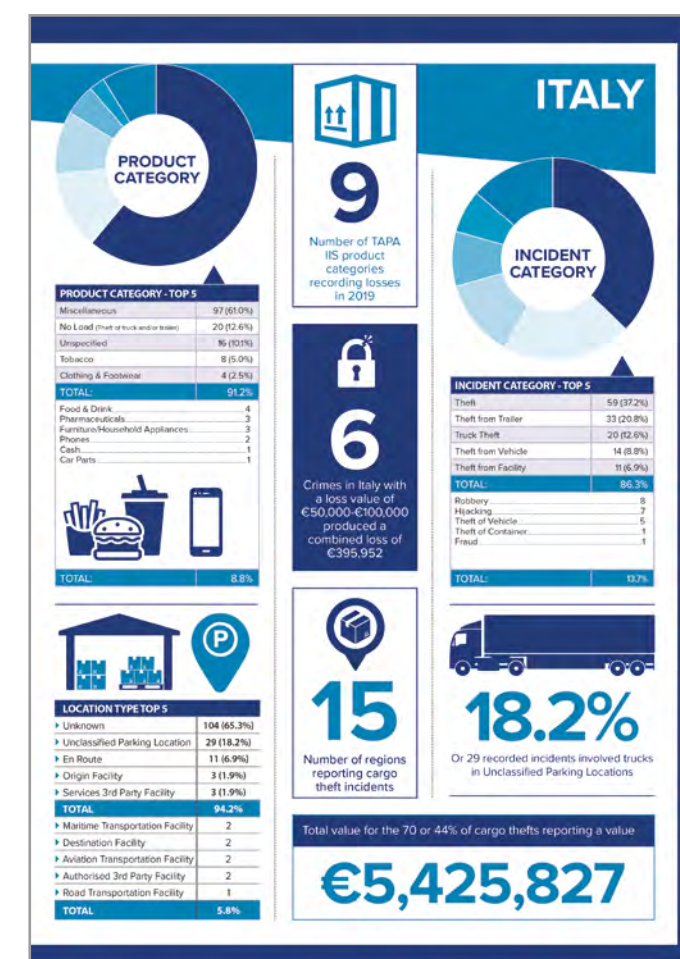
La gestione della supply chain riguarda diverse attività logistiche delle aziende, con l'obiettivo di controllare le prestazioni e migliorarne l'efficienza.

La "supply chain security" e, in genere, l'attività di sicurezza è collegata a molti altri aspetti della gestione del business. Nel settore della logistica, dello stoccaggio e del trasporto delle merci, la sicurezza e l'integrità dei beni dev'essere mantenuta per tutta la catena di approvvigionamento, al fine di soddisfare gli obiettivi di business e garantire la fornitura di prodotti di qualità ai consumatori.

Al fine di garantire che prodotti di qualità superiore siano consegnati ai consumatori, devono pertanto essere attuati severi controlli in ogni punto della catena distributiva.

Ridurre al minimo i rischi per le attività ed i processi logistici richiede un diligente ed efficace coordinamento. I security managers devono essere come detto qualificati ed adeguatamente formati per gestire al meglio la supply chain e le esigenze di protezione e tutela dei beni.

Combinando le persone giuste, processi e tecnologia e con un equilibrato sistema di sicurezza caratterizzato da supervisione e responsabilità, si garantisce che l'efficienza e l'efficacia non sia mai compromessa.



Estratto da Cargo Theft Analysis 2019 - TAPA

SFR&L 2021, la sicurezza delle Cose nella nuova normalità - L'importanza strategica per il Paese della legalità nella logistica

intervista a Massimo Marciani, Presidente del Freight Leaders Council

Durante il ciclo di tavole rotonde “SFR&L 2021” è emerso a più riprese il problema delle responsabilità dei committenti in relazione alle tariffe al massimo ribasso che, in determinate circostanze, possono risultare “criminogene” anche sul piano della sicurezza fisica dei lavoratori. Dal suo punto di osservazione di Presidente di un organismo come Freight Leaders Council, come valuta la situazione?

Il tema della correlazione fra basse tariffe per l'esecuzione di un servizio che possono risultare addirittura “criminogene” e il settore della logistica, potrebbe apparire strano a chi non si occupa tutti i giorni – sul campo – di queste tematiche e quindi potrebbe chiedersi se non sia pleonastico riaffermare la centralità del concetto di legalità. La legalità non dovrebbe essere infatti il prerequisito di base di ogni impresa in ogni filiera produttiva?

In realtà, purtroppo, in alcuni settori della nostra economia come l'agricoltura, l'edilizia ed anche la logistica, ci sono delle situazioni che necessitano di un supplemento di attenzione non solo da parte di tutti gli attori chiave del settore – Freight Leaders Council incluso – ma soprattutto da parte dei decisori politici. Una volta per tutte.

Il Freight Leaders Council ha come propria mission dar valore al sistema logistico: se questo settore non è guidato dai presupposti della legalità e del valore, allora la concorrenza diventa sleale, diventa un duello tra chi rispetta la legge e segue le normative e chi invece non le segue e si ritaglia in questo modo un'indebita condizione di vantaggio, praticando tariffe più basse per i propri servizi e quindi mettendo fuori mercato chi invece – come tutti dovremmo fare – rispetta la legge e le regole che ci siamo dati come comunità.



Se concordiamo sul fatto che la logistica è un settore strategico sul quale stiamo tutti lavorando per fare in modo di portare valore al suo interno, con un conseguente accrescimento di valore economico, non solo facciamo del bene a chi ci lavora ma, allo stesso tempo, evidenziamo un problema: dove si spostano i soldi, si spostano anche criminalità e infiltrazioni mafiose ed in prospettiva con “Next Generation UE” ancor di più dobbiamo essere in grado di attivare al meglio tutte le componenti dello Stato preposte al controllo, monitoraggio e verifica.

Un'altra caratteristica specifica della logistica è costituita dall'elevata intensità di manodopera. Questo dato porta ad avere necessità di capitali freschi e di conseguenza attira l'attenzione della malavita che dispone di ingenti quantità di denaro da riciclare.

Cosa si potrebbe fare per migliorare la situazione? È possibile/auspicabile pensare ad interventi normativi da parte delle Autorità tutorie?

Questa è una domanda molto delicata che richiede una risposta attenta per non urtare le diverse sensibilità degli attori coinvolti. Il primo elemento, a mio avviso, da contrastare in modo diretto ed efficace è il fenomeno del riciclaggio che sta investendo in modo massiccio questo come altri settori produttivi. Penso alla sanità, all'Ho.Re.Ca. e all'edilizia.

Il secondo elemento critico è l'elusione fiscale, che può essere declinato in diversi modi. Uno riguarda in particolare i mancati versamenti dell'IVA anche se la fatturazione elettronica può essere considerata un primo passo verso la via della regolarizzazione.

Il terzo elemento riguarda il caporalato. In questo settore, come nell'edilizia e nell'agricoltura, c'è una presenza evidente di caporalato, in alcuni casi basato anche su radici etniche, fenomeno tipico di tutti quei processi in cui si fa largo utilizzo di manodopera poco specializzata.

Ultimo elemento: nel settore non c'è una corretta applicazione del CCNL (Contratto Collettivo Nazionale del Lavoro). Capita spesso (come da rapporto del Ministero del Welfare 2020) che i lavoratori non vengano pagati adeguatamente rispetto alla loro mansione, in modo particolare per la catena di appalti e subappalti dove vengono rilevate irregolarità a seguito dei controlli dei soggetti pubblici incaricati di svolgere il monitoraggio.

Ritengo che ci sia una forte necessità di delegificare nel nostro Paese: aggiungere controlli su controlli genera uno stato di polizia che frena l'imprenditoria e la produttività. Meglio invece introdurre processi che trovino due soggetti contigui nella stessa catena del valore, avere interessi opposti e contrastanti in modo da non favorire pratiche irregolari di tipo collusivo.

Direi quindi che c'è necessità di sviluppare un sistema fiscale in cui il vantaggio di una parte coincida con la convenienza dell'altra. Ad esempio, andrebbe valutata con attenzione la possibilità di inserire anche nel settore logistico il cosiddetto *reverse charge* in modo da contenere l'evasione fiscale all'interno di valori fisiologici.

Qual è la situazione in termini di procedure e di formazione degli operatori?

Dobbiamo ancora lavorare molto sulle procedure in grado di garantire il contenimento dei costi del lavoro in modo legale, formando e qualificando al meglio gli addetti del settore. Cominciamo a dire che è necessario sviluppare un inquadramento contrattuale per la logistica rispondente alle necessità del settore con l'introduzione di figure professionali legate alla digitalizzazione e all'impatto tecnologico del settore. Dal momento che il settore si trova in piena fase di rinnovo contrattuale, questi sono due elementi che le parti datoriali e sindacali dovranno prendere in considerazione per poter dare in parte una risposta al tema della legalità e della formazione.

Infatti, se siamo in grado di avviare un processo di formazione in grado di preparare il terreno alla possibilità di impiegare correttamente delle risorse, quel processo deve essere gestito al meglio e quindi questo tema non può restare confinato nel tavolo di contrattazione del CCNL ma deve approdare nell'agenda di chi governa questo Paese. La logistica è un settore considerato, ora ancor di più per via della pandemia, strategico per l'intero Paese, e quindi deve essere inserita nelle strategie che ogni Stato rivendica come elementi propri per poter costruire una politica industriale efficace all'interno di un sistema sempre più globalizzato.

SFR&L 2021, la sicurezza delle Cose nella nuova normalità - Autotrasporti, si devono combattere le tariffe criminogene

intervista ad Alessandro Peron, Segretario Generale FIAP – Federazione Italiana Autotrasportatori Professionali

Durante il ciclo di tavole rotonde “SFR&L 2021” è emerso a più riprese il problema delle responsabilità dei committenti in relazione ai costi del servizio di trasporto al massimo ribasso che, in determinate circostanze, possono risultare “criminogene” anche sul piano della sicurezza fisica dei lavoratori. Dal suo punto di osservazione di Segretario Generale di FIAP come valuta la situazione?

Nel mercato dell'autotrasporto stiamo vivendo, soprattutto in questo ultimo periodo, una rincorsa da parte di molti committenti verso l'acquisizione di servizi di trasporto al minor prezzo. L'utilizzo oramai consueto dei cosiddetti “tender” informativi sta portando a risultati a volte, sinceramente, imbarazzanti.

La volontà è esclusivamente quella ridurre l'impatto economico del costo del trasporto, puntando ad un “risparmio” senza qualsiasi riguardo alla sostenibilità economica del servizio.

Il costo di un servizio di autotrasporto è facilmente calcolabile, dal momento che le voci che lo compongono sono semplici, di facile individuazione e, soprattutto, sono recuperabili tramite il portale del Ministero delle Infrastrutture e Trasporti (scusate, della Mobilità sostenibile...) che, con la pubblicazione dei costi di riferimento, ha reso trasparenti e ben identificabili le componenti che realizzano il costo del servizio.

“Costi di riferimento”, ribadisco, e non valori minimi, ai quali vanno aggiunti i costi “indiretti” di struttura e il margine di guadagno per l'impresa di trasporto.

L'offerta di un servizio di trasporto ad un prezzo inferiore dovrebbe immediatamente far insospettire il committente



perché dietro un valore più basso, come fa giustamente rilevare, e apparentemente più conveniente, potrebbe nascondersi una attività che utilizza pratiche “criminogene”. Come ho letto qualche tempo fa in un articolo scritto da un importante manager della committenza “si investe in marketing, nella qualità del prodotto, nella qualità del packaging e poi si lascia il trasporto ad una azienda magari irregolare che non garantisce i minimi standard di sicurezza nel servizio di trasporto”.

Voglio ricordare che in Italia è vigente una legge che richiama direttamente alla responsabilità il committente, il quale è sempre oggetto di sentenze di condanna in funzione dell'abuso della sua posizione di forza contrattuale.

Cosa si potrebbe fare per migliorare la situazione? È possibile/auspicabile pensare ad interventi normativi da parte delle Autorità tutorie?

Partiamo dall'assunto che la normativa già cogente ha

la necessità di essere applicata con più rigore, e che il ritorno “dei costi di riferimento”, i cui valori minimi possono essere ricondotti al concetto di sicurezza nella circolazione stradale e sociale, contribuirebbe, probabilmente, ad allontanare esercizi di dumping spietati.

Purtroppo, siamo anche coscienti che l'autotrasportatore, in qualsiasi scenario assoggettato al concetto di “libera concorrenza”, viene costantemente richiamato ai tavoli di trattativa da chi “usa” le ruote e non le ha, trovandosi dalla parte debole nella contrattazione.

Sarebbe, quindi, il caso di incrementare i controlli verso chi utilizza servizi “professionali” a prezzi troppo limati. Il ruolo della grande committenza e delle loro associazioni di categoria sarebbe probabilmente strategico e, allo stesso tempo, decisivo per provocare un cambiamento di mentalità.

Si verrebbe a creare una svolta verso una modalità di acquisto di beni e servizi “sostenibile” a 360° e non solo per la parte legata all'ambiente, con un'attenzione ed una valutazione dell'affidabilità del fornitore. L'utilizzo, poi, di un “rating”, come quello calcolabile attraverso il Protocollo TCR - Transport Compliance Rating - curato, gestito e implementato da un Osservatorio costituito dai rappresentanti di committenti appartenenti ad aree produttive e dei servizi differenti ed utilizzatori, potrebbe essere la chiave di volta di un sistema di valutazione sull'affidabilità dell'impresa. Un abbinamento costi / rating potrebbe essere un'ottima spinta verso un mercato più etico.

Qual è la situazione in termini di procedure e di formazione degli operatori?

Un'osservazione puntuale dello scenario rivela che la stragrande maggioranza dei soggetti che comprano, vendono o gestiscono servizi di trasporto hanno una conoscenza definibile, a dir poco, superficiale se non scarsa della normativa e delle implicazioni che tale approccio può comportare. Forse perché manca la concreta percezione di quali siano i rischi e relativi danni, anche solo potenziali, che derivano dall'utilizzo nelle proprie catene di approvvigionamento o di alimentazione del mercato, di vettori non affidabili.

Non a caso, come FIAP, ci siamo molte volte proposti come promotori di analisi di risk assessment, con lo scopo di far comprendere quali siano tali rischi, attribuendogli un peso, un valore. Questo a prescindere dal cosiddetto rischio “reputazionale” che ne potrebbe derivare. E quando si giunge alla valutazione anche di quest'ultimo elemento, in termini di “reputazione del marchio”, sia esso di prodotto ovvero d'impresa, si può comprendere molto bene quanto sia sconsigliato trattare la questione in modo inadeguato. In questo contesto emerge, tra l'altro ed in modo evidente, quanto possa essere importante, in questi “esercizi di valutazione”, il ruolo di una Federazione come FIAP per chi acquista e/o gestisce servizi di trasporto professionale, proprio per l'apporto di conoscenza approfondita della materia che può essere conferito nella valutazione. Un ausilio di conoscenza e contenuti di qualità e professionalità che non può fare altro che contribuire ad evitare effetti e scenari indesiderati.



SFRL&L 2021, la sicurezza delle Cose nella nuova normalità - Le società di sicurezza a fianco degli operatori della logistica

intervista a Marco Stratta, consigliere delegato Cittadini dell'Ordine SpA

Il cambiamento dei flussi delle merci destinate ai consumatori finali, conseguente alla diffusione dell'e-commerce accelerata dalla pandemia, ha modificato schemi e soluzioni per la loro sicurezza fisica. Dal vostro punto di osservazione, quali sono i cambiamenti più rilevanti e quali risposte possono offrire alla catena logistica gli operatori della vigilanza privata?

La pandemia probabilmente non ha ampliato la gamma di merci in circolazione ma, semplicemente, le modalità di acquisto ed i soggetti di destino, mantenendo inalterate le necessità connesse al trasporto e, a parte, alla logistica. La crescita dei volumi è invece una costante da diversi anni.

Le merci a "chilometro 0" sono infatti una bella cosa ma questo può valere per frutta e verdura, mentre tutto il resto deve fare migliaia di miglia per arrivare dal produttore al consumatore. In un mercato globalizzato, dove tutti possono avere tutto, la merce deve essere trasportata in tutto il mondo.

La sicurezza diventa quindi un elemento essenziale del contesto economico e, a riprova di ciò, basta vedere il numero di norme volontarie che si sono sviluppate negli ultimi anni, a partire dalla ISO 31000 sul risk management per passare alla serie 27000 sulla sicurezza delle informazioni e, ovviamente, alla 28000 che definisce il sistema di gestione della security lungo la supply chain di un'organizzazione.

Magazzini, hub, treni, camion, aerei, tutto necessità di essere protetto e controllato perché "contenitore" di una delle prede più ambite nei giorni nostri, i beni di consumo. Immaginiamo per un momento un bilico che trasporta



iPhone12: meriterebbe o no la scorta che si farebbe ad un furgone porta valori o ad un'importante opera d'arte? Alla consapevolezza sulle necessità di sicurezza, si aggiunge l'evoluzione della tecnologia nel campo, appunto, della sicurezza: vigilanza satellitare, app, barriere infrarossi, telecamere termiche, ad alta risoluzione, ecc, ecc. L'elemento tecnologico è ormai fondamentale perché permette di garantire la performance unita ad un contenimento del costo.

Pertanto, le risposte che devono dare gli operatori della vigilanza privata, ma preferisco parlare di operatori di sicurezza, vanno nella direzione di coniugare al meglio la capacità di consulenza specifica con l'offerta tecnologica. Dove per consulenza intendo analisi del rischio, assessment, conoscenza e corretta applicazione di

modelli organizzativi; per tecnologia, intendo una centrale operativa all'avanguardia, operatori preparati e prodotti validi.

Non sempre è una ricetta facile da mettere assieme.

Quali soluzioni offre in particolare il gruppo Cittadini dell'Ordine, che si propone come global service provider per la supply chain con soluzioni integrate di tecnologie e servizi?

Cittadini dell'Ordine, seppur sia il più antico istituto di vigilanza d'Europa, ha una mission rivolta al futuro ed ha scelto già da alcuni anni di dedicare i propri investimenti e le capacità progettuali per affermare la propria vocazione quale global security provider.

Grazie anche ad una serie di acquisizioni mirate, ha implementato fortemente l'elemento tecnologico, strutturando un'area tecnica dedicata all'impiantistica, investendo nella ricerca di nuovi prodotti, ampliando le attività connesse ai sistemi satellitari e ridefinendo le proprie centrali operative.

Il gruppo ha poi una vision europea ed internazionale essendo uno dei pochi se non l'unico operatore italiano ad aver proprie strutture in altri paesi europei e una società di diritto anglosassone che permette l'erogazione di servizi di analisi, verifica e supporto di persone all'estero.

La società ha poi strutturato un budget specificatamente dedicato all'evoluzione professionale dei propri operatori, nella consapevolezza che l'elemento umano è imprescindibile e solo la formazione continua permette di poter erogare un servizio di livello.

Diciamo che Cittadini dell'Ordine ha messo insieme gli ingredienti per una ricetta che può garantire la sicurezza di tutta la catena del prodotto, dalla sua produzione al trasporto, alla logistica.

In relazione alle problematiche di security e di safety legate alle dinamiche degli appalti dei servizi di trasporto nelle diverse fasi della supply chain, lei ha lanciato in occasione di SFR&L 2021 l'idea di riprendere l'esperienza delle Linee Guida per gli appalti dei servizi di sicurezza nel Retail, sviluppate tra le associazioni di utilizzatori e di fornitori di questi servizi. Come si potrebbe attuare questo progetto adattandolo al contesto?

Immaginiamo di entrare in una nuova casa e di ricevere il mazzo di tutte chiavi senza avere indicazioni. Potrebbe essere la trama di un film horror o il fantomatico incubo ricorrente; invece è la realtà di molte aziende o di loro manager che spesso si trovano a confrontarsi con fornitori di categorie particolari, per i quali non è sempre agevole conoscere o reperire regole e riferimenti. Difficile in questi casi qualificare il fornitore e quindi scegliere bene!

L'esperienza ci ha fatto capire che radunare gli stakeholder intorno ad un tavolo (seppur virtuale di questi tempi) permette di conoscersi e di delineare linee guida utili a migliorare le scelte e quindi le performance delle aziende. Nel retail si è fatta questa esperienza e per le aziende ed associazioni che vi hanno partecipato ha portato i suoi frutti.

La conoscenza porta alla competenza e la competenza porta alla capacità, propongo quindi di innescare questo circolo virtuoso anche per le aziende che operano nel contesto della supply chain.

Manager di buona volontà e rappresentanti di categoria di aziende acquirenti e fornitrici che scrivono insieme le best practice.

Il lavoro di base è già fatto, basta adattarlo al contesto ed avremo le "Linee Guida per la scelta degli operatori di sicurezza al servizio della Supply Chain"

SFR&L 2021, la sicurezza delle Cose nella nuova normalità - Come cambia la domanda di sicurezza nello store

intervista a Pietro Tonussi, Segment Specialista at AXIS Communications

Nell'esame dell'evoluzione del canale distributivo a seguito della pandemia siamo partiti dalla richiesta di diverse esperienze d'acquisto da parte dei clienti nei negozi per arrivare ai problemi di sicurezza legati alla proliferazione dei corrieri "last mile". Qual è la vostra interpretazione del nuovo scenario che si è delineato?

La pandemia COVID-19 ha cambiato il nostro modo di vivere, di lavorare e anche di fare acquisti.

A partire dell'anno scorso, infatti, abbiamo notato nel mondo del Retail importanti cambiamenti legati alla pandemia, tra i quali il più rilevante è senza dubbio il drastico incremento dello shopping online. I consumatori sono stati spinti a rivolgersi per i propri acquisti alle piattaforme di e-commerce ancora di più rispetto a quanto facevano abitualmente, portando la logistica a diventare la spina dorsale del comparto.

Per questo motivo, nei mesi scorsi il traffico della logistica è aumentato di oltre il 30%, così come è aumentata anche la necessità di saper gestire scorte, stoccaggio e distribuzione in sicurezza per garantire la capacità di un'azienda di rispondere alle richieste dei propri clienti e favorire i loro acquisti. Conseguentemente si è determinata un'ingente crescita anche nel comparto dei trasporti, in particolare nel segmento dell'ultimo miglio, con una maggiore richiesta di sicurezza in mobilità, anche se in questo ambito non sempre le imprese dispongono dei fondi necessari per investire in tecnologie di alto livello che garantiscano maggiore livello di sicurezza.

In quanto operatori internazionali, state rilevando differenze sostanziali tra quanto sta avvenendo in Italia e negli altri paesi?

Non stiamo rilevando delle differenze sostanziali nei Paesi in cui operiamo conseguenti ai comportamenti dei



consumatori ma, semmai, riscontriamo differenze nelle richieste degli operatori dovute a diverse policy delle aziende del Retail e della supply chain.

Come è stato rimarcato negli incontri del ciclo, le merci sono oggi meno dislocate nei negozi ma sono più presenti nei magazzini della logistica e a bordo degli automezzi che le trasferiscono tra le varie stazioni fino al domicilio del cliente finali, con diverse esigenze di sicurezza. Quali supporti offre AXIS Communications agli operatori della filiera?

I mesi trascorsi sono stati molto difficili per tutti e hanno imposto, soprattutto alle aziende di Retail, di modificare profondamente le proprie abitudini di gestione dei magazzini della logistica, dei punti vendita e delle proprie persone. Non esistono dei supporti standard da fornire agli operatori della filiera, ma in base alle necessità esistono diverse tecnologie.

Per cominciare, è importante sottolineare che con la pandemia è emerso in modo molto chiaro come un Security Manager deve affrontare il proprio lavoro pensando alle esigenze che l'azienda avrà negli anni a venire. Chi si era preparato per tempo scegliendo soluzioni 'a prova di futuro', ha potuto aiutare l'azienda ad adattarsi alle circostanze utilizzando i sistemi già presenti.

Chi non è stato previdente, ha dovuto agire in fretta e non ha potuto riflettere sulle implicazioni a lungo termine delle proprie scelte. La pandemia ci ha insegnato che proteggere gli asset è importantissimo, ma lo è altrettanto garantire la safety di dipendenti e di clienti. È per questo che, quando si parla di tecnologia, dobbiamo pensare a qualcosa di scalabile e integrabile per supportare meglio i nostri interlocutori.

Tutte le aziende hanno magazzini e tutte le aziende hanno punti vendita, al limite virtuali. Questi spazi sono già dotati di soluzioni per la sicurezza che, con poche integrazioni, permetterebbero di garantire il monitoraggio della safety senza intervenire sul sistema hardware già presente.

Da sempre Axis investe in ricerca e sviluppo per garantire le migliori soluzioni per le diverse esigenze sia in ambito Retail così come in quello Logistics.

Safety e Security sono le parole chiave che ci accompagnano e ci accompagneranno nel futuro.

In uno scenario ideale, la prima cosa da fare sarebbe quella di assicurarsi di mettere in sicurezza il personale, diretto e indiretto oltre ai propri clienti. Ad esempio, un sistema per il controllo degli accessi del personale in modalità touchless semplificherebbe il rispetto del distanziamento fisico e l'aumento dei requisiti di igiene.

Inoltre, anche i sistemi per il conteggio delle persone risultano fondamentali per il controllo del flusso sia dei lavoratori sia dei clienti. Impostando le soglie, è possibile gestire quante persone alla volta possono accedere a un determinato spazio.

Rimane tuttavia una questione cruciale per l'intera filiera del Retail: la disponibilità di risorse da investire in

queste tecnologie da parte delle imprese del comparto e dell'effettiva volontà di promuovere questi investimenti.

Come valutate in questa fase in Italia il fenomeno dell'ORC (Organized Retail Crime), ovvero gli attacchi predatori di bande che attaccano la filiera per rubare merci da rivendere su canali alternativi?

Una delle principali sfide per il settore del Retail è quello di prevenire reati nel proprio punto vendita e di gestire le loro conseguenze. Con l'evoluzione del settore è già in atto anche il cambiamento dell'attività criminale. Per stare al passo con questa evoluzione, nel futuro sarà opportuno avere telecamere con soluzioni più intelligenti, magari in quantità minore.

Per ridurre il più possibile il fenomeno dell'ORC sarà necessario fare degli investimenti in questa direzione per avere un sistema di videosorveglianza adeguato, non dimenticando che un sistema di videosorveglianza gioca sempre un ruolo centrale nella loss prevention, sia nei negozi sia durante il trasporto della merce.

Alle telecamere di rete si possono aggiungere ulteriori soluzioni da utilizzare come deterrenti. Ad esempio, si possono adottare soluzioni audio, fondamentali per influenzare il comportamento ed intervenire se e quando necessario, riducendo conseguentemente l'efficacia degli attacchi ORC.

Tuttavia, l'audio non è la sola soluzione. Di fatto, si è recentemente notato che durante la pandemia l'attenzione al cliente è aumentata in modo esponenziale. Essendo quindi i retailer più attenti al cliente, si è evidenziata una riduzione dell'ORC.

Infine, è importante sottolineare che la sorveglianza e la privacy non sono compagni naturali. In Axis, ci impegniamo per fornire ai nostri clienti la guida e gli strumenti migliori per aiutare le persone a rendere sicuri i propri dati video e salvaguardare la privacy. Per questo, incoraggiamo le organizzazioni ad essere consapevoli dei propri obblighi e fare un uso responsabile dei dati raccolti.

Cashless e normativa antiriciclaggio: il trasporto valori ad un bivio epocale

intervista ad Antonio Staino, Presidente di Assovalori

Il ciclo di webinar sulla compliance antiriciclaggio degli operatori non finanziari che gestiscono il contante, ovvero le società di trasporto valori, ha messo in evidenza che il settore sta rispondendo positivamente alle disposizioni sull'antiriciclaggio impegnative tanto sul piano organizzativo che economico, malgrado la pesante contrazione del contante movimentato. Come valuta il quadro attuale di un settore privato chiamato a svolgere un ruolo sussidiario alle Autorità di controllo statali senza alcun riconoscimento economico dal mercato?

Assovalori, nata nel 1978 per volontà dei principali CIT Italiani, è stata parte attiva promuovendo e coordinando il tavolo dei gestori del contante per l'iscrizione obbligatoria all'albo presente in Banca d'Italia, oltre che alla redazione delle linee guida, intravedendo nel ruolo che siamo stati chiamati a ricoprire l'opportunità di un maggiore riconoscimento all'attività svolta. Purtroppo, l'imprevedibile contrazione del contante movimentato causata dalla pandemia Covid-19 in aggiunta alle misure governative per la riduzione del suo utilizzo ("cashless"), ha determinato la riduzione di circa il 40% del fatturato, a fronte della quale si è invece verificato un sensibile aumento dei costi e delle responsabilità, peraltro non riconosciuti dal mercato e dalle istituzioni.

Possiamo stimare l'ammontare complessivo del denaro movimentato dai gestori del contante nel 2019 confrontandolo con i volumi attuali?

Possiamo tranquillamente sostenere che il valore del processato presso le sale conta ha subito la contrazione media di circa il 40% a fronte di un aumento del numero di banconote. Questa ultima considerazione è dettata dalla variazione dei tagli in circolazione, con l'aumento di tagli da € 20 e € 50 e la diminuzione dei tagli da € 100 con la quasi sparizione di tagli apicali (200 e 500) comportando



l'ulteriore aumento di costi sia in termini di ore lavoro che di usura delle macchine di sala conta.

Qual è la visione e quali sono le proposte di Assovalori per il futuro del settore?

Pur comprendendo le ragioni alla base delle azioni intraprese per la riduzione del contante, erroneamente collegato al solo sommerso, si ritiene che la libertà del suo utilizzo debba tenere conto delle esigenze sociali.

Fino a prova contraria, il contante rappresenta uno strumento di pagamento tuttora valido ed il suo contrasto può creare problemi a fasce molto consistenti della popolazione. Di riflesso, ha comportato anche uno stato di sofferenza per il settore, sovrapponendo l'inaspettata contrazione del mercato ai forti investimenti imposti per la compliance antiriciclaggio. Sofferenza che si sta manifestando con l'accelerazione dell'uscita dal mercato degli operatori minori.

Per quanto riguarda infine le società di trasporto valori sprovviste di sala conta, seppur non soggette alla disciplina di Banca d'Italia devono comunque adempiere a quanto previsto dalla normativa 231 in materia di antiriciclaggio, ed Assovalori si sta attivando per fornire loro il supporto e le informazioni necessarie.

Il nuovo ruolo del CIT - 1 Innovazione tecnologica e riorganizzazione aziendale per cogliere le nuove opportunità

intervista a Paolo Spollon, amministratore delegato BMC Battistolli Main Company - Gruppo Battistolli

La normativa antiriciclaggio attribuisce agli operatori del trasporto valori un ruolo centrale nel rilevamento delle operazioni sospette con l'impiego del contante, in un'ottica di sussidiarietà alle Autorità di riferimento. Come sta rispondendo il sistema ad un cambiamento di paradigma sostanziale, anche nei confronti dei committenti?

Mi preme evidenziare che, fino a pochi anni or sono, per poter fare impresa nel mercato del trasporto valori e del trattamento del contante si doveva affrontare una sfida molto impegnativa, rappresentata dalla ricerca dei massimi livelli di integrità, professionalità ed efficienza, il tutto sostenuto da ingenti investimenti economici.

Più di recente, si è aggiunta un'altra sfida non meno impattante, quella di conseguire la conformità alle norme antiriciclaggio per gli "operatori non finanziari gestori del contante" prevista dai D.Lgs 231/2007 e 125/2019 e dai Provvedimenti di Banca d'Italia e, per questi, con particolare riguardo all'obbligo per le aziende del settore di iscrizione all'Elenco dei Gestori del Contante, previsto dal Provvedimento del 23 Aprile 2019.

Si è quindi posto in essere un framework normativo in materia di contrasto al riciclaggio e al finanziamento al terrorismo specificatamente dedicato al nostro settore, di grande impatto sotto il profilo organizzativo e procedurale.

Tra gli adempimenti in carico ai numerosi profili aziendali coinvolti in questa evoluzione, spicca per rilevanza l'obbligo delle segnalazioni di operazioni sospette (cd. S.O.S) previsto dall'art. 22 del Provvedimento Organizzativo emanato da



Banca d'Italia, che fa parte del processo di adozione di norme dedicate agli Istituti di Vigilanza privata.

Un processo che assume particolare importanza, perché siamo ora considerati un anello determinante della catena di controllo in quanto, svolgendo attività di trattamento del denaro (cash management) per conto di più soggetti del comparto finanziario e non, disponiamo di un patrimonio informativo unico in termini di conoscenza di flussi di denaro contante.

Appare in modo inequivoco che ci troviamo di fronte ad un rilevante cambiamento, che sta influenzando fortemente le dinamiche che muovono e muoveranno nel prossimo futuro l'intero comparto del CIT (Cash in Transit).

A mio modesto avviso, d'ora in avanti le nostre aziende, oltre ad impegnarsi costantemente per mantenere intatte

le proprie caratteristiche “genetiche”, dovranno affrontare e soddisfare l’ineluttabile necessità di implementare le proprie capacità organizzative e reattive, per adeguarsi con celerità ai nuovi scenari.

Il tutto rafforzando l’interazione e la collaborazione con la committenza per trovare nuovi equilibri sotto gli aspetti contrattuali, operativi e, non da ultimo, economici, con l’obiettivo di evitare di venire relegati al mero ruolo di soggetti passivi e subalterni, con il risultato finale di rivestire il ruolo di unici destinatari dei costi di questa trasformazione.

La politica “cashless” del governo degli ultimi mesi ha ridotto drasticamente il movimentato. In che modo vi adeguate alla nuova situazione che allinea da una parte l’Italia agli altri paesi dell’Eurozona, dall’altra impone importanti modifiche strutturali alle aziende?

Imputare la riduzione dei flussi di contante esclusivamente alla “war on cash” avviata dal governo precedente mi sembra limitativo. Ritengo che gli vada quanto meno affiancato un altro fattore che, a mio avviso, va ricercato nella crisi economica generata dalla pandemia Covid-19. Inutile negare come sia forte la spinta verso il contactless e la riduzione dell’uso delle banconote e delle monete ma non va dimenticato che l’incremento recente di circa un milione di cittadini che sono purtroppo scesi sotto la soglia di povertà, sommandosi ai circa 3,5 milioni già esistenti, denunci una crisi economica generale che, inevitabilmente, riduce qualsiasi forma di pagamento, in primis quelle in contante. Va infatti ricordato che ci sono innumerevoli soggetti “unbanked”, sprovvisti cioè di un rapporto di

conto corrente con una banca e, ancora, persone che non possono permettersi di perdere il controllo della gestione delle proprie entrate, cosa che può avvenire facilmente con l’uso della moneta di plastica o elettronica.

Tutti questi soggetti ma, più in generale, tutti i cittadini hanno il diritto di poter usare il denaro contante e quanto meno di poter scegliere quale mezzo di pagamento usare. Questo porta a dire che, pur dovendo affrontare una riduzione nell’uso del contante, quest’ultimo continuerà a circolare come riserva di valore, protettore della privacy, garante dell’inclusione finanziaria e rifugio dalle crisi. Dovrà quindi continuare ad esistere un sistema che ne consenta la circolazione effettuando i necessari controlli, per far sì che mai venga meno la fiducia dei cittadini sulla disponibilità e la legalità del denaro pubblico.

Le aziende di CIT non possono che prendere atto di questo processo, predisponendo azioni che passino dalla propria ristrutturazione alla rivisitazione progettuale dei servizi tradizionali già presenti nel carnet delle offerte alla clientela e all’utilizzo di software avanzati per la gestione di servizi innovativi, già sperimentati da aziende del nostro settore in paesi Ue ed extra Ue.

In estrema sintesi, si dovrà promuovere l’utilizzo di suite di tecnologie ancora poco conosciute come, ad esempio, quella che viene genericamente denominata “CashTec”, che può essere utilizzata per semplificare l’utilizzo del contante, abbreviandone il ciclo e riducendone i costi.

Per tutte le parti coinvolte sarebbe quindi preferibile cercare nuove opportunità di business in un mercato dei pagamenti ancora innegabilmente ad alto utilizzo del contante, anziché farsi inutili “guerre” commerciali.

Il nuovo ruolo del CIT - 2

Un futuro di compliance antiriciclaggio, riduzione delle imprese, evoluzione digitale

intervista a Salvatore Fiorentino, Amministratore delegato alla Gestione del Contante – Coopservice scpa

La normativa antiriciclaggio attribuisce agli operatori del trasporto valori un ruolo centrale nel rilevamento delle operazioni sospette con l’impiego del contante, in un’ottica di sussidiarietà alle Autorità di riferimento. Come sta rispondendo il sistema ad un cambiamento di paradigma sostanziale, anche nei confronti dei committenti?

In base alla nostra esperienza, stiamo rilevando che il sistema ha ormai inserito tale attività nel normale processo di acquisizione del Cliente con personale adeguatamente formato in materia e adottando politiche informative continue e costanti sia all’interno (verso il proprio personale) che all’esterno (verso la propria Clientela).

Il supporto di strumenti informatici e il collegamento a banche dati è un altro elemento che agevola l’attività.

Quanto sopra ha imposto importanti investimenti in risorse e strutture tecnologiche e comporta continui costi di mantenimento.

Ricordo infatti che l’attività non si esaurisce quando viene espletata la adeguata verifica della clientela ma la parte più impegnativa sta nel monitoraggio continuo dell’attività, al fine di intercettare le operazioni sospette. Questo aspetto genera delle difficoltà per gli operatori e clienti di minori dimensioni che hanno bisogno di supporto sia operativo che di corretta interpretazione delle norme. Per quest’ultimo aspetto è attivo in modo costante una attività di supporto da parte di Banca D’Italia e delle associazioni di categoria.



La politica “cashless” del governo degli ultimi mesi ha ridotto drasticamente il movimentato. In che modo vi adeguate alla nuova situazione che allinea da una parte l’Italia agli altri paesi dell’Eurozona, dall’altra impone importanti modifiche strutturali alle aziende?

Non credo si possa attribuire, almeno in questo periodo, tutta la responsabilità della drastica riduzione del contante alla politica “cashless” ma piuttosto al risultato tra l’impatto negativo causato dalla pandemia Covid in aggiunta alla politica fatta dal governo contro l’uso del contante.

Il combinato disposto di questi due elementi ha portato la contrazione del ricircolo di contante che per alcuni settori ha superato il 60% con ripercussioni sull’intera filiera sia in termini occupazionali che di fatturato e la situazione non accenna a migliorare. È innegabile che la trasformazione digitale sia un processo inevitabile del nostro futuro ma riteniamo altresì che, essendo il denaro contante l’unico mezzo di pagamento pubblico, non potrà essere completamente eliminato. Sicuramente dovremo rivedere le modalità di erogazione del nostro servizio che immaginiamo vedrà ridursi il numero delle imprese sul mercato e modalità di erogazione del servizio più “snelle” rispetto a quelle attuate oggi.

Ricerca accademica, relazioni istituzionali e formazione: i cardini della mission di GRALE per la compliance antiriciclaggio

intervista al prof. Antonio Pagliano, Presidente di G.R.A.L.E. Spin off - Università della Campania "Luigi Vanvitelli" Servizio "La compliance Antiriciclaggio per gli operatori non finanziari gestori del contante" a cura della Redazione

Qual è la sua valutazione finale sul ciclo di webinar sulla compliance alla normativa anti riciclaggio rivolto agli operatori non finanziari gestori del contante appena concluso, in termini di partecipazione, di relatori che hanno partecipato e di risultati di apprendimento dei partecipanti?

Il ciclo di incontri in materia antiriciclaggio organizzato da essecome-securindex in collaborazione con GRALE e con il patrocinio di Assovalori, ha evidenziato, ancora una volta, la forte necessità che il settore continui nell'opera di sensibilizzazione al tema della compliance. Forte appare l'esigenza di coinvolgere ora anche gli operatori cosiddetti "minori" che rispetto alle grandi società del settore incontrano maggiori difficoltà organizzative.

L'attenzione alla conformazione del proprio assetto organizzativo alla normativa antiriciclaggio è divenuta, negli ultimi due anni, un'esigenza ineludibile anche, e soprattutto, a fronte dell'iscrizione obbligatoria all'elenco dei gestori del contante tenuto dalla Banca d'Italia.

A tal proposito, il tema della formazione ha assunto un ruolo cardine nel predisporre i corretti adempimenti in materia e alla sensibilizzazione di tutti gli attori aziendali coinvolti, al fine di un corretto funzionamento delle strutture societarie. Il dato rilevante emerso dal ciclo di incontri in materia antiriciclaggio è sicuramente rappresentato dalla partecipazione della grande maggioranza degli operatori coinvolti nella gestione del contante e dai risultati ottimali, nel 70% dei casi, in riferimento ai test di apprendimento predisposti al termine del ciclo.



Di sicuro, tali dati risultano confortanti in quanto segnali inequivocabili di un forte interesse, di una costante esigenza di aggiornamento professionale e di una peculiare forma di compartecipazione ai contenuti scientifici veicolati durante i vari webinar.

La massiva partecipazione e il confortante risvolto relativamente all'apprendimento costituiscono certamente un risultato positivo che va ad accrescere l'expertise dei diversi Soggetti – Responsabili, Addetti e Operatori – all'interno di un comparto per il quale è richiesto un sempre più alto grado di esperienza e professionalità.

Quali sono i progetti di GRALE in relazione alla compliance antiriciclaggio per gli operatori del trasporto valori?

Il decreto antiriciclaggio e la normativa secondaria prevedono espressamente la dinamicità e l'aggiornamento delle attività

formative, utili a garantire il corretto funzionamento dei meccanismi di compliance.

GRALE ha già predisposto un progetto di interlocuzione con le Autorità di settore per coadiuvare gli operatori nell'espletamento delle attività di controllo imposte ai Soggetti obbligati.

La formazione rappresenta, in questo panorama, un utile strumento per uniformare le varie linee di business coinvolte nel rischio riciclaggio e di finanziamento del terrorismo.

Come anticipato, con il ciclo di incontri in materia antiriciclaggio, tarato sugli assetti organizzativi regolamentati dalla Banca d'Italia, il trasporto valori sarà oggetto delle future attività istituzionali, di ricerca e formative da parte di GRALE.

Tali attività saranno svolte alla luce dell'esigenza, impellente, di favorire il dialogo tra Autorità e un coordinamento dei sistemi di conformità legale nei settori ultranei al raggio di azione del trattamento delle banconote in euro e afferenti al trasporto valori "puro" che ricadono, comunque, sotto

l'egida di controllo della Guardia di Finanza e del Ministero dell'Economia e delle Finanze.

GRALE ha ritenuto fondamentale, già con il ciclo di incontri in materia antiriciclaggio, sviluppare e favorire momenti di riflessione condivisa tra i diversi attori istituzionali che quotidianamente sono chiamati ad elaborare gli standard normativi e ad assicurarne la corretta osservanza. A tal proposito, il ciclo di incontri organizzato ha visto la partecipazione di rappresentanti della Guardia di Finanza, del Ministero dell'Economia, dell'Università e degli Operatori Gestori del Contante, nella cornice istituzionale e accademica che contraddistingue la mission di GRALE. Le attività formative, svolte e programmate, saranno dunque sempre orientate alla massima partecipazione trasversale, nella consapevolezza di poter consentire, ai Soggetti obbligati, di ricevere risposte certe ai quesiti interpretativi nel tentativo di prevenire distorsioni di sistema e deficit attuativi in grado di arrecare danni all'operatività dei singoli Operatori.

LA COMPLIANCE ANTIRICICLAGGIO PER GLI OPERATORI NON FINANZIARI GESTORI DEL CONTANTE



CICLO DI WEBINAR FORMATIVI CON TEST DI APPRENDIMENTO

A cura di securindex formazione in collaborazione con G.R.A.L.E. Spin Off Research and Consulting con il patrocinio di Assovalori.

Il ciclo completo di 3 webinar con test finale è riconosciuto da ICMQ-CERSA per il rilascio di 8 crediti formativi per:

- professionisti Security certificati UNI 10459
- esperti/auditor/componenti organismo di vigilanza D.lgs 231/01

Tutelare le imprese sane nei periodi di crisi. La collaborazione tra banche e trasporto valori

intervista a Emmanuele Di Fenza, Responsabile Segnalazione Operazioni Sospette Intesa Sanpaolo
Servizio "La compliance Antiriciclaggio per gli operatori non finanziari gestori del contante" a cura della Redazione

Dal suo punto di osservazione di responsabile della segnalazione delle operazioni sospette della più grande banca italiana, quanto incidono pandemia e lockdown sull'arrivo di denaro di provenienza illecita nell'economia reale? Quali sono i settori più esposti?

Reputo che l'immissione del denaro di provenienza illecita nell'economia reale risponda a tre distinte esigenze criminali: il profitto, il lavaggio del denaro sporco e l'interferenza nei mercati e nelle organizzazioni.

Per quanto ovvio, ogni singola attività criminale può essere ricondotta ad una, a due o a tutte le tre finalità.

In ogni caso la costante è data dalla totale assenza di trasparenza.

In estrema sintesi, la compagine criminale, operando all'oscuro o sotto protezione e fruendo dei suoi capitali di provenienza illecita, può puntare, di volta in volta: al proprio arricchimento (*determinando guadagni non necessariamente immediati*); all'allontanamento dei profitti dall'origine illecita (*attività in genere onerosa*); alla turbativa dei mercati o delle organizzazioni (*al fine di determinare condizioni più favorevoli per il futuro*).

Tutti comprendono che qualsiasi difficoltà (ad esempio fallimenti o crisi di liquidità) o brusca evoluzione che si manifesti nello scenario economico (oscillazione dei mercati o riorganizzazioni aziendali in primis) rappresenta, per le imprevedibilità che genera nei confronti dei precedenti equilibri strutturali, un obiettivo vantaggio per favorire l'immissione occulta di denaro di provenienza illecita.

Come si può ricavare dalle sintesi fornite dalle Autorità vigilanti, anche la pandemia Covid sta puntualmente determinando, in uno scenario di crisi epocale, oggettive



e potenziali occasioni di operazioni con regia criminale. Nelle prime fasi, sono stati osservati puntuali e fisiologici casi di indebiti profitti collegati ad imprese operanti nell'offerta e nella distribuzione di prodotti correlati ai nuovi fabbisogni (mascherine, guanti e altri dispositivi), per poi assistere all'accesso indebito ai finanziamenti di Stato per i settori in crisi.

Ciò premesso, appare altresì evidente che non esiste un solo settore di attività che possa essere reputato al riparo dall'aggressione criminale al maturare degli effetti della crisi.

Opinione diffusa è, infatti, che il controllo sulla titolarità effettiva, da parte delle entità tenute al controllo dei mercati, possa risultare cruciale, in questo delicato momento, al fine di contrastare l'acquisizione di settori sani dell'economia fruendo di capitali di provenienza illecita. Su tale direttrice si pone anche l'azione normativa europea ed italiana che prevede l'adozione di un registro pubblico adeguatamente controllato.

Quanto può incidere nel riciclo il denaro contante?

Con riferimento alle operazioni con cui si immette denaro di provenienza illecita nell'economia, la storia delle azioni di contrasto internazionale ha previsto un'iniziale prevalente attenzione dedicata al contante, poi evoluta anche al controllo sui bonifici.

Le attività di controllo su contanti e bonifici hanno generato una corposa "letteratura" in materia di controllo transazionale tramite algoritmi, prevedendo un'analisi oggettiva dell'operazioni correlata agli aspetti soggettivi sia di chi si priva di una somma e sia di chi la percepisce. Fermo restando che le organizzazioni criminali ricorrono ai canali di volta in volta reputati più opportuni prescindendo dalla "letteratura" consolidata, da un lato appare evidente che il contante sia uno strumento ideale per le intrinseche caratteristiche "al portatore" ma, dall'altro, appare altresì evidente che le attuali tecniche di pagamento, tra cui i bonifici stessi, la moneta elettronica, le criptovalute e tanti altri, rappresentino strumenti altrettanto efficaci laddove rientranti in un preordinato schema generatore di opacità. Non vi è infatti organizzazione criminale, dalla più complessa ed evoluta alla più semplice e improvvisata, che non sia consapevole della necessità di aggirare gli strumenti di controllo previsti dalle attuali misure antiriciclaggio.

Per quanto ovvio, quanto più è complessa, potente o

protetta, un'organizzazione sarà maggiormente in grado di fornire strutturate disposizioni ai propri canali al fine di mascherare le operazioni come normali e lecite, non solo in fase di esecuzione ma anche nelle ipotesi di successivi approfondimenti al fine di neutralizzarli o addirittura di evitarli.

Non vi è dunque miglior ricetta per contrastare l'immissione di denaro di provenienza illecita che disporre di competenze, informazioni e strutture organizzative allenate ad operare in maniera lecita e senza pregiudizi tecnici, condividendo le informazioni con altri soggetti (Autorità stesse o aziende tenute al controllo).

Come valuta la relazione operativa tra il sistema bancario e le società di trasporto valori ai fine della rilevazione di operazioni sospette?

La Banca d'Italia ha più volte richiamato i soggetti tenuti all'azione di contrasto al riciclaggio a collaborare tra loro sia quando condividono clienti sia quando partecipano alla medesima operazione.

In tale ottica è più che auspicabile un sano spirito di collaborazione tra le organizzazioni al fine di perseguire il medesimo irrinunciabile obiettivo: la difesa dei mercati dall'inquinamento determinato dai capitali di origine illecita intuitivamente più pericoloso nei momenti di grave crisi.



Antiriciclaggio, il ruolo centrale dei soggetti non finanziari gestori del contante

intervista a Giuseppe Miceli, Ragioneria Territoriale dello Stato di Roma - Ministero dell'Economia e delle Finanze; già Guardia di Finanza
Servizio "La compliance Antiriciclaggio per gli operatori non finanziari gestori del contante" a cura della Redazione*

Compliance a antiriciclaggio: in che modo si dovrebbero/potrebbero sensibilizzare i soggetti non finanziari che possono trovarsi coinvolti anche involontariamente in episodi di riciclaggio, per tutelare se stessi dalle conseguenze sanzionatorie?

Gli "operatori non finanziari" di cui al punto 5 dell'art. 3 del decreto Antiriciclaggio, altrimenti indicati con la locuzione di "service bancari", offrono come noto servizi di trasporto, custodia e trattamento del contante. Pertanto, sono in possesso di un rilevante bagaglio informativo, basti pensare alla esatta conoscenza della dislocazione territoriale di considerevoli quantità di denaro contante. Ritengo, quindi, di primaria rilevanza riuscire a mettere in campo un'attività informativa e, anche, formativa tesa a sensibilizzare tali soggetti in ordine all'importanza del ruolo che sono chiamati a interpretare, nell'ottica della prevenzione e del contrasto al fenomeno del riciclaggio dei proventi illeciti e del finanziamento del terrorismo, nonché alla valorizzazione di quel patrimonio informativo, che risulta particolarmente utile nell'ambito delle attività investigative poste in essere dalle Autorità Antiriciclaggio. In tale ottica, ecco che l'obbligo dei service bancari di effettuare le segnalazioni periodiche AML/CFT assume un significato portante rispetto al più ampio "catalogo" di adempimenti Antiriciclaggio che il Legislatore ha posto a carico di tale categoria di "Soggetti obbligati".



In virtù di quanto qui sinteticamente esposto e per rispondere alla domanda, ecco che si dovrà sensibilizzare maggiormente quel soggetto che, all'interno dell'organizzazione aziendale dei service bancari, è chiamato a svolgere la funzione di responsabile del presidio Antiriciclaggio di cui devono essere dotati tutti i "Soggetti obbligati" per quanto di interesse in questa sede: gli operatori non finanziari.

*Le considerazioni espresse dall'Autore sono espressione del suo pensiero personale e non vincolano in alcun modo la P.A. di appartenenza.

Possiamo fare una sintesi del quadro sanzionatorio che può riguardare gli operatori non finanziari gestori del contante, ovvero le società di trasporto valori, anche in relazione al Dlgs 231/01?

Nei confronti degli operatori non finanziari, si deve evidenziare una distinzione fondamentale che comporta ricadute in termini di competenza dell'attività ispettiva, in ordine al corretto adempimento degli obblighi Antiriciclaggio e, quindi, al potere sanzionatorio che si pone a valle di quella competenza.

Ecco quindi che gli operatori non finanziari iscritti in apposito elenco, ovvero, quei "soggetti che esercitano l'attività di custodia e trasporto di denaro contante e di titoli o valori a mezzo di guardie particolari giurate, in presenza della licenza di cui all'articolo 134 TULPS" risultano essere assoggettati

ai poteri normativi, di controllo e sanzionatori esercitati dalla Banca d'Italia, in qualità di Autorità di vigilanza di settore. Invece gli operatori non finanziari che svolgono trasporto di valori ma non di contante sono assoggettati ai poteri ispettivi e sanzionatori esercitati direttamente dal MEF.

Fatta questa doverosa distinzione, possiamo rilevare che, a fronte di un identico quadro sanzionatorio applicabile alle due tipologie di soggetti, emergono differenze rispetto al procedimento amministrativo sanzionatorio, riconducibili alla differente titolarità del procedimento stesso, che spetta, rispettivamente, alla Banca d'Italia e al MEF.

A fattor comune, va detto che la condanna a sanzioni Antiriciclaggio, anche di natura amministrativa, comporta notevoli implicazioni anche in termini di responsabilità amministrativa degli enti, ai sensi del D.Lgs. 231/2001.



Riciclaggio, su 120 miliardi di operazioni illecite all'anno il 10% è in contanti

intervista al prof. Ranieri Razzante, docente di legislazione antiriciclaggio Università di Bologna - Presidente AIRA - Consulente Commissione Parlamentare Antimafia e del Prefetto Antiracket - Direttore Centro di Ricerca su Sicurezza e Terrorismo
Servizio "La compliance Antiriciclaggio per gli operatori non finanziari gestori del contante" a cura della Redazione

Il riciclaggio implica tautologicamente che il denaro riciclato provenga da azioni illecite. È possibile fare una stima complessiva del fenomeno allo stato attuale?

Il riciclaggio in Italia si stima tra i 100 e 120 miliardi di euro, per lo più attuato nei settori delle imprese e, assai meno, del commercio. Collocherei tra le prime le operazioni societarie, soprattutto se straordinarie (cessioni, fusioni, acquisizioni di partecipazioni); la costituzione di nuove imprese; i salvataggi, soprattutto in epoca di Covid, di imprese in difficoltà. I settori più colpiti sono l'edilizia, l'immobiliare, il nautico, il trattamento dei rifiuti, le energie alternative, l'agroindustriale, i servizi alle imprese.

Ricordiamo che la stima mondiale si attesta intorno al 7%, con i passaggi di denaro tramite le borse che vengono attestati intorno al 50% delle transazioni giornaliere. Le più colpite sono per l'appunto le borse, e poi le banche e gli altri intermediari finanziari.

Non si dimentichi mai - come spesso accade nelle analisi superficiali che si leggono - che il riciclaggio è l'unico reato che "rende" anche tramite operazioni in perdita e, quindi, viene realizzato più agevolmente. L'interesse a riciclare è il placement del denaro sporco, non immediatamente il rendimento, che sta già nell'aver occultato la provenienza delittuosa delle ricchezze.

È possibile stimare la componente sul totale delle operazioni illecite realizzate con denaro contante?

Dai nostri studi, il riciclaggio realizzato con il contante risulta intorno al 10%. Ciò si spiega agevolmente con la accresciuta difficoltà nel trasporto, soprattutto individuale, di grosse quantità di banconote, che sarebbero più facilmente intercettabili. Ciò appare di palmare evidenza.

Il micro-riciclaggio avviene ancora in parte con il contante, soprattutto attraverso "reti" di ristoranti, spacciatori, sale giochi, ovvero attività ove si possa usare il contante per tradizione e per vocazione. Queste ultime non sono, all'evidenza, facilmente accertabili in quanto questa modalità di pagamento, in quelle sedi, è naturale.

Per converso, la criminalizzazione dell'uso del contante in sé sarebbe sbagliata, dato che la maggior parte dei cittadini europei usa il contante in quanto moneta ufficiale.

Compliance antiriciclaggio: in che modo si dovrebbero/potrebbero sensibilizzare i soggetti non finanziari che possono trovarsi coinvolti anche involontariamente in episodi di riciclaggio?

La sensibilizzazione passa attraverso la formazione; una "cultura del controllo" che si utilizza già a presidio dei rischi più tradizionali, mentre quello di riciclaggio viene ancora troppo spesso trascurato.

Senza dire degli investimenti in software e consulenza che, in proporzione, sono ancora scarsi.

Non si capisce come venga dato per "fisiologico" ormai il rischio di evasione fiscale e di reati finanziari, celandosi dietro il fatto che gli intermediari e i liberi professionisti, ad esempio, non abbiano strumenti "investigativi" per rintracciare le movimentazioni anomale. In realtà, con le migliorie alle normative e ai gestionali informatici, si può dire che il livello di analisi pre-investigativa, in particolare da parte delle forze dell'ordine, abbia raggiunto livelli che possono tranquillizzare.



Compliance antiriciclaggio e riduzione del contante, sfide e opportunità per il sistema del trasporto valori

intervista all'avv. Pietro Marzano, avvocato Cassazionista, consulente d'impresa e socio di Grale Spin Off Universitario
Servizio "La compliance Antiriciclaggio per gli operatori non finanziari gestori del contante" a cura della Redazione

È possibile stimare il livello attuale di compliance alla normativa antiriciclaggio presso i soggetti interessati, tenuto conto della sua recente entrata in vigore?

Gli operatori di maggiori dimensioni hanno raggiunto un livello adeguato e consapevole di applicazione della normativa, dotandosi di strumenti informatici opportuni e formando in modo idoneo le figure aziendali interne. Restano ancora delle sacche di resistenza in alcune strutture ma il confronto e la condivisione delle informazioni, ormai obbligatoria, stanno portando ad un complessivo avanzamento del grado di applicazione ed interpretazione delle norme.

Gli operatori minori stanno seguendo un percorso più difficoltoso ma stanno acquisendo maggiore consapevolezza, sforzandosi di adeguare le proprie strutture ad una mole di adempimenti a volte davvero impegnativa.

In generale il sistema è rivoluzionato, in senso positivo, rispetto ad alcuni anni addietro. A questo processo ha contribuito senz'altro la *moral suasion* di Banca d'Italia e la spinta delle associazioni di categoria, che hanno funzionato in modo uniforme da propulsori per le aziende. L'unità delle associazioni e la capacità del sistema di accogliere gli operatori ed accompagnarli nel processo di adeguamento è stato un valore aggiunto molto prezioso.



Quali sono i livelli di awareness sul tema da parte degli Organi di gestione e/o delle proprietà?

I costi per la compliance sono spesso oggetto di preoccupazione per gli stakeholder, azionisti o soci in genere, e per gli organi di gestione. Sembrano "costi improduttivi" da evitare o comprimere. Ma quello che il sistema ha ben compreso è la natura delle norme che rappresentano sia un presidio di legalità imprescindibile ma anche, e soprattutto, una opportunità di maggiore qualificazione del mercato. Se oggi si vuole competere in

questo settore, si deve possedere una efficace gestione del rischio riciclaggio ed un sistema di controlli costante. Asset che aumentano il valore delle aziende in termini di capitale umano e garantiscono la possibilità di restare protagonisti in una fase storica che tende sempre più ad aggregare gli operatori, dando lo scettro a coloro che maggiormente hanno investito nel capitale umano e di conoscenze delle aziende.

Gli impatti organizzativi con i relativi costi per adempiere alla normativa potranno influire, secondo lei, nel processo di riorganizzazione del settore conseguente alla riduzione sistemica del circolante?

La riduzione del circolante è una notizia, a mio giudizio, non positiva. La demonizzazione di questo sistema di pagamento nasconde diverse insidie e interessi. I costi occulti dei pagamenti elettronici generano utili ad altri operatori e il sistema attuale consente una tracciabilità dei pagamenti realizzabile da soggetti privati e non solo dallo

Stato, con la sempre maggiore creazione di occasioni di invasione della privacy di ciascuno di noi.

Ciò premesso, il processo di riduzione appare avviato e, di certo, un minor quantitativo di banconote e monete circolanti porterà una aggregazione degli operatori. Ma non una riduzione dei controlli e delle verifiche che gli operatori sono chiamati a fare. In futuro si dovrà seguire la strada di funzioni più votate alla *intelligence* che utilizzano strumenti informatici di analisi abbattendo il costo delle attività oggi demandate ad interi uffici.

E' la strada seguita già oggi da alcuni operatori che hanno formato al loro interno delle competenze di primo livello in grado di analizzare e contrastare il fenomeno del riciclaggio.

Maggiore qualità e consapevolezza dei rischi potrà portare ad una gestione meno pesante, anche sul piano finanziario, del rischio riciclaggio. In questo senso è utile prepararsi per tempo, sul piano organizzativo, per cogliere i cambiamenti che arriveranno.



Business Unit Safe Storage di Gunnebo Italia: Una presenza attiva sul territorio nazionale per aggiungere valore al business dei clienti

comunicato aziendale

La Business Unit **Safe Storage** del Gruppo Gunnebo svolge attività di progettazione, produzione, installazione, manutenzione e riparazione di soluzioni e prodotti di sicurezza fisica.

Attore primario nel mercato della sicurezza passiva, il team Safe Storage in Italia è al fianco ed al servizio dei propri Clienti con **innovazione** e forte **orientamento alle loro esigenze** proponendo **progetti e soluzioni ad alto valore aggiunto** come:

1. **Sistemi robotizzati di cassette di sicurezza SafeStore Auto;**
2. **Camere e porte corazzate;**
3. **Cassette di sicurezza SDL;**
4. **Armadi SecureIT;**
5. **Casseforti e armadi personalizzati.**



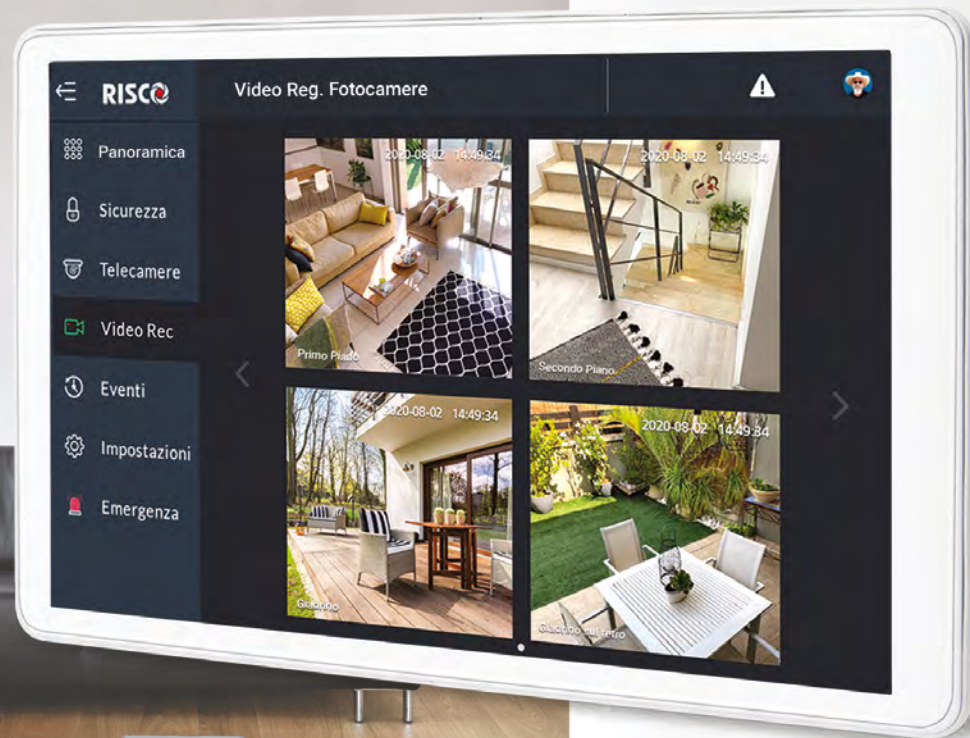
Gunnebo Italia Safe Storage soddisfa ogni esigenza di sicurezza volta a proteggere beni, valori e documenti dai rischi di furto, rapina, incendio, esplosione, vandalismo e aggiunge valore al business dei Clienti.

Per maggiori informazioni scrivi a clienti.it@gunnebo.com oppure visita i nostri siti:
www.cassefortilipsvago.it | www.gunnebosafestorage.com/it-IT

Il **Gruppo Gunnebo** opera in tutto il mondo fornendo prodotti, software e servizi innovativi per controllare il flusso di oggetti di valore, denaro e persone. Gunnebo offre controllo accessi, stoccaggio sicuro, gestione del contante e soluzioni di sicurezza integrate ai clienti principalmente all'interno di negozi al dettaglio, trasporti di massa, edifici pubblici e commerciali, siti industriali e ad alto rischio e banche. Il gruppo ha un fatturato di 5.500 milioni di corone svedesi.

RisControl

Tastiera Touchscreen



RisControl è la nuova Tastiera Touchscreen dotata di tecnologia all'avanguardia e dal design elegante, per LightSYS™ e ProSYS™Plus!

Offri ai tuoi clienti una esperienza di utilizzo senza paragoni con la tastiera Touchscreen RisControl. Dispone di un'interfaccia utente intuitiva e simile a quella di uno Smartphone, ideale sia in contesti residenziali sia commerciali.

Grazie al suo aspetto e a funzionalità di semplice fruizione, l'utente può avere con pochi tocchi sullo schermo lo stato del suo sistema, inserirlo e disinserirlo e accedere a video live o alle registrazioni delle telecamere IP VUpoint.



Video Verifica

Ideale per impianti dotati di Video Verifica dell'allarme in tempo reale, con sensori radio da interno e da esterno con fotocamera integrata, o VUpoint.



Tastiera Touchscreen

Esperienza d'uso senza paragoni, permette il controllo di allarme, video e smart home da una singola interfaccia intuitiva e di semplice utilizzo.



Sicurezza Superibrida

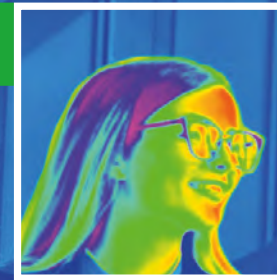
Adatta per installazioni di ogni dimensione con le centrali ibride di RISCO, da 8 a 512 zone, Grado 2 e Grado 3.



Per maggiori informazioni visitate il sito www.riscogroup.it
RISCO Group S.R.L | Via Robecco, 91 – Cinisello Balsamo (MI)



36.4



38.7



WISeNET

RILEVAZIONE TEMPERATURA E ANALISI VIDEO DEEP LEARNING

**Telecamera bi-spectrum certificata IEC 60601
per rilevazione temperatura, face detection
e analisi video AI Deep Learning**



TNM-3620TDY

www.hanwha-security.eu/it

RISCO GROUP, un partner di riferimento affidabile per le società di vigilanza

intervista a Ivan Castellan, Branch Manager di RISCO GROUP Italia

Ci parli di RISCO Group, una società indipendente leader a livello globale nei sistemi integrati di sicurezza.

RISCO Group è stata fondata alla fine anni '70, in Israele, vicino a Tel Aviv, dove ha tuttora la propria sede, il reparto R&D e la produzione. Nonostante le molte evoluzioni nel corso degli anni, non è mai cambiato l'obiettivo principale dell'azienda: sviluppare, produrre e distribuire soluzioni professionali per gli operatori professionisti della sicurezza in tutto il mondo. RISCO è un produttore indipendente e vuole mantenere questa identità, senza creare possibili conflitti con incroci di diversi interessi, come nel caso delle società di vigilanza, con le quali RISCO collabora in tutto il mondo ed alle quali si è sempre rivolta per offrire soluzioni di campo. Non abbiamo mai proposto sistemi di ricezione, lasciando questo compito e ruolo alle aziende che, invece, hanno scelto di sviluppare sistemi di ricezione: solo in questo modo si mantiene vivo l'interesse di RISCO di adottare in trasmissione tutti i protocolli standard più rilevanti e, dal lato dei sistemi ricezione, di adottarli tutti, con il massimo beneficio per le società di vigilanza stesse.

Quali linee di prodotti avete in portfolio raccomandate per le società di vigilanza?

Abbiamo sempre tenuto in considerazione le esigenze che i professionisti, di tutto il mondo, ci hanno fatto pervenire e, di conseguenza, abbiamo sviluppato l'attuale catalogo. Abbiamo riscontrato che seppur una società si concentri su uno specifico target, ad esempio l'installazione residenziale, resta sempre concreta la possibilità che si presentino necessità o opportunità di realizzare impianti diversi o più complessi. Per questo motivo, abbiamo realizzato un ecosistema di soluzioni, basato su tre diverse centrali



che tra loro condividono programmazione ed accessori, in grado di risolvere ogni esigenza dal piccolo sistema residenziale al grande impianto industriale, sempre con la stessa professionalità, garanzia e certificazioni G2 e G3. In questo modo, sapendo installare una centrale, si è in grado anche di installare le altre e l'accessorio che si ha in magazzino lo si può usare per ogni esigenza. Una soluzione particolarmente apprezzata dalle società di vigilanza nostre partner è la video verifica, realizzabile sia utilizzando sensori radio con fotocamera che associando telecamere IP (VUpoint) alle nostre centrali. Tramite una particolare funzione del cloud, chiamata TENANT, le società di vigilanza possono ricevere nelle proprie sale operative gli eventi e, quando associate, immagini o clip video, oltre a poter gestire il live.

In che modo vi proponete come partner per le società di vigilanza?

RISCO, per fornire il miglior servizio e supporto ai propri partner, ha sviluppato una rete di distributori professionali,

ognuno con competenze commerciali e tecniche, oltre a corsi online, grazie ai quali è possibile ricevere formazione quando lo si desidera restando al proprio domicilio. Siamo anche disponibili a formazione in presenza, sia presso i nostri uffici che presso quelli del cliente.

Ci può parlare della certificazione alla Norma EN 50136-3:2013 del vostro collegamento in cloud degli impianti periferici?

Il nostro cloud offre diversi servizi: per l'utente finale, per gli installatori ed anche per le società di vigilanza.

Al fine di offrire e garantire la massima sicurezza, sia per la continuità del servizio che per la riservatezza dei dati, abbiamo scelto di collaborare con Microsoft e far ospitare la nostra piattaforma su Azure, uno dei servizi cloud più certificati e sicuri del mercato.

Inoltre, per le società di vigilanza, abbiamo ottenuto la certificazione EN 50136-3:2013, rilasciata ai dispositivi di ricetrasmittente (**Receiving Centre Transceiver – RCT - without Annunciation Equipment**): con noi gli operatori della vigilanza possono essere certi dell'impegno profuso per offrire quanto di meglio possibile.



applica
TEST & CERTIFICATION

Certificate No. 30505-01-20

Certificate History		
Revision	Description	Issue Date
-	Initial Issue	2020-08-27

Product Covered by this Certificate		
Product Name	Product Description	Applied Standards
RISCO Cloud	Receiving Centre Transceiver (RCT) without Annunciation Equipment (AE)	EN 50136-3:2013 in conjunction with EN 50136-1:2012

Application/Limitation

- The product is intended to be used as RCT located in alarm station. For the purposes of conforming to EN 50136-3:2013 RISCO Cloud shall be used together with Annunciation Equipment (AE) conforming to EN 50131-3:2013.

Document Reviewed	
Document ID	Description
RISA5_EN 50136-3.27944	Test report according to: EN 50136-3:2013 in conjunction with EN 50136-1:2012

Terms and Conditions

The certificate is subject to the following terms and conditions:

- The Certificate is only valid for the product listed above
- The product is to be used in accordance with the manufacturer installation and operation instructions
- The product listed in this certificate have been found to comply with the requirements of ISO/IEC 17065:2012 and ISO/IEC 17067:2013 for Product Certification Scheme 1b

The following may render this Certificate invalid:

- Changes in the design, construction and/or software of the product
- Changes in the test methods requirements included in the standards, used to assess the performance of the declared characteristics

END OF CERTIFICATE



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

Arriva in Italia AddSecure, leader europeo nelle soluzioni IoT per la sicurezza delle comunicazioni e dei dati critici

intervista a Antonio Cuccurullo, Country Manager Smart Alarms di AddSecure

Ci racconti di AddSecure, la storia, l'organizzazione e le sue linee di prodotti e servizi.

AddSecure è un fornitore *leader* in Europa di soluzioni Internet of Things (IoT) ad elevato valore tecnologico ed affidabilità, particolarmente per quanto riguarda la sicurezza delle comunicazioni e dei dati critici.

Fondata all'inizio degli anni '70, l'azienda proviene dai più grandi operatori di telecomunicazioni e sicurezza dei paesi nordici, con una conoscenza e competenza distintive nell'ambito della comunicazione e della sicurezza di allarmi *wireless*, sviluppando, sin dal millennio, soluzioni basate su *cloud* per comunicazioni ad alta criticità.

La società impiega oggi più di 880 persone in 15 paesi ed ha sede a Stoccolma in Svezia, con uffici regionali e una rete di distributori in tutta Europa.

Le attuali 6 linee di business della società sono: [Smart Alarms](#), [Smart Care](#), [Smart Grids](#), [Smart Rescue](#), [Smart Transport](#) e [Smart Surveillance](#), con oltre 100.000 clienti che operano in diversi settori, tra cui quelli della Security e della Safety, dei fornitori di servizi di soccorso, sicurezza e automazione degli edifici, assistenza digitale, trasporto e logistica, servizi pubblici e altro ancora.

Smart Surveillance rappresenta l'ultima aggiunta al portafoglio di AddSecure, con soluzioni di sicurezza e monitoraggio per cantieri, centri logistici, strutture industriali e pubbliche.

L'azienda presta grande attenzione ai temi della sostenibilità e si impegna a diminuire l'impatto ambientale per quanto riguarda la produzione, l'imballaggio e il trasporto. Altri obiettivi chiave includono la riduzione della necessità di *hardware* tramite funzionalità evolute ed "intelligenti", la connessione di sistemi di allarme e l'ottimizzazione dei



viaggi, da parte dei tecnici per l'assistenza e la gestione delle strutture, utilizzando app mobili.

AddSecure è controllata in maggioranza da Fondi gestiti da Castik Capital, un fondo di *private equity* europeo fondato nel 2014 con un approccio di lungo termine alla creazione di valore.

Quali proposte presenta al mercato italiano e per quali categorie di utenti?

Per il mercato italiano, la società si concentra inizialmente sull'offerta del portafoglio della linea *Smart Alarms*, in particolare la soluzione *Alarm-over-IP* certificata secondo il più alto accreditamento EN54-21 CPR per la trasmissione affidabile di allarmi antincendio.

Alla luce dei regolamenti di questo specifico settore, riteniamo infatti che anche il mercato italiano seguirà gli stessi sviluppi in corso in tutta Europa.

La nostra soluzione, basata sui comunicatori della serie IRIS-4 4xx e sul software del ricevitore ISA-4, è conforme alla normativa nazionale di sistema UNI 9795. Le categorie di utenti che possono beneficiare dei prodotti certificati EN 54-21 appartengono ad un ampio spettro di attività aziendali, a partire naturalmente da quelle soggette al codice nazionale per la prevenzione incendi, ma non solo.

AddSecure adotta una rigorosa politica di gestione della qualità con investimenti ed un costante impegno nell'ottenere la certificazione per i suoi prodotti, come EN, VdS, SBSC, INCERT, NFA2P, KIWA-NCP e altri. I certificati del prodotto AddSecure aiutano anche gli installatori e gli utenti delle apparecchiature a dimostrare la piena conformità ai requisiti locali delle società di assicurazione.

L'accreditamento EN54-21 CPR riconosce i terminali IRIS-4 modelli 400 (4G), 420 (IP) e 440 (IP/4G) come una soluzione di trasmissione di allarme su IP affidabile e sicura per l'industria europea della sicurezza antincendio.



Quali sono i canali di distribuzione che avete attivato in Italia e quali modalità di supporto offrite agli utenti finali?

AddSecure ha avviato la presenza diretta in Italia all'inizio del 2020 al fine di sviluppare una struttura distributiva indiretta nel mercato.

I distributori dei combinatori telefonici IRIS-4 sono rappresentati da *partner* a valore aggiunto, mentre la vendita della soluzione di ricevitore software ISA-4 è svolta principalmente come attività diretta. Tuttavia, come noto

il mercato della sicurezza antincendio coinvolge molti *stakeholder* e affrontare lo specifico mercato locale richiede comunque anche un adeguato livello di flessibilità.

I *partner* sono tradizionalmente rappresentati dai produttori di centrali antincendio, i quali includono talvolta nella loro catena del valore anche fornitori di soluzioni di gestione degli allarmi, e come tutti gli altri *partner* sono considerati un elemento chiave delle relazioni dell'azienda e le *partnership* vengono effettuate con programmi di formazione e seguendo i valori aziendali di AddSecure:

- Centralità del cliente: prendersi cura e soddisfare le esigenze di ogni singolo *account*;
- Semplicità operativa: tecnologia facile da usare ed efficace, gestita con procedure chiare;
- Spirito di squadra e cooperazione: sviluppo comune del mercato locale e condivisione della conoscenza e dell'esperienza acquisite nei diversi mercati internazionali.

In questo modo è possibile garantire agli utenti finali il miglior supporto possibile, a partire dal primo livello effettuato da parte dei *partner* locali fino al supporto di livello più alto, quando necessario, da parte del supporto centrale AddSecure disponibile 24h/24 x 365 giorni l'anno.

Qual è il vero valore aggiunto delle vostre soluzioni proposte per il mercato antincendio italiano?

Il valore aggiunto dei prodotti e delle soluzioni di AddSecure è rappresentato da soluzioni certificate e conformi alle normative e agli standard di riferimento, che rappresentano quanto più possibile investimenti "a prova di futuro" e con una ottimale integrazione nelle piattaforme di gestione degli allarmi esistenti, rispondendo alle esigenze di progettisti di sistemi, distributori, installatori, manutentori, centrali di ricevimento allarmi e utenti finali.

Tale salvaguardia degli investimenti si applicherà anche al mercato italiano a seguito della fine delle linee PSTN analogiche e del processo di digitalizzazione delle telecomunicazioni in corso.

In molti paesi questo sta già accadendo oggi.

ADD:SECURE®

Contatti:
AddSecure International AB
Tel. +39 347 9977 838
marketing@addsecure.com
www.addsecure.com

DEKRA Italia entra nella security con la certificazione di aziende e figure professionali

intervista a Marco Trionfetti, Technical Operations Manager Service Unit Business Assurance DEKRA Italia

Ci può presentare DEKRA e le sue attività nel mondo?

DEKRA è attualmente una delle principali organizzazioni a livello mondiale specializzata nei servizi professionali e di consulenza per i settori automotive, industriale e terziario avanzato.

La mission di DEKRA è quella di garantire la sicurezza in tutto il mondo attraverso tecnologia e attrezzature, standard e best practices, mentalità e comportamento. Questa esigenza fondamentale delle persone è soddisfatta dalla nostra forza lavoro di oltre 45.000 persone in oltre 60 paesi in tutti i continenti con una vasta esperienza, servizi ad ampio raggio e impegno appassionato. Sintetizzo alcuni dei principali servizi attraverso i quali realizziamo quotidianamente questo panorama:

a. Claims & Expert Services: Offriamo servizi di gestione sinistri a varie compagnie assicurative, società di Leasing, agenzie governative e grandi aziende in tutto il mondo. Gestiamo sinistri di tutti i rami, R.C.A., Trasporti e Logistica, Property, R.C. Generale, Infortuni e Malattia, nonché rimesse e sinistri particolarmente gravi, derivanti da eventi speciali. La conoscenza approfondita di DEKRA all'interno della Divisione Servizi Claims & Expertise offre indipendenza, innovazione e qualità.

b. Certificazioni di Sicurezza delle informazioni: La certificazione di sicurezza informatica di terze parti fornisce prove accreditate e indipendenti di cui i nostri clienti hanno bisogno per dimostrare che i loro prodotti e processi sono conformi ai requisiti e agli standard di sicurezza riconosciuti a livello globale con la certificazione ISO 27001 e per ottenere un certificato riconosciuto a livello internazionale che ne attesti efficienza e prestazioni.

c. Cyber Security Testing & Certification: Il Common Criteria for Information Technology Security Evaluation (CC) è uno standard internazionale (ISO 15408) per la certificazione della



sicurezza informatica atta a garantire che l'implementazione, la specifica e la valutazione di un prodotto o sistema siano state condotte in modo corretto e ripetibile.

d. DEKRA è l'ente che nel mercato italiano offre una certificazione per le aziende e le persone che installano e fanno manutenzione di impianti antincendio e/o sistemi di sicurezza attraverso degli schemi di certificazione proprietari. Il percorso di certificazione valorizza le figure professionali quali Esperti nella progettazione, installazione, manutenzione e riparazione di impianti di allarme intrusione/rapina e videosorveglianza.

Con quali servizi si propone alla filiera della sicurezza?

La sicurezza è senza dubbio il fil rouge che unisce idealmente i nostri servizi e processi in una galassia protetta per i Clienti. Possiamo però sostenere, come anticipato, che tra i principali servizi con cui DEKRA si propone alla filiera della sicurezza possiamo annettere:

a) certificazione delle aziende che installano i sistemi antincendio, sistemi di rivelazione e allarme incendio e sistemi di controllo fumo e calore;

b) certificazione delle aziende che installano i sistemi di sicurezza, sistemi antintrusione e allarme, sistemi di controllo accessi, sistemi di sicurezza sul perimetro esterno e sistemi di video sorveglianza.

Queste certificazioni sono atte a verificare le capacità tecniche, procedurali e personali dell'azienda che installa queste tipologie di impianti al fine di proteggere cose e persone; tali requisiti sono controllati nel tempo da DEKRA attraverso verifiche annuali sia documentali che sul campo, con sopralluoghi in fase di installazione da parte di nostri tecnici competenti.

DEKRA ha inoltre predisposto e offerto al mercato anche uno schema di certificazione del personale addetto alla progettazione e all'installazione/manutenzione degli stessi impianti che, attraverso un percorso formativo (con corsi qualificati DEKRA), porta il professionista a svolgere un esame per dimostrare oggettivamente le sue competenze stabilite dalle norme e leggi vigenti.

Tutti questi servizi danno garanzia al mercato su diversi aspetti:

- La garanzia da parte di un ente terzo indipendente che il fornitore installi prodotti conformi e secondo la regola d'arte, nel rispetto dei requisiti tecnici e legali, e che i suoi dipendenti abbiano le competenze necessarie;
- Permettere al datore di lavoro di dimostrare oggettivamente di aver attuato tutte le possibili azioni al fine di ridurre al minimo il rischio che la propria azienda con i propri dipendenti possano provocare incidenti o danni;
- Responsabilizzare tutti gli attori della filiera (fornitori, dipendenti, committenza).

Intendiamo con queste iniziative portare nel mercato italiano della sicurezza l'esperienza e i valori maturati dal Gruppo

in 95 anni di attività a livello internazionale, nel momento in cui anche questo settore si sta uniformando sempre più velocemente ai modelli ed agli standard europei per garantire la qualità e la sicurezza dei prodotti e dei servizi agli utenti finali. Insomma, una sicurezza al quadrato per i nostri clienti...!

In che modo interagiranno secondo voi le certificazioni di sistema e delle figure professionali con le direttive europee in materia di sicurezza dei dati (GDPR e NIS) che responsabilizzano i fornitori nella tutela degli interessi degli utenti finali?

DEKRA, attraverso queste certificazioni, permette di avere garanzia che il personale sia costantemente a conoscenza delle regole sulla privacy, la gestione dei dati personali, e che le aziende abbiano e applichino correttamente nel tempo procedure interne che garantiscano la gestione e la protezione di tali dati. Oggigiorno, sempre più gli aspetti legati alla gestione dei dati sensibili/personali e la protezione delle reti (Cyber Security) sono aspetti fondamentali: ad esempio, un'azienda che installa un sistema anti-intrusione con allarme, potrebbe interconnettersi alla rete aziendale e deve quindi conoscere e attuare procedure chiare e rigorose al fine di non mettere a rischio la totalità dei dati aziendali. Perciò questo tipo di certificazioni ha una doppia valenza: migliorare la reputazione dell'azienda installatrice e allo stesso tempo rendere sicura e protetta la rete dell'azienda finale. Vogliamo essere il Partner globale per un mondo sicuro in modo reale, diventare un punto di riferimento non solo per le aziende ma per le persone e le comunità in generale, con la speranza di poter contribuire a migliorare e rendere sempre più protetta la vita quotidiana di tutti noi, in ogni ambito.



Contatti:
DEKRA Italia
Tel. +39 344 1883602
marco.trionfetti@dekra.com

Intelligenza artificiale per le smart city

comunicato aziendale



Utilizzare le moderne tecnologie dell'Intelligenza Artificiale, come il Machine Learning e il Deep Learning, rappresenta senz'altro il futuro delle applicazioni e dei prodotti per la Visione Artificiale. Tali tecnologie, infatti, permettono di conseguire enormi miglioramenti prestazionali accompagnati da un'elevata capacità degli applicativi ad adattarsi a condizioni di lavoro molto diversificate.

A.I. Tech è partita con grande anticipo nello sviluppo di prodotti basati sul "deep learning" e ad oggi quasi tutte le sue soluzioni sono basate su tali approcci. Questo ha reso possibile lanciare sul mercato prodotti che sono tra i pochissimi a livello mondiale in grado di poter essere eseguiti direttamente a bordo delle telecamere, nonostante le poche risorse a disposizione.

Lo sviluppo di prodotti basati sul deep learning non consiste semplicemente nel prendere una tra le famose reti profonde disponibili sul web (ad esempio YOLO), che molto probabilmente anche i meno addetti ai lavori ormai conoscono, ed utilizzarla su un server. Le risorse hardware necessarie per l'utilizzo di queste reti sono infatti così elevate da renderle utilizzabili soltanto su server molto costosi e quindi inutilizzabili sulle telecamere, anche solo per funzionalità semplici.

A.I. Tech, grazie alle avanzatissime competenze in questo settore, progetta e realizza le proprie reti profonde, oggetto

anche di pubblicazioni scientifiche. Questo consente di mantenere le prestazioni molto vicine alle migliori reti profonde, ma abbattendo di decine di volte le risorse computazionali richieste, potendo così essere utilizzate su telecamere e sistemi embedded.

Uno dei settori in cui tale vantaggio competitivo è più evidente, è sicuramente quello delle smart city. **A.I. Tech** ha infatti innumerevoli prodotti che consentono di realizzare i progetti più ambiziosi in ambito smart cities, mediante una piattaforma avanzata per il monitoraggio dei veicoli, dei pedoni e dell'ambiente.



SMART TRANSPORTATION

L'innovativa e ampia piattaforma per lo Smart Transportation di **A.I. Tech** è finalizzata al monitoraggio dei flussi veicolari (AI-ROAD3D-DEEP) e al rilevamento di comportamenti di guida anomali (AI-INCIDENT-DEEP). Più nello specifico, viene offerta la possibilità di effettuare il conteggio e la classificazione dei veicoli, stimando per ciascun veicolo la velocità media e il colore. Inoltre, è possibile rilevare veicoli che percorrono strade contromano o corsie riservate; verificare la presenza di veicoli o pedoni lungo la carreggiata o fermi nelle piazzole di sosta. La soluzione si completa con la possibilità di rilevare le targhe dei veicoli, grazie alla combinazione delle più avanzate tecniche di deep learning con un motore semantico (AI-LPR-DEEP).

SMART PARKING

La piattaforma dedicata allo Smart Parking è pensata per la gestione intelligente dei parcheggi e la videosorveglianza degli stessi, consentendo di monitorare lo stato di occupazione di ciascun posto, fornendo in tempo reale l'informazione relativa, e quindi se il posto sia libero o occupato (AI-PARKING-DEEP). La soluzione, eventualmente combinata con un cruscotto dashboard (AI-DASH-PRO), può essere impiegata sia in parcheggi su strada che in parcheggi perimetri. In quest'ultima situazione, inoltre, l'applicazione per il conteggio dei veicoli ai varchi (AI-ROAD3D-DEEP) piuttosto che il sistema di lettura targhe (AI-LPR-DEEP) possono essere altresì utilizzate per il monitoraggio dei varchi.



SMART PEDESTRIANS

Elemento fondamentale e non trascurabile di una smart city riguarda il controllo e il monitoraggio del flusso pedonale, della gestione delle folle, e più recentemente delle problematiche legate alla diffusione del contagio da Coronavirus che impongono un'attenta gestione degli assembramenti e del distanziamento sociale (AI-CROWD-DEEP), oltre che del controllo delle persone che non indossano la mascherina (AI-FACEDTECT-DEEP). Il sistema quindi offre un supporto effettuando il conteggio delle persone e stimando il numero di persone presenti all'interno

di un'area o la percentuale di occupazione, generando un allarme in caso di sovraffollamento o assembramenti (AI-RETAIL-DEEP).

SMART ENVIRONMENTS

Non dobbiamo infine dimenticare la messa in sicurezza dell'ambiente. Questa può concretizzarsi attraverso il rilevamento precoce di principi di fiamme (AI-FIRE-DEEP) e fumo (AI-SMOKE-DEEP), soprattutto in ambienti quali quelli cittadini in cui i tradizionali sensori anti-incendio sono poco efficaci o non possono essere utilizzati. Monitorare l'ambiente significa inoltre poter rilevare in tempo reale la presenza di spazzatura abbandonata sul ciglio della strada, attraverso il rilevamento di oggetti abbandonati (AI-LOST).

A.I. Tech: L'esperienza di oltre 30 anni di ricerca e trasferimento tecnologico nei settori dell'Intelligenza Artificiale e della Visione Artificiale, coniugata con competenze di ingegnerizzazione di soluzioni hardware, software e di progettazione su sistemi embedded, consentono ad **A.I. Tech** di proporre soluzioni innovative e all'avanguardia nel settore della analisi video intelligente. Il suo team giovane e dinamico, guidato da menti brillanti ed esperte, è capace di ideare, progettare e realizzare sistemi in grado di rendere intelligente una normale telecamera di sorveglianza. Grazie ai prodotti di **A.I. Tech**, la telecamera non si limita alla semplice osservazione della scena, ma diventa capace di comprendere cosa sta avvenendo attraverso il riconoscimento degli oggetti e l'analisi del loro comportamento. I prodotti di **A.I. Tech** possono essere utilizzati nei più svariati mercati verticali: dal retail alla business intelligence, dal monitoraggio del traffico all'ambient assisted living, fino alla video sorveglianza intelligente.



Contatti:
A.I. Tech srl
Tel. +39 393 8384253
www.aitech.vision

La Guida ELAN ai cavi sicurezza e alla Normativa CPR

comunicato aziendale

La normativa CPR è, da tempo, argomento di discussione sia per gli installatori che per i progettisti della Sicurezza. Il **Regolamento Prodotti da Costruzione (CPR)** è la normativa europea che definisce i requisiti base e le caratteristiche essenziali armonizzate che tutti i prodotti progettati per essere installati in maniera permanente in opere di costruzione devono soddisfare nell'ambito di applicazione dell'UE.

Tutti i cavi installati in edifici e opere di ingegneria civile soggetti a requisiti prestazionali di reazione al fuoco, siano essi di energia o di comunicazione oppure a fibra ottica, devono essere classificati.

L'obiettivo del Regolamento CPR è, di fatto, di uniformare una volta per tutte le diverse normative presenti.

Le norme sui cavi presenti a livello europeo differiscono, infatti, da quelle nazionali, originando quindi livelli di sicurezza differenti.

Il CPR introduce nuovi criteri di classificazione e classi comuni, le cosiddette "Euroclassi", per l'intero territorio europeo.

Chi è coinvolto?

La norma coinvolge tutti gli operatori economici della filiera:

- fabbricante: qualsiasi persona fisica o giuridica che fabbrichi un prodotto da costruzione o che faccia progettare o fabbricare tale prodotto e lo commercializzi con il suo nome o con il suo marchio (Art.11);
- mandatario: qualsiasi persona fisica o giuridica stabilita nell'Unione Europea che abbia ricevuto da un fabbricante un mandato scritto che la autorizza ad agire per suo conto in relazione a determinati compiti (Art.12);
- distributore: qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fabbricante o all'importatore, che metta un prodotto da costruzione a disposizione sul mercato (Art.13);
- importatore: qualsiasi persona fisica o giuridica, stabilita nell'Unione Europea, che immetta sul mercato dell'Unione Europea un prodotto da costruzione proveniente da un paese terzo (Art.14).

Quali sono gli obblighi?

I soggetti coinvolti sono tenuti a mostrare:

- la marcatura CE
- la Dichiarazione di Prestazione (DoP)
- il Sistema di valutazione e verifica della costanza delle prestazioni (AVCP). A seconda della classificazione l'appartenenza ad una determinata classe e la costanza delle prestazioni, dovranno essere controllate e certificate da Organismi Notificati (i cosiddetti Notified Bodies) indipendenti (es. IMQ).



Classificazione della reazione al fuoco

I cavi sono classificati in **7 classi di Reazione al Fuoco** identificate dalle lettere **da F ad A** e dal pedice "ca"(cable) in funzione delle loro prestazioni crescenti. Ogni classe prevede soglie minime per il rilascio di calore e la propagazione della fiamma.

CLASSE	SISTEMA	COMPITI DEL FABBRICANTE	COMPITI DELL'ORGANISMO NOTIFICATO
A _{ca}	AVCP 1+	Piano di controllo della Produzione (FPC)	Campionamento prove tipo iniziale (ITT) Prove tipo iniziale (ITT) Ispezione iniziale FPC Sorveglianza FPC Sorveglianza prodotti prima dell'immissione sul mercato
B _{1ca}			
B _{2ca}			
C _{ca}			
D _{ca}	3		Prove tipo iniziale (ITT)
E _{ca}			
F _{ca}	4	Piano di controllo della Produzione (FPC) Prove tipo iniziale (ITT)	

Oltre a questa classificazione principale, le autorità europee hanno regolamentato anche l'uso dei seguenti parametri aggiuntivi:

"a": acidità che definisce la pericolosità dei fumi per le persone e la corrosività per le cose. Varia da a1 a a3.

"s": opacità dei fumi. Varia da s1a a s3.

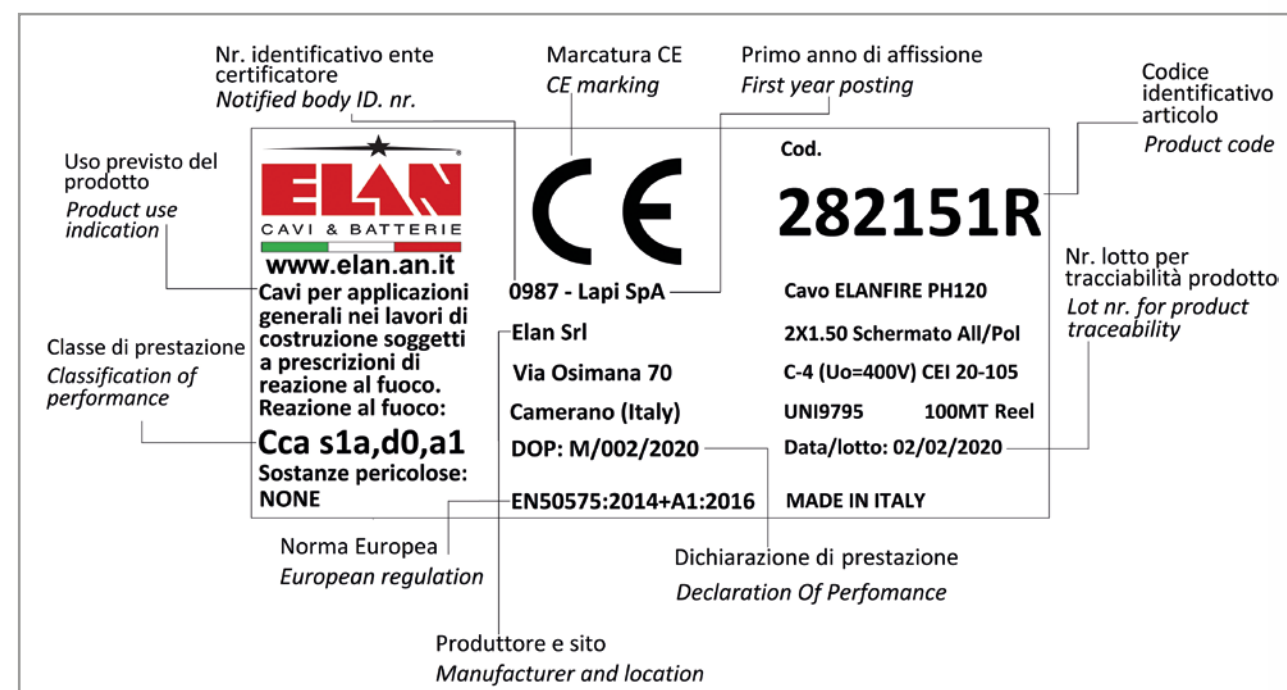
"d": gocciolamento di particelle incandescenti che possono propagare l'incendio. Varia da d0 a d2.

Dalla classe C alla classe A deve essere effettuata la valutazione e verifica della costanza della prestazione (Assessment and verification of Constancy of performance – AVCP), inclusa la prova iniziale e il controllo della produzione in fabbrica (Factory Production Control – FPC).

A _{ca} - B _{1ca} - B _{2ca}	C _{ca}	E _{ca}
Aerostazioni, stazioni ferroviarie, stazioni marittime, metropolitane in tutto o in parte sotterranee. Gallerie stradali di lunghezza superiore a 500 mt. e ferroviarie superiori a 1.000 mt..	Strutture sanitarie, locali di spettacolo e intrattenimento in genere, palestre e centri sportivi. Alberghi, pensioni, motel, villaggi, residenze turistico-alberghiere. Scuole di ogni ordine e grado. Locali adibiti ad esposizione e/o vendita all'ingrosso o al dettaglio. Aziende ed uffici con oltre 300 persone presenti; biblioteche ed archivi, musei, gallerie, esposizioni e mostre. Edifici civili con altezza incendio superiore a 24 mt.	Aziende ed uffici con meno di 300 persone presenti; edifici destinati ad uso civile con altezza antincendio inferiori a 24 mt; centri elaborazione dati con meno di 25 addetti; alberghi, pensioni, villaggi turistici, bed and breakfast etc. fino a 25 posti letto. Locali adibiti ad esposizione e/o vendita all'ingrosso o al dettaglio con superficie lorda fino a 400 mq. Studi medici di prestazione ambulatoriale e/o diagnostica di superficie fino a 500 mq. Altre attività ove non esiste il rischio incendio e pericolo per
Airports, railway stations, ports, subways completely or partially underground. Road tunnels more than 500 mt. length and rail tunnels more than 1.000 mt length.	Health facilities, entertainment venues in general, gyms and sports centers. Hotels, pensions, motels, villages, tourist residences. Schools of all types and levels. Premises used for display and/or wholesale or retail sale. Companies and offices with over 300 people present; libraries and archives, museums, galleries, exhibitions and art galleries. Civil buildings higher than 24 meters.	Companies and offices with less than 300 people present; buildings intended for civil use with less than 24 meters height; data processing centers with less than 25 employees; hotels, pensions, resorts, bed and breakfasts etc. up to 25 beds. Premises used for display and/or wholesale or retail sale with gross area up to 400 sqmt. Outpatient and/or diagnostic medical offices up to 500 sqmt. Other activities where there is no fire risk and danger for people and/or things.

Per tutti i cavi il fabbricante ha l'obbligo di redigere una dichiarazione di prestazione (DOP) e apporre il marchio CE. L'etichettatura del cavo deve contenere elementi fondamentali per l'identificazione del prodotto immesso sul mercato e la rintracciabilità dei lotti e dei relativi materiali utilizzati (sistema AVCP 1+).

Di seguito è possibile vedere un esempio di etichetta ELAN:



CEI 20-105 V2

CEI 20-105 v2: Cavi resistenti al fuoco, non propaganti la fiamma, senza alogeni, con tensione nominale 100/100V per applicazioni in sistemi fissi automatici di rivelazione e di segnalazione allarme incendio.

La norma tratta nello specifico:

4.1 Comportamento al fuoco

4.1.1 Reazione al fuoco – classificazione CPR

Tenuto conto del grado di sicurezza che questi cavi devono garantire, i cavi della presente Norma devono superare le prove previste dalla classe di reazione al fuoco Cca-s1b,d1,a1 secondo le indicazioni riportate nella Norma CEI-UNEL 35016. I requisiti di prestazione, le prove e i metodi di valutazione della reazione al fuoco dei cavi al fine di permettere la classificazione secondo il Regolamento Prodotti da Costruzione sono specificate dalla Norma EN 50575.

6.1 Regolamento Prodotti da Costruzione CPR (305/2011)

Per quanto riguarda la sicurezza in caso di incendio (Reazione al fuoco), l'appartenenza ad una determinata classe e la costanza delle prestazioni del cavo, dovranno essere controllate e certificate da Organismi Notificati indipendenti. A seguito del rilascio da parte dell'Organismo Notificato del Certificato di Costanza della Prestazione (AVCP)*, il fabbricante dovrà redigere la propria "Dichiarazione di Prestazione" (DoP) per poter porre la marcatura CE.

Sin dall'inizio, **ELAN** ha costantemente lavorato per rendere conformi i propri cavi sicurezza LSZH e i cavi antincendio alla normativa CPR. Sul sito e sul catalogo online si possono osservare tutti i prodotti certificati, con la relativa Classe di appartenenza.

Nello specifico, i cavi resistenti al fuoco **ELANFIRE** rientrano nella classe **Cca – s1a, d0, a1**.

Questi cavi sono conformi alla EN 50200 PH120 (resistente al fuoco a 850°C per 2 ore), alla CEI 20-105, UNI 97-95 e CEI 36762. Tutte le **DOP** (Declaration of performance), le **schede tecniche** e le **conformità** di questi cavi sono liberamente scaricabili sul sito web ELAN: www.elan.an.it

Tutti i cavi ad oggetto sono disponibili in matasse da 100mt e bobine da 500mt.



Contatti:
ELAN SRL
Tel. +39 071 7304258
www.elan.an.it



Hanwha Techwin lancia una nuova gamma di NVR per applicazioni con telecamere AI Deep Learning

comunicato aziendale

Tre nuovi modelli di NVR da 32 e 64 canali, con funzioni innovative ottimizzate per la gestione dei metadata AI generati dalle telecamere, consentendo attività di ricerca e classificazione eventi basata su algoritmi avanzati di analisi video.

I nuovi NVR sono stati progettati per applicazioni "mission critical". In particolare il modello **XRN-6410B4**, da 64 canali, è corredato da un doppio alimentatore a commutazione (SMPS) per garantire la continuità della registrazione in qualsiasi evenienza.

I tre NVR sono compatibili con tutte le telecamere **Wisenet AI** che includono analisi video AI Deep Learning senza necessità di installare licenze aggiuntive. Le analisi rilevano e classificano contemporaneamente vari tipi di oggetti, inclusi persone, veicoli, visi e targhe, e sono supportate dagli algoritmi AI di Wisenet.

Questi ultimi, esclusiva di Hanwha Techwin, identificano gli attributi di oggetti e persone, come la fascia di età, il sesso o il colore dei vestiti indossati.

Gli attributi sono quindi salvati come metadata sugli NVR insieme alle immagini acquisite dalle telecamere, permettendo agli utenti di effettuare rapide ricerche di oggetti o eventi specifici. Gli algoritmi sono inoltre in grado di riconoscere se una persona sta indossando gli occhiali o tenendo una borsa.

Business intelligence e Sicurezza

NVR e telecamere AI offrono insieme un elevato livello di precisione di rilevamento, riducendo al minimo i falsi allarmi. Inoltre, offrono agli operatori di sale di controllo e al personale addetto alla sicurezza uno strumento efficace per identificare e rispondere con rapidità a eventuali attività sospette.



In aggiunta, offrono alle aziende e, in particolare, al settore della vendita al dettaglio, l'opportunità di acquisire e analizzare i dati di business intelligence, che consentono di esaminare le fasce demografiche dei clienti, ottenendo una comprensione maggiore del comportamento e migliorando in ultima analisi l'esperienza dei clienti stessi. A questo proposito, poiché l'Intelligenza Artificiale è in grado di gestire scene estremamente affollate e dinamiche, è molto più adatta per ambienti di vendita al dettaglio rispetto alle analisi video tradizionali.

WiseStream II

Oltre a H.265, H.264 e MJPEG, i nuovi NVR supportano **WiseStream II**, una tecnologia di compressione complementare, fornita in esclusiva da Hanwha Techwin, che controlla in maniera dinamica le operazioni di codifica, bilanciando qualità e compressione a seconda del movimento nell'immagine. Quando viene combinata alla compressione H.265, WiseStream II rende l'utilizzo delle risorse di rete fino al 75% più efficiente in confronto alla tecnologia H.264.

Facile da configurare

Il tempo necessario per l'installazione è ridotto al minimo poiché è possibile collegarsi da remoto agli NVR tramite uno smartphone o un tablet senza dover configurare una rete

complessa, usando P2P e codici prodotto QR univoci. Gli NVR, in aggiunta, possono essere configurati con rapidità e semplicità in modo da soddisfare le esigenze specifiche di un utente finale tramite un'interfaccia utente Wisenet aggiornata e con l'aiuto di una nuova procedura guidata di installazione.

Backup di ripristino automatico

Se la comunicazione tra uno degli NVR e una telecamera Wisenet dotata di scheda SD viene interrotta, il backup di ripristino automatico (ARB) agevola il trasferimento e l'archiviazione delle immagini memorizzate sulla scheda SD quando la connessione di rete viene ripristinata. Ciò consente di ottenere una continuità di registrazione e riduce il rischio di perdere preziose prove video.

Tra le altre funzioni chiave sono incluse:

- 16 bay per HDD per fino a 16 TB di dati da registrare e memorizzare su scheda in modalità non RAID. Supporto per RAID 5 e 6 (8 HDD per 2 array).

- Compatibilità con telecamera Wisenet migliorata con supporto per 4K, 8K, imaging termico, PTZ e modelli multi-sensore.
- Due uscite per display HDMI.
- Riproduzione simultanea su tutti i canali.
- Nuovo display grafico user-friendly che offre agli operatori un'ampia gamma di funzioni pratiche, tra cui "Instant", timeline e anteprima in miniatura dell'evento.
- Notifiche push relative all'evento sugli smartphone.
- Conformità al profilo S ONVIF.

"Le nostre telecamere AI, supportate da questi nuovi NVR, ci permettono di offrire soluzioni di videosorveglianza a prova di futuro che offrono un livello di funzionalità che sarebbe stato difficile anche solo immaginare fino a qualche anno fa", ha detto Uri Guterman, Head of Product & Marketing per Hanwha Techwin Europe. "Sono una chiara dimostrazione del fatto che Hanwha Techwin si impegna a sfruttare la potenza della tecnologia AI per consentire ai nostri clienti di utilizzare al meglio i propri sistemi di videosorveglianza."


Hanwha Techwin Europe

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

Cybersecurity e privacy by design dei produttori, consapevolezza degli utenti finali: i punti chiave di Genetec contro le minacce informatiche

intervista a Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc.

Ci può parlare di Genetec, della sua storia e delle sue linee di prodotto?

Genetec Inc. è un provider innovativo con un ampio portafoglio di soluzioni nel campo delle tecnologie per la sicurezza unificata, per la protezione delle operations e nelle soluzioni di business intelligence. Fondata nel 1997, e con sede a Montreal, Canada, Genetec raggiunge i propri clienti grazie a un'estesa rete di rivenditori, integratori, partner di canale certificati e consulenti in oltre 80 paesi.

Il prodotto di punta dell'azienda è **Security Center**, una piattaforma dall'architettura aperta che è in grado di unificare sistemi di videosorveglianza su IP, controllo accessi, riconoscimento targhe (ALPR), comunicazioni e analitica.

Genetec sviluppa, inoltre, soluzioni e servizi cloud-based progettati per migliorare la sicurezza e contribuire a nuovi livelli di intelligenza operativa in strutture governative, aziende, trasporti e le comunità in cui viviamo.

L'esempio più chiaro di questa intelligenza operativa è rappresentato da **Mission Control**, un sistema collaborativo di gestione delle decisioni che fornisce una supervisione completa su tutti i sistemi, dispositivi e sensori.

In combinazione con procedure guidate, tracciamento visivo e capacità di collaborazione, Mission Control offre un quadro operativo comune nelle organizzazioni in cui affidabilità e tempi di risposta rapidi sono fondamentali.

A quali categorie di utenti si rivolge in Italia e come è strutturata sul piano organizzativo?

In Italia ci rivolgiamo principalmente a end-user che lavorano in vari mercati, dall'industria agli enti governativi, dalle aziende alla public safety (mi riferisco a trasporti, sorveglianza



cittadina estesa, strutture sanitarie) e poi infrastrutture critiche (porti, aeroporti, energia e utility, Building & Industrial) e retail (centri commerciali e punti vendita, banche).

Negli ultimi mesi molti end-user, operanti in settori strategici per la sicurezza (trasporti, energy utility e retail), si sono avvicinati alle nostre soluzioni di sicurezza unificata e con molti di questi stiamo sviluppando, attraverso i nostri system integrator e consulenti, progetti sempre più complessi.

Per quanto riguarda la nostra organizzazione in Italia, mi confronto giornalmente con il Direttore Vendite Sud Europa Rafael Martin Enriquez, ed insieme possiamo contare sulla competenza di Vito Candiloro, Channel Sales Specialist e di Jordi Charles Rodriguez, Sales Engineer.

Infine, stiamo cercando nuovi talenti per ampliare il nostro team, garantendo così una maggiore e più tempestiva presenza sul territorio, potendo sempre contare sul supporto tecnico della filiale di Parigi e della sede a Montreal.

Qual è la vostra visione del mercato globale della sicurezza fisica nel 2021?

Negli ultimi mesi, abbiamo osservato notevoli prove di resilienza e intraprendenza da parte di molte imprese, che si sono adattate alle necessità imposte dalla COVID-19, utilizzando le tecnologie di sicurezza fisica come strumento strategico per la lotta alla pandemia. Ecco perché sarà necessario andare oltre alle applicazioni tradizionali, per offrire sempre più innovazione.

Ma questa innovazione dovrà necessariamente andare di pari passo con la privacy e la sicurezza informatica, aspetti, questi, che imporranno ai vendor la creazione di soluzioni software sempre più sicure contro gli attacchi informatici e sempre più resilienti, per garantire la protezione dei dati senza comprometterne la disponibilità.

Ci aspettano ancora mesi di tracciamento dei contagi, oltre a tutta una serie di sfide sociali che andranno affrontate con trasparenza, progettando prodotti responsabili e innovativi che abbraccino le metodologie della privacy by design così che non sia più necessario dover scegliere tra proteggere la privacy individuale e tutelare la sicurezza fisica.

Il tutto in un mondo in cui l'infrastruttura cloud pubblica diventerà sempre più diffusa. Pensiamo all'aumento del lavoro da remoto dell'ultimo anno.

Ecco perché dovremo superare la presunta dualità cloud/sistemi di sicurezza on-premise: per andare sempre più verso un uso ibrido dell'infrastruttura di sicurezza fisica, implementando applicazioni specifiche sul cloud e mantenendo i sistemi on-premise esistenti. Questo permetterà di stare al passo con l'evoluzione delle organizzazioni, lavorando, di concerto con i dipartimenti IT, su scalabilità, ridondanza e disponibilità.

Infine, ma non per importanza, proprio per questo sodalizio ormai consolidato fra sicurezza fisica e strategia IT, le aziende dovranno realizzare una selezione oculata di produttori, fornitori e distributori. Tutta la supply chain dovrà rendere conto della sicurezza e affidabilità dei propri sistemi, fornendo risposte trasparenti sulle vulnerabilità dei propri prodotti, i partner con cui lavorano e le politiche privacy e dati.

Dal vostro punto di osservazione, come valutate il livello di consapevolezza del rischio cyber nel nostro paese?

Fino ad oggi il rischio di un attacco hacker esterno è sempre stato snobbato dagli addetti ai lavori con la giustificazione della disconnessione della rete LAN aziendale da quella utilizzata dalle telecamere, perché la security IP era relegata alla sola videosorveglianza o poco più. Oggi lo scenario sta rapidamente evolvendo verso un'integrazione di sistemi di sicurezza che vanno oltre il semplice video. Le reti interconnettono sistemi di controllo accessi, impianti tecnologici, interfonia che generano ingenti quantità di dati che spesso vengono utilizzati anche da sistemi di gestione aziendale al fine di produrre, monitorare e gestire processi molto complessi.

Genetec, da sempre, è attenta alla cybersecurity - sin dalla fase di progettazione - di qualsiasi suo prodotto software e hardware, che sottopone a test specifici tramite aziende indipendenti e specializzate.

Credo vi sia un gran bisogno di sensibilizzare e fare più formazione sui rischi legati alla sicurezza informatica. Nel contesto attuale e con il numero di attacchi in continuo aumento, certamente c'è più consapevolezza rispetto al passato, ma forse non è ancora sufficiente.

Prendiamo molto sul serio la cybersecurity e già da molti anni operiamo attivamente in questo ambito, muovendoci su quattro pilastri: identificazione e mitigazione del rischio, offerta di soluzioni affidabili, costruzione di una rete fidata, trasparenza e apertura.

Genetec™

Contatto:
Genetec Inc.
www.genetec.com

ERMES presenta i terminali SOS per Spazi Calmi

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



Nella progettazione delle vie di esodo verticali in caso di incendio, deve essere prevista la predisposizione di adeguati locali, detti **Spazi Calmi**, dove possano trovare rifugio le persone con ridotte capacità motorie in attesa di soccorsi.

Lo spazio calmo è definito nel D.M. 09/04/1994 come "Luogo sicuro statico contiguo e comunicante con una via di esodo verticale od in essa inserito; tale spazio non deve costituire intralcio alla fruibilità delle vie di esodo e deve avere caratteristiche tali da garantire la permanenza di persone con ridotte o impedito capacità motorie in attesa di soccorsi".

Tali spazi, oltre ad avere adeguate protezioni dal fuoco e dal fumo, è prescritto siano dotati di un sistema di comunicazione audio bidirezionale sia per segnalare la presenza della persona disabile agli operatori del posto centrale sia per consentire a questi di comunicare con gli utenti in difficoltà per evitare situazioni di panico durante l'attesa dei soccorsi.

ERMES dispone di una gamma di apparati appositamente sviluppati per tale impiego tra cui gli Help Point in IP con pulsante di chiamata touchless e gli Help Point con collegamento in GSM.

In particolare, gli apparati in IP utilizzano un protocollo di comunicazione Peer-To-Peer e si prefigurano come terminali stand alone collegati alla LAN direttamente senza la necessità di interfacce, unità ausiliarie o server di alcun tipo; il sistema, inoltre, è continuamente monitorato in modo da fornire una immediata segnalazione di allarme in caso di anomalia.

Nuovo modulo per la gestione di 4 obiettivi remoti miniaturizzati Wisenet

HANWHA TECHWIN EUROPE LTD
(+39) 02 36572 890
www.hanwha-security.eu/it



Il modulo telecamera **Wisenet PNM-9000QB** è progettato per bancomat, vendita al dettaglio e altre applicazioni nascoste.

Gli obiettivi remoti miniaturizzati comprendono sensori dotati di obiettivo con ottica fissa e pinhole. Sono progettati per essere installati remotamente dagli altri componenti di una telecamera e ciò significa che possono essere installati in maniera discreta all'interno di un bancomat o un altro spazio ristretto o posizionati nell'angolo di una stanza o di un ascensore con l'aiuto di staffe di montaggio.

Grazie al potente chipset **Wisenet7** di **Hanwha Techwin**, il modulo telecamera **PNM-9000QB** è in grado di elaborare immagini provenienti da 4 obiettivi remoti contemporaneamente. Con un numero ridotto di cavi e switch di rete necessari, i tempi e costi di installazione sono ridotti. Con una sola connessione IP è sufficiente acquistare un'unica licenza VMS.

Quando sono collegati tramite cavi appositamente progettati e installati a distanza dal modulo, gli obiettivi remoti sono totalmente isolati dalla rete. Un'ulteriore protezione deriva dal Rilevamento anti-manomissione (inclusa nella suite di IVA del modulo, così come il rilevamento di defocus, movimento e loitering) che genera un allarme nel caso in cui una persona copra o modifichi l'area visualizzata.

La tecnologia **Wide Dynamic Range (WDR) "extreme"** offre prestazioni fino a 120 dB per abilitare ciascuno degli obiettivi remoti al fine di acquisire immagini Full HD da 2 MP nitide e definite alla massima velocità di trasmissione anche nelle condizioni di illuminazione scarsa ed elevato contrasto.

Addsecure IRIS-4 combinatore telefonico IP/4G EN 54-21 per allarmi incendio/guasto

ADDSECURE INTERNATIONAL AB
(+46) 20 32 20 00
(+39) 347 9977 838
www.addsecure.com



Alloggiabile all'interno del pannello allarmi incendio oppure nell'apposito contenitore anch'esso certificato

La serie **IRIS-4 4** di combinatori telefonici rappresenta la soluzione "Swiss Knife" di AddSecure in quanto è adatta alla trasmissione di allarmi antifurto, antincendio e tecnici, o una combinazione di questi.

Caratterizzata dai più elevati criteri di sicurezza, unitamente alla semplicità e flessibilità operativa, la serie IRIS-4 4 prevede 3 possibili modelli:

- IRIS-4 400 trasmissione 4G a percorso singolo
- IRIS-4 420 trasmissione IP a percorso singolo
- IRIS-4 440 trasmissione a doppio percorso IP / 4G

Soluzione universale

Grazie all'ampia gamma di interfacce, la serie IRIS-4 4 è compatibile con tutti pannelli di controllo per allarmi esistenti, di qualsiasi costruttore.

- Connessione Dialport (PSTN emulata) con support di un' ampia gamma di protocolli analogici (Contact ID, SIA, Scancom Fast Format, CESA, Telim, Robofon)
- Connessioni RS-485, RS-232 e TTL bus
- Ingressi logici programmabili con messaggi di allarme e ripristino in protocollo SIA, Contact ID o messaggi di testo SMS
- CAN bus standard industriale per interfacciamento con sistemi HVAC/domotica e integrazione del sistema di allarme con soluzioni di Smart Building Management

Implementazione semplice e rapida

La serie IRIS-4 4 presenta di serie il rinomato touch screen IRIS che consente la programmazione e la messa in servizio in meno di 3 minuti con menu di configurazione interattivi che guidano rapidamente tutto il processo di installazione.

È possibile anche l'utilizzo della suite di software denominata IRIS Toolbox utilizzabile da personal computer collegato direttamente tramite porta USB.

essecome
ONLINE

n. 2/2021
Anno XLI
Periodico fondato da Paolo Tura

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

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



*Non scherzate con noi.
Conosciamo Kung fu, Karate, Judo
ed altre 27 pericolosissime parole!*



LA SOLUZIONE È SAN GIORGIO.

AMBITI

FORMAZIONE PER LE GPG
SICUREZZA SUSSIDIARIA
AVIATION SECURITY
TRAINING SU CBT: X-BAG
FORMAZIONE CONTINUA FINANZIATA
SICUREZZA SUL LAVORO

AGGIORNAMENTO DM. 269 E 154
AVSEC TUTTE LE CATEGORIE
COVID-19 PER LA SECURITY
GESTIONE CENTRALE OPERATIVA
TECNICHE DI COMUNICAZIONE PER L'UTENZA
GESTIONE DELLE EMERGENZE
ANTIRAPINA
ARMI ED ESPLOSIVI
ANTITERRORISMO

ALCUNI CORSI

TRAINING SOLUTIONS

SAN GIORGIO SRL