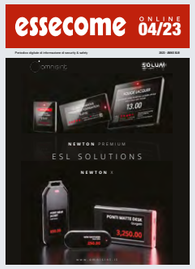
essecome ONLINE 04/23

Periodico digitale di informazione di security & safety

2023 · ANNO XLIII

Cover Story

ETICHETTE ELETTRONICHE SOLUM. ELEGANTI, RESISTENTI, UNICHE.



Inizialmente sviluppate per rispondere alla crescente necessità dei retailer di aggiornare i prezzi dei numerosi articoli esposti nel punto vendita in pochi secondi e più frequentemente, le etichette elettroniche vengono oggi impiegate per svariate funzioni anche nel settore industriale, logistico, in edifici istituzionali, hotel, università e sedi aziendali. Non solo un semplice strumento per la gestione del cambio prezzo, ma un imprescindibile tool per la comunicazione digitale in negozio, per il digital signage, per la gestione dei magazzini e per molto altro ancora.
Le etichette elettroniche **SOLUM** della linea NEWTON, offerte da **Omnisint**, rappresentano l'ultima innovazione nel settore ESL. Le caratteristiche:

- Migliore efficienza energetica per una maggiore durata della batteria
- La velocità di aggiornamento dati più veloce sul mercato
- Maggiore risoluzione del display
- Elevata resistenza agli urti grazie alla protezione del display
- Maggiore interazione con LED e PULSANTI
- Compatibilità dei gateway per utilizzare tutte le diverse gamme Newton nello stesso sistema

SOLUM crea soluzioni che non solo rendono le aziende più efficienti, ma le aiutano anche a rimanere più sostenibili nel lungo termine. L'obiettivo è quello di aiutare le aziende a progredire commercialmente, e allo stesso tempo essere sostenibili per il pianeta.
Eliminare la carta è uno dei tanti sforzi che molte aziende stanno compiendo per diventare più ecologiche.
Come suggerisce il nome, le etichette elettroniche da scaffale ti danno la possibilità di sostituire le etichette cartacee con una soluzione più sostenibile. Altri processi aziendali, come la gestione dell'inventario, possono essere trasformati in digitale. Ciò riduce il consumo di carta di quasi il 90%, razionalizzando e automatizzando le operazioni e riducendo i costi a lungo termine.

Riduzione del consumo di energia
La gamma di ESL Newton ha una durata della batteria di dieci anni, che significa meno sostanze chimiche tossiche nelle discariche. La riduzione del consumo energetico fa risparmiare denaro alle aziende e riduce le emissioni di gas serra che contribuiscono al cambiamento climatico.
Inoltre, le batterie rimovibile delle ESL Newton permettono di rispettare il regolamento sulle batterie imposto dalla UE, che richiede che i prodotti siano efficienti dal punto di vista energetico e progettati in modo ottimale per una facile raccolta delle batterie esauste.

Raggiungere una tecnologia sostenibile attraverso processi di produzione efficienti
Con i nostri impianti di produzione in Vietnam e in Messico, ci assicuriamo inoltre che tutti i prodotti siano fabbricati in ambienti sicuri.
Seguiamo rigorosi programmi di garanzia della qualità, che permettono al marchio di ottenere certificazioni internazionali sulla qualità del prodotto, l'ambiente e la sicurezza dei dipendenti.

Sommario

05 Nessuno deve sentirsi un "poveraccio a mano armata"

06 Videosorveglianza e Intelligenza Artificiale (AI): quale impatto "concreto"?

12 Idee e proposte da Axis Cybersecurity Summit 2023

16 Security, sustainability, building management: un'integrazione obbligata

18 Security Intelligence in ambito aziendale, una sfida impegnativa

20 Sicurezza sussidiaria, ampliare gli spazi di intervento

22 Ominsint all'avanguardia per la digitalizzazione delle operazioni in-store

24 Sicurezza bene collettivo e mercato: le nuove proposte di San Giorgio Formazione

28 Perché dare priorità e investire nella resilienza è importante nel settore dei trasporti

30 La sicurezza per i porti secondo DAB Sistemi Integrati

32 Sicurezza di gallerie ferroviarie, assaggi a livello e depositi: i vantaggi della tecnologia LiDAR

34 Affrontare le sfide della sicurezza fisica nella logistica e nel trasporto: la soluzione Reconeyez

36 Port Facility Security Plan per il Porto di Termini Imerese

38 Merci e customer experience, le nuove frontiere della Supply Chain

40 OPTEX, come garantire la sicurezza di persone e beni all'interno di un porto

42 Travel Risk Management nel XXI secolo

44 Sicurezza aeroportuale e prevenzione antiesplosivi. La tutela dei viaggiatori a cuore di Cittadini dell'Ordine Spa

48 Redazionali Tecnologie

Nessuno deve sentirsi un "poveraccio a mano armata"

E' fattuale, direbbe il Feltri by Crozza: lo sgradevole titolo dell'articolo de L'Espresso del 25 giugno (pag. 76) è uno schiaffo in faccia alla vigilanza privata made in Italy e spazza gli ultimi residui di credibilità di un'imprenditoria incapace di superare gli arcaici modelli di business basati sullo sfruttamento di massa dei lavoratori.
Paolo Biondani e Gloria Riva raccontano nell'articolo in questione dell'inchiesta della Procura di Milano che ha coinvolto finora Mondialpol e Sicuritalia con Esselunga quale utilizzatore su presunti aggiramenti del divieto di intermediazione della manodopera con un sistema di cooperative fasulle.
Già che erano sul pezzo, sono andati a scandagliare anche le retribuzioni dei lavoratori del settore "scoprendo" che una guardia giurata con 20 anni di servizio guadagnerebbe 1.120 euro netti per 173 ore di lavoro e che il famigerato "livello F" del CCNL - scaduto nel 2015 e appena rinnovato - prevede una paga oraria di euro 3,90 sotto la soglia di povertà costituzionale, arrivando alla mortificante conclusione che le guardie sarebbero solo dei "poveracci a mano armata".

Sul piano della comunicazione, la sentenza di condanna è già emessa e sarà molto arduo ricostruire l'immagine dell'intero sistema.
Adesso non conta puntualizzare che in realtà le guardie giurate abbiano anche altre componenti retributive che integrano in modo robusto e legittimo le buste paga, come i buoni pasto e le molteplici indennità di funzione frutto di anni di contrattazione territoriale; né che tanti imprenditori si siano tenuti alla larga dagli appalti di pura manovalanza al massimo ribasso investendo invece sui servizi a valore aggiunto, sull'innovazione tecnologica, sulla crescita professionale dei propri dipendenti.
Adesso fanno notizia solo l'inchiesta penale e l'imbarazzante situazione salariale che portano l'opinione pubblica a considerare tutti gli imprenditori dei poco di buono e tutte le guardie degli incapaci neanche in grado di fare altri mestieri dove guadagnerebbero di più come, ad esempio, i camerieri contesi da bar e ristoranti in ogni parte d'Italia a suon di aumenti dello stipendio.

Ci sarà da capire con quale fiducia le aziende, i privati cittadini, le stesse PA affideranno la propria sicurezza a soggetti di tale reputazione ma anche, e questo potrebbe essere il vero punto di caduta, con quali aspettative si presenteranno le persone per venire assunte in quelle aziende e con quale spirito andranno al lavoro. Un lavoro che, non dimentichiamo, può anche comportare dei rischi pesanti per l'incolumità personale.
A questo punto, se gli imprenditori della vigilanza vogliono pensare seriamente al futuro devono recuperare credibilità con urgenza ridando prima di tutto dignità ai lavoratori affinché nessuno possa sentirsi un "poveraccio a mano armata".
Ma nemmeno disarmata, per favore.

Videosorveglianza e Intelligenza Artificiale (AI): quale impatto “concreto”?

L’introduzione della AI nella videosorveglianza spingerà le soluzioni “edge” invece che “cloud” per l’analitica video. Nell’articolo l’ing, Angelo Carpani, libero professionista iscritto nell’Ordine degli Ingegneri della Provincia di Como n.2368 sez.A e docente per securindex formazione, spiega perché.

Affermare che l’intelligenza artificiale avrà un impatto importante anche nel mondo della videosorveglianza è scontato e quasi banale. Scrivo volgendo lo sguardo al futuro ma, in realtà, le cose stanno già cambiando e le nuove tecnologie di AI sono già presenti nel mercato della videosorveglianza.

Cambieranno i paradigmi nella scelta di una telecamera e nell’architettura dei sistemi di videosorveglianza. Rispetto a quest’ultimo aspetto, sono già intervenuto in diverse occasioni affermando che il mondo della videosorveglianza evolve sempre di più verso l’*edge* anziché il *cloud*.

Gestire a livello centralizzato su un server (modalità *server-based*) gli algoritmi di intelligenza artificiale applicati a centinaia di telecamere richiederebbero delle prestazioni in termini di capacità computazionali della CPU o GPU (Graphics Processing Unit) estremamente elevati, anche in termini di costi e consumi di energia. L’introduzione dell’AI nel mondo della videosorveglianza spingerà quindi ancora di più verso le soluzioni in *edge* anziché in *cloud*: le analitiche video basate su AI vengono applicate direttamente sulle telecamere (modalità *edge-based*) dotando le stesse di acceleratori hardware dedicati come *MLPU (Machine Learning Processing Unit)* e *DLPU (Deep Learning Processing Unit)*, evitando la complessità e i costi per il trasferimento dell’immagini su cloud per la loro elaborazione.

Dell’intelligenza artificiale ne sentiamo parlare ogni giorno sempre di più ed è un campo vastissimo, con innumerevoli applicazioni; in questo breve articolo vorrei soffermarmi in particolare sulle implicazioni nel mondo della videosorveglianza che sono, a mio parere, due.

Della prima ne ho già accennato sopra e riguarda le implicazioni sull’architettura dei sistemi di videosorveglianza in cui si sta attuando un passaggio nell’elaborazione delle immagini dalla *modalità server-based* alla *modalità edge-based*, quindi con una elaborazione delle immagini bordo camera e non su server.

La seconda riguarda la scelta della telecamera e non è così scontato/necessario e conveniente che si debba optare per forza per telecamere che implementano algoritmi di intelligenza artificiale come *Machine Learning* o *Deep Learning* più costose. Sarebbe forse necessario illustrare prima il vocabolario dei termini e delle tecnologie che si usano ma, senza entrare in troppi dettagli tecnici (piuttosto complessi e che richiederebbero molte pagine) mi limito ad accennarne qualcuno peculiare nell’elaborazione delle immagini.

Sentiamo ad esempio parlare di reti neurali che implementano algoritmi matematici per imitare il processo decisionale del cervello umano. I neuroni del cervello vengono replicati in un modello matematico della rete neurale umana per generare un algoritmo. Ad es. per il riconoscimento di immagini è più adatta una *rete neurale convoluzionale (CNN – Convolutional Neural Network)*, mentre una *rete neurale ricorrente (RNN – Recurrent Neural Network)* è più indicata per l’elaborazione del parlato.

Dicevo: non è così scontato/necessario e conveniente che si debba optare per forza per telecamere che implementano algoritmi di intelligenza artificiale. Ad esempio, per applicazioni di videosorveglianza in cui si debbano rilevare delle intrusioni in un ambiente in cui lo sfondo è fisso (ad esempio, una persona che entra in una reception) è sufficiente l’adozione di una telecamera che implementi un classico algoritmo di video analisi come la “sottrazione dello sfondo” *(background subtraction)*.

La “sottrazione dello sfondo” richiede una potenza di elaborazione molto bassa ed è mirata agli oggetti in movimento, ignorando tutti quelli statici.

L’adozione invece di telecamere che implementano algoritmi di intelligenza artificiale come *Machine Learning* (ML) e *Deep Learning* (DL) dipende dal target che si vuole rilevare.

Prima di entrare nel merito occorre sapere che le telecamere che implementano algoritmi di intelligenza artificiale, per imparare a riconoscere gli oggetti e a classificarli in determinate categorie (classi), *vanno addestrate* con una grande quantità di dati campione o *dati di addestramento*; questi ultimi vengono etichettati, o meglio *annotati*. L’addestramento può essere fatto dal costruttore con un apprendimento di tipo:

- *supervisionato:* è il metodo più utilizzato nel Machine Learning e può essere descritto come un apprendimento basato su esempi. I dati di addestramento vengono annotati (o etichettati) chiaramente: i dati di input sono già abbinati ai risultati di output desiderati;
- *per rinforzo:* l’algoritmo non utilizza coppie dati/etichetta per l’addestramento, ma impara da solo dagli errori ricevendo un premio quando compie le scelte giuste.

Ebbene, senza farla troppo complicata (perché la materia è davvero complicata), possiamo dire che:

- se si ha necessità di riconoscere all’interno di una scena un “qualsiasi” oggetto in movimento, è sufficiente l’adozione di una telecamera che implementi un classico algoritmo di video analisi di tipo “background subtraction”;
- se si vogliono riconoscere solo “oggetti specifici”, occorre adottare una telecamera che implementi algoritmi di AI di tipo *Machine Learning* addestrata sul campo (generalmente sono necessari 100-300 campioni e necessita di ridotte risorse hardware);
- se si vogliono riconoscere determinate “classi” di oggetti (es. automobili piuttosto che motociclette), occorre adottare una telecamera che implementi algoritmi di AI di tipo *Deep Learning* addestrata dal costruttore (generalmente sono necessari 20.000-100.000 campioni e necessita di una elevata potenza computazionale).

La scelta di una telecamera non si baserà quindi più solo sui classici paradigmi quali la risoluzione, la sensibilità del sensore, il tipo di ottica, ecc. ma anche sul tipo di AI in funzione della scena che si vorrà inquadrare (ad esempio se lo sfondo è statico come la parete di una stanza, o in continuo movimento come i veicoli che percorrono una strada con traffico intenso) e degli oggetti che si vorranno rilevare (ad esempio se sono “specifici” o se ci si vuole limitare a rilevare il tipo o la “classe”).

Nella progettazione di un impianto di videosorveglianza, con l’introduzione dell’AI, bisognerà quindi fare riferimento “concretamente” a dei nuovi paradigmi che riguardano sia l’architettura degli impianti (sempre più verso l’*edge*) che la scelta delle telecamere.

everbridge™

Mantenere le persone in sicurezza e le operazioni in funzione.

Di fronte ad eventi critici quali, disastri naturali, guasti infrastrutturali, conseguenze reputazionali post gravi incidenti, Everbridge garantisce piena consapevolezza sulle situazioni vigenti mediante risposte integrate abilitando approccio collaborativo.

- Proteggere persone e beni
- Rispondere più velocemente
- Ridurre al minimo le interruzioni

www.everbridge.com

@everbridge

OPTEX
Sensing Innovation

PROTEZIONE DA OGNI LATO

Rilevamento a lungo raggio con REDSCAN Pro

REDSCAN Pro utilizza la tecnologia LiDAR per rilevare con precisione intrusioni e oggetti in movimento fino ad una distanza fino a 50 x 100 m, il che rende questo prodotto particolarmente adatto per la protezione di siti di massima sicurezza. Inoltre, grazie alla possibilità di creare schemi di rilevamento rettangolari ad alta risoluzione, non si creano spazi vuoti, per cui è possibile coprire ogni tipo di superficie, dalle facciate alle recinzioni, dai soffitti ai tetti. La logica intelligente a zone multiple del sensore consente di configurare ogni zona di rilevamento in modo indipendente, mentre il modulo telecamera offre assistenza visiva per la configurazione e l'analisi post-allarme.

www.optex-europe.com/it

ONVIF® | S

ONVIF is a trademark of Onvif, Inc.

INTRUSION DETECTION | VISUAL VERIFICATION | TAILGATING DETECTION | VEHICLE DETECTION | PEOPLE COUNTING

Ad APR 2023 il caso studio della nave rigassificatrice a Piombino

Angelica Cestari, Head of Security Services & Operations di Snam e Vice Presidente di AIPSA, ha descritto ad APR 2023 il progetto del rigassificatore di Piombino, la cui progettazione, messa in opera e gestione coinvolge ogni aspetto della sicurezza

Partiamo dal caso della nave rigassificatrice di Piombino, quali sono gli aspetti più probanti di un intervento che coinvolge security, safety, impatto ambientale?

Il progetto che ha portato il Paese a dotarsi, attraverso il lavoro di Snam, del rigassificatore di Piombino è sorto da un'esigenza legata al conflitto russo-ucraino e quindi da uno scenario già delicato in partenza. Tutte le fasi che hanno portato la Golar Tundra ad arrivare nel porto di Piombino hanno quindi rappresentato una sfida importante sotto gli aspetti della sicurezza comunque declinati.

Come Head of Security Services & Operations di Snam ho coordinato una profonda attività di analisi dei rischi connessi ad ogni potenziale minaccia e legati ad un progetto dalla portata simile: sicurezza delle persone e degli asset, fattibilità logistica, quadro autorizzatorio. Molti sono stati poi gli interlocutori che abbiamo coinvolto e con i quali, di volta in volta, ci siamo interfacciati: istituzioni, forze dell'ordine, autorità portuale e partner esterni, solo per citarne alcuni. Proprio l'elevato numero di attori interessati ha rappresentato un altro elemento che ha richiesto notevoli sforzi. Il fattore tempo ha poi rappresentato uno degli elementi più sfidanti. Posso affermare che Snam è riuscita a portare a termine una "missione" di fondamentale importanza per la sicurezza energetica del Paese, in un tempo record. In circa 6 mesi è stato, infatti, possibile dotare il Paese di questa Fsru, un'alternativa efficace alla progressiva diminuzione delle forniture di gas provenienti dalla Russia. Per il Team di Security una delle sfide è stata proprio quella di dover fare i conti con tempistiche brevi. Abbiamo dovuto impiegare un gruppo di lavoro multidisciplinare con una serie di competenze specifiche per poter traguardare il risultato atteso e ci siamo trovati a dover fronteggiare anche rischi connessi a manifestazioni contrarie all'opera.

Molti sostengono che l'approccio al femminile alla sicurezza sia un valore aggiunto. Cosa ne pensa la Vicepresidente di AIPSA?

Sono d'accordo nel sentir dire che l'istinto femminile possa rappresentare un valore aggiunto per quanto attiene le dinamiche legate al settore della sicurezza. È un'affermazione in cui credo fermamente. Per naturale inclinazione, il punto di vista di noi donne offre una visione d'insieme all'insegna della pragmaticità. In particolare, oltre al mio ruolo di Head of Security Services & Operations di Snam, la mia esperienza ai vertici di un'organizzazione attiva nell'ambito della sicurezza come nel caso di Aipsa (Associazione Italiana Professionisti Security Aziendale), in cui ricopro il ruolo di Vicepresidente dal 2022, è iniziata con il precedente mandato nel 2018, in cui ero già all'interno del Consiglio direttivo. Sono stata la prima donna a ricoprire il ruolo vicario, aspetto che è sicuramente motivo di orgoglio. L'impegno di Aipsa nel promuovere il ruolo delle donne e dei giovani è sicuramente un segnale forte nel settore e dimostra come nessun incarico o ambito siano preclusi alle donne che perseguono i propri obiettivi con determinazione e passione.

Quali indicazioni ritiene di dare ai giovani interessati ad entrare nel mondo della security?

I suggerimenti che ritengo opportuno condividere con i giovani interessati ad entrare nel mondo della security sono: seguite sempre le vostre passioni e soprattutto informatevi sulle opportunità in ambito formativo e lavorativo. A differenza di diversi anni fa, adesso, c'è molta attenzione nei confronti del settore della sicurezza e le università offrono percorsi molto interessanti in grado di fornire gli strumenti utili per poi intraprendere una carriera in questo settore. Ci sono poi le aziende, tra cui Snam, che offrono stage per i laureati che vogliono approcciarsi all'affascinante e delicato mondo della "Security", consentendo ai giovani di formarsi sul campo ed essere affiancati da professionisti già affermati. Un'occasione davvero da non perdere per uno studente intenzionato a passare dalla teoria alla pratica così da poter ambire ad essere un security manager del futuro.

Idee e proposte da Axis Cybersecurity Summit 2023

intervista a Matteo Scomegna, Regional Director Southern Europe di Axis Communications

Possiamo tracciare un bilancio dell'edizione 2023 dell'AXIS Cybersecurity Summit?
L'Axis Cybersecurity Summit di Roma e di Milano si inserisce nel contesto più ampio di un ciclo di incontri che abbiamo organizzato in diversi paesi del Sud Europa, a partire da Parigi lo scorso giugno. Alla base di queste iniziative c'è la volontà di Axis di organizzare dei momenti di confronto tra tutti gli attori principali del nostro settore, nazionali e internazionali, con l'obiettivo di condividere ciascuno le proprie esperienze e, allo stesso tempo, sensibilizzare su quella che è una tematica molto attuale e complessa.
In questo senso, possiamo ritenerci soddisfatti, perché l'adesione al Cybersecurity Summit italiano è stata alta, così come l'interesse mostrato dai partecipanti e dagli speaker. Più nel dettaglio, nel corso dei tre panel di discussione sono emersi numerosi spunti che hanno permesso di approcciare la cybersecurity da diverse prospettive. Una prima occasione di confronto ha riguardato l'aumento preoccupante delle minacce informatiche e la definizione delle responsabilità; seguita da un approfondimento sul quadro normativo attuale e futuro, a partire dalle Direttive NIS I e II, dalla Direttiva CER, passando per il Regolamento DORA; fino alle proposte ancora oggetto di discussione del Cyber Resilience Act e del Cyber Solidarity Act.
A conclusione dell'evento si è quindi ripresentata con forza la domanda: come lavorare insieme per ridurre i rischi legati alla cybersecurity? La priorità per affrontare queste nuove sfide, dal nostro punto di vista, risiede infatti nella collaborazione e nel fare della sicurezza informatica una responsabilità condivisa tra produttori, system integrator e utenti finali, implementando le migliori pratiche e una vigilanza e manutenzione continua, all'insegna della massima trasparenza. Naturalmente, alla luce di quanto detto e della necessità di concepire la cybersecurity come un processo continuo, l'impegno di Axis in questa materia non si ferma di certo qui; al contrario, puntiamo a essere riconosciuti come centro focale nel nostro ecosistema e a dare sempre di più il nostro contributo.

Quest'anno è stata riproposta con forza la questione delle criticità in termini di sicurezza della supply chain, in altre parole della difficoltà delle PMI ad adeguarsi agli standard previsti dalle normative. Dal vostro punto di vista, i vendor possono avere un ruolo per migliorare la situazione?
Uno dei trend più evidenti degli ultimi anni è sicuramente quello della digital transformation di imprese e organizzazioni, in cui si assiste, da un lato, a una sempre maggiore convergenza tra mondo fisico e digitale, con un considerevole ampliamento della superficie di attacco, e, dall'altro, all'emergere di nuove tecnologie come l'AI, l'IoT e il multi-cloud, che creano nuove vulnerabilità per tutti i partner e i fornitori di quello che è ormai un ecosistema interconnesso. Ne deriva che la cybersecurity debba necessariamente essere una priorità a tutti i livelli della catena di collaborazione, dai produttori ai system integrator, fino agli end-user, e naturalmente anche i vendor svolgono un ruolo chiave, offrendo delle soluzioni progettate secondo il principio *secure by default*.
Ciascuno è chiamato a fare la sua parte, in un'ottica di massima trasparenza e collaborazione. Questa è la filosofia che guida anche noi di Axis nello svolgimento delle nostre attività e che ci porta a credere fermamente nel concetto di *shared responsibility.* Soprattutto all'interno di un quadro normativo articolato, che alza i requisiti di sicurezza per le organizzazioni, in particolare per quelle che operano nel segmento delle infrastrutture critiche, la rete di partner e clienti è fondamentale per rispettare gli standard ed essere *compliant*. Questo vale a maggior ragione per le PMI, che possono incontrare maggiori difficoltà nel reperire al proprio interno le risorse necessarie.

E quali potrebbero essere le leve per indurre le PMI ad essere compliant?
Come accennavo prima, le imprese e le organizzazioni non possono essere considerate a sé stanti, ma vanno osservate in quanto parte di un più ampio network, innovativo e digitale, in cui è necessario stabilire un continuativo e proficuo scambio di best practice tra tutti gli attori coinvolti per essere sempre aggiornati sulle normative e rendere le proprie soluzioni il più *cyber-safe* possibile. In questo modo anche le PMI possono trarre vantaggio da un contesto collaborativo, implementando misure di sicurezza più avanzate e diventando più resilienti.
Un altro tema emerso, determinante per le PMI, è quello della formazione, che riguarda sia la necessità di creare nuove figure altamente specializzate sia di diffondere una cultura sulla sicurezza informatica all'interno di tutte le organizzazioni interessate. Le PMI sono, infatti, tendenzialmente più propense a sottovalutare la gravità degli attacchi e la portata dei danni che ne possono derivare, in parte anche per una limitata cultura aziendale sulla tematica. In questo senso, la formazione e la messa a fattor comune delle esperienze degli altri player svolgono un ruolo cruciale nell'incrementare l'awareness sui rischi e sulle migliori best practice da implementare.
Più in generale, è però importante sottolineare come la formazione e l'educazione siano aspetti che interessano trasversalmente tutti gli operatori del comparto, non solo le PMI. Questo perché una delle sfide da affrontare risiede nella ricerca di professionisti con skill e competenze specifiche, verso cui si registra attualmente una forte richiesta, che il mercato non riesce ancora a soddisfare. La componente umana dovrebbe quindi essere una priorità, così che tutti possano agire e diventare loro stessi un fattore di sicurezza.
Dal punto di vista più tecnico invece, per aiutare PMI e non solo, ad essere compliant, noi di Axis e tutte le parti coinvolte nell'evento abbiamo chiarito che la cybersecurity deve essere la priorità assoluta per il management, identificando e comprendendo risorse, sistemi e obiettivi aziendali. Implementare un framework su cui innalzare la sicurezza e gestire il rischio delle risorse e delle operazioni sono i passi successivi. Infine, stabilire un processo di reporting conforme ai requisiti NIS2 e sfruttarlo attivamente contro le minacce.

È riaffiorata anche la questione della security by design dei device, con la questione dell'affidabilità degli stessi vendor. Come si potrebbe divulgare una maggiore consapevolezza presso le centrali di acquisto/procurement?
Certamente la questione della security by design dei device è emersa più volte nel corso dell'evento, come requisito in capo ai vendor per essere riconosciuti come partner di fiducia dagli end customer. Questi ultimi infatti sono i primi a richiedere specifiche e dettagli sulla progettazione delle soluzioni, al fine di assicurarsi che il prodotto di

interesse sia il più sicuro possibile. Una spinta affinché i vendor adottino questo approccio arriva quindi dai loro stessi clienti.

D'altra parte, però, gli end customer, così come i system integrator, devono avere ben chiare le feature di sicurezza di questi prodotti, in modo tale da poterli configurare nel modo più opportuno e adottando le migliori pratiche; quindi, rendere note le best practice, così come i rischi e le debolezze con l'obiettivi di aumentare la consapevolezza della security by design dei device per ogni parte coinvolta, è pertanto un altro fattore rilevante.

In sostanza, come dicevamo, non è solo la tecnologia a impattare sulla sicurezza di un prodotto, ma anche la sua corretta installazione e configurazione, ogni attore è quindi chiamato in causa per far sì che nei vari step si riducano al minimo le vulnerabilità e i rischi che potrebbero subentrare in un momento successivo, qualora non vengano adottate delle procedure adeguate. La parola chiave resta quindi sempre awareness, insieme alla condivisione di conoscenze e best practice.

AXIS COMMUNICATIONS

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

Security, sustainability, building management: un’integrazione obbligata

In occasione del 20° anno di attività di Alesys, il fondatore e CEO Alessandro Ferrari riassume la storia, i prodotti e la visione del futuro dell’integrazione dei sistemi per la sicurezza, la sostenibilità e la gestione degli edifici. Il tema verrà sviluppato il 19 settembre nel convegno organizzato con la collaborazione di securindex presso Eataly Teatro Smeraldo di Milano.

Ci racconti di Alesys, della sua storia, del percorso compiuto in venti anni?
Alesys nasce nel 2004 come società di consulenza nello sviluppo software e, nei suoi primissimi anni, si occupa di progettare applicativi personalizzati per clienti di varia tipologia. In questo periodo iniziano ad apparire i primi dispositivi di sicurezza gestibili in rete e arrivano sempre più spesso richieste di integrazione in quelle che erano soluzioni SCADA. Queste piattaforme arrivavano sempre dal mondo del controllo industriale e richiedevano molto tempo e risorse per una buona implementazione. Dove il budget non lo permetteva, si optava per piantine cartacee o sinottici a led nei migliori dei casi. Nasce così nel 2006 l’idea di realizzare una piattaforma facile da utilizzare e configurare, pensata per essere installata in ambienti medio-piccoli dove, fino ad allora, una supervisione era assolutamente impensabile in termini di costi e complessità. Nel 2007 viene rilasciata la versione 1.0 e da quel momento lo sviluppo non si è mai arrestato aggiungendo sempre nuove funzionalità, tecnologie e nuovi driver. Attualmente i driver disponibili supportano più di cinquanta prodotti integrabili.

Qual è la vostra organizzazione attuale e quali le linee di prodotti?
L’organizzazione di Alesys è sempre stata improntata da una vocazione tecnica e, infatti, la maggior parte dei collaboratori si dedica alla ricerca e sviluppo. Questa struttura permette di sviluppare internamente i nostri prodotti in modo dinamico e reattivo, rispondendo in modo rapido e personalizzato alle richieste del cliente. Il prodotto principale è la piattaforma “Integro” che permette l’integrazione e la supervisione di sistemi di sicurezza e non solo. La proposta di Alesys si completa con una serie di prodotti e applicazioni “accessorie” alla soluzione, in modo da supportare il cliente nella realizzazione del sistema. Ultima, ma non meno importante, è la parte di servizi che supportano i clienti nella transizione verso un mondo sempre più orientato verso l’information technologies.

A quali categorie di utenti finali vi rivolgete principalmente?
Non esiste una categoria specifica di utilizzatori delle nostre soluzioni. Tutti gli edifici, i campus o realtà multi-sito in cui è previsto un monitoraggio, una portineria o una guardiania possono utilizzare le nostre soluzioni per velocizzare e migliorare la gestione degli allarmi e degli impianti. In questi vent’anni le soluzioni realizzate spaziano dal terziario all’industriale fino alle infrastrutture come tramvie, stadi o ospedali. Le esigenze di gestione sono in realtà molto simili sia che si parli, ad esempio, di aziende farmaceutiche che, sempre per fare un esempio, di aziende del mondo della moda. Il miglioramento della connettività internet ha permesso, inoltre, di estendere in modo efficace l’utilizzo delle soluzioni di supervisione anche per i piccoli siti non presidiati la cui sicurezza è comunque importante quali, ad esempio, campi fotovoltaici, ATM o locali tecnici.

Parliamo di integrazione tra building management, security, sustainability. Qual è il ruolo di uno PSIM?
Nel tempo, i punti da monitorare e gli allarmi sono cresciuti in modo esponenziale e gli scenari sono diventati sempre più complessi. Diventa, così, necessario fornire uno strumento facile ed immediato che possa permettere, anche a personale non tecnico, la gestione delle informazioni. In un edificio moderno sono tante le figure specialistiche: dalla manutenzione, alla prevenzione incendi fino alla sicurezza fisica. Il corretto instradamento delle informazioni e la rapidità di gestione possono fare la differenza. Un esempio classico è la segnalazione di un sistema antincendio dove ogni singolo minuto può fare la differenza.
Un altro aspetto importante è la comunicazione e la collaborazione tra le varie tipologie di sistema ad oggi, molto spesso implementate con architettura a silos. La sicurezza può essere vista anche come “sensore” per il risparmio energetico: ad esempio è possibile utilizzare l’inserimento di un’area antintrusione per gestire luci e riscaldamento. Considerando che il mondo IP permette di realizzare un numero elevato di interazioni solo software, il limite, molto spesso, è la sola fantasia.

Quali sono le prospettive per il futuro del mercato dell’integrazione, dal vostro punto di osservazione?
Il mercato dell’integrazione tenderà sempre più all’unificazione delle interfacce di gestione andando ad integrare sempre nuovi domini e ambiti quali, ad esempio, la comunicazione al pubblico o l’asset tracking.
I nuovi dispositivi smart trasformeranno la gestione di impianti centralizzati in sistemi distribuiti dove la raccolta dati e la loro rappresentazione dovrà essere in carico ai sistemi di gestione, che permetteranno all’utente di visualizzare solo le informazioni necessarie e generare gli allarmi in modo da avere un’operatività ad evento. Questa modalità ridurrà il rischio di essere sommersi da troppe informazioni e focalizzarsi, invece, sulla gestione delle reali segnalazioni.
Altro tema è l’infrastruttura di rete che diventa un punto fondamentale nella gestione dell’edificio intelligente. Il networking per lo smart building dovrà passare da “accessorio” a critico perché rappresenterà la spina dorsale dell’intero edificio.
Diventa quindi necessario progettare una rete affidabile, scalabile e performante per permettere la corretta fruizione di tutti i dati. Anche la rete stessa dovrà diventare un nuovo livello di integrazione in modo da monitorarne problemi e malfunzionamenti. A questo aspetto è necessario aggiungere tutti concetti di Cyber Security, necessari a proteggere il corretto funzionamento dell’edificio. La protezione della rete è ancor più necessaria considerando che, in molti casi, i dispositivi utilizzano protocolli datati e non più corrispondenti ai moderni requisiti di sicurezza.

ALESYS
SECURITY MADE SIMPLE

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

Security Intelligence in ambito aziendale, una sfida impegnativa

Security intelligence in ambito aziendale, una sfida impegnativa anche per un convegno. Chiediamo a Salvatore Castiglia, general manager di Kriptia un bilancio di quello organizzato il 20 giugno con un parterre di relatori di primissimo piano.

La Security Intelligence da sempre è un bene essenziale in cui le aziende hanno investito e che imprenditori illuminati hanno utilizzato come base per i loro progetti.
Purtroppo, negli ultimi anni si sta divulgando un trend piuttosto pericoloso che vuole il dirottamento della security aziendale nella cyber security, addirittura confondendo o sovrapponendo i ruoli. Le aziende non erano in passato – e spesso non sono oggi – preparate a rispondere alle minacce cyber, questo anche perché sempre meno aziende, soprattutto PMI, si affidano a società esterne per analizzare i loro rischi. Di conseguenza si nota come abbiano spostato gran parte dei budget di security fisica nella cyber security. Inoltre alcuni security manager senza nessuna competenza in cyber security ne sono diventati responsabili, unificando così i ruoli. Volendo fare un paragone, è come se l'HR manager diventi improvvisamente anche il responsabile commerciale. Sempre meno infatti si assiste a strutture organizzate, dove un team con diverse peculiarità lavora sul progetto e senza demandare al singolo manager la responsabilità (e quindi il budget) di tutto ciò che è security.
Il 20 giugno abbiamo voluto dare voce a quei professionisti che lavorano su settori diversi ma sempre in ruoli inerenti alla funzione di security aziendale. Abbiamo sentito dalla dott.ssa Gubbiotti e dalla dott.ssa Pieroni come i dati e la loro analisi sia un valore per le aziende e che non sempre queste siano disponibili ad investire soldi e tempo in questo tipo di attività. Abbiamo ascoltato il dott. Farris e il dott. Florio per quanto riguarda il tema della sicurezza fisica in relazione ai temi del Risk Management e della Travel Security. Abbiamo approfondito con il dott. Colella e l'ing. Tofalo il tema cyber nelle aziende e le relazioni tra cyber e fattore umano all'interno delle aziende. Per ultimo, ma non meno importante, con il prof. Pigoli abbiamo trattato l'uso dell'intelligence in ambito aziendale a fronte dell'ecosistema produttivo italiano, unendo così i temi di sicurezza fisica e cyber security.

Una delle conclusioni del convegno è la ritrovata centralità della persona, tutt'altro che scontata nell'era della A.I. Quali sono i presupposti che hanno portato a questa conclusione?
Il fattore umano è da sempre un tema centrale, in tutti i settori. Anche nell'automazione, senza dei bravi ingegneri non riusciremmo ad automatizzare nulla. Il sottile confine sta nel limitare l'utilizzo di AI e delle varie tecnologie di automatizzazione per velocizzare i processi e quindi essere più produttivi. Al contrario, sbagliando, si tende a pensare di poter sostituire semplicemente l'essere umano con la macchina.
Nell'ultimo periodo ho letto diverse notizie sull'automatizzazione di analisi e report. Mi preme però sottolineare che lo stesso concetto di analisi prevede una ricerca e comprensione di diversi elementi che spesso non possono essere sostituiti da un algoritmo.
Allo stesso tempo, il fattore umano spesso può rappresentare il punto debole della catena di security, basti pensare alle mail di phishing o ad un badge lasciato in auto. Entrambi questi esempi, per quanto sembrino due problemi inerenti a settori diversi (fisico e cyber), rappresentano invece allo stesso modo una criticità per la sicurezza dell'azienda, da trattare sia nella parte fisica che nella parte cyber.

Un'altra conclusione, più scontata, è la necessità di raggiungere le PMI, l'anello debole della cybersecurity, per aumentare il loro livello di sicurezza. Quali sono gli strumenti indicati?
In realtà le PMI spesso riflettono ciò che il mercato propone come best practise e di solito sono le grandi aziende a svolgere il ruolo di "influencer" in tutti i settori, dall'HR, alla contabilità, alla security. Quindi bisogna sottolineare che purtroppo anche i malcostumi e tendenze controproducenti alcune volte possono essere generate da multinazionali o associazioni di categoria, le quali spesso diffondono messaggi sbagliati o addirittura fuorvianti. Entrando nel merito, non sempre le PMI hanno le competenze per analizzare e comprendere questi messaggi e quindi si assiste ad amministratori di aziende di PMI che non disponendo di security manager affrontano anche problematiche complesse senza strategie adeguate, con il rischio di provocare danni maggiori.
Proprio per aiutare le PMI, Kriptia ha pensato di creare una piattaforma che possa gestire i rischi aziendali ed essere in linea con la normativa, rendendo così l'azienda sempre più compliant. Lo strumento che abbiamo creato si chiama Krion e gestisce i rischi legati alla sicurezza con audit di security (cyber e fisico), analisi controparte e travel security.

Partenariato pubblico-privato: in che modo può venire realizzato in modo efficace?
Il partenariato pubblico-privato (PPP) nella security aziendale è una forma di collaborazione tra enti governativi e privati per garantire la sicurezza delle aziende e degli impianti. Questa forma di partenariato coinvolge solitamente organizzazioni governative responsabili della sicurezza pubblica, come forze dell'ordine, agenzie di intelligence e agenzie di sicurezza, insieme a società private che offrono servizi di sicurezza aziendale.
L'obiettivo principale del partenariato pubblico-privato nella security aziendale è proprio quello di migliorare la prevenzione e la gestione delle minacce alla sicurezza, proteggendo le aziende da rischi come il furto, il danneggiamento, l'accesso non autorizzato, la violazione dei dati e il terrorismo.
In un modello di PPP, le autorità governative possono fornire informazioni sulle minacce alla sicurezza, offrire consulenza sulla pianificazione e la gestione della sicurezza e partecipare a operazioni di intelligence condivise. Le aziende private, d'altra parte, contribuiscono con le proprie risorse e competenze nella sicurezza aziendale, mettendo in atto misure di sicurezza, ad esempio, implementando sistemi di sorveglianza avanzati, addestrando il personale aziendale alla gestione delle emergenze e fornendo servizi di consulenza sulla sicurezza.
A mio avviso, i vantaggi del partenariato pubblico-privato nella security aziendale includono una maggiore efficacia nella prevenzione e nella risposta alle minacce alla sicurezza, una condivisione più rapida e accurata delle informazioni pertinenti e una migliore allocazione delle risorse. Inoltre, esso può promuovere la collaborazione e la condivisione delle migliori pratiche tra le organizzazioni pubbliche e private, contribuendo a creare un ambiente di sicurezza più resiliente. Tuttavia, è importante garantire che il partenariato pubblico-privato nella security aziendale sia basato su una solida base legale, che vengano rispettati i diritti e le norme sulla privacy e che venga stabilita una chiara responsabilità delle attività svolte. La collaborazione deve essere trasparente e i ruoli e le responsabilità di ciascuna parte devono essere definiti in modo chiaro per evitare ambiguità o abusi di potere.

Quindi che ruolo ha la Security Intelligence nell'azienda e quali sono le sfide future?
La Security Intelligence svolge un ruolo fondamentale nell'azienda nel rilevare, analizzare e rispondere alle minacce alla sicurezza. Questa funzione si concentra sulla raccolta di informazioni provenienti da una varietà di fonti, inclusi i dati interni dell'azienda, le informazioni pubbliche, i rapporti di intelligence governativa e le informazioni provenienti da partner esterni. L'obiettivo principale della Security Intelligence è fornire una visione approfondita delle minacce e delle vulnerabilità per prendere decisioni informate e implementare misure di sicurezza adeguate.
Per quanto concerne le sfide future, sicuramente sarà sempre più rilevante la crescita del volume dei dati a disposizione, ciò richiede l'adozione di strumenti e tecnologie avanzate come, per esempio, il machine learning e l'intelligenza artificiale, per estrarre informazioni significative dai dati in modo rapido ed efficace. Questo a fronte di una "guida" umana che deve essere sempre garantita anche solo per verificare che siano rispettate le normative sulla privacy. Le sfide coincidono anche con minacce sempre più sofisticate e la Security Intelligence deve essere in grado di adottare misure preventive adeguate e tenere il passo con le ultime tendenze e tecniche utilizzate dagli aggressori.
Come si diceva per le PMI, la mancanza di personale qualificato in queste aree rappresenta sicuramente una sfida per molte aziende, che devono investire nella formazione interna o cercare soluzioni esterne per colmare questa lacuna.
In conclusione, per affrontare queste sfide è importante che le aziende investano nella Security Intelligence come parte integrante delle proprie strategie di sicurezza. Ciò include l'implementazione di infrastrutture tecnologiche adeguate, l'aggiornamento costante delle competenze del personale e la collaborazione con partner affidabili nel settore della security.

KRIPTIA
SECURITY AND SAFETY SOLUTIONS

Contatti:
Kriptia
Milano +39 02 40031293
Miami (USA) +1 888 2496107
info@kriptia.it

Sicurezza sussidiaria, ampliare gli spazi di intervento

intervista a Giulio Gravina, co-fondatore del Gruppo Italpol Vigilanza

Ci può riassumere prima di tutto la storia di Italpol?
Italpol nasce nel 1975 da una intuizione di mio padre. Oggi l'azienda, condotta dalla seconda generazione, si articola in tre anime: Italpol Vigilanza, l'azienda autorizzata ai sensi dell'art. 134 del TULPS, Italpol Servizi Fiduciari, specializzata nei servizi di sicurezza disarmati e Socyb, l'azienda tecnologica che in questo momento ha posto il suo focus sui servizi di Cybersecurity.

Quali sono le dimensioni attuali, l'area operativa, i servizi effettuati?
Oggi il gruppo Italpol fattura più di 100 milioni di euro ed impiega 3.000 addetti tra personale armato e disarmato. Si pone pertanto tra i maggiori player nazionali. Siamo autorizzati ad operare nel Lazio, Lombardia, Campania, Sardegna, Umbria, Alto Marche, Trapani (Pantelleria), ed eroghiamo tutte le attività disciplinate dagli artt. 134 al 141 del TULPS. L'Azienda ha comunque acquisito in questi anni un particolare know-how nell'erogazione dei servizi sussidiari così come definiti dall'art. 18 del DL 21 luglio 2005, n. 144, guadagnando una posizione di leader di mercato. Oggi i luoghi di transito più importanti del Paese sono vigilati da personale ITALPOL opportunamente formato nel rispetto del D.M. n. 154/2009.

Quali sono i progetti per il futuro?
Consolidare l'esperienza acquisita nei servizi sussidiari e crescere ulteriormente in questo ambito con l'auspicio che lo Stato assuma consapevolezza dell'apporto fornito dai privati e ne allarghi gli spazi d'intervento.

Ci può spiegare più in dettaglio?
Il contributo dato dagli Istituti di vigilanza privata in termini di sicurezza sussidiaria, ormai consolidato negli anni, non mi sembra ricevere la giusta considerazione da parte dello Stato; significativo in tal senso il recente accordo concluso tra Ministero dei Trasporti e Ferrovie dello Stato per la gestione in house delle necessità di sicurezza presso le stazioni ferroviarie. Una delle motivazioni è probabilmente

da individuarsi nella mancata produzione di uno studio empirico che quantificasse i reali vantaggi e l'ottimizzazione nell'allocazione delle risorse statali, che deriverebbero dall'affidamento a guardie giurate dipendenti di istituti di vigilanza privata dei servizi di sicurezza sussidiaria presso i luoghi di transito contemplati dal D.M. n. 154/09.

L'esperienza acquisita sinora è positiva. Quale potrebbe essere l'evoluzione dei servizi di sicurezza sussidiaria?
I recenti fatti di cronaca ci dicono che l'esigenza di sicurezza non è solo limitata ai luoghi di transito in senso stretto e che sempre più spesso i reati avvengono nei luoghi di prossimità ai luoghi di transito come ad esempio le vie limitrofe alle stazioni ferroviarie. Sarebbe pertanto utile approfondire la possibilità d'impiego dei servizi di sicurezza sussidiaria anche in queste aree, sempre a garanzia e vantaggio di una maggiore sicurezza urbana.

Come vede invece il futuro dell'intero comparto dei servizi di vigilanza privata?
Il quadro normativo di settore implementato negli ultimi 15 anni ha contribuito a creare un mercato nazionale dei servizi di sicurezza privata, preservando in ogni modo la permanenza di player di dimensione medie-piccole espressione di territori specifici. Il comparto ha dimostrato una buona duttilità nel recepire ed allinearsi alle nuove disposizioni, dimostrando di essere pronto per una nuova fase d'innovazione normativa, a mio avviso necessaria e che sia volta a generare una modernizzazione, un consolidamento e uno sviluppo del settore della vigilanza privata, orientandolo verso il concetto più ampio di sicurezza privata e individuando così nuovi ambiti d'intervento sempre in una logica di complementarietà e sussidiarietà alla sicurezza pubblica, sfruttando l'esperienza acquisita in questi ambiti.
Un ulteriore elemento di riflessione, in termini di ampliamento dell'area d'intervento della vigilanza privata, è dato dai provvedimenti emanati negli anni recenti riguardo la sicurezza integrata ed urbana. In particolare, il decreto legge n. 14/2017 convertito dalla L. 18/04/17, n. 48 ha introdotto la definizione si sicurezza urbana definendola come il bene pubblico relativo alla viabilità e al decoro delle città, da perseguire anche con il contributo congiunto degli enti territoriali attraverso i seguenti interventi: riqualificazione e recupero delle aree/siti più degradati; eliminazione dei fattori di marginalità e di esclusione sociale; prevenzione della criminalità, in particolare di tipo predatorio; promozione del rispetto della legalità; più elevati livelli di coesione sociale e convivenza civile.
Una visione innovativa, che possa tracciare un orizzonte nuovo per il comparto e che mi sembra senz'altro degna d'attenzione, è la tendenza che negli anni recenti ha visto produrre in rapida sequenza da parte del Ministero dell'Interno, in particolare sul tema delle manifestazioni pubbliche, una serie di direttive e circolari volte a delineare una cornice di riferimento complessiva per gli operatori sui temi della safety e della security, sottolineando l'opportunità di un approccio integrato che metta a sistema il coordinamento dei servizi di security e safety.

Cosa intende quando parla di scatto di modernità?
Intendo l'implementazione di un progetto di lobbying di alto respiro mai sviluppato prima nel settore della rappresentanza della vigilanza privata, un vero salto di qualità. L'obiettivo deve essere quello di risvegliare l'attenzione delle Istituzioni verso il comparto dei servizi di sicurezza privata, oltre a lanciare un nuovo corso, ispirato a principi di modernità e collegialità per la rappresentanza datoriale di settore.
La rappresentanza delle istanze datoriali dovrebbe essere improntata alla promozione della SICUREZZA PRIVATA intesa in tutte le sue forme, partendo dalle attività disciplinate dagli artt. dal 134 al 141 del TULPS e dai relativi articoli del Regolamento d'esecuzione, oltre che da regolamenti e leggi speciali, sino alla figura di addetto ai servizi di sicurezza privata in tutte le sue declinazioni attuali e prospettiche.

ITALPOL
VIGILANZA

Contatti:
Gruppo Italpol Vigilanza
Tel. 800327311
www.italpolvigilanza.it

Ominsint all'avanguardia per la digitalizzazione delle operazioni in-store

Emiliano Mercurio, Technical Director di Omnisint, descrive le caratteristiche delle etichette elettroniche SOLUM che permettono ai clienti un'esperienza d'acquisto moderna, digitale e personalizzata. Le ESL consentono infatti non solo di aggiornare i prezzi da remoto con un click e in tempo reale, ma anche di venire incontro ogni giorno alle esigenze dei consumatori, offrendo un servizio e una customer experience più evoluti.

Per quale motivo sempre più aziende decidono di introdurre i sistemi di pricing elettronico?
Le aspettative del mercato e, di conseguenza, le esigenze aziendali di molte organizzazioni sono radicalmente cambiate nell'ultimo periodo. Sempre più aziende stanno nettamente trasformando i propri punti vendita, digitalizzando le operazioni in-store e permettendo ai clienti di interagire con i prodotti, principalmente attraverso display digitali.
Ora i clienti si aspettano un'esperienza d'acquisto moderna, digitale e personalizzata. Le ESL consentono non solo di aggiornare i prezzi da remoto con un click e in tempo reale, ma anche di venire incontro ogni giorno alle esigenze dei consumatori, offrendo un servizio e una customer experience più evoluti.

Quali sono i punti di forza delle vostre etichette elettroniche (ESL) e cosa vi distingue dalla concorrenza?
SOLUM, come spin-off di Samsung, rappresenta un brand affermato con garanzia sui suoi prodotti, con un background di qualità e di leadership nello sviluppo tecnologico. Questo la rende senza dubbio un partner affidabile nella trasformazione digitale, in grado di fornire una soluzione realmente completa.
Omnisint insieme a SOLUM offre vantaggi sinergici sia a livello di qualità tecnologica e di affidabilità del prodotto che di assistenza al cliente e capacità progettuale. Siamo in grado di garantire un'implementazione fluida e rapida di questa sofisticata tecnologia e una gestione controllata della complessità del progetto. Infatti, l'installazione viene effettuata nel giro di pochi giorni e la soluzione è pronta all'uso.
Omnisint offre inoltre supporto locale e formazione al personale, personalizzando le soluzioni ESL e adattandole all'infrastruttura IT esistente nel punto vendita.

Qual è la line up delle etichette elettroniche SOLUM?
SOLUM offre soluzioni complete e innovative. Tutte le linee della gamma Newton (Lite e Premium) offrono una incredibile qualità dei materiali, ottima resa dei display a livello di grafica e colori visualizzati e soprattutto ottime prestazioni in termini di trasmissione dei dati.
Grazie alla velocità di scambio dati e alla robustezza dell'interfacciamento con il sistema, possiamo pianificare aggiornamenti in tempo reale in tutti i negozi e ridurre i costi dell'infrastruttura senza compromettere la sicurezza dei dati.
Le etichette Newton Premium, inoltre, attraverso i pulsanti multifunzione e i LED luminosi, permettono di svolgere le operazioni in negozio più rapidamente ed efficientemente, come le attività di Picking o rifornimento a scaffale per ogni settore della GDO, dell'Electronics, del Fashion.
SOLUM ha da poco lanciato la linea di etichette elettroniche Newton CORE. Si tratta di una nuova linea di etichette che combina i vantaggi delle etichette Premium, ma senza vetrino. Ciò si traduce in una perfetta leggibilità anche in particolari ambienti Retail, come quelli dei supermercati.

Come si possono sfruttare le potenzialità delle soluzioni SOLUM nei negozi Retail?
La trasformazione digitale permette di abbandonare l'etichettatura manuale a scaffale e di aggiornare tutti i prezzi da remoto in tempo reale. Questa soluzione aiuta anche a rafforzare la brand identity aziendale, in quanto le etichette Newton possono essere personalizzate per includere nome e logo, con una resa grafica eccellente.
Le ESL possono anche essere molto utili per creare promozioni in-store efficaci e di maggiore impatto sui consumatori.
Un ulteriore vantaggio è la chiarezza delle informazioni e dei prezzi riportati sulle ESL, che sono sempre coerenti con quelli battuti in cassa.
I Retailer possono usufruire di una maggiore disponibilità del personale di vendita, che non perde più tempo ad aggiornare ogni volta i prezzi manualmente, e questo si traduce in un miglioramento generale del livello di servizio percepito.
Diversi clienti hanno anche affermato che il punto vendita appare più ordinato con le etichette elettroniche Newton, grazie al loro design moderno e accattivante.

Quali sono le soluzioni Software per l'utilizzo delle ESL?
La tecnologia ESL di SOLUM migliora l'esperienza d'acquisto dei clienti in negozio.
Esistono varie possibilità di utilizzo del software AIMS: local, centralizzato o in cloud. La soluzione AIMS LOCAL prevede l'installazione di un server per ogni negozio. Il vantaggio è quello di avere un sistema locale che si rende indipendente da qualsiasi problematica relativa a connessione MAN/WAN. Con questa soluzione, la continuità degli aggiornamenti è garantita anche in caso di problemi di connettività del punto vendita.
Utilizzando invece varie caratteristiche di AIMS Central Server è possibile aumentare le performance con risorse limitate e aumentare la sicurezza delle informazioni. AIMS Central può dividere i carichi di lavoro che arrivano al server in modo bilanciato. Ciò permette al server di utilizzare le risorse disponibili (RAM e CPU) equamente in istanze diverse. Assicuriamo inoltre una attenzione particolare alla sicurezza dei dati, mitigando i rischi con data recovery robuste e backup, user authentication e disaster recovery. Infine, AIMS SaaS in Cloud, i nostri esperti si occupano di tutte le esigenze di infrastruttura e manutenzione.

- Implementazione più rapida ed economica
- AIMS SaaS consente di distribuire il SW più rapidamente e a un costo inferiore
- Massime prestazioni e sicurezza
- Stabilità e ottime prestazioni del sistema scalando automaticamente il server, garantendo livelli di security all'avanguardia per la protezione dei dati
- Supporto operativo 24 ore su 24, 7 giorni su 7 AIMS SaaS è monitorato H24 dai team sistemistici più qualificati ed esperti in Corea, India, Stati Uniti ed Europa, garantendo sempre la continuità del servizio.

Fondata nel 2001 da un team di esperti del settore, **Omnisint** è specializzata nell'implementazione di soluzioni tecnologiche altamente innovative per il mercato retail e non solo, è leader in Italia con oltre 40.000 impianti installati e telegestiti in tutto il paese. Omnisint è una realtà in continua crescita, tra i clienti consolidati vi sono i maggiori brand e retailer internazionali e vanta la più alta quota di mercato in termini di nuovi sistemi installati. È stata scelta tra i "Campioni della crescita 2023" dall'**Istituto Tedesco di Qualità ITQF** e **Repubblica Affari&Finanza**, studio che raccoglie i punteggi delle aziende relativi al livello di servizio offerto ai clienti ottenuti in base ai giudizi di oltre 300mila consumatori italiani.

Contatti:
Omnisint srl
Tel. +39 02 26708493
marketing@nedapretail.it

Sicurezza bene collettivo e mercato: le nuove proposte di San Giorgio Formazione

L'Ing. Roberto Marino, responsabile per lo sviluppo tecnologico e innovazione della San Giorgio, affronta alcuni temi caldi nel mercato, in uno scenario che, già dal primo Rapporto sulla filiera della sicurezza in Italia redatto dal Censis nel 2018, sanciva un allargamento della sicurezza privata, in tutte le sue componenti, come un fatto ineludibile.

Come si muove la San Giorgio in un settore che chiede in modo pressante alle imprese di vigilanza servizi adeguati a prezzi che consentano di impiegare operatori competenti e qualificati?
Diciamo che per gli esperti del settore il processo di trasformazione della filiera della sicurezza privata è evidente da anni. Il nostro posizionamento si è sviluppato insieme a quello delle imprese che sono cresciute in dimensioni di mercato e in professionalità. La San Giorgio ha scelto di essere protagonista al fianco delle aziende, favorendo quel processo di sviluppo della sicurezza privata che è sempre più qualificata, diversificata in ruoli e funzioni, e normata in modo ben strutturato e definito.

Questo dal punto di vista della vostra proposta al mercato come si traduce? Perché, se è vero che la sicurezza privata ha il ruolo sussidiario e complementare rispetto alla forza pubblica, il confronto competitivo conduce ad un bagno di realtà sul versante costi ma anche su quello dell'efficienza nella gestione, sempre più complessa, della formazione in obbligo di legge.
Quando ho detto che la San Giorgio cresce insieme alle aziende non ho certo buttato lì una frase retorica. I nostri clienti sanno che la nostra area Ricerca e Sviluppo lavora per trovare soluzioni di alta qualità e sostenibilità economica. Il catalogo San Giorgio rappresenta la fotografia dell'offerta integrata, che offre soluzioni ad ogni bisogno delle aziende. Parlo di titoli e contenuti così come di modalità. Per questo il nostro catalogo si arricchisce in modo dinamico e selettivo, anche anticipando le esigenze delle aziende.
La componente tecnologica costituisce parte fondante del "Metodo San Giorgio". Innovazione per garantire alle aziende flessibilità, opportunità di beneficiare di corsi online in diverse modalità, con tutti i vantaggi del learning management system e la qualità dei nostri progettisti ed istruttori.

Ancora oggi alcuni imprenditori, ma anche molti formatori, ritengono che i corsi obbligatori debbano essere diciamo "modesti" per essere sostenibili. Noi non la pensiamo affatto così!
La San Giorgio è cresciuta in modo davvero importante e, come sa, le maggiori dimensioni aziendali permettono fattori di scala. Ecco perché possiamo rivoluzionare l'idea "finanziato quindi mediocre" e proporre corsi "finanziati e di eccellenza".
Basta guardare il nostro catalogo: i nostri corsi on line (D.lgs. 81/08 iniziale e aggiornamento, corso obbligatorio iniziale D.M. 269/10 e suoi aggiornamenti, antiterrorismo, inglese tecnico, PRM, etc.), sono sviluppati con docenti che conducono i corsisti come in un film, anche grazie ad una vera e propria regia professionale, slide parlate ed animate, quiz interattivi, interviste, gaming e molti test. L'obiettivo è quello di tenere alta l'attenzione dei corsisti e contribuire, con efficacia e concretezza, al miglioramento professionale.
In sintesi: prodotti eccellenti in contenuti, struttura e metodo, proposti alle aziende a prezzi sostenibili, se non addirittura più bassi della concorrenza.

E in termini di proposte commerciali come si traducono le soluzioni San Giorgio?
Il nostro tratto distintivo è dare soluzioni alle aziende: la star delle novità San Giorgio è la nostra "Formula Flat". Abbiamo lanciato sul mercato questa formula già a inizio estate ed è stata da subito un successo. L'idea è nata mettendoci nei panni dei clienti. Sempre più corsi, certificazioni, scadenze che si traducono in costi e tempi. La soluzione è una proposta su misura per ogni azienda, che porti significativi vantaggi economici.

A impatto sembra davvero qualcosa che non c'era. Ci spieghi meglio, ci illustri in dettaglio la Formula Flat.
Provi a immaginare il Responsabile dell'Istituto di Vigilanza che ogni anno deve pianificare la formazione necessaria per gli addetti e per i nuovi ingressi, con un occhio attento alle gare e al mercato. Un'attività delicata, che spesso porta a parcellizzare i fornitori per avere economie marginali che però si traducono in costo lavoro e potenziali inefficienze.
Ecco noi della San Giorgio lo abbiamo fatto, cioè lo abbiamo immaginato.
Il risultato è la Formula Flat, che permette di ottenere la formazione necessaria per la propria struttura, pianificandola annualmente, e di avere a disposizione un numero adeguato di accessi per i corsi on line riguardanti la formazione obbligatoria per gli Istituti di Vigilanza, sia per le normative sul D.M.269/10 che quelle sul D.lgs. 81/08, l'offerta si può estendere ad una serie di corsi inerenti le diverse materie in ambito Security, sempre più utili per la partecipazione alle gare d'appalto, con un servizio "su misura".

Può spiegare meglio la questione del "su misura"?
Guardi, si torna sempre alla nostra filosofia: alta qualità e metodo. Ogni cliente per noi è unico, quindi le nostre proposte non possono che essere ritagliate sulle sue specifiche esigenze. La nostra squadra di sviluppo commerciale è in grado di eseguire un'attenta analisi dell'organico aziendale e del turnover specifico, proiettare i fabbisogni formativi anche in ottemperanza agli obblighi di legge vigenti, ed elaborare un'offerta quali-quantitativa che rende più vantaggioso l'approvvigionamento di corsi necessari, attraverso l'acquisto del proprio "pacchetto" a cui si aggiungono servizi e corsi aggiuntivi utili o necessari per la partecipazione alle Gare.

Marino, tornando all'aspetto dello sviluppo tecnologico e alle innovazioni cosa ci può dire?
La nostra area Ricerca e Sviluppo lavora a stretto contatto con tutti i team della San Giorgio, concentrandosi sull'ideazione, sperimentazione e produzione di strumenti che fanno differenza. La logica è sempre quella di creare e offrire servizi diversi da quelli generalisti e decisamente evoluti. Gli ambiti sono diversificati, dai gestionali come il Training Planner che stiamo testando, fino a uno dei gioielli della San Giorgio X-BAG, *X-ray Baggage scAnner Gate simulator*, il simulatore di ultima generazione di scanner a raggi X, per le esercitazioni e certificazioni degli screener di porti e aeroporti.
Insomma, anche in questo caso, una cosa innovativa e unica, targata San Giorgio.

Contatti:
San Giorgio Srl
formazione@sangiorgionet.com
www.sangiorgionet.com

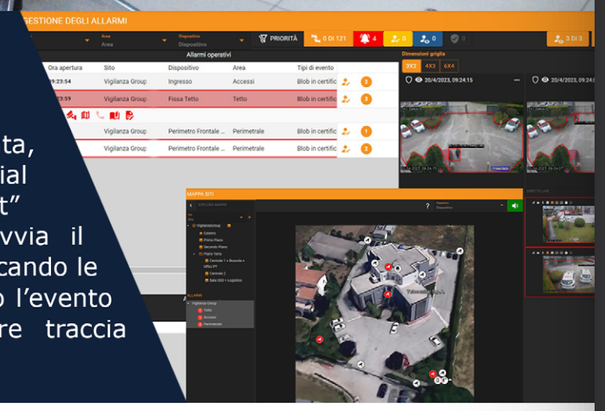
VIGILANZA GROUP

Passione e innovazione dal 1946

VIDEOANALISI e CENTRALE OPERATIVA

Un binomio indissolubile

I metadati prodotti dai sistemi di televigilanza avanzata, vengono analizzati, discriminati, rielaborati dall'Artificial Intelligence a bordo e consegnati sotto forma di "alert" all'operatore della Centrale Operativa, il quale avvia il processo di gestione convertendoli in allarme e innescando le procedure di reazione e intervento oppure chiudendo l'evento nei casi di evidente regolarità, lasciando sempre traccia documentata e videoreport dell'attività.



WOLF SICUREZZA | WOLF ASSICURAZIONI | VIGILO 4YOU | RVI RETE VIGILANZA ITALIA | INTERNATIONAL MEDICAL CENTER '84

VIGILANZA GROUP Soc. Coop. a r.l.
Via Fura 14, 25125 – Brescia – Italy
www.vigilanzagroup.it | Mail clienti@vigilanzagroup.it

Numero Verde
800 485 771
Servizio Assistenza

TKH GROUP | TKH SECURITY

TKH GROUP skilleye

TKH Skilleye,

tecnologia e riservatezza commerciale a servizio dei professionisti della sicurezza.

- TVCC Analogica ed IP, Controllo Accessi
- Analisi Video Avanzata, Deep Learning, con classificazione degli oggetti
- Conteggio Persone, Riconoscimento Facciale ed Auto-Tracking
- Antintrusione per esterno, con qualsiasi condizione climatica
- Lettura Targhe per gestione automatica di varchi
- Panoramiche Starlight 180° e 360° senza distorsione delle immagini
- Tecnologia termico-ottica per la rilevazione intrusione e temperatura
- Centralizzazione Video e Allarmi per Windows e MAC

SKILLEYE

SCARICA LA NUOVA APP SIQURPLAY PRO

TKH SECURITY SRL | +39 0438 179 2811 | info.it@tkhsecurity.com | www.tkhsecurity.it

Perché dare priorità e investire nella resilienza è importante nel settore dei trasporti

di Michela Carloni Gammon, Account Executive Everbridge Italia

Con migliaia di visitatori di passaggio che cercano di salire su treni, aerei e autobus in tempi stretti, le strutture di trasporto possono essere messe in crisi da incidenti meteorologici, interruzioni informatiche e attività criminali. Mantenere i dipendenti, i passeggeri, i visitatori e i membri della comunità al sicuro e informati sulle situazioni di emergenza, sulla chiusura dei cancelli, sul traffico e altro ancora è fondamentale per garantire la sicurezza delle persone e il regolare svolgimento delle operazioni.

Eventi critici come maltempo, disordini civili e attacchi informatici non solo sono diventati più frequenti negli ultimi anni, ma hanno modificato il modo in cui molte organizzazioni di trasporto operano quotidianamente. Se a questi eventi si aggiungono le sfide poste dalla pandemia COVID-19, è chiaro che queste situazioni hanno il potenziale di influire direttamente sul benessere dei dipendenti e delle operazioni, ma si sta facendo abbastanza per mitigare o prevenire il loro impatto?

Sebbene le organizzazioni del settore dei trasporti non possano impedire il verificarsi di eventi critici, possono essere proattive nelle loro decisioni per ridurne l'impatto. Con la tecnologia automatizzata, le organizzazioni dispongono di una risorsa importante per identificare, rispondere e mitigare i danni degli eventi critici, garantendo la resilienza in mezzo a una moltitudine di minacce.

Cosa significa essere resilienti?

La resilienza è definita come la capacità di resistere o di riprendersi rapidamente dalle difficoltà. Quando un'azienda è resiliente, ciò non influisce solo sulla sua stabilità finanziaria, ma anche sulla sua percezione agli occhi di clienti e potenziali clienti nonché sul morale dei membri del team che svolgono un ruolo nell'aiutare l'azienda a evitare le cadute. Le organizzazioni più performanti non sono solo visionarie, ma realizzano obiettivi e strategie di resilienza.

Con quale frequenza si verificano eventi critici? Nel "Cost of a Data Breach Report 2022" di IBM è stato rivelato che l'83% delle organizzazioni ha subito almeno una violazione dei dati. Inoltre, Forbes ha dichiarato che nel 2022 sono stati battuti diversi record di eventi meteorologici estremi, dato che il cambiamento climatico diventa sempre più drammatico in tutto il mondo. Le aziende di trasporto hanno la responsabilità di mantenere dipendenti, passeggeri, visitatori, inquilini e membri della comunità al sicuro e informati. Con il volume senza precedenti di eventi critici, è fondamentale per loro rafforzare la propria resilienza attraverso avvisi multimodali su situazioni di emergenza, chiusura di cancelli, traffico e altro ancora.

La digitalizzazione sarebbe rapidamente vantaggiosa per la maggior parte delle organizzazioni del settore dei trasporti. Automatizzando le procedure di notifica e integrandosi con gli allarmi SCADA e di sicurezza esistenti, i fornitori di servizi di trasporto possono comunicare in modo rapido, chiaro ed efficiente con gli utenti - primi soccorritori, dirigenti, dipendenti e passeggeri - attraverso tutti i metodi di contatto.

Come possono le organizzazioni raggiungere la resilienza?

Le organizzazioni possono rafforzare la loro resilienza implementando un sistema di allerta precoce per identificare i rischi più rilevanti per persone, beni o strutture specifiche in qualsiasi parte del mondo e allertare i primi soccorritori

appropriati. IBM ha inoltre riportato che occorrono in media 197 giorni per identificare e 69 giorni per contenere una violazione della sicurezza informatica, ma le aziende che riescono a contenere una violazione in meno di 30 giorni risparmiano oltre 1 milione di dollari rispetto a quelle che impiegano più tempo. Investire in una posizione come quella del Chief Resilience Officer, con un budget ragionevole, potrebbe essere un ottimo ponte tra i dirigenti e i team che si occupano della protezione dei dipendenti e delle risorse. Comunicare l'importanza della sicurezza e della resilienza ai dirigenti del consiglio di amministrazione è un passo importante verso il miglioramento, soprattutto mostrando gli impatti in termini di perdita di fatturato o di incapacità di generare ricavi, come identificato dallo studio IBM.

Migliorare la sicurezza dei trasporti con Everbridge | Caso di studio del Porto di Los Angeles

Il Porto di Los Angeles fa parte del dipartimento portuale della città di Los Angeles, che ha giurisdizione su un'area compresa tra San Pedro e Wilmington, in California. È costituito da numerosi terminal, tra cui terminal merci, terminal carburante, porti turistici e attrazioni per residenti e turisti. Il porto conta regolarmente tra i 10.000 e i 20.000 dipendenti. La sicurezza dei trasporti è una priorità assoluta per i funzionari portuali, per garantire che le navi e i dipendenti che vi lavorano siano sempre collegati e avvisati in caso di crisi.

Data la posizione e la funzione del Porto di Los Angeles, sono numerosi gli eventi che possono colpirlo. Il dipartimento aveva bisogno di raggiungere in modo rapido ed efficace il personale e le parti interessate durante eventi critici come terremoti e incendi di imbarcazioni. Per garantire la sicurezza e l'efficienza dei trasporti, i dipendenti del porto dovevano essere in contatto con i funzionari e costantemente informati di tutti gli incidenti, critici o di routine, che richiedevano la loro attenzione.

Il Porto di Los Angeles ha scelto la Unified Critical Communication Suite di Everbridge per collegare il personale, i soccorritori e le parti interessate durante gli eventi. Grazie al sistema Everbridge, i soccorritori del porto sono in grado di trasmettere messaggi in modo rapido e affidabile durante gli eventi di emergenza e non. I funzionari possono ora garantire la sicurezza dei dipendenti e dei trasporti utilizzando modelli di messaggi al volo o predeterminati per contattare in modo rapido ed efficiente coloro che devono essere informati di un determinato scenario.

Investire nella resilienza

Per essere più resilienti, le aziende di trasporto devono apportare cambiamenti coordinati a livello di personale, tecnologia, processi e cultura: un tipo di trasformazione sistematica e su larga scala che comporta un impegno notevole da parte dei leader. Non sarà facile. Ma quando è il momento giusto per fare i primi passi? Adesso. Nessuno sa quando arriverà il prossimo ciclo negativo, quanto durerà o quanto sarà profondo. Tuttavia, come dimostra la storia, le aziende che si preparano meglio ai periodi difficili ne escono rafforzate. Investire oggi nella giusta tecnologia e nell'automazione può aiutare a identificare, rispondere e gestire gli effetti di futuri eventi critici.

everbridge™

Contatti:
Everbridge Italia
www.everbridge.com

La sicurezza per i porti secondo DAB Sistemi Integrati

a cura dell'Ufficio Stampa DAB

I porti sono ambienti strutturalmente complessi, caratterizzati da perimetri estesi e dalla gestione quotidiana e in tempi stretti di flussi rilevanti di persone, merci e mezzi spesso difficilmente controllabili.
La continuità del servizio è minacciata dalla presenza di numerosi punti critici come, ad esempio, la molteplicità di varchi e di obiettivi sensibili, a rischio terrorismo, furti, intrusioni, incendi, esplosioni, manomissioni, sabotaggi e contaminazioni.
È fondamentale basare una corretta progettazione della soluzione di Sicurezza sull'analisi delle esigenze di ciascuna area di criticità portuale per:

- Aumentare l'efficacia della rilevazione di situazioni di rischio
- Incrementare il livello di sicurezza e di gestione delle emergenze
- Incrementare negli utenti la percezione di Sicurezza del sito aeroportuale
- Supportare le attività di investigazione da parte delle autorità competenti (es. Polizia di Frontiera, Guardia di Finanza)
- Aumentare l'efficacia dei controlli delle persone e delle merci che ogni giorno sono in arrivo o in partenza

A livello internazionale, la normativa di riferimento sulla sicurezza portuale è l'**ISPS Code** (International Ship and Port Facility Security Code), adottato dall'Unione Europea per garantire la sicurezza marittima per la prevenzione e la repressione di atti illeciti intenzionali richiedendo l'identificazione di autorità, competenze e obiettivi atti a stabilire e mantenere le misure di sicurezza.
In questo contesto avviene la definizione di un **Port Security Plan** redatto dal **Port Security Officer (PSO)**, che tenga conto dell'analisi dei rischi delle navi e dell'intero impianto portuale. Parimenti identifica le responsabilità

delle **Port Facility** e rientranti nel sedime portuale ed i compiti dei rispettivi **Port Facility Security Officer (PFSO)**.
E' rilevante notare che molti porti italiani sono a tutti gli effetti parti delle città e, pertanto, il frazionamento delle zone sottoposte a controlli di sicurezza presenta maggiori complessità.
Un ulteriore questione rilevante è il fatto che le criticità di sicurezza sono correlate in maniera sostanziale con il tipo di traffico che il porto svolge, come per esempio Ro - Ro (Roll In, Roll out), Ro - Pax, Container, Merci sfuse, croceristica, etc.
Ne consegue che è richiesta una specifica esperienza e conoscenza sia al PSO che agli altri soggetti coinvolti, non ultimo proprio al System Integrator che deve realizzare gli impianti di sicurezza.

La soluzione prevede l'interazione e la cooperazione di:
- Tecnologie innovative di Security
- Risorse umane
- Processi organizzativi
- Sistemi interattivi di supporto alle emergenze

Il nucleo del Modello di Sicurezza DAB è la Centrale Operativa, costituita da una piattaforma tecnologica aperta, affidabile e scalabile in grado di interagire in modalità bidirezionale con i sottosistemi funzionali presenti in campo.
Si tratta di un software di supervisione e gestione integrata di sistemi complessi di Sicurezza Fisica (PSIM – Physical Security Information Management) in grado di centralizzare, monitorare e interagire con diverse tipologie di sensori, apparati e sistemi multi-brand di Security, Safety e Controllo Tecnologico, ottimizzando la sicurezza totale.
La piattaforma permette il controllo dei flussi portuali – carico, scarico, stoccaggio, accesso ed imbarco di passeggeri, bagagli, merci e mezzi – in maniera efficace e con una rilevante ottimizzazione delle risorse di vigilanza fisica.

Sistemi integrati di videosorveglianza, controllo accessi, antintrusione, lettori di targhe, ispezione sotto veicolare, metal detector e identificazione passeggeri sono gestiti da una Centrale operativa, nucleo del processo di controllo, che analizza i dati raccolti e coordina gli interventi in modo mirato in caso di eventi critici ed è in grado di interagire in modalità bidirezionale con i sistemi e sottosistemi funzionali presenti in campo, attraverso l'utilizzo delle moderne reti di telecomunicazione.
Il termine **sicurezza in ambito portuale** include, quindi, sia aspetti di **safety** per la tutela dei lavoratori e delle persone che frequentano i luoghi dove si svolgono le operazioni portuali, sia aspetti di **security**, ovvero la prevenzione di persone e impianti rispetto a possibili azioni criminose.

DAB SI
SISTEMI INTEGRATI

Contatti:
DAB Sistemi Integrati
Tel. +39 06 412121
www.dabsi.it

Sicurezza di gallerie ferroviarie, passaggi a livello e depositi: i vantaggi della tecnologia LiDAR

di Marco Censi, Regional Sales Manager Italia per OPTEX

In ambito ferroviario, in Italia si avviano numerose opere strategiche e si rinnovano le strutture esistenti anche grazie agli investimenti previsti dal Pnrr. Per citarne alcune, vedremo la realizzazione della nuova linea Terzo Valico, che migliorerà i collegamenti del sistema portuale ligure con le principali arterie del Nord Italia e l'Europa, il Passante Alta Velocità di Firenze, con circa 7 km sotterranei su due gallerie parallele e il potenziamento della tratta Napoli – Bari. Inoltre, Rete Ferroviaria Italiana realizzerà entro il 2026 un nuovo collegamento ferroviario lungo circa 6 km tra l'Aeroporto del Salento e i poli urbani di Brindisi, Lecce, Taranto e Bari.

Allo stesso tempo, l'Agenzia Nazionale per la Sicurezza delle Ferrovie e delle Infrastrutture Stradali e Autostradali (ANSFISA), comunica che "Nel 2023, le attività di supervisione [...] nel settore ferroviario saranno complessivamente 153, per la verifica di circa 6.000 elementi tra infrastrutture, treni e sottosistemi."

Oggi più che mai, per chi gestisce le reti ferroviarie, è fondamentale che ogni elemento sia valutato attentamente, nel momento di scegliere e implementare le soluzioni di sicurezza, per il bene di passeggeri e lavoratori.

Proteggere la vita umana nelle gallerie ferroviarie

Sempre secondo ANSFISA, "La rete ferroviaria italiana conta oltre 1.700 tunnel. [...] Tra il 2017 e il 2022 gli incidenti significativi sono stati meno del 3% sul totale, di cui il 60% dovuto a contesti manutentivi e il 40% a presenze indebite sulla sede ferroviaria."

Rilevare con precisione una persona che entra in un ambiente buio come le gallerie non è semplice, farlo mentre i treni transitano è ancora più complesso ma questa sfida si può vincere con la combinazione di sensori laser innovativi, come la tecnologia LiDAR di OPTEX.

Grazie all'analitica integrata, la serie REDSCAN Pro può analizzare la dimensione e la distanza degli oggetti in movimento e di quelli presenti sulle rotaie, fornendo la rilevazione precisa mediante la traccia delle coordinate X e Y per prevenire, in questo modo, gravi incidenti. Un ulteriore vantaggio della tecnologia LiDAR è che la prestazione dei rilevamenti è stabile in ogni momento, e non viene influenzata dalle variazioni di luce o di temperatura. L'algoritmo che li controlla è configurato in modo da ignorare il transito dei treni e far scattare l'allarme solo in caso di intrusione da parte di oggetti più piccoli, anche se ciò avviene contemporaneamente.

Migliorare la sicurezza dei passaggi a livello

Le barriere dei passaggi a livello rappresentano un ostacolo che pedoni e ciclisti sono impazienti di superare. I sistemi di rilevamento laser scansionano l'area di attraversamento quando il passaggio a livello è attivo, e consentono il passaggio del treno solo quando l'area è sicura. Grazie all'integrazione dei sensori LiDAR con telecamere a circuito chiuso, gli operatori e le forze dell'ordine possono inoltre avere prova delle dinamiche dell'eventuale infrazione. I sistemi di rilevamento REDSCAN di OPTEX sono stati utilizzati e implementati con successo in numerosi siti ferroviari britannici, tra cui oltre 400 passaggi a livello del Regno Unito per conto di Network Rail.

Prevenire gli atti vandalici

Gli ingressi abusivi nelle gallerie ferroviarie o lungo i binari non costituiscono solo un rischio per la vita di passeggeri e lavoratori, ma comportano un costo significativo per le ferrovie. Come riportato da Trenord, nel 2021, si sono registrati 167.470 mq di graffiti (+8% sul 2020) e 614 vetri frantumati (+22%). Nel 2022 le squadre di Trenord hanno rimosso oltre 219mila mq di graffiti: solo questa azione ha comportato per l'azienda un costo di 1,5 milioni di euro. Gli interventi di pulizia e ripristino comportano costi ingenti per l'azienda, a cui si aggiungono quelli derivanti dalle soste impreviste dei treni in deposito, per la manutenzione. I depositi spesso sono di grandi dimensioni, il che rende l'individuazione degli intrusi una vera e propria sfida.

I sistemi di antintrusione vengono comunemente utilizzati allo scopo di tutelare un'area perimetrale, sia che si tratti di un treno che di un deposito ferroviario, e le tecnologie disponibili per ottenere tale protezione comprendono la LiDAR, la Fibra Ottica o i sensori a infrarossi passivi - PIR. Nel caso della rilevazione mediante LiDAR, il sensore REDSCAN Pro con telecamera Onvif-compliant integrata può essere utilizzato anche per verificare visivamente la natura della segnalazione: consente infatti un rilevamento ancor più rapido e preciso degli intrusi, concentrandosi sulla posizione o sull'area dove stanno avvenendo atti vandalici.

Le soluzioni OPTEX

I sensori con tecnologia LiDAR sono la soluzione ideale per ambienti chiusi, con un forte eco, bui e spesso umidi come le gallerie, essendo immuni a tali fattori. Inoltre, i sensori OPTEX sono dotati di scansione ambientale all'aperto, per regolare l'area d'azione, registrare automaticamente i cambiamenti e indicare al sistema di controllo se la capacità di rilevamento è limitata, ad esempio, da una lente sporca. La serie REDSCAN può offrire un rilevamento a 190 gradi, fino a 50 x 100 m, consentendo di proteggere ampie zone con un unico sensore. L'area di rilevamento può essere divisa fino a 8 zone indipendenti e per ognuna di esse è possibile personalizzare la dimensione dell'oggetto target, la sensibilità e l'uscita d'allarme. Offre una grande flessibilità nell'adattare le impostazioni a seconda della posizione delle zone e del livello di pericolo.

In conclusione, all'aperto o al chiuso, le soluzioni OPTEX possono contribuire a migliorare ulteriormente la sicurezza lungo i binari, i passaggi a livello, i depositi e i tunnel nella rete ferroviaria italiana.

OPTEX
Sensing Innovation

Contatti:
OPTEX
Tel. +39 351 9272789
enquiry-it@optex-europe.com
www.optex-europe.com/it

Affrontare le sfide della sicurezza fisica nella logistica e nel trasporto: la soluzione Reconeyez

di Stefano Torri, VP South Europe Sales di Reconeyez

Il settore della logistica e dei trasporti in Italia è costretto ad affrontare una miriade di minacce alla sicurezza fisica, che possono ritardare o vanificare gli sforzi organizzativi, compromettere le risorse e mettere a rischio la sicurezza del personale. Episodi di furti di merci, vandalismi e sabotaggi continuano ad affliggere con frequenza crescente il settore, rendendo necessarie solide misure di sicurezza. Quali sono le principali sfide in ambito sicurezza affrontate dai professionisti del settore della logistica e dei trasporti in Italia? E, soprattutto, quali sono le possibili soluzioni per mitigare questi rischi? In questo articolo, analizzeremo le principali sfide, presentando un sistema di sicurezza intelligente e facile da usare che aiuta a superarle.

Combattere i furti del carico: proteggere le spedizioni di valore

Il furto di merci rimane un problema persistente per il settore, causando perdite finanziarie significative e interruzioni della catena di approvvigionamento. I criminali spesso prendono di mira aree non protette, inclusi piazzali di stoccaggio, banchine di carico e vie di transito, rendendo fondamentale attrezzare questi luoghi con efficaci misure di sicurezza.

L'implementazione di protocolli di sicurezza completi, compreso il dispiegamento di sistemi di allarme per esterni e telecamere di sorveglianza, può fungere da potente deterrente contro i furti di merci. Le immagini ad alta risoluzione, il monitoraggio in tempo reale e il rilevamento intelligente del movimento offerti dai moderni sistemi di sicurezza e sorveglianza consentono ai professionisti di rilevare tempestivamente attività sospette e reagire prontamente di conseguenza. Tali prove possono inoltre aiutare le forze dell'ordine ad arrestare i colpevoli e recuperare i beni rubati.

Mitigare il vandalismo e il sabotaggio: proteggere le infrastrutture critiche

Gli atti di vandalismo e di sabotaggio pongono gravi minacce alle infrastrutture di trasporto, con conseguenti interruzioni e potenziali rischi per la sicurezza. L'Italia ha subito casi di sabotaggio ferroviario, che hanno causato notevoli disagi ai servizi di trasporti su rotaia. La protezione delle infrastrutture critiche, compresi gli scali ferroviari, i porti, gli aeroporti e gli snodi intermodali, richiede misure di sicurezza proattive. L'implementazione strategica di telecamere di sicurezza avanzate per esterni può migliorare le capacità di sorveglianza e consentire il monitoraggio in tempo reale delle infrastrutture. I filmati ad alta risoluzione, combinati con l'accesso remoto e l'analisi intelligente, consentono ai professionisti di rilevare e rispondere rapidamente ad atti di vandalismo o sabotaggio. L'intervento tempestivo riduce al minimo i tempi di inattività, limita le perdite finanziarie e garantisce il flusso ininterrotto di beni e servizi.

Il furto di merci, gli atti di vandalismo e le minacce di sabotaggio rappresentano tutti rischi per le operazioni, la stabilità finanziaria e la sicurezza pubblica. Affrontare queste sfide richiede un approccio globale, che combini misure di sicurezza fisica con tecnologie avanzate, protocolli rigorosi e collaborazione tra diversi settori.

Sfruttando le telecamere di sorveglianza per esterni e implementando solide strategie di sicurezza, i professionisti della logistica possono migliorare la propria capacità di scoraggiare, rilevare e rispondere agli incidenti di sicurezza. Investire in un framework di sicurezza olistico aiuta a proteggere le spedizioni di valore, salvaguardare le infrastrutture critiche e garantire l'integrità delle risorse digitali. Grazie a questi sforzi concertati, il settore della logistica e dei trasporti in Italia può navigare nel complesso panorama della sicurezza con resilienza, fiducia e tranquillità. Centinaia di società di sicurezza in più di 50 paesi installano soluzioni Reconeyez per proteggere le risorse dei propri clienti. Reconeyez dimostra che la sicurezza esterna non deve essere complicata o costosa. Il sistema di antintrusione Reconeyez può essere implementato in pochi minuti e la sua distribuzione può essere facilmente scalata e alterata per adeguarsi alla dinamicità dei siti logistici, che per definizione

si adeguano continuamente ai flussi di merci e di mezzi di trasporto. Inizialmente sviluppata per il controllo delle frontiere e applicazioni di carattere militare, la soluzione Reconeyez segue le più severe misure di sicurezza ed è costruita per durare nel tempo, anche nelle condizioni ambientali ed atmosferiche più estreme.

La soluzione è molto semplice ed offre alcuni innegabili vantaggi; innanzitutto è composta da soli due componenti principali: uno o più Detector (sensore ad infrarossi dotato di telecamere HD a doppia ottica ed illuminatore per la visione notturna) ed un Bridge (dispositivo di comunicazione dotato di SIM 4G per la trasmissione dei dati e delle immagini al cloud). Entrambi sono wireless e completamente autonomi: funzionano a batterie ricaricabili di lunga durata (fino a 400 giorni con una carica), in base al numero di allarmi ricevuti e trasmessi. Anche la comunicazione tra dispositivi e la trasmissione degli eventi e delle immagini è totalmente autonoma: sfruttando la rete mobile si collega al cloud in modo sicuro e criptato. Un elemento imprescindibile è poi l'intelligenza artificiale, che analizza in tempo reale le immagini ricevute dal campo, per confermare (o scartare) gli allarmi in base alla presenza o meno degli "attori" di interesse. L'intrusione è causata da persone o da veicoli delle tipologie selezionate? Allarme confermato. Il sensore è stato attivato da un ramo mosso dal vento, un animale o un foglio di plastica volante? Allarme scartato.

Il sistema è basato su architettura cloud, il che lo rende estremamente sicuro, non utilizza memorie removibili locali (in linea con le disposizioni GDPR sulla protezione dei dati personali), e può essere monitorato ovunque sia disponibile una connessione ad internet, anche a migliaia di km di distanza. È disponibile un'app mobile gratuita che consente la ricezione di messaggistica push in caso di allarmi ed in grado di visualizzare in tempo reale le immagini degli eventi. In alternativa il sistema è integrato con le principali piattaforme di ricezione degli allarmi, in uso alle vigilanze e alle centrali operative, che quindi possono ricevere gli eventi e le relative immagini nei protocolli nativi da loro utilizzati. Ogni cliente ha quindi sia la possibilità di effettuare il monitoraggio in autonomia, che di utilizzare i servizi di vigilanza ed invio di pattuglie di professionisti della sicurezza.

Se le Guardie di Frontiera possono fidarsi di Reconeyez, possono esserci altri dubbi?

reconeyez

Contatti:
Reconeyez Italia
stefano.torri@reconeyez.com
www.reconeyez.com/it

Port Facility Security Plan per il Porto di Termini Imerese

comunicato aziendale

Nel 2017 l'Autorità di Sistema Portuale del Mare di Sicilia Occidentale, nell'ottica di un progetto di rilancio della struttura portuale di Termini Imerese, ha indetto un bando di gara per la realizzazione delle infrastrutture ed impianti necessari per il Port Facility Security Plan.

La necessità è quella garantire la sicurezza dell'impianto portuale per controllarne l'accesso, in particolare delle aree di ancoraggio e di ormeggio, per monitorare le aree riservate, per assicurarne l'accesso alle sole persone autorizzate, per provvedere alla supervisione della movimentazione dei carichi, alla movimentazione delle provviste di bordo e alla disponibilità delle comunicazioni di sicurezza.

Per raggiungere questo obiettivo, l'Autorità portuale ha indetto una gara per individuare una piattaforma integrata di sicurezza che permettesse di gestire sistemi di videosorveglianza, controllo accessi, antintrusione, gestione degli accessi ai varchi veicolari, comunicazioni intercom, il tutto supervisionato e gestito da una piattaforma software aperta e scalabile, sviluppata secondo i più alti standard di sicurezza informatica, in grado di interfacciarsi con sistemi di terze parti.

Nel 2018 la gara è stata aggiudicata al RTI **Agostaro Rosario** s.r.l. (capogruppo) e **DAB Sistemi integrati** s.r.l. per la realizzazione e manutenzione degli impianti necessari per l'implementazione dei sistemi di Sicurezza previsti nel Port Facility Security Plan.

Agostaro Rosario Srl è l'azienda specializzata in opere di consolidamento di edifici civili ed industriali, una realtà affermata nel campo dell'edilizia siciliana che ha eseguito i lavori di impiantistica dell'intero progetto.

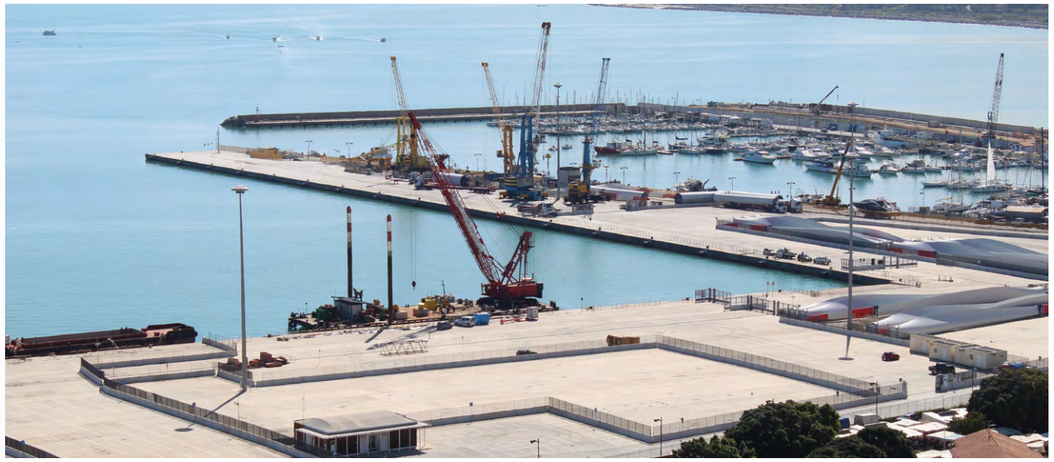
DAB Sistemi Integrati, system integrator leader nella realizzazione, gestione e manutenzione di sistemi avanzati di security, safety e controllo tecnologico, ha risposto alla gara offrendo come piattaforma software di supervisione **GALASSIA Global PSIM Solution** e come partner tecnologico ha scelto le soluzioni innovative dell'azienda **TKH Security.**

Galassia è la piattaforma di supervisione e gestione integrata di sistemi complessi di sicurezza fisica (PSIM- Physical Security Information Management) di **DAB Sistemi Integrati.**

La piattaforma è in grado di centralizzare, monitorare e interagire con diverse tipologie di sensori, apparati e sistemi multi – brand di security, safety e controllo tecnologico ottimizzando la sicurezza totale. È una soluzione client/server di livello 'enterprise', aperta, scalabile e flessibile per realizzare centrali di monitoraggio e controllo evolute che gestiscono sistemi presenti in uno o più siti geograficamente distribuiti. All'interno della piattaforma Galassia sono collegati, gestiti e integrati i moduli di controllo accessi, lettura targhe e videosorveglianza di TKH Security.

TKH Security è una società del gruppo TKH Group, con sede, ricerca e sviluppo in Olanda ed è rappresentata in Italia da TKH Security srl.

TKH Security da più di quarant'anni sviluppa soluzioni di sicurezza pensate specificatamente per applicazioni verticali, quali porti, aeroporti, stabilimenti marine oil & gas, infrastrutture critiche ed asset & site management. TKH Security sviluppa, insieme al cliente, soluzioni che nascono dalle opportunità che il mercato richiede, con un approccio rivolto ai progetti e con una visione tipicamente europea. La soluzione scelta per proteggere il porto di Termini Imerese utilizza la piattaforma **VDG Sense** come cuore della videosorveglianza, in una architettura che utilizza 7 server in configurazione di fail-over ridondata. Questa soluzione permette di garantire sempre la continuità di servizio anche in caso di guasto di un singolo componente o di un server del sistema, dal momento che il sistema è in grado di auto-ripristinarsi autonomamente.



VDG Sense è la piattaforma VMS del gruppo TKH Security, aperta e scalabile, utilizzata in numerose applicazioni di massima sicurezza nel mondo, che offre funzionalità di analisi video intelligente. La stessa piattaforma protegge la banchina ed il perimetro del porto con ben 70 telecamere **TKH Siqura** BC822 con analisi video intelligente, che permette di generare un allarme immediatamente qualora ci sia un tentativo di intrusione non autorizzata. L'analisi video consente di classificare gli oggetti, riconoscere una persona e generare istantaneamente un allarme quando questa supera una linea di confine o entra in un'area non consentita, permettendo di mettere in atto immediatamente le procedure di sicurezza programmate nel sistema. In totale sono state installate 180 telecamere TKH Siqura tra fisse e PTZ per garantire la sicurezza del porto.

All'interno del sistema di videosorveglianza sono state proposte come miglioria e poi installate **2 colonnine SOS Cometa** slim di DAB Sistemi Integrati.

Cometa è un totem di sicurezza equipaggiato con videocitofono IP, lampeggiante, telecamera speed dome IP e antifurto che unisce le funzionalità di videosorveglianza con la possibilità da parte di un utente di effettuare Richieste di Soccorso sia audio che video.

Nel caso di chiamate effettuate dai passeggeri, gli operatori della centrale operativa avranno un quadro preciso della situazione, sia tramite la telecamera che inquadra il viso del chiamante, che tramite la telecamera speed dome che permette di analizzare rapidamente tutto lo spazio che circonda il totem.

In combinazione con la piattaforma di controllo accessi TKH iProtect, 16 telecamere **TKH Siqura BL860M2IR** gestiscono l'accesso veicolare dei varchi con la lettura targhe. Il sistema TKH Security infatti consente di gestire gli accessi ai varchi utilizzando la lettura della targa, combinandola con la lettura del badge di prossimità, per una doppia verifica di sicurezza.

Inoltre, nel porto di Termini Imerese, per garantire gli accessi in modo sicuro, sono stati installati i controllori di nuova generazione **Pluto** e **Orion**, in abbinamento con i lettori di tessere serie **Sirius i80p**. Questa tecnologia, sviluppata da TKH Security, garantisce una sicurezza end-to-end dei dati, in quanto assicura che le informazioni vengano trasmesse e protette secondo i più alti standard di sicurezza informatica in tutto il processo di gestione del dato. Dalla trasmissione del numero di tessera al lettore sino all'elaborazione del dato su ogni postazione client, l'informazione infatti viene protetta da tecnologie fully encrypted (end-to-end), utilizzando tecnologie quali AES128, AES256, SSL.

Questa attenzione maniacale verso la sicurezza informatica caratterizza da sempre l'R&D di TKH Security nello sviluppare soluzioni che rappresentino un punto di riferimento per chi necessita di soluzioni di massima affidabilità.

VDG Sense e iProtect sono due piattaforme della più vasta proposta di TKH Security per la gestione della sicurezza, nativamente integrate, per offrire un'esperienza unica al cliente; permettono di integrarsi con sistemi di terze parti via LDAP, XML SQL, JDBC servers SDK e API.

Contatti:
TKH Security
Tel. +39 0438 1792811
www.tkhsecurity.it

Merci e customer experience, le nuove frontiere della Supply Chain

di Lucio Piccinini, Direttore commerciale di Vigilanza Group

Riavvolgiamo il nastro e pensiamo a quanto accaduto negli ultimi tre anni, due e mezzo dei quali attraversati nella gestione di una pandemia che ci aveva rinchiuso in casa limitando la nostra libertà. Con i negozi fisici chiusi, tutto è cambiato. Ognuno di noi, da allora in avanti ha acquistato il suo oggetto del desiderio esposto in una vetrina virtuale e puntualmente si è visto consegnare a casa la propria merce da un corriere. Tutto scontato o quasi: un click per ordinare, un secondo click per pagare e voilà, dopo qualche giorno la merce è stata consegnata a domicilio al consumatore 4.0.
Appena proviamo ad approfondire, scopriamo che dietro le quinte di quell'acquisto ci sono almeno due elementi imprescindibili: **organizzazione e sicurezza**.
Alla prima sono deputate le aziende che offrono servizi logistici integrati capaci di stoccare e spostare le merci anche in modo intermodale, a livello nazionale ed Internazionale. Di conseguenza, queste aziende hanno un'elevata necessità di sicurezza dovendo proteggere:
- *gli operatori che movimentano le merci in ogni fase;*
- *il mezzo che trasporta le merci;*
- *le merci stesse sia nelle fasi di spostamento che di sosta.*

Tutto si ripete qualunque sia il mezzo di trasporto utilizzato - aereo, nave treno o veicolo gommato – e il luogo di destinazione, fino ad arrivare al fatidico 'ultimo miglio'.
Chi si occupa di logistica sa che l'ultimo miglio dev'essere protetto da frodi e da attacchi di ogni genere: rapine, furti, infedeltà aziendale, errori amministrativi, ecc. Queste sono le minacce da contrastare perché contribuiscono a far impennare le differenze inventariali generando perdite per l'azienda e mettono in discussione la sua affidabilità nei confronti dei clienti, dai più famosi brand del lusso e dell'elettronica fino alla grande distribuzione organizzata.
Questa, in estrema sintesi è la Supply Chain che tanto sfida ed altrettanto appassiona gli addetti ai lavori. Un tema assai complesso, la cui risposta di sicurezza deve essere obbligatoriamente costruita in modo 'sartoriale' da parte delle aziende di servizi che desiderano essere punto di riferimento di questo settore.

Un approccio consulenziale che inizia sempre da un risk assessment per un'attenta individuazione e valutazione dei rischi utile a stilare lo stato di fatto e lo stato di progetto, a partire dall'hub nel quale quotidianamente vengono stoccate e smistate le merci, con molte persone interne ed esterne che ricoprono ruoli completamente diversi: dal dirigente aziendale al facchino, dall'autista alle dipendenze dirette al 'padroncino' al quale viene affidata la merce per il trasporto a destinazione
Per difendere questo patrimonio vengono tuttora utilizzati diffusamente servizi tradizionali di vigilanza con presidi fissi e ronde armate a scopo di deterrenza, soprattutto nelle ore notturne. Ma si riscontra anche una forte domanda di personale fiduciario in orario diurno, al quale vengono affidate mansioni di controllo accessi dei veicoli e dei pedoni con filtro in ingresso e uscita, supporto di back-office, bollettamento, ecc.
Tuttavia è la tecnologia ad offrire opportunità sempre più concrete ed evolute con cui costruire una soluzione capace di soddisfare appieno le complessità sopra esposte.
Pensiamo al polo logistico, sempre più oggetto di attacchi rapidi ed organizzati da parte di bande organizzate.
Come proteggerlo?
Riportiamo alcuni esempi di applicazioni prese da case history di successo dei nostri clienti:

• sistema di controllo accessi veicolare automatizzato con telecamere a lettura targa e gestione 'black & white list'. Per particolari esigenze, le telecamere di lettura targa permettono l'apertura del varco di ingresso uscita (sbarra o cancello) solo se viene rispettato l'abbinamento delle targhe della motrice e del rimorchio;
• videocitofono collegato h24 alla centrale operativa;
• controllo accessi tramite badge con rfid programmabile da remoto;
• sistemi tvcc esterni con intelligenza artificiale a protezione delle aree di lavorazione;
• sistemi tvcc interni ad alta risoluzione a protezione delle merci e time line user friendly per un abbattimento del tempo impiegato nella ricerca dell'evento di interesse (es. per analisi ex post di eventuali ammanchi);
• sistemi antincendio e relativo collegamento presso centrale operativa remota certificata 50518 conformi alla normativa UNI9795;
• sistemi antintrusione e loro collegamento presso centrale operativa remota certificata 50518 con sistemi radar di ultima generazione e sistemi di filodiffusione ip che permettono un'interazione real time tra l'operatore ed il sito vigilato;
• sistemi rfid sulle merci;
• satellizzazione flotta e trasporto merci in massima sicurezza anche con l' impiego di sigilli elettronici digitali per monitorare costantemente i prodotti in transito e l'esatta esecuzione della missione affidata all'autista;
• protezione degli autisti attraverso l'impiego di sistemi safety and security (app e braccialetti) connessi con la centrale operativa;
• controllo del personale impiegato nell'hub con sorteggio imparziale svolto in remoto attraverso sistemi audio video connessi con la centrale operativa "perquisizione virtuale"
• diagnostica impianti attraverso piattaforme software evolute e gestione predittiva delle manutenzioni straordinarie;
• polizze assicurative all risk che tengano conto dell'abbattimento dei rischi e garantiscano, a parità di condizioni, un premio assicurativo sostenibile;

In generale, questi sono solo alcuni dei servizi a valore aggiunto che possono essere offerti ai clienti che si occupano di Logistica.
Ovviamente la tecnologia fornisce dati che vanno gestiti e allora sorge spontanea la domanda: chi è deputato a prendersi in carico tutte queste informazioni?
Per chiudere il cerchio è imprescindibile dotarsi di una cabina di regia: la centrale operativa o, meglio il centro decisionale. Il luogo fisico nel quale vengono "stoccate" al sicuro da ogni attacco fisico e cibernetico i dati dei clienti, al cui interno opera personale altamente qualificato e costantemente formato, capace di reagire rapidamente ed attivare le procedure concordate, soprattutto in situazioni di emergenza reale sia di safety che di security.
Una progettazione assai complessa che impegna molte figure professionali: progettisti, produttori di tecnologie, security manager, system integrator, HSE/RSPP e gestori del servizio, tutti attorno ad un tavolo a ragionare e cercare soluzioni atte a garantire la business continuity per il committente che sempre più necessita di veri e propri partner che lo coadiuvino nella gestione puntuale e sicura della merce.

Contatti:
Vigilanza Group
lucio.piccinini@vigilanzagroup.it
www.vigilanzagroup.it

OPTEX, come garantire la sicurezza di persone e beni all'interno di un porto

di Nikitas Koutsourais, OPTEX presales and support consultant Western Europe

I porti sono infrastrutture vitali per il commercio globale in quanto punti di ingresso e di uscita per le navi che trasportano merci e passeggeri. Luogo di incontro tra mare e terra, spesso esposti a condizioni atmosferiche estreme, i porti rivestono un ruolo significativo per l'economia mondiale, dove risulta essenziale disporre di misure di sicurezza per prevenire le minacce provenienti da fonti esterne e interne. I porti costituiscono infatti nodi intermodali cruciali nella rete di trasporto, nonché importanti punti di controllo delle frontiere.

Cosa si intende per "Sicurezza dei porti": l'importanza del codice ISPS

La sicurezza dei porti si riferisce alle misure adottate per salvaguardare i beni del porto, compreso il suo perimetro, le navi, il carico e il personale. Comprende misure proattive e reattive per ridurre al minimo il rischio di danni fisici, furti, sabotaggi, atti terroristici e altri incidenti di sicurezza. L'obiettivo della sicurezza portuale è prevenire qualsiasi atto illecito intenzionale che possa minacciare la sicurezza dei cittadini (lavoratori, passeggeri o equipaggio) e incidere sull'economia (ad esempio, danni alla proprietà, perdita di entrate, interruzione del commercio).

Dal 2004, l'Organizzazione Marittima Internazionale (IMO) ha concordato un nuovo regime di sicurezza per il trasporto marittimo, la cui pietra miliare è il codice ISPS (International Ship and Port facility Security), emendamento alla convenzione SOLAS (Safety of Life at Sea).

In tale regolamento, la sicurezza marittima è definita come l'insieme delle misure preventive volte a proteggere la navigazione e gli impianti portuali dalle minacce di atti illeciti intenzionali. L'obiettivo principale dell'ISPS è la sicurezza del naviglio e delle loro interfacce terrestri. La valutazione deve essere aggiornata periodicamente, tenendo conto dell'evoluzione delle minacce e, in ogni caso, deve essere riesaminata in caso di cambiamenti importanti nell'impianto portuale.

La sicurezza dell'impianto portuale comprende, tra le varie cose, l'identificazione della protezione del perimetro, del controllo degli accessi e l'identificazione dei punti deboli nell'infrastruttura, compresi i fattori umani.

Tecnologia LiDAR per la sicurezza dei punti deboli all'interno dell'infrastruttura

Una delle soluzioni più utilizzate per aumentare la sicurezza dei porti è l'utilizzo della videosorveglianza/AI ma l'ambiente salino, la brezza e l'umidità corrodono le telecamere e possono comprometterne l'operatività. Un altro elemento di disturbo per il corretto funzionamento del sistema video può essere rappresentato dalle occlusioni dell'area visibile bloccata dai container o dalla scarsa luminosità.

OPTEX offre una soluzione di sicurezza ottimale nelle aree portuali grazie alla serie REDSCAN, dotata di tecnologia LiDAR, attraverso la quale è possibile:

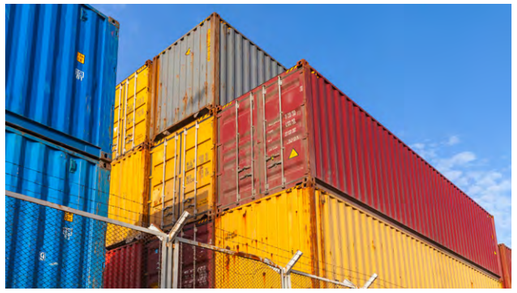
- proteggere gli edifici all'interno del perimetro del porto (tetti, facciate);
- proteggere le aree vulnerabili del perimetro, come le aree di accesso per i veicoli;
- monitorare veicoli fermi agli incroci e assicurare il proseguimento dell'operatività;
- garantire il rilevamento con un numero minimo di falsi allarmi grazie alla velocità e precisione del laser;
- creare un supporto alle misure di controllo degli accessi.

Tecnologia antitrusione per la sicurezza delle aree perimetrali

Uno dei componenti critici della sicurezza fisica del porto è la protezione dell'intera area perimetrale. Recinzioni, barriere e illuminazione possono essere utilizzate per limitare l'accesso all'area portuale e monitorare qualsiasi ingresso non autorizzato, ma non sempre queste misure sono sufficienti. Data la natura dell'infrastruttura, gli ingressi non autorizzati possono avvenire via mare e via terra. Il fatto che il perimetro del porto sia regolarmente pattugliato dal personale di sicurezza o che siano stabiliti punti di controllo dell'accesso, non garantisce che solo le persone autorizzate entrino nel porto.

Ci sono aree nel porto delimitate da un perimetro fisico, come un muro o recinzioni rigide o semirigide, come ad esempio, la LAZ (Logistics Activities Zone), un'area situata in prossimità di porti e terminal container, che offre una logistica intermodale ben collegata al trasporto aereo, ferroviario o stradale. Queste aree hanno spesso perimetri molto ampi, punti di ingresso multipli (veicolari, pedonali e marittimi), e un'alta presenza di presenza di veicoli e attività permanenti in cui il sistema di sicurezza non deve interferire.

La tecnologia in fibra ottica può rappresentare la soluzione ideale per la protezione del perimetro di queste aree. Montata su recinzione o interrata, è flessibile e si adatta all'ambiente, resiste alla corrosione e alla salinità, e non è influenzata da fenomeni atmosferici avversi come la nebbia e i fulmini. La serie EchoPoint™ utilizza algoritmi di rilevamento intelligenti per individuare con precisione la posizione di un'intrusione



con un margine di +/- 6 metri in un raggio d'azione fino a 100 km. Operando solo a livello perimetrale, non interferisce con l'attività della zona LAZ, né richiede spazi liberi dove effettuare il rilevamento, ma consente il preallarme nel caso in cui qualcuno si avvicini alla recinzione o provi a scavalcarla.

Conclusioni

La sicurezza fisica dei porti è essenziale per tutelare le infrastrutture critiche, le navi, il carico e le persone che, a diverso titolo, sono presenti in queste aree. Implementando adeguate misure di sicurezza fisica, controllo del carico e del personale, sorveglianza, monitoraggio e pianificazione della risposta alle emergenze, i porti possono prevenire e ridurre al minimo le minacce ai loro beni. L'efficace attuazione delle misure di sicurezza dei porti è fondamentale per mantenere il flusso del commercio internazionale e la sicurezza del porto per tutti gli utenti. Le soluzioni OPTEX possono rappresentare un valido supporto all'intero sistema porto.

OPTEX Sensing Innovation

Contatti:
OPTEX
Tel. +39 351 9272789
enquiry-it@optex-europe.com
www.optex-europe.com/it

Travel Risk Management nel XXI secolo

di Mirko A. Ruggeri – Madama Group International

Cos'e' il TRM?
Travel Risk Management e' un insieme di attivita' di sicurezza, gestione e logistica che le aziende devono porre in essere per tutelare i dipendenti che viaggiano all'estero. La normativa che regola questa attivita', la ISO 31030 (entrata in vigore nel 2021) e' arrivata con un ritardo di oltre un decennio rispetto alle politiche gia' adottate da aziende multinazionali a livello globale.
Il primo passo, per ogni azienda, e' la creazione di politiche aziendali relative al Travel Risk Management che si adattino alle esigenze dei viaggiatori d'affari ed all'unisono l'adeguamento delle polizze assicurative che devono prevedere emergenze mediche, disastri naturali, tumulti e proteste ed ogni evento eccezionale che possa sottoporre a rischio i viaggiatori o che richieda un'immediata evacuazione.

Come venivano gestiti i viaggi d'affari prima della ISO-31030?
A livello internazionale, le aziende si occupavano quasi esclusivamente delle prenotazioni dei mezzi di trasporto, hotels, ristoranti e dell'organizzazione di riunioni ed eventi ai quali i dipendenti dovevano partecipare. L'azienda ospitante era responsabile della sicurezza e di fornire assistenza ai partecipanti.
In molti paesi la situazione rimane invariata ma recentemente, a causa di incidenti occorsi a viaggiatori d'affari all'estero, solo le aziende direttamente interessate sono state costrette ad adeguare le politiche aziendali adottando una postura "reattiva", ovvero soffrendo una perdita economica prima e correndo ai ripari solo a cose fatte.

Quali sono gli aspetti da considerare in un programma di TRM?
Definire questa "disciplina di sicurezza del XXI secolo" richiede l'elaborazione dei vari aspetti che la compongono:
- Analisi dei rischi e delle minacce;
- Audit patrimoniali e reputazionali;
- Determinazione del livello di rischio a 360 gradi e valutazione delle misure e contromisure di sicurezza;
- Valutazione dei rischi dovuti ad emergenze sanitarie o possibili disastri naturali;
- Valutazione dei livelli di assistenza sanitaria, servizi di emergenza ed evacuazione;

- Creazione piani di contingenza;
- Valutazione dei mezzi di trasporto;
- Selezione delle risorse appropriate per ciascun incarico;
- Studio delle condizioni climatiche del paese da visitare per evitare eventi avversi ricorrenti quali la stagione delle piogge, tornado, uragani, ecc.;
- Studio delle leggi, regolamenti, norme, leggi religiose, tradizioni locali, culti religiosi ed ogni idiosincrasia che possa sottoporre i viaggiatori a rischi, in caso di violazione delle norme o mancanza di rispetto della cultura o della religione locale;
- Stabilire relazioni con le autorita' locali, consolati ed ambasciate al fine di ottenere collaborazione in caso di emergenza e fornire ai viaggiatori un'assistenza concreta durante il soggiorno all'estero.

Le suddette attivita' devono essere supportate da una rete internazionale di fornitori di sicurezza di comprovata esperienza e fiducia, non solo per le attivita' di sicurezza e protezione delle persone e dei beni aziendali ma soprattutto per corroborare l'attivita' preliminare di intelligence e fornire aggiornamenti in tempo reale in caso di eventi socio-politici che possano aumentare il livello di rischio.
La sola attivita' di intelligence online senza un'attivita' di riscontro sul territorio espone i viaggiatori a rischi elevati e l'azienda a potenziali danni di immagine, reputazionali ed a perdite economiche, in caso di incidenti.

Prevenire e minimizzare i rischi e' il punto focale di questa attivita'.

Quali sono le responsabilita' delle imprese?
Le imprese, i cui dipendenti viaggiano all'estero sia regolarmente che in modo sporadico, sono responsabili della sicurezza fisica degli stessi a 360 gradi in quanto le normative che regolano la sicurezza nei luoghi di lavoro, si trasferiscono automaticamente in qualsiasi luogo dove i dipendenti svolgano attivita' lavorative in nome e per conto del datore di lavoro.
E' chiaro che le suddette norme, quando si parla di scenari internazionali, richiedono uno sforzo significativo da parte dell'azienda e spesso vengono percepite solo come un costo ed un impiego di risorse addizionale che influisce in modo significativo sul budget destinato al comparto sicurezza.

Benefici del TRM
Un termine che circola da molti anni nel mondo della sicurezza e che puo' essere adottato in ogni settore ed attivita', e' "postura proattiva".
Per un'azienda, prevenire e pianificare, ridurre i rischi ed aumentare il livello di sicurezza delle persone e dei beni e' chiaramente una strategia "PROATTIVA".
Il TRM e tutte le attivita' poste in essere per la protezione dei viaggiatori d'affari e degli interessi aziendali forniscono grandi benefici in quanto valutare i rischi ed adottare contromisure di sicurezza permette all'azienda di ridurre la possibilita' di incidenti le cui conseguenze a livello economico e reputazionale potrebbero essere disastrose.

Case study
Nel 2014 un'azienda tecnologica americana organizzo' una conferenza a Las Vegas dove i direttori di area del Nord America si ritrovavano una volta all'anno per discutere strategie, creare nuove sinergie ed ampliare la propria rete di collaboratori.
Un direttore di 52 anni, cardiopatico, non aveva informato l'azienda della sua condizione né aveva adottato le dovute precauzioni durante il soggiorno.
A seguito di una partita di golf sotto il sole, ad oltre 40 gradi, l'uomo soffri' un infarto e collasso' gia' privo di vita sul campo.
L'azienda dovette incaricarsi delle spese mediche, del trasporto e tumulazione presso il luogo di residenza del dipendente e dovette indennizzare la famiglia, in quanto, secondo le leggi vigenti, l'azienda venne considerata responsabile di grave negligenza. Il tutto costo' all'azienda oltre 3 milioni di dollari.
L'azienda non aveva un programma di TRM né un servizio di protezione esecutiva al seguito dei dipendenti.

MADAMA Group grazie ad un'esperienza ultraventennale in campo nazionale ed una leadership formata nelle forze dell'ordine e nel settore privato e la sinergia creata con **RONIN Consulting** per le attivita' internazionali e' in grado di assistere la propria clientela in oltre 75 paesi a livello globale. Travel Risk Management, Protezione Esecutiva, Trasporti di sicurezza, intelligence in tempo reale, organizzazione, logistica ed ogni aspetto di sicurezza in occasione di viaggi d'affari, riunioni, eventi ordinari o su larga scala e la pianificazione di soggiorni di vacanza per famiglie ed impresari di alto profilo sono i fiori all'occhiello della collaborazione tra le due societa'.

Bio
Mirko Ruggeri, ex appartenente alla Polizia di Stato, opera da oltre 30 anni come esperto di Travel Risk Management e Protezione Esecutiva a livello internazionale, al fianco di multinazionali, impresari e famiglie di alto profilo ed ONG. Mirko ha condotto operazioni di sicurezza in 35 paesi a livello mondiale e contribuito alla creazione di programmi di TRM e Protezione Esecutiva per alcune delle aziende tecnologiche di interesse mondiale nella Silicon Valley, California. Mirko ha prodotto corsi di formazione alla sicurezza negli Stati Uniti, impartiti ad appartenenti alle Forze dell'Ordine, Forze Armate, Personale Medico e professionisti della sicurezza privata. Nel 2021 ha fondato RONIN Consulting, un servizio di consulenze di sicurezza e protezione esecutiva che opera in EMEA e APAC in oltre 75 paesi. Nel 2022 Mirko, in collaborazione con ANIVP a messo a disposizione del mercato italiano sei corsi di sicurezza innovativi ed adattati alle esigenze del settore privato nazionale ed internazionale a cui hanno partecipato operatori, supervisori, dirigenti e titolari di licenze di sicurezza.

Sicurezza aeroportuale e prevenzione antiesplosivi. La tutela dei viaggiatori a cuore di Cittadini dell'Ordine Spa

comunicato aziendale

La sicurezza aeroportuale è una priorità assoluta per garantire viaggi sicuri e protetti per i passeggeri in tutto il mondo. **Cittadini dell'Ordine Spa**, leader nel settore della sicurezza da oltre 150 anni e partner per la security aeroportuale di numerose strutture, è consapevole dell'importanza dell'argomento e lavora costantemente per implementare ed aggiornare le misure adottate per prevenire, tra le tante, la minaccia degli esplosivi negli aeroporti.

Attraverso controlli rigorosi, tecnologie avanzate e personale formato come disposto dalle normative per ottenere le certificazioni ENAC, Cittadini dell'Ordine si impegna a creare un ambiente aeroportuale sicuro per tutti i viaggiatori.

Un componente chiave della sicurezza aeroportuale è il controllo dei bagagli. Attraverso l'uso di scanner a raggi X, i bagagli dei passeggeri vengono attentamente esaminati per individuare la presenza di oggetti proibiti o esplosivi. Questi controlli sono effettuati in modo accurato e tempestivo, garantendo che ogni bagaglio venga esaminato attentamente per la sicurezza di tutti.

Oltre ai controlli dei bagagli, Cittadini dell'Ordine effettua controlli approfonditi sui passeggeri stessi. I dispositivi di screening avanzati, come i metal detector e gli scanner per i liquidi, vengono utilizzati per individuare potenziali minacce.

I passeggeri possono anche essere selezionati casualmente per controlli ulteriori, come la scansione del corpo tramite body scanner. Questi controlli mirano a individuare oggetti o sostanze sospette che potrebbero rappresentare una minaccia per la sicurezza dei viaggiatori.

I nostri professionisti lavorano a stretto contatto con le forze dell'ordine e altri soggetti adibiti alla sicurezza per individuare comportamenti sospetti e prevenire potenziali minacce.

Per quanto riguarda la prevenzione degli esplosivi, Cittadini dell'Ordine adotta misure specifiche per rilevare e prevenire l'introduzione di dispositivi proibiti negli aeroporti. Gli scanner a raggi X per i bagagli consentono agli operatori di individuare oggetti sospetti, inclusi materiali organici e non metallici che potrebbero essere utilizzati per la creazione di esplosivi. I rilevatori di tracce sono utilizzati anche per individuare la presenza di residui esplosivi su oggetti personali o bagagli.

I rilevatori di tracce (ETD - Explosive Trace Detection) vengono utilizzati per individuare la presenza di tracce di esplosivi su soggetti e oggetti come bagagli a mano, documenti, abbigliamento o attrezzature. Questi dispositivi utilizzano tecniche chimiche o fisiche per rilevare le particelle di esplosivo o i loro residui. Possono essere impiegati anche cani addestrati per rilevare gli odori degli esplosivi.

Un addetto della sicurezza aeroportuale ha il compito di passare una striscia di tessuto sulle mani e sulla cintura del passeggero, per prendere un campione e poi verificare la presenza di sostanze esplosive. Ha inoltre il compito di tamponare le mani dei passeggeri con questa striscia per assicurarsi che non vi siano esplosivi. E' una specie di tampone che raccoglie le tracce presenti sulle mani e sugli indumenti.

Dopo di ciò, il campione viene inserito in un'apposita macchina che analizza e rileva eventuali tracce di esplosivo producendo il "foglietto anti esplosivi", una delle misure per combattere il terrorismo.

È importante sottolineare che Cittadini dell'Ordine si impegna costantemente nella ricerca e nello sviluppo di tecnologie avanzate per migliorare la sicurezza aeroportuale. Queste tecnologie includono sistemi di riconoscimento facciale per il controllo dei passeggeri, sensori per la rilevazione di sostanze esplosive e sistemi di monitoraggio video ad alta definizione per sorvegliare le aree critiche degli aeroporti.

In conclusione, la sicurezza aeroportuale e la prevenzione antiesplosivi sono priorità assolute per **Cittadini dell'Ordine** che attraverso controlli rigorosi e l'utilizzo di tecnologie avanzate si impegna a garantire un ambiente aeroportuale sicuro per tutti i viaggiatori. La protezione dei passeggeri rimane al centro delle operazioni di Cittadini dell'Ordine, impegnati a prevenire minacce e garantire la massima sicurezza negli aeroporti.

Contatti:
Cittadini dell'Ordine S.p.A.
www.cittadinidellordine.com
contatti@cittadinidellordine.com

reconeyez

Odiamo i falsi allarmi

www.reconeyez.com/it

Nessun cavo, meno falsi allarmi, maggior durata delle batterie.

Rilevamento d'intrusioni intelligente.

Fino a 400 giorni di batteria

Rilevamento fino a 35 metri

Veloce da installare

OPTEX

FlipX Advanced

SICUREZZA INTERNA

FLX-A-AM

PIR CON ANTIMASCHERAMENTO

FLX-A-DAM

DOPPIA TECNOLOGIA
CON ANTIMASCHERAMENTO

Sensore di movimento di grado 3 per interni con lente flessibile per la protezione contro le intrusioni di siti di fascia alta e ad alto rischio.

- 15 m, 85 gradi (fascio ampio)
- 24 m (fascio stretto)

HESA

Da ERMES la colonnina segnalazione incendi per campeggi

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

Sono ormai scaduti i termini previsti per l'adeguamento di campeggi, villaggi turistici e strutture ricettive all'aria aperta a quanto previsto dal DM del 02.07.2019, in materia di prevenzione incendi.
Il decreto introduce la nuova versione della regola tecnica che prescrive l'installazione di un sistema di segnalazione incendi a disposizione degli ospiti che, in caso di necessità, permetta di allertare in maniera tempestiva il personale del posto presidiato affinché possa intervenire in modo rapido ed efficace.
Le colonnine in IP sviluppate da **ERMES** consentono di inviare una segnalazione di allarme al posto presidiato ed allo stesso tempo di attivare una comunicazione audio in viva voce tra la colonnina e l'operatore.
Questi potrà interloquire con la persona che ha attivato l'allarme in modo da accertarsi della esatta natura dell'evento e, se lo ritiene opportuno, potrà attivare, come previsto dalla norma, direttamente dalla console la sirena di allarme integrata su ogni colonnina.
Il collegamento degli apparati può essere realizzato in rame, fibra o wifi ma è disponibile anche la versione con collegamento in LTE/4G che non necessita dell'installazione di infrastrutture di collegamento.
La colonnina può essere alimentata a 230Vac ma anche con un pannello fotovoltaico e relativa batteria in tampone per cui nel caso si utilizzi il collegamento in LTE/4G il sistema risulta particolarmente semplice e veloce da installare.
Per ultimo, nel caso si voglia dotare la struttura di un sistema di diffusione sonora, è possibile sostituire la sirena di allarme con un proiettore di suono in grado di svolgere la duplice funzione di sirena e di altoparlante per la diffusione di annunci.

Inim: la nuova sirena da esterno DS100

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

È da ora disponibile un **nuovo modello di sirena per installazioni da esterno**.
DS100 di Inim è il connubio perfetto tra design, efficienza e sicurezza.
Una soluzione moderna studiata per racchiudere prestazioni elevate in un dispositivo compatto e minimale.
DS100 è dotata di emettitori acustici piezoelettrici e segnalazioni luminose progettate per garantire un'intensità elevata e limitare il consumo di energia, così da funzionare anche con bassa carica della batteria tampone.
DS100 offre:
• Installazione e manutenzioni facilitate
La leggerezza e allo stesso tempo la resistenza della plastica adottata per la realizzazione dell'alloggiamento facilitano l'installazione del dispositivo e gli interventi di manutenzione, fornendo anche una maggiore stabilità nel tempo.
• Interventi di manutenzione ridotti
Il nuovo sistema di ricarica intelligente è studiato per proteggere la batteria tampone ottimizzando la tensione di carica in base alla temperatura ambientale ed evitando il verificarsi della scarica profonda: in questo modo si prolunga notevolmente la vita utile della batteria, limitando ulteriormente la necessità di intervento da parte dell'installatore.
• Programmazione rapida e flessibile
La configurazione di default consente di installare il dispositivo in modo rapido e renderlo immediatamente operativo (Plug & Play). La sirena prevede anche un'ottima flessibilità di programmazione che consente di modificare le impostazioni secondo le esigenze e preferenze di ogni cliente.

essecome ONLINE

n. 04/2023
Anno XLIII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Angelo Carpani, Michela Carboni Gammon, Marco Censi, Nikitas Koutsourais, Lucio Piccinini, Mirko Ruggeri
Stefano Torri

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
- Registro pubblico Operatori di Comunicazione (ROC) n. 34727

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
lilian@lilastudio.it