essecome ONLINE 02/22

Periodico digitale di informazione di security & safety

2022 · ANNO XLII

Ks: la nuova era

Ks Series

Fitness Sorter

LBM ITALIA

LAUREL

MONEY COMPETENCE

Cover Story

LBM ITALIA S.P.A. PRESENTA LA SELEZIONATRICE KS SERIE

LBM Italia S.p.a. è una realtà che nasce nel 2013 dalla collaborazione tra una piccola azienda italiana e **Laurel Bank Machines**, storica azienda produttrice giapponese.
Questa unione ha permesso l'introduzione, in Italia, della tecnologia e dei prodotti Laurel, già esportati prima in America e, successivamente, in diversi paesi europei.

Sin dalla sua fondazione nel 1946, Laurel, produttore specializzato in macchine per il trattamento delle banconote e delle monete, è stata costantemente all'avanguardia mondiale nello sviluppo delle ultime tecnologie del settore che hanno contribuito notevolmente all'efficienza e al progresso delle operazioni di gestione del contante in tutto il mondo.
Ad oggi, **Laurel Bank Machines Japan** è un leader mondiale, ha tre stabilimenti a Tokyo e Osaka (con più di 1400 dipendenti), opera direttamente o con le sue consociate in oltre 140 paesi del mondo e vanta 3000 brevetti, derivanti da un costante e notevole impegno nell'area della ricerca e sviluppo e della qualità.

Le selezionatrici **serie K** sono il risultato di 40 anni di innovazioni e di esperienza nel settore del trattamento delle banconote. Il successo di queste apparecchiature risiede nella dedizione verso ogni singola componente. Ciò ha permesso che, negli anni, l'evoluzione non sia stata circoscritta alle sole caratteristiche tecniche, ma anche al design e al consumo ridotto. La **serie K**, dunque, nasce già proporzionata all'intensità di utilizzo (con una versatilità di capacità a tre, quattro, otto o dodici cassetti), garantendo così le stesse prestazioni in termini di velocità, efficienza e versione del software per ogni modello. Oggi, a distanza di decenni dalla prima selezionatrice della serie K, a seguito di aggiornamenti continui, Laurel Bank Machines presenta al mercato l'ultima nata: **KS serie**.

Perché KS può fare la differenza?
Perché è una macchina progettata per offrire altissime capacità prestazionali:
- la modularità dei suoi cassetti (gruppi da 4), che permette di arrivare a montarne fino a 24 in linea;
- la struttura di impilamento verticale dei cassetti riduce la larghezza del sistema e ne incrementa la produttività;
- Il nuovo validatore JDU-70 che, grazie alla sua alta tecnologia, mette a disposizione prestazioni mai raggiunte prima;
- un'elevata capacità di contazione, che può arrivare fino a 1200 banconote al minuto;
- un sistema user-friendly che rileva il movimento della mano dell'operatore e si attiva automaticamente.

La **KS Serie** è stata realizzata nel 2021 ma, a causa della pandemia, ha subito dei rallentamenti nella produzione massiva. Oggi, anche grazie all'entrata di **Nova Service** nella già affermata e consolidata sinergia tra **LBM Italia S.p.A.** e **Laurel Bank Machines Japan**, siamo lieti di presentare in Italia la **KS Serie** con la certezza che avrà un grande successo, grazie al suo notevole potenziale.

Sommario

Due passi per la sicurezza della nostra libertà

Si sta parlando molto dei rischi legati allo strapotere dei GAMF (Google, Amazon, Microsoft, Facebook) che, grazie al controllo dell'informazione ed alla profilazione di massa degli utilizzatori, avrebbero sopravanzato gli Stati nell'esercizio della sovranità nei confronti dei propri cittadini e perfino nelle relazioni con gli altri Stati, come ha fatto capire la recente contrapposizione tra USA e UE sulla tassazione dei profitti delle Big Four.
In un recente saggio, **Jacques Attali** sostiene che *"la democrazia e i suoi compromessi saranno sempre meno amati e difesi, con gli Stati che diventeranno solo dei prestanome di grandi multinazionali planetarie"* e aggiunge che: *"passeremo dall'attuale situazione di ipersorveglianza all'autosorveglianza, quando le persone saranno rassegnate a fornire volontariamente ogni informazione su di sé in cambio di sicurezza."* (*'Disinformati'* - ed. Salani, 2021).

Si parla invece meno degli altrettanto sostanziosi rischi legati alla globalizzazione delle tecnologie di uso comune.
Il cloud è forse l'esempio più noto e immediato di strumenti che sovrastano e annullano i confini geo-politici degli Stati, ma sappiamo quanti e quali sono i servizi e i prodotti critici per la salute, la sicurezza e la continuità operativa delle comunità e dei singoli individui realizzati utilizzando componenti fisiche, informazioni e software sviluppati in luoghi diversi del mondo? In luoghi i cui governanti potrebbero all'improvviso farsi la guerra o, più semplicemente, entrare in competizioni commerciali senza esclusione di colpi?

Se il coronavirus ha fatto capire che la ricerca scientifica globalizzata ha consentito lo sviluppo di vaccini in tempi brevissimi, la guerra in Ucraina ha fatto invece "scoprire" che l'antivirus più diffuso al mondo è russo, di una nazione diventata improvvisamente ostile per le altre in Occidente con le quali aveva tranquillamente commerciato fino al giorno prima. E in questo momento ci sono purtroppo anche motivi per temere una crisi nel Pacifico per la sovranità di Taiwan, che potrebbe determinare effetti devastanti in tutto il mondo occidentale non solo per l'approvvigionamento di dispositivi elettronici (e non), la cui fabbricazione è stata negli anni completamente delegata alla Cina per motivi economici, ma anche per la sicurezza dei dati acquisiti da quei dispositivi installati ovunque in Occidente, ove non venissero adeguatamente protetti.

Di fronte ad uno scenario così articolato e complesso, non sarebbe il caso che le organizzazioni pubbliche e private (ma anche le singole persone, su un piano diverso) facessero una bella analisi delle minacce attuali e future alle quali ritengono di essere esposte e si attrezzassero per tempo per difendere quanto c'è di buono della globalizzazione digitale?
Partendo dalla scelta consapevole delle informazioni su se stessi da mettere online per arrivare alla crittografia end-to-end e agli IoT gateway passando per la verifica dei fornitori, le soluzioni ci sono e non sono impossibili da realizzare.
Se rendersi conto che si può fare è il primo passo, volerlo fare sarebbe il secondo per mettere in sicurezza la nostra libertà.

Foto: Viandante sul mare di nebbia – Caspar David Friedrich 1818

securindex formazione

SAN GIORGIO

APR - SECURITY & SAFETY PER LE INFRASTRUTTURE DEL TRASPORTO

Sicurezza fisica e cibernetica negli aeroporti italiani. Il punto della situazione.

---

23 giugno | ore 14.30 -18.00

NH Collection Roma Vittorio Veneto

Con il convegno sul tema *"Sicurezza fisica e cibernetica negli aeroporti italiani. Il punto della situazione"* si apre il ciclo **APR – security & safety per le infrastrutture del trasporto** organizzato da **essecome editore** in partnership con l'ente di formazione **San Giorgio**, nel corso del quale verranno affrontati i diversi aspetti della sicurezza delle strutture e degli impianti del trasporto pubblico: **aeroporti, porti, ferrovie, trasporti urbani, infrastrutture stradali e autostradali.**

Il progetto si rivolge agli operatori delle filiere interessate e sarà articolato in eventi in presenza, webinar e approfondimenti editoriali ai quali verranno affiancati percorsi formativi finalizzati al rilascio ed al mantenimento delle certificazioni delle competenze previste per le diverse figure professionali coinvolte.

Verranno invitati i rappresentanti delle istituzioni di riferimento, delle associazioni di categoria e degli operatori pubblici e privati per analizzare gli aspetti di sicurezza più rilevanti e attuali assieme ai più noti esperti e docenti delle diverse materie, e per conoscere le migliori pratiche con il supporto di vendor e service provider di livello internazionale.

Il primo appuntamento del ciclo è dedicato ad una valutazione delle minacce di tipo fisico, informatico e combinato che riguardano gli aeroporti che, per le peculiari caratteristiche del trasporto aereo civile, utilizzano in modo condiviso a livello globale i modelli organizzativi, le procedure e le tecnologie più evolute e consolidate, sviluppando in tal modo esperienze ed indicazioni fruibili anche in contesti diversi dal trasporto aereo.

Verrà inoltre fatto il punto della situazione del livello di consapevolezza delle molteplici tipologie di rischio in capo alle diverse figure che operano nel contesto aeroportuale e del ruolo della formazione continua.

Questo il programma del convegno del 23 giugno 2022:

14.00 - *registrazione*
14.30 - *il quadro della situazione della cybersecurity nelle IC del Trasporto.*
Keynote speaker: Corrado Giustozzi
15.00 - *presentazione del progetto ENAV - Assaeroporti*
15.30 - *soluzioni e best practices per la sicurezza combinata in ambito aeroportuale*
16.00 - *il ruolo della formazione degli operatori (Università della Tuscia - San Giorgio)*
16.30 - *tavola rotonda: "Cybersecurity, tutela per le infrastrutture del trasporto e risorsa per il Sistema Paese".*

L'evento è riservato ad appartenenti alle Istituzioni di riferimento, operatori delle infrastrutture del trasporto (società di gestione, handler, service provider) e security manager certificati UNI 10459.

Ai partecipanti all'evento in presenza ed a distanza su piattaforma Zoom verrà rilasciato attestato di partecipazione ai fini dell'ottenimento di crediti formativi.

Per informazioni e pre-iscrizioni:
segreteria@securindex.com | 02.36757931

Travel security, l'analisi del legale per la tutela dell'impresa. L'importanza del modello organizzativo

intervista all'avv. Antonio de Capoa – Founder & Partner Studio Legale de Capoa

Sul piano giuridico, ritiene che la recente pubblicazione della Norma UNI ISO 31030 possa compensare il vuoto legislativo a livello internazionale sulle responsabilità dei datori di lavoro in ordine ai rischi per il personale viaggiante?

La risposta è solo parzialmente affermativa, alla luce anche dei recenti orientamenti giurisprudenziali espressi dai Tribunali penali, non solo italiani, in materia di travel security, nonostante l'indubbia autorevolezza dell'International Organization for Standardization (più nota come ISO) e dell'UNI, che hanno predisposto la summenzionata Norma.
E' importante sottolineare che le norme tecniche (i c.d. "standards") sono delle disposizioni elaborate da organismi riconosciuti a livello internazionale o nazionale, la cui osservanza non è, però, obbligatoria.
Di fatto, la norma/standard - per consuetudine o per l'autorevolezza dell'organismo che l'ha predisposta - pur non nascendo come un atto cogente e vincolante, lo diventa dopo, costituendo uno dei parametri cui fanno riferimento le pubbliche amministrazioni, le compagnie assicuratrici e le stesse autorità giudiziarie che, in linea generale, si attengono proprio agli standard per stabilire l'eventuale grado di colpevolezza del datore di lavoro e/o dell'organo gestorio di una impresa.
Ne consegue che l'importanza della Norma UNI ISO 31030 sia assolutamente fuori di discussione e la sua adozione da parte delle imprese, delle università, dei centri di ricerca, delle ONG, dei consulenti e, più in generale, di chiunque organizzi trasferte all'estero di propri collaboratori e/o dipendenti, comporterà una serie di indiscutibili benefici in termini di adeguata valutazione e gestione dei rischi connessi alle trasferte all'estero, in termini organizzativi e di gestione delle risorse umane, in termini di riduzione dei premi assicurativi e, certamente, di riduzione se non financo di eliminazione del rischio di subire una condanna penale.
Tutto ciò è indiscutibile e, quindi, è di solare evidenza che tutti i soggetti e le entità che inviano persone all'estero abbiano la massima convenienza ad adottare il modello organizzativo predisposto dalla Norma. Infatti, avendo anche a mente la normativa italiana di riferimento in materia di sicurezza sui luoghi di lavoro, è noto che spetta all'entità datrice di lavoro dimostrare di avere adottato e, quindi attuato prima che si avveri l'evento dannoso, adeguati modelli organizzativi accompagnati da sistemi di controllo idonei a prevenire l'accadimento dell'evento configurante l'illecito.
L'Ordinamento italiano, analogamente agli Ordinamenti degli altri Paesi europei e della stessa Unione Europea, prevede la creazione di uno "scudo protettivo" nell'interesse delle stesse aziende e datori di lavoro, scudo rappresentato per l'appunto dalla adozione di modelli organizzativi finalizzati a dimostrare la non volontarietà dell'evento lesivo, con la conseguenza dell'esclusione o, quantomeno di una riduzione sensibile della responsabilità del datore di lavoro.
Fatta questa premessa, e per capire la complessità della domanda sottopostami, rilevo che bisogna operare una distinzione tra il caso in cui il "trasfertista" sia un lavoratore dipendente, e quello in cui sia un collaboratore esterno, ausiliario o comunque, un soggetto non sottoposto (quantomeno a livello formale) al vincolo di dipendenza e, quindi, di lavoro subordinato.

Una seconda distinzione va effettuata in base alla natura della trasferta, ossia se trattasi di trasferta meramente temporanea pur se prolungata nel tempo (financo qualche mese), oppure se trattasi di un vero e proprio distacco, con la conseguenza che il trasfertista viene assunto od ingaggiato, per un determinato arco di tempo, dall'impresa o dall'entità straniera presso la quale viene distaccato.
Una terza ed ultima distinzione riguarda la c.d. "natura transnazionale" del rapporto di lavoro, ovvero se la transnazionalità è originaria oppure se è acquisita. Più esattamente, con l'espressione di rapporto di lavoro a "transnazionalità originaria" si intendono quei rapporti di lavoro nei quali il prestatore dell'attività viene assunto/ingaggiato appositamente per espletare la sua attività all'estero, mentre l'espressione di rapporti di lavoro a "transnazionalità acquisita" designa quei rapporti nell'ambito dei quali solo in epoca successiva alla sua nascita l'azienda datrice di lavoro chiede ed ottiene dal lavoratore/collaboratore la disponibilità a recarsi all'estero per ivi svolgere determinate attività.
Per quanto riguarda la prima delle tre problematiche sopra esposte, sottolineo che viene comunemente considerato collaboratore esterno od ausiliario quella figura che agisce in proprio ma per conto e nell'interesse della azienda o della entità preponente, in forza di un mandato o di un rapporto contrattuale o di ogni altra forma di collaborazione professionale.
Purtuttavia, al di là delle innumerevoli declinazioni che ha conosciuto nel nostro Ordinamento la figura del lavoratore autonomo/consulente/collaboratore autonomo - ovviamente senza includere i professionisti iscritti agli Albi professionali o quei professionisti che, pur senza essere iscritti in un Albo, svolgono effettivamente ed incontrovertibilmente una attività libero-professionale con propria organizzazione di mezzi e di risorse anche umane, o del ricercatore o del collaboratore, quali, ad esempio, il consulente a progetto, etc - in base al quadro normativo attuale ed alla giurisprudenza vigente si può affermare che, in aggiunta alle ipotesi di collaborazione professionale definibili come "parasubordinazione" e quindi inquadrabili nell'ambito del lavoro subordinato, *"..... omissis .....si applica la disciplina del rapporto di lavoro subordinato anche ai rapporti di collaborazione che si concretano in prestazioni di lavoro esclusivamente personali, continuative e le cui modalità di esecuzione sono organizzate dal committente anche con riferimento ai tempi e al luogo di lavoro"* in base a quanto disposto dall'art. 2 del D.Lgs nr. 81/2015. Trattasi della c.d. "etero-organizzazione" la cui definizione si ricava da una Circolare del Ministero del Lavoro e delle Politiche Sociali del 1 febbraio 2016, che recita: *" ..... omissis ..... ogniqualvolta il collaboratore operi all'interno di una organizzazione datoriale rispetto alla quale sia tenuto ad osservare determinati orari di lavoro e sia tenuto a prestare la propria attività presso luoghi di lavoro individuati dallo stesso committente .....omissis.....".*
In tutti i casi in cui un'impresa o un'entità invii all'estero un trasfertista, sia esso un proprio dipendente o un collaboratore o ausiliario e benchè esso sia formalmente, ed anche dal punto di vista fiscale, un lavoratore autonomo, o, addirittura se trattasi di forme di collaborazione basate sul "volontariato" ma operi nell'ambito di una "etero-organizzazione", l'impresa o l'entità diventano responsabili della sua sicurezza e, quindi, devono anche essere dotate di un modello organizzativo adeguato che includa espressamente anche tutta la tematica della travel security, comprensiva pure della figura del collaboratore formalmente non alle sue dirette dipendenze, se vogliono cercare di essere esonerati da responsabilità o, quantomeno, che la responsabilità sia sensibilmente ridotta nel caso in cui si verifichi un evento dannoso (i.e. malattia, sinistri, eventi delittuosi, etc), nel senso di provare l'assenza di dolo o di colpa grave.
Per concludere e, quindi, rispondere alla domanda, osservo che il nostro Paese che, come è sin troppo noto, nonostante si caratterizzi per una abnorme produzione legislativa e normativa, così come per un'altrettanto abnorme produzione giurisprudenziale, e che si è dotato di un ampio e complesso sistema normativo in materia di sicurezza dei luoghi di lavoro e di salute dei lavoratori, oltre che in tema di igiene, salubrità, etc, ha trattato in maniera estremamente sommaria ed inadeguata la materia della sicurezza e salubrità dei lavoratori inviati all'estero, in forma sia saltuaria che stanziale, con la conseguenza che sin troppo spesso si sono verificati, anche in tempi recenti, episodi che hanno fatto emergere le vistose lacune in tema di sicurezza nei confronti di coloro i quali svolgono la loro prestazione lavorativa al di fuori del territorio nazionale, nel senso che i prestatori di lavoro chiamati ad operare all'estero non godono, di fatto, delle stesse tutele di coloro che lavorano in Italia.

Conclusivamente, è indubbio che la pubblicazione della Norma UNI/ISO 3130 consentirà l'adozione di modelli organizzativi adeguati per individuare e, quindi, mitigare i rischi connessi alla travel security ma è altrettanto indubbio che occorra anche un intervento legislativo, a livello nazionale o dell'Unione Europea per colmare una serie di vuoti e lacune normative, soprattutto per ciò che attengono le responsabilità di tipo penale, vista la natura particolarmente sensibile di questo tipo di responsabilità e per tutto ciò che comporta.

Calandoci nel contesto giudiziario italiano, quali misure/procedure deve osservare (e poter dimostrare di averlo fatto) un datore di lavoro per mitigare i rischi di sanzioni e risarcimenti in caso di sinistro?

Certamente l'adozione e la concreta attuazione di un modello organizzativo basato sulla Norma UNI/ISO che sia effettivamente adeguato e coerente con le caratteristiche della entità datrice di lavoro, rappresenterebbe un "bel passo in avanti" per quanto riguarda la mitigazione dei rischi di subire sanzioni e/o dover pagare risarcimenti di varia natura.

Ma, in aggiunta all'adozione del modello organizzativo, è indispensabile che il datore di lavoro, a prescindere dal fatto che sia un soggetto pubblico o privato, persona fisica o giuridica, di piccole o di grandi dimensioni, effettui tutte le più opportune verifiche in ordine alla rischiosità del Paese di destinazione e dei Paesi di attraversamento (dal punto di vista sanitario, della sicurezza sociale e di quella politica, della presenza di conflitti o meno, della normativa in materia di sicurezza e di igiene sui posti di lavoro e previdenziale, e così di seguito) così come deve assumere tutte le informazioni possibili sui luoghi presso i quali il trasfertista svolgerà la sua attività in termini di sicurezza, di igiene e della sicurezza personale.

Premesso che la soluzione migliore sarebbe quella di affidarsi ad una impresa specializzata nel settore della travel security quantomeno per avere una "griglia" o una linea guida per mappare i rischi potenziali, qualora per le più svariate ragioni il datore di lavoro optasse di gestire da solo le problematiche, dovrà cercare di assumere tutte le informazioni dal sito del Ministero degli Affari Esteri dedicato proprio ai viaggi all'estero, consultando il sito dell'Organizzazione Mondiale della Sanità, e, più in generale, tutti i siti accessibili e consultabili che possano fornire le adeguate informazioni, dopo di che dovrà trasferire a sua volta queste informazioni al proprio dipendente.

In base alla mia esperienza, raramente le aziende da sole possiedono gli strumenti e le tecnicalità per predisporre degli efficaci modelli organizzativi per gestire questo tipo di rischio, con la conseguenza che esse si espongono a dei forti rischi.

Il mio consiglio è che il datore di lavoro adotti un modello organizzativo ben fatto, avendo a mente anche le problematiche da me poc'anzi delineate.

Su un piano più specifico, come si devono comportare per non incorrere in sanzioni le PMI che mandano dipendenti all'estero e non hanno le dimensioni o la possibilità di implementare un sistema interno di TRM compliant alla UNI ISO 31030?

Bisogna che comunque adottino un modello organizzativo che, per poter essere veramente efficace, deve comunque essere supervisionato da un esperto nella tematica della travel security. Fare da soli comporta dei forti rischi, tenuto conto del contesto attuale geopolitico (alla data odierna, nel mondo vi sono ben 37 Paesi, sui 193 che fanno parte dell'ONU, in cui sono in corso dei conflitti armati) e del perdurare della pandemia.

Orbene, in un mondo così complicato e pieno di tensioni, inviare dei dipendenti o collaboratori in giro per il mondo richiede grande attenzione e l'acquisizione di molte conoscenze oltre a dover adottare molteplici precauzioni, non limitandosi a stipulare polizze assicurative speciali.

Va poi segnalato che il trasfertista italiano, inviato all'estero dall'azienda o dall'entità italiana, potrà fruire sia della protezione assicuratagli dalle norme imperative previste dalla legge italiana (in particolare, dalla L. 631) che della protezione delle norme imperative in materia antinfortunistica previste dalla legge del Paese in cui è stato inviato a prestare la sua attività lavorativa.

Una deroga al suindicato principio è rappresentata dal caso in cui il dipendente (e, conseguentemente, non il lavoratore para-subordinato) venga distaccato dall'azienda o entità italiana in via permanente e, conseguentemente, venga assunto direttamente dalla azienda o dall'entità del Paese in cui viene distaccato, sia essa una branch od una subsidiary dell'azienda italiana, o, più semplicemente, una impresa od un'entità che intrattiene rapporti di stretta collaborazione con la propria datrice di lavoro (pensiamo ai grandi appalti od al montaggio di impianti industriali, allo scambio di ricercatori, e così via).

In questi casi, in linea teorica, sarebbe applicabile per intero la sola normativa del Paese di destinazione.

Purtuttavia, affinchè l'azienda o l'entità italiana possa essere esonerata, in questi casi, da coinvolgimenti e da responsabilità, deve provare di aver verificato e riscontrato: (i) se la normativa prevenzionistica del Paese esiste, e, in caso affermativo, se offra un adeguato sistema protezionistico ed il suo grado di efficacia; (ii) l'accettabilità degli standard di sicurezza dei luoghi di lavoro in cui il dipendente presterà la propria attività; (iii) il contesto globale del Paese o, più, specifico, dei luoghi in cui il trasfertista vivrà, dal punto di vista della sicurezza globale.

Incombe pertanto all'azienda/entità Italiana che decide di inviare proprio personale all'estero, sia esso dipendente o parasubordinato, l'onere di adeguare sia il DVR che il DUVRI (quest'ultimo nei casi in cui l'invio di personale sia legato alla esecuzione di contratti di appalto o di somministrazione) rispetto alle problematiche specifiche connesse al tipo di trasferta, alla sua durata, alla mission del trasfertista, alla tipologia del Paese di destinazione e così via. Dovrà comunque adottare un preciso modello organizzativo per il lavoro all'estero, oltre che effettuare tutte le necessarie verifiche.

Anche nei casi di distacchi per periodi prolungati o permanenti, che comportano il passaggio del trasfertista alle dirette dipendenze dell'azienda /entità del Paese di destinazione, l'azienda/entità italiana ha l'obbligo di effettuare quelle verifiche sopra accennate.

Ci si permette di raccomandare di prestare la massima attenzione, al momento di stipulare contratti od accordi con controparti ubicate in Paesi extra UE, alla tematica della privacy atteso che, normalmente, nell'ambito di uno stretto rapporto di collaborazione tra aziende, vi è uno scambio di dati tra cui anche dati sensibili.

A questo riguardo sottolineo che, in base ad una Decisione della UE del 2010 (che deve ritenersi tuttora in vigore, nonostante l'intervenuta modifica della normativa ad opera del Regolamento 2016/679 - GDPR), i contratti di qualsiasi genere stipulati con Paesi extra UE che non offrono sufficienti garanzie in materia di raccolta, trattamento e conservazione di dati sensibili, possono essere dichiarati inefficaci e financo nulli.

Infine, sottolineo che il sempre più diffuso utilizzo delle tecnologie informatiche e del conseguente trasferimento sempre più massiccio di dati in via telematica, comporta l'onere in capo all'azienda Italiana di prestare la massima attenzione alla tematica della cybersecurity ed alle conseguenze, anche molto rilevanti, sul piano risarcitorio che possono derivare da attacchi informatici che violino non solo i segreti aziendali, ma anche i dati sensibili che ineriscono al trasfertista (pensiamo alle notizie sulla sua persona, sulla sua famiglia, sulle sue condizioni di salute, convinzioni politiche o religiose, i suoi spostamenti, etc), dovuti ad una non adeguata protezione dei sistemi informatici, o dalla mancanza di procedure di sicurezza nell'utilizzo delle reti e di mancato rispetto delle norme tecniche che forniscono indicazioni e criteri utili per gli operatori e delle "best practices" vigenti nel settore.

Per ultimo, quali supporti può dare uno Studio legale internazionale per la tutela delle imprese italiane che lavorano all'estero?

Per prima cosa, lo studio legale dovrebbe avvisare i propri clienti della importanza di adottare le opportune misure per accertare e, quindi, mitigare i rischi connessi alle trasferte all'estero dei propri dipendenti e collaboratori. Questa funzione di sensibilizzazione è estremamente importante.

In secondo luogo, è decisivo suggerire ai propri assistiti di prevedere queste problematiche nelle negoziazioni e, quindi, nei contratti con i clienti, partners e, comunque, con i soggetti presso i quali devono recarsi i propri dipendenti/collaboratori, in modo che vengano identificati i fattori di rischio e contrattualizzata la loro mitigazione. Quindi, andranno inserite nei contratti stipulati con controparti straniere (siano essi di fornitura più montaggio, appalto, franchising e così di seguito) tutte le più opportune clausole relative al tema della travel security, inclusa anche la sicurezza nei luoghi di lavoro ove materialmente i trasfertisti dovranno svolgere la loro attività.

Di estrema rilevanza è anche inserire le opportune clausole di salvaguardia nei confronti dei trasfertisti, siano essi dipendenti o collaboratori esterni.

Infine, lo studio legale dovrebbe rapportarsi ed interagire con le società di consulenza che predispongono i modelli organizzativi in base allo Standard UNI/ISO, in modo da collaborare - ciascuno per quanto di sua competenza - affinchè il modello organizzativo predisposto sia il più completo possibile ed adeguato alle specifiche dimensioni ed esigenze del cliente, sia esso pubblico o privato.

Quali rischi per i viaggiatori aziendali se la travel security la compra il procurement aziendale?

intervista a Daniela Valenti, Global Project Manager – Pyramid Temi Group

Recentemente ICoCA (International Code of Conduct Association), l'associazione mondiale delle organizzazioni fornitrici di servizi di protezione per le persone, riconosciuta dall'ONU, ha sollevato la questione che molte aziende scelgono i fornitori di Travel Security attraverso il procurement, senza fare opportuna attività di due diligence. Ci può dare un commento?

E' molto frequente, nel mondo delle grandi aziende, che la gestione degli acquisti avvenga attraverso il procurement. Questo riguarda non solo merci e servizi legati al core business dell'azienda, ma anche servizi specializzati di varia natura. Travel security è uno di questi.

La delicatezza di questo settore richiede che, per valutare un provider di servizi di sicurezza, specialmente se si tratta di attività svolte all'estero, si disponga di una preparazione specifica in materia. Si può presumere che il procurement abbia una preparazione adeguata per quanto riguarda gli acquisti relativi al core business aziendale, ma è poco probabile che abbia conoscenze approfondite in tutti gli altri campi.

Per questo motivo, ci dovrebbe essere un doppio controllo qualificato da parte del management ma sappiamo, invece, che la scelta finale di un fornitore di travel security viene presa solitamente dal procurement, cosa che spesso equivale a un salto nel buio. Per non parlare delle gare di appalto, sviluppate talvolta senza una chiara visione dei reali bisogni dell'organizzazione. Nelle specifiche viene richiesto di tutto magari senza alcuna logica per finire, a volte, con l'assegnazione finale attraverso asta elettronica al ribasso. Un'autentica follia!

Quali possono essere i rischi di queste scelte e le conseguenze per le aziende?

Così facendo, le aziende corrono il rischio di illudersi di aver provveduto alla sicurezza, quando invece non è vero. Innanzitutto, per i viaggiatori significa non ricevere adeguata protezione, con un aumento di rischio per la loro incolumità fisica; per il management dell'azienda, significa correre il rischio di essere accusato di negligenza con conseguenze, anche pesanti, in ambito civile e penale.

Possiamo riassumere il tutto in una parola: *accountability*, che vuol dire responsabilità.

Per legge, il datore di lavoro, ossia il top management che rappresenta legalmente l'azienda, è responsabile in sede civile e penale delle conseguenze dell'eventuale inadeguatezza delle misure di protezione delle persone che rientrano nel Duty of Care. Davanti alla legge, queste responsabilità non sono delegabili come un semplice compito da svolgere o una merce da acquistare. In altre parole, se la responsabilità operativa di selezionare i fornitori è in capo al procurement, la responsabilità legale rimane sempre in capo al top management.

Come mai siamo arrivati a questo punto?

E' probabilmente un effetto distorto della comprensibile volontà di evitare "favoritismi" nella selezione dei provider ma, soprattutto, dell'esigenza di contenere i costi. Purtroppo, l'adozione di un processo che dovrebbe dimostrare e garantire buona governance e qualità di gestione, in alcune situazioni può portare a risultati contrari e la travel security è tra questi.

Il nuovo standard UNI/ISO 31030 tratta questo problema? Che cambiamento ha portato?

Certamente l'argomento viene trattato nello standard. Riporto un passaggio (7.4.2) che rappresenta un ottimo esempio di attenzione al tema:

f) accertarsi che nel processo di selezione dei fornitori e subfornitori vengano verificate le competenze e le esperienze che dimostrino:

- *appropriato accreditamento, certificazioni e licenze*
- *prove che dimostrino una precedente specifica esperienza e il livello di reputazione sia a livello professionale, sia etico (se opportuno, occorre anche avviare un processo di prequalificazione)*
- *adeguata copertura assicurativa e una copertura geografica che possa supportare i viaggiatori nella destinazione desiderata.*

L'organizzazione deve mantenere opportuna documentazione a riprova della competenza specifica.

Si tratta di indicazioni molto chiare, che non lasciano spazio ai dubbi.

La Norma UNI/ISO 31030 - Travel Risk Management è il primo documento di riferimento del settore riconosciuto a livello globale, che ha portato finalmente chiarezza e supporto concreto per la sicurezza in viaggio.

A questo punto, c'è una considerazione molto importante da fare, in particolare dai top manager delle aziende. Mentre prima della pubblicazione della UNI/ISO 31030 le accuse di negligenza erano possibili solo dopo il verificarsi di un incidente (vedi il "caso Bonatti"), adesso esistono protocolli, riconosciuti in Italia e nel resto del mondo, che permettono a chi di competenza di fare indagini e, se il caso, di avviare un processo per negligenza anche in assenza di incidenti.

Alla luce di ciò, è necessario che la norma venga integrata tra le norme di governance delle aziende, altrimenti ci sarà sempre il rischio di non fornire protezione adeguata ai viaggiatori e di subire condanne per negligenza.

Travel Security, dalla Norma UNI ISO 31030 alla UNI/PdR 124:2022

intervista a Roger Warwick, CEO Pyramid Temi Group

Ci può riassumere i punti essenziali della UNI/PdR 124:2022, sviluppata dopo la pubblicazione dello standard ISO 31030?
Per realizzare un sistema di TRM all'interno di aziende che inviano personale all'estero è fondamentale avvalersi di persone qualificate. Nello Standard ISO 31030 si fa riferimento a questo concetto, senza entrare nel dettaglio di quali competenze siano necessarie per operare nel settore del Travel Security. L'esigenza di una Prassi di Riferimento nasce proprio da qui. Confindustria Emilia Area Centro e UNI hanno sviluppato e pubblicato, per primi nel mondo, la UNI/PdR 124:2022 *"Attività professionali non regolamentate – Figure professionali operanti nell'ambito della travel security – Requisiti di conoscenza, abilità, autonomia e responsabilità"* con l'obiettivo di supportare le aziende nell'individuare e selezionare coloro che sono in possesso degli opportuni requisiti per operare nell'ambito della gestione della sicurezza delle trasferte.
La Prassi individua e descrive i requisiti di tre figure chiave: il Travel Security Officer, che assicura che il processo di travel security management sia adeguato ed appropriato alle esigenze dell'organizzazione e delle persone; il Travel Security Manager, che si occupa della gestione operativa della security, safety e health delle persone che viaggiano per conto dell'organizzazione; e il Travel Security Analyst, che fornisce alla gestione operativa, tramite raccolta, analisi e valutazione delle informazioni rilevanti, le informazioni utili per la security, safety e health di chi viaggia all'estero.

Esistono dei percorsi di formazione per chi volesse intraprendere questa attività lavorativa?
Certamente. Confindustria Emilia insieme a FAV- Fondazione Aldini Valeriani, la scuola di Industrial Management di Confindustria Emilia, ha ideato e sviluppato, in partnership con Pyramid Temi Group e UNI, una Masterclass aperta alle imprese che vogliono formare il proprio personale, oppure a privati che intendono intraprendere una carriera in questo settore. Un progetto innovativo che partirà il prossimo 24 Maggio con la formazione indirizzata al Travel Security Manager, alla quale sarà possibile abbinare un percorso si certificazione con RINA.

Come ritenete si possano organizzare le PMI che hanno personale viaggiante all'estero ma non hanno le dimensioni sufficienti per dotarsi internamente delle figure previste dalla PdR pur volendo essere compliant?
In primo luogo le aziende devono analizzare il proprio contesto, capacità e esigenze. Lo scopo è quello di comprendere se possono gestire il processo di Travel Security in autonomia, oppure se necessitano di supporto esterno. Si può procedere con la formazione dello staff già presente in organico, con l'assunzione di nuovo personale qualificato, oppure delegare la gestione del processo ad aziende specializzate nel settore. La PdR è dunque un punto di riferimento per le aziende, perché è la chiave per individuare e selezionare le persone più adatte a ricoprire un incarico molto delicato. Ricordiamoci che l'accountability, ovvero la responsabilità legale, rimane sempre in capo ai vertici aziendali, quindi per il Datore di Lavoro è imprescindibile affidarsi a chi dimostra di essere in possesso delle giuste competenze. Per concludere, possiamo dire che con la nuova Prassi, e naturalmente, con la ISO 31030, le aziende hanno finalmente a disposizione tutti gli strumenti per dimostrare buona governance e compliance.

Travel Security, l'importanza della consapevolezza delle imprese

intervista a Andrea Giacominelli, Funzionario dell'Area Ambiente e Sicurezza di Confindustria Emilia | membro del tavolo di esperti che ha realizzato la UNI/ PdR 124:2022

Dal suo punto di osservazione, qual è il livello di consapevolezza delle imprese sulle responsabilità del datore di lavoro in merito ai rischi del personale viaggiante?
Gli accadimenti che si sono succeduti in questi ultimi due anni, a livello nazionale ed internazionale, hanno posto all'attenzione della governance aziendale la complessa rete di adempimenti e le conseguenti responsabilità che ne derivano, connesse alla predisposizione di viaggi e o trasferte di lavoro per i propri collaboratori. Oggi il livello di consapevolezza e le misure messe in campo delle aziende sono decisamente più elevati rispetto al periodo pre-pandemico. Tanto può essere ancora fatto poiché, tipicamente, si tende a concentrare la propria attenzione ed a focalizzarsi su aree geografiche da tutti ritenute critiche, trascurando però zone ritenute meno problematiche. Gli eventi terroristici accaduti negli ultimi anni in paesi a noi culturalmente molto vicini hanno fatto comprendere come tale approccio debba essere considerato un semplice punto di partenza per l'implementazione di un sistema teso alla sicurezza del personale viaggiante, anche per garantire la Business Continuity.

Più in generale, quali azioni ritiene siano più opportune ed efficaci per elevare l'attenzione degli imprenditori verso temi "no core" come la sicurezza in senso lato dei lavoratori ma che possono provocare pesanti conseguenze per la stessa continuità aziendale?
A nostro avviso occorre intervenire sulla governance aziendale, ad esempio organizzando momenti di confronto e di divulgazione della tematica, quale quello promosso da Confindustria Emilia Area Centro lo scorso 13 aprile, inserendo, dove possibile, il riferimento a casi concreti che rappresentano elementi tangibili ed immediatamente comprensibili. Il processo di innalzamento della cultura della sicurezza deve comunque coinvolgere i collaboratori aziendali a tutti i livelli ed al riguardo si possono organizzare momenti formativi più mirati al personale direttamente coinvolto nelle fasi organizzative e valutative (ad esempio gli RSPP e gli HR).
Per completare il quadro, non si può poi trascurare la necessità di disporre di figure professionali competenti e qualificate per il presidio di queste tematiche all'interno delle aziende. La Prassi di Riferimento 124/2022 promossa da Confindustria Emilia e pubblicata da UNI, nasce proprio da questa necessità. Ed è sempre in questa stessa ottica che va inquadrato il progetto formativo realizzato da Fondazione Aldini Valeriani, la scuola di industrial management di Confindustria Emilia, con la collaborazione di Pyramid Temi Group SRL, per la preparazione delle figure che in azienda si devono occupare della pianificazione, organizzazione e gestione delle trasferte.

Parte la Masterclass della Fondazione Aldini Valeriani per Travel Security Manager

intervista a Enrica Bonzani, responsabile Area Formazione per le imprese della Fondazione Aldini Valeriani

Quali sono i contenuti e la struttura della Masterclass sulla Travel Security che avete organizzato in base alle indicazioni della PdR UNI 124?
La Masterclass "Travel Security Manager" nasce dall'esigenza di tradurre in un percorso formativo le competenze della figura professionale delineata dalla PdR UNI 124.
Fondazione Aldini Valeriani, che ha partecipato dal 2020 al tavolo di lavoro UNI con Pyramid Temi Group, ha delineato la prima edizione della Masterclass per Travel Security Manager; il percorso, della durata di 100 ore, a partire dal 24 maggio, formerà il Travel Security Manager, figura professionale che si occuperà della gestione operativa della security, safety e health delle trasferte del personale aziendale. Si svilupperà su 6 moduli, che avranno come focus le normative di riferimento, gli scenari del travel risk management, le tecniche di comunicazione, la costruzione di un travel risk management, la selezione e la gestione dei rapporti con i provider.
Al termine del percorso sarà possibile ottenere, dopo il superamento dell'esame finale, la certificazione rilasciata da Rina - Ente di certificazione.

Il corso è riservato alle aziende del circuito di Confindustria Emilia o è aperto a tutti gli interessati?
La Masterclass non è solo riservata alle aziende di Confindustria ma è aperta alle tutte le aziende che vogliono formare il proprio staff oppure ai privati che intendono specializzarsi verticalmente sul tema della business travel security e proporsi alle aziende.

Come si svolgeranno le lezioni e quali saranno i docenti di riferimento?
La Masterclass si svolgerà sia in forma di webinar che in presenza. Per chi lo preferirà, verrà data la possibilità di frequentare il percorso interamente da remoto, utilizzando dotazioni tecnologiche e digitali d'avanguardia. Saranno comunque previste sessioni in presenza per chi, invece, vorrà partecipare "dal vivo".

Le sessioni in presenza si svolgeranno presso Fondazione Aldini Valeriani, via Bassanelli 9/11- Bologna, mentre quelle da remoto con piattaforma Gotomeeting. La Masterclass, coordinata da FAV e da Pyramid Temi Group, sarà condotta da alcuni dei maggiori esperti di security di grandi gruppi internazionali in possesso di competenze specialistiche, maturate a seguito di esperienze lavorative di almeno otto anni. Trasversali al percorso, trainers Fondazione Aldini Valeriani condurranno sessioni dedicate alle tecniche di comunicazione manageriale.

Ci può riassumere le attività della Fondazione Aldini Valeriani?
Fondazione Aldini Valeriani è la Scuola di Industrial Management di Confindustria Emilia Area Centro che nasce nel cuore tecnico di Bologna, luogo in cui si sono formati gli industriali bolognesi che, con le loro storie e attività, hanno reso la nostra regione famosa ed unica al mondo.
Fondazione Aldini Valeriani, che lavora da 30 anni nell'ambito della formazione aziendale, ha lanciato Industrial Lounge, un brand dedicato all'alta formazione d'Impresa, una vera e propria officina della formazione manageriale, un nodo di un network internazionale costituito da centri di ricerca, università e luoghi di business. Nell'ultimo decennio, opera in grandi gruppi industriali grazie al possesso accreditato di competenze metodologiche, acquisite in tanti anni di progettazione formativa in qualità di partner dell'azienda. Sempre tesa all'innovazione, offre alla community percorsi d'avanguardia sia in termini di nuovi profili richiesti dal mercato che di design della formazione.

Attacchi cyber e attacchi sui social, la posizione di AIPSA

intervista ad Andrea Chittaro, presidente AIPSA

Come si può commentare il recente attacco cyber subito dalle Ferrovie dello Stato sul piano della prevenzione e delle capacità di reazione della struttura?
Da quello che leggo e dalle informazioni che sono girate nel network di settore, la struttura di security, assieme alle altre funzioni aziendali coinvolte, ha reagito tempestivamente e con efficacia. I danni al core business, in questo caso il trasporto ferroviario, sono stati estremamente contenuti. Se l'obiettivo degli attaccanti era quello di fermare un'infrastruttura critica nazionale, direi che non è stato conseguito.
Nemmeno sul fronte del pagamento di un eventuale riscatto, peraltro.
La strategia di segmentare opportunamente la rete ha consentito di isolare un'area ben definita, dove operare in fase di response e recovery.

Cosa sta alla base, invece, delle pesanti critiche lanciate sui social alle Ferrovie dopo l'attacco?
I social, per loro natura, sono praterie dove si esercitano in libertà commentatori di ogni genere. Ad ogni attacco subito da un'azienda o da un'Istituzione va in scena il solito copione "del giorno dopo". Io mi limito a rilevare le parole del Capo della Polizia Postale, il Dott. Ivano Gabrielli che ha, sostanzialmente, confermato l'impressione di un intervento rapido ed efficace da parte della struttura preposta.
Chiunque abbia solo una lontana idea di come oggi è complesso il mondo infrastrutturale ed applicativo di una qualsiasi realtà, sa bene che è impossibile chiudere ogni porta, blindarsi in una sorta di castello che ricorda i paradigmi della sicurezza di 40 anni fa. Un margine di esposizione resterà sempre anche a fronte di modelli di prevenzione particolarmente maturi. Allora, prima di lanciarsi in facili quanto approssimativi giudizi, sarebbe bene approfondire e capire, oltre alle cause, anche quanto un'azienda abbia investito in tecnologie e competenze. La security è un'attività da praticare con umiltà e con la consapevolezza che non esiste un modello perfetto.

Riprendendo invece i risultati della recente indagine realizzato per conto di Everbridge e Spike Reply in collaborazione con AIPSA sul livello di resilienza delle imprese italiane, quali azioni si potrebbero adottare per migliorare i livelli di preparazione alla gestione di eventi critici?
Innanzitutto, già dotarsi di un'organizzazione preposta alla gestione di questi eventi sarebbe un'ottima base di partenza. Sembra quasi banale dirlo ma, nella realtà, non sempre c'è una struttura di processo dedicata e dotata della giusta autonomia, del necessario budget e delle altrettanto essenziali competenze.
La storia recente ci ha insegnato come il mondo possa cambiare nel giro di poco. Come le certezze a cui ci eravamo ancorati possano venire meno. Due crisi di portata globale come la pandemia e il conflitto Russia-Ucraina non hanno memoria recente. Ed hanno sconvolto radicalmente abitudini, progetti, annullando ogni comfort zone. Credo che ci aspettino anni complicati, dove la percezione di insicurezza globale crescerà e dove strutturarsi per affrontare le sfide discendenti non sarà più un optional ma una ineludibile necessità.

Cosa farà AIPSA in questo senso?
Continuerà nella sua instancabile opera di sensibilizzazione, a tutti i livelli, e di promozione culturale della security e della consapevolezza verso questi temi. Credo sia venuto il momento per affermare definitivamente il ruolo delle funzioni di security aziendale e la loro rilevanza strategica rispetto ad ogni business.

Kaspersky e le garanzie di affidabilità nei momenti di crisi

intervista a Cesare D'Angelo, General Manager di Kaspersky Italia | a cura di Raffaello Juvara

Partiamo dalla domanda d'obbligo in questo momento di crisi. In merito alle preoccupazioni che in occidente tutti hanno rispetto ad un'ipotetica azione coercitiva da parte del governo di Mosca nei confronti di una società privata come Kaspersky che, comunque è russa, cosa rispondete?

Faccio una piccola premessa perché, giustamente, hai parlato di una società russa. In realtà, per quanto la sede e l'origine dell'azienda siano in Russia, Kaspersky è un'azienda globale con la capogruppo registrata a Londra da ormai più di vent'anni. Di fatto, oggi non si può parlare di un'azienda solo russa ma di una multinazionale a tutti gli effetti con la capogruppo registrata, appunto, in UK.

Per rispondere alla tua domanda, quello che abbiamo fatto da tempo e che è ancora più importante ribadire in questa situazione, è stata l'adozione di processi sia per lo sviluppo delle soluzioni che per il loro controllo che ci portano a dire che oggi un'azione coercitiva da parte di un qualsiasi governo difficilmente avrebbe successo per diversi motivi.

Intanto, perché il nostro CEO ha già dichiarato, in più occasioni che, qualora dovesse essere in qualche maniera spinto o obbligato dal governo a mettere in piedi determinate azioni, la sua risposta sarebbe negativa.

Da un'altra parte, ci sono processi e dati oggettivi con tanto di certificazioni, che aiutano a capire come questo sarebbe veramente difficile da realizzare.

Abbiamo spostato da tempo in Svizzera i nostri data center che processano le informazioni che arrivano su base volontaria da parte dei clienti. A Zurigo abbiamo il "Transparency Center", il luogo fisico dove i clienti governativi e le aziende accreditate, dopo una selezione a valle della loro richiesta, possono ispezionare il codice sorgente del prodotto e capire come vengano gestiti i

processi di sviluppo del software e gli aggiornamenti prima che vengano distribuiti ai clienti.

Per questo Transparency Center abbiamo ottenuto due certificazioni da parte di analisti esterni.

Una delle "Big Four" ha rilasciato la certificazione SoC di livello 2 ai nostri processi di scrittura, aggiornamento e distribuzione del software, avendo rilevato la conformità agli standard di sicurezza previsti da questo format, mentre TUV Austria ha rilasciato la certificazione ISO 27001 per la qualità di gestione dei dati dei clienti.

Ultimamente, anche il Garante della Privacy in Italia ha aperto un'istruttoria per capire come noi gestiamo i dati dei nostri clienti. Abbiamo risposto al Garante nei tempi dovuti dando tutte le informazioni richieste e siamo confidenti che venga confermato anche ufficialmente il rispetto delle norme sul trattamento dei dati dei clienti.

In sintesi, le soluzioni di cui stiamo parlando oggi, che sono tipicamente soluzioni di "endpoint protection" o antivirus come vengono chiamate più comunemente, garantiscono ai nostri clienti che non si possono trasformare da strumento di difesa a strumento in attacco, come gli enti esterni hanno certificato relativamente ai processi con cui questi prodotti vengono poi portati sul mercato.

Non da ultimo, questi processi sono stati pensati e realizzati in modo che, prima di arrivare sui device dei nostri clienti, tutti gli aggiornamenti vengano lavorati, analizzati e verificati in più step, in più country. Il passaggio finale, prima della distribuzione ai nostri clienti, viene fatto fuori dalla Russia.

Quindi pensare oggi che ci possa essere da un momento all'altro una modifica del nostro software per portare un attacco o, come alcuni sostengono, per tralasciare qualche verifica e far passare qualche cosa che non dovrebbe passare, è veramente un'ipotesi molto remota.

Remota significa però che non è impossibile, che non si può escludere completamente…

Questo è, in realtà, un problema generale dal momento che tutti i sistemi, avendo accesso ad ogni file del computer, potrebbero diventare degli strumenti in grado di fare qualcosa di diverso rispetto a quello per cui sono stati pensati.

Nel nostro caso, l'ipotesi che viene discussa più spesso è che da un giorno all'altro qualcuno si presenti in ufficio e ordini che il prodotto debba diventare un "attaccante" o che passi delle informazioni. È uno scenario che, se si dovesse verificare, richiederebbe settimane, mesi o addirittura anni, dal momento che oggi il nostro prodotto è basato su miliardi di interazioni quotidiane. Abbiamo 400 milioni di utenti sparsi in tutto il mondo e parte di questi utenti ha deciso di condividere le proprie informazioni alimentando il motore nel cloud basato su algoritmi di intelligenza artificiale che, negli anni, ha raggiunto la capacità di distinguere ciò che è malevolo da quello che non lo è, di segregarlo e di neutralizzarlo. E' pertanto impossibile che dal mattino al pomeriggio qualcuno decida di modificare questo motore e, se dovesse mai succedere, sarebbe comunque un lavoro che richiedebbe tempo e verrebbe in qualche modo intercettato.

Nella sostanza, tu affermi che chi sia eventualmente esposto a questo tipo di rischio avrebbe tempo e modo di potersi difendere e mettersi in sicurezza, giusto?

Diciamo che se anche qualcuno a monte del processo intendesse modificare il perimetro, a valle di quella modifica sono previsti dei controlli finalizzati ad annullare le modifiche fatte a monte proprio sulla base di quei processi che sono stati certificati, come ti ho spiegato. E questo era stato fatto già in tempi precedenti il conflitto, proprio per evitare che un ipotetico cybercriminale molto bravo si inserisse nei nostri sistemi e portasse delle modifiche.

Torniamo su un altro tema più generale, che hai toccato prima sottolineando che Kaspersky non è più un'azienda solamente russa ma è un'azienda globale. Parliamo dell'autonomia dei vendor globali rispetto ai governi. Questo passaggio storico sta facendo emergere anche l'esigenza che i fornitori globali possano garantire a tutti gli utilizzatori, siano enti governativi, aziende private o singoli cittadini, la propria autonomia rispetto alle prese di posizione dei governi che, chiaramente possono toccare ambiti più elevati, più sensibili dal punto di vista strategico. Puoi dirci qualcosa su questo tema?

Per come la viviamo e la interpretiamo noi, la sicurezza è un elemento che si basa su tanti attori che lavorano contemporaneamente verso lo stesso obiettivo, per cui la questione della maggiore o minore sovranità di qualche vendor rispetto ad altri è forse più vera a parole che nei fatti. Per esempio, parti delle nostre soluzioni o servizi sono presenti anche in soluzioni o servizi di nostri competitor o di terze parti e sarebbe veramente difficile rimuoverle.

In definitiva, dal punto di vista delle tecnologie, è davvero complicato parlare di autonomia totale.

Poi ogni fornitore ha delle peculiarità che concorrono a una sicurezza globale più solida. Quando parliamo ad esempio di "threat intelligence", le analisi delle minacce informatiche svolte dagli analisti per prevenire gli attacchi dei cybercriminali, noi siamo molto forti nell'analisi e nel contrasto delle minacce che vengono dalla parte est del globo, quindi dall'Asia e dalla Russia. Altri vendor sono invece più presenti e più forti in altre aree, per cui va da sé che mettendo insieme le diverse forze il risultato sia migliore per tutti i clienti.

In definitiva, il mondo digitale si muove con logiche diverse da quelle delle mappe o delle cartine geografiche che hanno dei confini.

Viene difficile pensare che in un mondo in cui si lavora sul cloud - il cui funzionamento e potenza di calcolo non sono necessariamente argomenti di interesse per l'utente finale, a patto che sia rispettato il GDPR - si possa pensare a dei confini come quelli geografici. Lavorando in un mondo globale, dobbiamo essere capaci di attivare al meglio le risorse che arrivano da aziende che hanno una copertura globale, come siamo noi, rispettando tutte le regole legate al trattamento dei dati dei clienti.

A questo punto vorrei farti una domanda in merito ad un altro tema, ovvero la sicurezza delle telecamere, cinesi e non. Adesso il problema è diventato scottante in Italia per la gara Consip ma vorrei analizzarlo da un punto di vista più generale. I timori di diversi governi occidentali, fra cui USA, Gran Bretagna, Australia e, adesso almeno in parte, anche il nostro, riguardano la sicurezza delle telecamere in rete e degli IoT sia sul piano della penetrabilità da parte di estranei che della deviazione dei dati verso destinatari sconosciuti. Come valutate questo problema?

Cercherò di darti una risposta coerente con quello che noi facciamo, rifacendomi a due argomenti.

Da un lato l'argomento tecnico: che si tratti di una telecamera piuttosto che di un registratore di cassa o di qualsiasi altro sensore sul territorio, dal momento in cui è in rete e comunica dati, c'è una vulnerabilità. Noi abbiamo introdotto sul mercato una soluzione che è, appunto, uno "IoT gateway", vale a dire un oggetto che serve a mettere in sicurezza la comunicazione tra i vari sensori sparsi sul territorio e il server centrale al quale devono arrivare le informazioni. Aggiungendo questo "strato", questo livello ulteriore di cybersecurity, mettiamo in sicurezza anche le informazioni che girano tra i vari device e il server che le deve raccogliere rispetto ai possibili attacchi per intercettare questi dati. Quindi, al di là del fatto che si parli di una telecamera cinese piuttosto che di altro, la vulnerabilità e la sicurezza dei dati possono venire gestite e indirizzate.

Poi c'è l'argomento politico che, in questo momento, ci vede sotto i riflettori.

Non entro nel merito se sia giusto o sbagliato puntare il dito su tale fornitore o su tale governo ma, essendo stati tra i primi ad essere oggetto di questo tipo di attenzioni dal 2017 in poi, cosa abbiamo fatto in Kaspersky?

Abbiamo deciso di portare i nostri data center in Svizzera che, oltre ad essere neutrale, è la nazione che all'interno dell'Europa ha le normative più stringenti in termini di data privacy e di sicurezza dei dati dei clienti.

Abbiamo deciso di rendere disponibile, a chi abbia le capacità e l'interesse di farlo, il nostro codice sorgente del prodotto. Questo nell'ottica della massima apertura e trasparenza anche verso le istituzioni governative.

Nel campo della cybersecurity mi risulta che siamo gli unici ad aver fatto un'operazione del genere e non ho evidenza di iniziative simili neanche in altri settori.

Solo dieci giorni fa sono stato a Zurigo con un ospite a far vedere il Transparency Center, qualcosa che si può toccare, si può vedere e si può capire quali garanzie possa dare.

In conclusione, la mia risposta su questo tema è che, al di là delle attenzioni nei confronti di questo o quel governo, c'è modo di rendere affidabili e trasparenti le comunicazioni con i clienti, come abbiamo fatto noi, permettendo di andare a investigare e capire quanto siano sicuri i prodotti.

Come identificare i dispositivi a rischio di cyberattacchi nei sistemi di sicurezza fisica delle aziende

di Gianluca Mauriello, Regional Sales Manager Italia, Genetec Inc

Molte aziende si ostinano a utilizzare vecchi modelli di telecamera e sistemi di controllo accessi obsoleti, sostituendoli solo quando non si può più evitarlo o quando il loro costo è stato completamente ammortizzato.

Purtroppo i dispositivi datati, a maggior ragione se si parla di telecamere, presentano spesso una limitata capacità di sicurezza e gli hacker conoscono bene una serie di fattori che aiutano a prenderne il controllo e a utilizzarli per accedere alla rete. Andiamo a scoprire quali.

Un design di rete obsoleto

In passato, la sicurezza fisica non aveva bisogno di dedicare grande attenzione al versante informatico. I dispositivi erano tipicamente collegati in un design di rete chiuso, che non ha tenuto il passo con il diversificarsi e approfondirsi delle esigenze di sicurezza legate a connessioni internet, WiFi o cellulari. Insomma, si è accumulato un ritardo nell'integrazione di funzionalità e tecnologie.

Manutenzione inadeguata

La gestione della sicurezza fisica non sempre integra le prassi migliori per la sicurezza informatica, come modificare di frequente le password o sostituire dispositivi che, invecchiando, non ricevono più firmware aggiornati dal produttore.

Carenza di conoscenze

Il personale che ha installato e gestito i sistemi di sicurezza fisica potrebbe essere andato in pensione o aver abbandonato l'azienda, lasciando un vuoto di conoscenze su dispositivi, configurazioni ed esigenze di manutenzione.

Dispositivi vulnerabili

Non tutti i modelli di telecamere presenti sul mercato sono affidabili dal punto di vista del rischio informatico. Alcuni paesi stanno già scoraggiando l'uso di determinati prodotti, a causa di conclamate pratiche discutibili da parte del produttore.

Per identificare i dispositivi a rischio, si possono eseguire le seguenti operazioni:

- Creare un inventario aggiornato di tutte le telecamere e dei sistemi di controllo collegati alla rete, anche tramite connessione Wi-Fi o cellulare.
- Verificare l'inventario effettuando controlli di persona, in loco, per rilevare i dispositivi che potrebbero essere stati dimenticati.
- Disporre di informazioni dettagliate su ciascun dispositivo di sicurezza fisica (ad esempio, età, modello della telecamera, produttore e versione del firmware).
- Identificare i tipi di crittografia e le funzionalità di cybersecurity supportate su ogni dispositivo o versione del firmware.
- Verificare la fonte e la legittimità di ogni aggiornamento del software prima dell'installazione, poiché uno di essi potrebbe essere usato per installare codici dannosi.
- Verificare l'inventario dei dispositivi sulla base delle informazioni pubblicate sui produttori e i modelli che hanno rivelato rischi per la sicurezza. Stabilire se dare priorità a questi dispositivi perché siano sostituiti anticipatamente.
- Aspetto più importante e impegnativo, riunire la sicurezza fisica e la sicurezza informatica al di sotto di un unico team con operazioni integrate.

Contatto:
Gianluca Mauriello,
Regional Sales Manager Italia, Genetec Inc.
Tel. +39 327 739 8560
www.genetec.com

Resilienza organizzativa e prevenzione dei rischi cyber, i trend secondo Spike Reply

intervista a Sonia Crucitti, Partner e CEO di Spike Reply

Ci può parlare di Spike Reply e delle sue attività nel mercato italiano?
Spike Reply è la società del Gruppo Reply focalizzata sulla Cybersecurity e sulla Data Protection.
Dal 2002 la nostra missione, grazie al contributo dei nostri professionisti specializzati sulle principali tecnologie e soluzioni di cyber security e attivi presso i principali organismi e istituti internazionali è quella di supportare i nostri clienti nel prevenire e rispondere agli attacchi cyber, nonché quella di aiutarli ad innalzare la loro security posture e nel rendere la sicurezza un fattore abilitante nei percorsi di digital transformation.
Questi obiettivi vengono raggiunti grazie ad un'offerta completa e integrata, che coniuga l'anima tecnica di Reply, tramite il disegno e l'implementazione di soluzioni di sicurezza innovative, con servizi di advisory e di consulenza strategica per la definizione di programmi di gestione dei rischi cyber in linea con gli obiettivi strategici e il risk appetite dei nostri clienti.

La recente indagine che avete sviluppato con Everbridge sul livello di resilienza delle aziende italiane evidenzia che ci sono ampi margini di miglioramento in termini di preparazione per gestire eventi critici. Dal vostro punto di osservazione, cosa sarebbe opportuno fare per migliorare la situazione, sia a livello aziendale che di sistema?
Dal nostro punto di osservazione confermiamo che vi sono ancora diversi ambiti su cui lavorare per migliorare la gestione di un evento critico e riteniamo che le aziende possano effettuare ulteriori step decisivi per incrementare la propria capacità di resilienza facendo sinergia tra le diverse discipline che, a vario titolo, indirizzano queste tematiche in azienda (corporate e cyber security e business continuity in primis).
In primo luogo, per quanto riguarda le azioni di natura preventiva, molte aziende non hanno ancora messo in campo, o lo hanno fatto solo parzialmente, attività di simulazione e test delle proprie procedure di gestione degli eventi critici, con il conseguente rischio di non essere adeguatamente preparate.
A nostro avviso, la definizione di un programma di simulazioni e stress test delle procedure di risposta ad un evento critico è una delle azioni fondamentali per il corretto monitoraggio dell'efficacia della propria strategia di resilienza.
Le simulazioni, siano esse table top o test reali (ad esempio in ambito cyber attività di red teaming) sono dal nostro punto di vista tra le iniziative più efficaci e concrete per mettere alla prova le reali capacità di un'azienda di rispondere ad un evento critico.
Sono degli strumenti al contempo di testing e di formazione e awareness che, per essere efficaci, devono utilizzare scenari "threat and risk-intelligence-led" e coinvolgere tutta l'organizzazione, compresi il top management e la supply chain.
Per migliorare la situazione, occorre anche investire sulle tecnologie adottando soluzioni che favoriscano la gestione centralizzata delle crisi, mettendo i team preposti nella condizione di governare tramite un'unica interfaccia gli stakeholder e le risorse necessarie per accelerare i tempi di ripristino, mantenendo il comando e il controllo qualora la crisi evolva in modo inatteso e garantendo la continuità delle attività business-critical.
Il corretto funzionamento di processi e tecnologie non può inoltre prescindere da fonti informative e attività di risk intelligence adeguate, utili a garantire una migliore comprensione dell'evento critico.
Infine, in ottica di miglioramento continuo, risultano esservi spazi per migliorare la raccolta e la sistematizzazione dei KPI, adottando processi e tecnologie per raccogliere dati in maniera automatica e standardizzata, in modo da utilizzare le evidenze raccolte per correggere eventuali criticità ma, soprattutto, per implementare modelli predittivi che consentano di anticipare la manifestazione di un evento critico (analisi predittive "data driven").
L'implementazione di questi spunti di miglioramento porta benefici non solo al livello di resilienza della singola azienda ma anche a livello di sistema, andando a incrementare la capacità complessiva di interi settori e, in una logica più ampia, della supply chain, consentendo così di rispondere ad eventi critici con impatto sistemico.
Il fattore chiave perché questo avvenga è che le diverse realtà che popolano gli ecosistemi aziendali collaborino tra loro in ottica di scambio e cooperazione, condividendo informazioni, partecipando ad attività comuni (ad esempio, esercitazioni e simulazioni) e concordando degli standard da applicare a tutti gli attori della catena di approvvigionamento.

Parlando di prevenzione dei rischi cyber a livello generale, quali trend prevedete nel prossimo futuro?
Per il prossimo futuro prevediamo il consolidamento di tre trend che, seppur in modo diverso, abbiamo già avuto modo di osservare sul campo.
Il primo riguarda uno shift degli investimenti in cybersecurity, shift che vede lo spostamento dello spending dalle contromisure necessarie alla prevenzione dell'attacco, agli investimenti necessari a migliorare le capacità di risposta e gestione dello stesso. Questo cambiamento nelle priorità è, se vogliamo, collegato al concetto stesso di resilienza e, quindi, non alle abilità che consentono di prevenire eventi avversi, ma allo sviluppo di quanto necessario ad affrontarli e superarli con successo. Nel contesto attuale le aziende hanno ormai capito che quando si parla di attacchi cyber la variabile non è più "se" ciò avverrà, ma "quando".
Il secondo trend riguarda invece la visione della cybersecurity come elemento pervasivo e nativamente integrato nell'organizzazione e nei propri prodotti/servizi digitali. Sulla falsa riga di quanto già fatto in passato per la qualità, le organizzazioni più virtuose hanno iniziato a considerare la cybersecurity come un elemento pervasivo, in grado di contagiare ed essere integrato in tutte le attività dell'organizzazione stessa. La sicurezza non è più qualcosa da aggiungere a difesa e protezione, ma una caratteristica intrinseca di ogni asset e processo.
Il terzo ed ultimo trend riguarda invece una visione di stampo sistemico per quanto riguarda gli aspetti di security impattanti sulla propria organizzazione. Ogni organizzazione, ed in particolare i servizi digitali che ne rappresentano il cuore pulsante, sono ormai composti attraverso la creazione di ecosistemi complessi e dinamici, ecosistemi che prevedono l'integrazione e l'interazione con fornitori di varia natura. Questo implica che il perimetro da considerare nelle valutazioni di sicurezza debba necessariamente considerare la supply chain nella sua interezza. La capacità di resilienza non dipende più solo da quanto sotto il controllo di un'organizzazione, ma dal livello di resilienza di ogni attore coinvolto il tale ecosistema. L'anello più debole, anche se apparentemente non rilevante, potrebbe infatti compromettere la resilienza di un intero ecosistema.

Le capacità di resilienza delle aziende italiane. Indagine di SPIKE REPLY ed EVERBRIDGE con AIPSA

di Federica Maria Rita Livelli - Business Continuity & Risk Management Consultant (*)

Scenario

Lo scenario erratico in cui stiamo vivendo mette a dura prova la resilienza delle nostre organizzazioni.

Spike Reply ed **Everbridge** - in collaborazione con **AIPSA** - hanno recentemente svolto un'indagine per valutare il livello di capacità delle aziende italiane nel gestire i rischi, la continuità organizzativa ed operativa e identificare le strategie atte a garantirne la resilienza.

L'indagine - presentata da Spike Reply ed Everbridge lo scorso 24 marzo durante l'evento patrocinato da AIPSA e titolato *"La capacità di resilienza delle aziende italiane: scenari attuali e prospettive future"* – ha coinvolto 45 medio-grandi organizzazioni operanti sia sul territorio nazionale sia a livello internazionale.

Il livello di capacità delle organizzazioni nel gestire eventi critici e nel garantire la continuità del business è stato misurato utilizzando un Maturity Model - strutturato in cinque livelli (i.e. in ordine crescente: ad hoc, reattivo, gestito, proattivo, ottimizzato) e riferito a quattro fasi di gestione degli eventi critici, quali:

- valutazione di minacce e impatti
- localizzazione
- risposta alla manifestazione dell'evento
- analisi della capacità di prendere decisioni data-driven prima (i.e.: identificazione dei rischi prima che si trasformino in eventi critici), durante e dopo l'evento critico/dirompente

I risultati dell'indagine hanno evidenziato come la maggior parte delle organizzazioni coinvolte - pur avendo predisposto procedure per la gestione degli eventi critici - non effettui regolari aggiornamenti dei modelli, rischiando di prepararsi inadeguatamente alla gestione di un evento critico.

Inoltre, risulta quanto mai importante individuare e censire correttamente i cosiddetti asset critici che, nella maggior parte dei casi, sono gestiti in modo integrato, pur risultando ancora diffusi i sistemi basati su fogli di calcolo o piattaforme interne (soprattutto per gli asset materiali). Ne consegue che risulta difficile garantire sia una visione globale degli assetti, sia la raccolta di informazioni coerenti.

Le organizzazioni, per quanto riguarda le risorse umane, utilizzano sia piattaforme di localizzazione automatizzate per censire/mappare il personale viaggiante o gli expatriate sia piattaforme centralizzate di HR Management per i dipendenti in sede.

Di seguito i risultati dell'analisi del Livello di Maturity delle organizzazioni intervistate:

- **Livello di Maturity "Reattivo" nella fase di "valutazione" - Il 43%** identifica i rischi prima che si trasformino in eventi critici, ma non sufficientemente in anticipo da garantire ottimali tempi di risposta e di recupero. I rischi sono individuati solitamente tramite indagini via internet; mentre le valutazioni in termini di gravità e di impatto sugli asset sono eseguite manualmente, rallentando così l'attivazione dei piani di risposta e compromettendo il controllo della situazione in caso di evento dirompente.

- **Livello di Maturity "Gestito" nella fase di "localizzazione" - Il 38%** localizza e comunica efficacemente con i team di risposta e con chi è stato impattato dall'evento dirompente, i dipendenti e gli stakeholder, utilizzando sistemi di geolocalizzazione o check-in ed Emergency Call System. Tuttavia, solo il 5% delle organizzazioni ha un sistema unificato per la gestione di crisi o eventi critici.
- **Livello di Maturity "Gestito" nella fase di risposta alla manifestazione dell'evento - Il 46%** riesce a mitigare l'impatto di un evento dirompente e a comunicare efficientemente con le risorse impattate. Tuttavia, il 48% delle organizzazioni non risultano avere in essere una procedura di escalation sufficientemente automatizzata atta a ottimizzare i flussi informativi, ridurre tempi di reazione, garantire una migliore risposta all'emergenza.
- **Livello di Maturity "Gestito" nell'analisi della capacità di prendere decisioni data-driven prima, durante e dopo l'evento critico/dirompente - Il 43%** effettua la raccolta ed il monitoraggio dei dati in tempo reale, impiegando processi standardizzati che, pur richiedendo spesso un intervento manuale, permettono di: riesaminare regolarmente le informazioni; anticipare eventi futuri; apportare migliorie ai piani di risposta. Inoltre, risulta che l'aggregazione dei dati richiede spesso un intervento manuale.

Nessuna delle organizzazioni ha raggiunto il Livello "Ottimizzato" mentre, in termini di "Livello Medio di Maturity", la situazione è la seguente:

- **"Gestito" - Il 43,20%** dimostra buone capacità di risposta agli eventi critici, grazie ad un approccio maturo durante le fasi di identificazione e valutazione delle minacce, di individuazione dei team di risposta, di predisposizione delle strategie e dei piani di gestione delle crisi (che vengono testati ed aggiornati regolarmente).
- **"Reattivo" - Il 35,10%** dispone di piani e di protocolli di risposta che vengono attivati solo al verificarsi dell'evento dirompente.
- **"Proattivo" - Il 16.20%** ha processi solidi e tecnologie per l'identificazione anticipata dei rischi. Inoltre, gestisce in modo controllato l'evento critico, potendo contare anche sulla collaborazione degli stakeholder.

Conclusioni e prospettive future

Il quadro scaturito dall'indagine non fa che confermare come i principi di Risk Management, Business Continuity e Cybersecurity possono convertirsi in leve strategiche in grado di gestire e garantire la resilienza operativa e organizzativa in scenari sempre più erratici e digitalizzati.

Ovvero, le organizzazioni - di fronte alla cosiddetta "imprevedibile certezza del rischio" - devono dimostrare di essere più agili, flessibili e adattive, acquisendo il massimo grado di conoscenza e consapevolezza sia di sé (come organizzazione e come persone) sia del contesto interno ed esterno in cui si opera, oltre a garantire l'implementazione di sistemi di gestione efficaci ed efficienti in continuo aggiornamento e miglioramento.

Di fatto, si tratta di concepire l'organizzazione resiliente come un'orchestra i cui "esecutori" conoscono il proprio repertorio e contribuiscono insieme all'esecuzione ottimale della "sinfonia organizzativa". Ne consegue che, in una trasposizione "ardita", Risk Management & Business Continuity, Cybersecurity e Security Manager, unitamente alle altre funzioni di sicurezza, dovranno "suonare all'unisono" e favorire organizzazioni che operano in modo fluido e senza silos.

Federica Maria Rita Livelli

In possesso di certificazione Business Continuity - AMBCI BCI, UK e CBCP DRI, USA, Risk Management FERMA Rimap®, consulente di Business Continuity & Risk Management, svolge attività di diffusione e di sviluppo della cultura della resilienza presso varie istituzioni ed università.

Socia AIPSA (Italian Association of Security Managers) ed UNI (Italian Regulatory Institute); Board member di: ANRA, BCI Italy Chapter, CLUSIT Scientific Committee e Commissioni tecniche UNI.

Docente di moduli ISO 22301 e 31000 presso diverse università (POLIMI–BOCCONI, Verona, Cagliari, Padova, Statale di Milano e LIUC Castellanza).

Relatrice e moderatrice in seminari, conferenze nazionali ed internazionali.

Autrice di articoli su numerose riviste online, Ha partecipato, in qualità di coautrice, a: Edizioni 2020, 2021 e 2022 del Rapporto Clusit - Cyber Security; Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021); Libro "Lo Stato in Crisi" ed. Angeli.

Con Feedo il contante viene gestito in negozio come una carta di credito

intervista a Roberto Licinio, CEO di Gunnebo Cash Management Italy

L'uso del denaro contante è un tema molto divisivo, sia in Italia che nel resto del mondo, per il quale si contrappongono posizioni fra loro distanti, pur essendo tutte comprensibili.
Da una parte, alcuni governi e istituti di credito spingono periodicamente per sostituire le banconote con le forme digitali di pagamento allo scopo di abbattere i costi di gestione del denaro fisico e garantire la tracciabilità delle transazioni per contrastare l'evasione fiscale e il riciclaggio; dall'altra, gran parte dell'opinione pubblica e diverse forze politiche difendono il contante non solo come fattore di libertà e di inclusione sociale ma anche di resilienza individuale e collettiva nelle situazioni di crisi, come è stato dimostrato durante il lockdown per la pandemia ed ora nella guerra in Ucraina.
E' possibile trovare una sintesi tra queste argomentazioni apparentemente inconciliabili?
Una prima risposta ad alcune di esse può darla Feedo, una piattaforma di cash management elettronico che si propone come riferimento per il mondo bancario e il retail per trattare il denaro fisico incassato nei punti vendita dei retailer e della GDO come se fosse una transazione elettronica abbattendo i tempi morti, riducendo i trasferimenti materiali ed aumentando sia la sicurezza fisica nei punti vendita che la protezione dei dati.
Abbiamo chiesto a **Roberto Licinio**, CEO di **Gunnebo Cash Management Italy**, partner del progetto, di spiegare cosa sia Feedo.

Quali sono le principali caratteristiche innovative di Feedo?
Feedo è un servizio di "cash virtualization" offerto in Italia dalla fine dello scorso anno a coloro che svolgono attività che comportano la raccolta di denaro contante da depositare e vorrebbero gestirlo con la stessa dinamicità ed efficienza dei pagamenti digitali (carte di credito, bancomat) tramite una "Fintech", superando le modalità tradizionali di cash handling proposte dalle società di trasporto dei valori. Feedo garantisce al cliente una facile gestione in tempo reale del contante e dei propri conti bancari ma ciò che lo rende un servizio esclusivo è l'operatività all'interno del circuito della rete bancaria, grazie al partner SIA Spa che oggi fa capo a NEXI.
Si tratta, in sintesi, della prima gestione della liquidità di tesoreria arrivata oggi sul mercato, che è stata subito apprezzata dagli operatori del mondo del retail e della GDO e, non a caso, sono già numerosi i clienti che oggi la utilizzano.

In che modo Gunnebo partecipa a questo progetto?
Oltre a SIA, molte altre importanti realtà collaborano con Feedo per apportare competenze specializzate ad un servizio fortemente innovativo, fra le quali rientra anche Gunnebo Cash Management Italy.
La nostra partecipazione si articola sia attraverso la fornitura dei prodotti fisici (casseforti) che la messa a disposizione del nostro software ZEN per assicurare la migliore gestione dei dispositivi. ZEN lavora attraverso SIACloud.com all'interno del circuito bancario e questo permette di raggiungere il massimo livello di sicurezza utilizzato dagli istituti di credito per la protezione dei dati dei clienti.

GUNNEBO®
Cash Management

Contatti:
Gunnebo Cash Management Italia S.r.l.
Tel. +39 02.26710431
www.gunnebocashmanagement.com/it-IT

Feedo, la garanzia della rete interbancaria nazionale per la sicurezza del contante in negozio

intervista a Sergio Pellerey, direttore generale Feedo System srl

Ci può riassumere i vantaggi per un retailer apportati dall'utilizzo del servizio Feedo?
Il retailer, attraverso l'utilizzo del servizio di cash management Feedo, riacquista la propria centralità rispetto ad altri servizi similari sul mercato, erogati principalmente da società portavalori. Feedo azzera ogni rischio per l'esercente/retailer nella gestione del denaro contante, trasformando le banconote fisiche in "contante digitale" nel punto vendita e lasciandogli solo i vantaggi della liquidità.
Si può dire che la banca entri nel punto vendita del retailer, il quale perde la titolarità di quel contante subito dopo l'inserimento nella *FeedoSafe* (così si chiama la cassaforte intelligente integrata con tecnologia Feedo, ossia la *FeedoChain*) e, contemporaneamente, acquisisce la titolarità dell'esatto controvalore finanziario sul proprio conto corrente tecnico.
Il versamento del retailer viene fatto pro soluto e non pro solvendo o con la previsione del salvo buon fine. Quindi, qualsiasi cosa accadesse al denaro contante depositato nella *FeedoSafe* (ad esempio, rapina, estorsione, furto, incendio, ecc.), ne risponderebbe soltanto la banca tecnica titolare di quel contante.
Analogamente, qualora si verificassero delle squadrature in sala conta, per banconote mancanti oppure sospette di falsità, nessuna responsabilità verrebbe addebitata al retailer.
Il retailer può inoltre gestire in totale autonomia il contante incassato nel proprio punto vendita, trasferendo le somme introitate nella *FeedoSafe* anche su più IBAN (multi IBAN) di proprio riferimento purché in area SEPA, anche se fisicamente ancora nel punto vendita.
Feedo assicura l'ottimizzazione nella gestione delle operazioni contabili (governo della liquidità, abbattimento dei tempi di riconciliazione, deterrenza e contrasto infedeltà) e consente di coordinare al meglio le varie figure coinvolte: soggetto versante, responsabile del punto vendita, amministrazione centrale, CFO, ecc.
In ultimo, ma sicuramente non per importanza, Feedo opera attenendosi a processi e linee guida di Banca d'Italia.

Quali sono i partner attuali di Feedo?
Attualmente sono ormai diversi i nostri principali partner:
- **SIA** (oggi NEXI): è uno dei *founder* di Feedo. SIA e Feedo hanno condiviso obiettivi sia a breve che a lungo termine, in particolare l'evoluzione in ottica industriale delle due componenti del servizio di cash management: la cash *virtualization* (trasformazione del denaro contante in flusso informativo - ciclo virtuale) e il *cash handling* (trasporto

del denaro contante dal punto vendita alla sala conta e deposito in caveau – ciclo fisico).

- GUNNEBO Cash Management (oggi GardaWorld): partner che ha investito per primo in Feedo per essere leader nel settore del cash management. Gunnebo prevede la produzione di casseforti *FeedoSafe* native, ossia già integrate della tecnologia Feedo.

- TOSHIBA GLOBAL COMMERCE SOLUTIONS: partner strategico sia nell'operatività del servizio Feedo (é gestore dello SPOC e responsabile dell'attivazione del servizio presso il punto vendita) sia nella promozione del medesimo sul mercato nazionale e internazionale.

- GRUPPO BANCA PROMOS: partner bancario che ha compreso da subito l'innovazione che Feedo apporta sul mercato nonché i risvolti istituzionali ed etici.

- CIVIS spa: partner operativo del mondo CIT che ha contribuito allo sviluppo del progetto Feedo apportando le proprie competenze ed esperienze nel cash handling.

Vorrei inoltre sottolineare come il servizio Feedo intenda essere una piattaforma inclusiva di tutti quei soggetti che oggi già operano sul mercato e sono elementi fondamentali nella filiera della gestione del denaro contante, ive incluse le banche. A tal proposito, la nostra società ha in corso diverse interlocuzioni con importanti players, nazionali ed internazionali facenti parti dei settori della sicurezza, bancario e finanziario.

Ci può descrivere in che modo Feedo assicura ai propri clienti maggiore sicurezza e continuità operativa rispetto ad altre soluzioni di cash-management per il mondo del retail?

Per rispondere a questa domanda è necessario un approfondimento, anche tecnico, per spiegare in che modo vengono tutelati i retailer che utilizzano il servizio Feedo, affinchè gli operatori del settore siano informati dei vantaggi esclusivi che offre la sua infrastruttura tecnologica in termini di tutela dei dati sensibili, cybersecurity e business continuity.

Prima di tutto, la piattaforma CMCA *(Cash Management Control Application)* è un'applicazione creata appositamente da SIA spa, che oggi fa capo a NEXI, come componente centrale del sistema Feedo per la gestione del contante in negozio.

CMCA è una soluzione sviluppata applicando le competenze acquisite in ambito bancario e beneficia delle strutture di erogazione di SIA appoggiandosi alla rete nazionale interbancaria (RNI).

Vorrei sottolineare questo aspetto, in quanto RNI garantisce da più di 40 anni l'interoperabilità tra gli istituti di credito europei (vedi *"Banca in Negozio"*) ed è un'infrastruttura scalabile per l'accesso ai nuovi servizi di pagamento.

Sviluppata dunque secondo gli standard di eccellenza tecnologica e robustezza proprie delle infrastrutture interbancarie, la piattaforma CMCA di Feedo è in grado di offrire ad entrambi i soggetti (banche ed esercenti/retailer) la gestione automatizzata dell'intero ciclo del contante con un presidio h24 per 365 gg/anno.

Il cuore tecnologico del servizio Feedo sono i componenti centrali composti da elementi fisici (rete SIAnet.NG / rete Cloudnet) ed elementi procedurali (sistema centrale "a.k.a" - piattaforma ECIS/CMCA), entrambi disegnati, sviluppati ed erogati dallo stesso soggetto che fornisce servizi mission critical per il sistema interbancario e finanziario domestico e internazionale, ovvero SIA spa.

L' impostazione architetturale e strutturale dei componenti centrali di Feedo garantisce:

- *alta disponibilità: i dati sono gestiti utilizzando una struttura "active-active" geograficamente distribuita*
- *ridondanza: tutte le componenti dell'intero sistema sono replicate in due siti distinti, perfettamente equivalenti in termini di prestazioni e resilienza*
- *business continuity/disaster recovery: i test (scenari) di failover sono effettuati periodicamente e documentati secondo rigorosi piani di business continuity e disaster recovery*

Come detto, l'interconnessione tra le componenti strutturali, applicative e centrali di Feedo avviene attraverso la rete privata SIAnet.NG di SIA, i cui circuiti sono realizzati con connessioni sicure e cifrate basate su VPN, con collegamenti fisici differenziati per istradamento e azienda fornitrice (carrier).

La rete SIAnet.NG garantisce:

- *link logici indipendenti dalla topologia fisica di rete*
- *interfacce omogenee e flessibili*
- *elevata disponibilità supportata da un'architettura di rete progettata sui due livelli logico e fisico, in modo da garantire resilienza e continuità*
- *re-indirizzamento automatico del traffico in caso di guasto alle portanti fisiche.*

La gestione sistemica dei processi operativi Feedo si basa sull'integrazione di piattaforme in grado di assolvere al meglio specifici compiti operativi.

Come già detto, le piattaforme interagiscono tra loro utilizzando, come struttura di comunicazione e controllo, la RNI gestita da SIA S.p.A.

Lo scambio delle informazioni tra le varie piattaforme è, al pari dell'infrastruttura dedicata, continuamente monitorato da sistemi che operano in parallelo rispetto al flusso informativo. La ridondanza e la separazione del flusso informativo (data management) rispetto quello di controllo (device e process management) garantisce verifiche puntuali e rigorose, mettendo in evidenza i degradi funzionali dell'intero sistema.

La rete SIAnet.NG, per mezzo della RNI, collega tra loro:

- *Centri elaborazione dati di Banca d'Italia*
- *Istituti bancari*
- *Ente Poste*
- *Consorzi*
- *Centri applicativi*
- *Società d'intermediazione mobiliare (SIM),*
- *Servizi di post-trading*
- *Operatori dei mercati internazionali.*

Il vantaggio della soluzione SIAnet.NG / RNI è l'indipendenza dal tipo di hardware e di software adottato, salvaguardando così gli investimenti e l'indipendenza tecnologica, oltre a fornire l'accesso ai principali servizi ausiliari interbancari, quali:

- *Centrale rischi di Banca d'Italia*
- *Sistema informatizzato prevenzione amministrativa frodi carte di pagamento.*

La rete SIA Cloudnet permette ai servizi di terze parti ospitati in Amazon VPC *(virtual private cloud)* o Microsoft AZURE di accedere all'ecosistema SIA tramite l'infrastruttura di rete privata SIAnet.NG e garantisce inoltre un collegamento veloce, stabile, affidabile e sicuro quando si rende necessario trasferire e ricevere dati/transazioni da e verso:

- *Banche*
- *Fintech*
- *GDO*
- *Utility*
- *Telco*
- *Compagnie petrolifere*
- *Assicurazioni*
- *Media*
- *Trasporti*

Il risultato è un'esperienza di rete all'insegna dell'efficienza rispetto alle connessioni basate su Internet.

SIA collega i "punti di presenza" (*PoP*) di rete dei Cloud Providers rispettando le opzioni di connettività e le raccomandazioni sulla resilienza previste dalle piattaforme Cloud AWS e Azure.

Il traffico in ingresso e in uscita - gestito dall'Infrastruttura SIA Cloudnet - è crittografato in conformità agli standard dei circuiti di pagamento.

Inoltre, i criteri di routing dinamico permettono al cliente la continuità di accesso ai servizi centrali di SIA anche in caso di eventi negativi.

Pandemia e guerra in Ucraina, il ruolo determinante del contante nell'Eurozona

intervista a Antonio Staino, presidente Assovalori e Paolo Spollon, vice presidente Assovalori

Paolo Spollon

Antonio Staino

Partiamo dalla situazione della circolazione del contante in Itala e nell'Eurozona. Qual è il trend, in base ai dati ufficiali distinguendo la quantità del circolante dalle transazioni?

Negli ultimi tempi si parla spesso di denaro contante e del fatto che, secondo alcuni osservatori, esso sia "destinato a scomparire" in favore della moneta elettronica, in un futuro più o meno prossimo. Ma è davvero così?

Partiamo da un fatto: la Banca Centrale Europea, tra i suoi compiti fondamentali, ha assunto l'impegno di assicurare la disponibilità del contante, renderlo accessibile a tutti i cittadini e facilitarne l'uso per i pagamenti, con l'obiettivo di garantirne l'autonomia, la privacy e l'inclusione sociale.

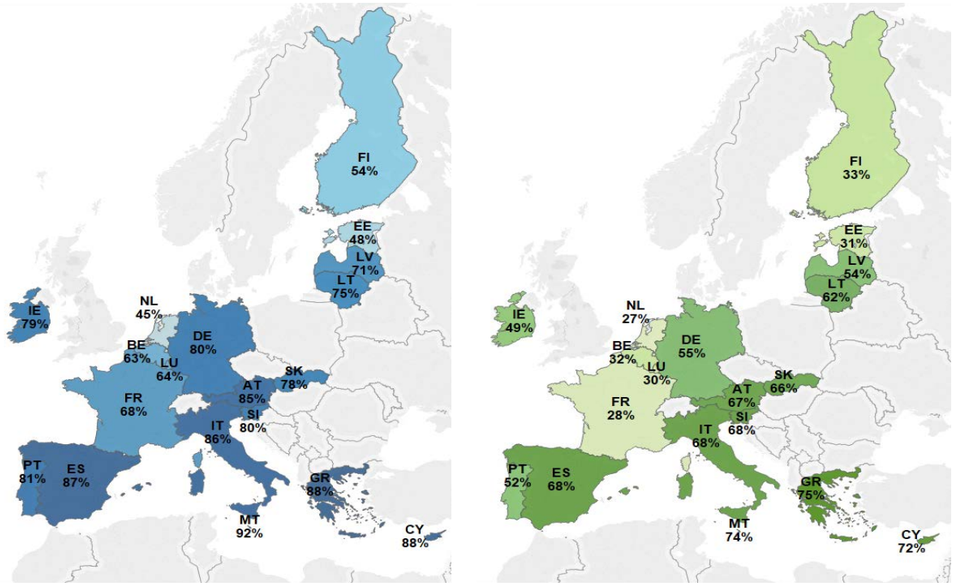
Uno studio condotto dall'Eurosistema nel 2019 sull'atteggiamento dei consumatori dell'area euro nei confronti dei pagamenti (SPACE: *Study on the payment attitudes of consumers in the euro area*), segnala che il contante rimane il mezzo di pagamento più utilizzato nelle transazioni tra persone e all'interno dei negozi fisici, sia per numero (73%), sia in valore. Monete e banconote sono regolarmente utilizzate da cittadini europei di tutte le età, tutti i livelli di istruzione e tutte le fasce di reddito, prevalentemente per acquisti di valore medio-basso (al di sotto di 40€). Quando si tratta di importi elevati – che rappresentano il 24% circa del totale delle transazioni – i cittadini europei scelgono altri strumenti di pagamento, in particolare carte di debito e credito e bonifici bancari.

Entrando nel dettaglio, scopriamo che Malta è il paese europeo dove si utilizza maggiormente il contante, con l'88% delle transazioni regolato in monete e banconote, seguita da Spagna e Cipro (83%).

L'Italia si attesta su una percentuale dell'82%, ben al di sopra della media europea.

All'estremo opposto troviamo la Finlandia e i Paesi Bassi, rispettivamente al 35% e 34% di transazioni regolate in contanti.

Lo stesso studio dimostra come i pagamenti digitali siano in crescita a velocità variabile nei diversi Paesi, di pari passo con la digitalizzazione dell'economia e con lo sviluppo dell'e-commerce come nuova modalità di acquisto.



Distribuzione per Paese delle transazioni in contanti per punto vendita– quantità a sinistra, valore a destra
Fonte: ECB, Deutsche Bundesbank and De Nederlandsche Bank).

Questa tendenza ha subito un'accelerazione nel 2020 e nel 2021 a causa della pandemia da coronavirus (COVID-19), favorita dalla chiusura dei negozi al dettaglio e delle attività di ristorazione fuori casa ma anche dal timore, poi dimostrato infondato, che il denaro contante potesse essere veicolo d'infezione.

Negli ultimi anni, sono state avviate in diversi paesi numerose politiche di limitazione all'utilizzo del contante e di incentivo all'uso della moneta elettronica. Misure che, giustificate con la lotta all'evasione fiscale, tuttavia sollevano molti dubbi sia in termini di efficacia, sia in termini di rispetto della libertà di scelta, di privacy e di inclusione dei cittadini.

D'altronde, la competenza sui mezzi di pagamento è prerogativa della BCE che ha la responsabilità di garantire a tutti i cittadini l'accesso al contante per i pagamenti.

E, infatti, il Governo italiano è stato richiamato formalmente dalla BCE, che ha definito il "cashback una misura sproporzionata rispetto agli obiettivi".

Vediamo ora come sia evoluta l'espansione delle carte di credito/debito negli ultimi sette anni:

- il numero delle carte di credito è passato da 12,275 a 15,342 milioni (+ 24,2%) e quelle di debito da 48,046 a 59,418 milioni (+23,6%)
- Il numero delle operazioni con carte di credito è passato da 643,958 a 1.156,427 milioni (+ 79,6%)
- in miliardi di euro, il valore delle operazioni con carte di credito è passato da 53,415 a 75,402 (+ 41,2%).

(Fonte: Banca d'Italia)

Analizzando questi dati ci si aspetterebbe una forte diminuzione del contante in circolazione e del suo utilizzo ma, se passiamo a confrontare il valore delle banconote messe in circolazione da Banca d'Italia (esitate) e quello delle banconote rientrate in Banca d'Italia (introitate) rileviamo che:

- nell'anno 2020 Banca d'Italia ha distribuito 84,2 miliardi di euro e ne sono rientrati 62,1 (- 22,1)
- nel primo semestre 2021 sono stati distribuiti 35,9 miliardi di euro e ne sono rientrati 27,4 (- 8,5)

Questa differenza tra esitate e introitate fa comprendere come per i cittadini italiani il contante rappresenti ancor oggi uno dei più importanti strumenti di riserva di valore, trattenuto in vari modi dalle singole persone e che, malgrado si stiano progressivamente diffondendo i pagamenti elettronici e contactless, in particolare nel periodo pandemico, l'uso del contante sia stato e sia attualmente ancora il mezzo di pagamento preferito dai cittadini italiani.

Venendo alla situazione generata dalla crisi ucraina, si nota come la domanda di contanti sia aumentata in modo significativo, in particolare nei paesi del Nord Europa come la Norvegia, dove è cresciuta del 20% e in Svezia attorno al 30% (fonte Statement ESTA), questo a confermare, se ancora ce ne fosse bisogno, che l'accesso al contante diventa determinante in situazioni critiche.

Se il circolante aumenta ma le transazioni in contanti diminuiscono, vuole dire che la gente mette le banconote sotto il letto?
Abbiamo già detto che Il contante rappresenta una riserva di valore perché, oltre ad essere uno strumento di pagamento, rappresenta una forma di risparmio. Non a caso, nei periodi di crisi la domanda di denaro contante aumenta.
La BCE ha confermato che nel 2020 l'ammontare delle banconote emesse dall'Euro sistema ha superato del 4% il valore medio registrato nel precedente quinquennio, via via crescendo fino a raggiungere un aumento dell'8% tra la fine del 2020 e l'inizio del 2021. Questo non può che confermare come il contante sia senza dubbio un efficace mezzo per far fronte all'incertezza generata dalla crisi. Così possiamo probabilmente spiegare l'apparente paradosso rappresentato dall'incremento della domanda di banconote e dalla concomitante flessione dei pagamenti in contante: i consumatori, specialmente quelli con basso reddito, hanno ridotto gli acquisti di beni e servizi e aumentato la propria scorta di liquidità.

Cosa sta insegnando la crisi ucraina di queste settimane? Quali sono le reazioni delle persone in Italia?
La crisi ucraina non fa che confermare che il contante è un mezzo per contrastare le incertezze sia di natura economica che psicologica, così è stato percepito dai paesi baltici e/o confinanti con la Russia. Al momento non si notano reazioni particolari legate alla crisi ucraina da parte dei cittadini italiani, ancora alle prese con il perseverare dei negativi effetti economici prodotti dal proseguimento della pandemia.

Cosa proponete alle Autorità per trovare una sintesi equilibrata tra l'irreversibile digitalizzazione dei pagamenti e l'irrinunciabile ruolo del contante come "disaster recovery"?
I dati suggeriscono che nessun mezzo di pagamento può soddisfare in toto le esigenze dei consumatori; ciascuno utilizza un mix di strumenti di pagamento in funzione del proprio paniere di acquisti e della propria condizione socio-economica. Resta quindi fondamentale offrire alle persone la possibilità di scegliere come pagare, garantendo in tutti i casi velocità, sicurezza, costi contenuti e semplicità di accesso e di utilizzo.
Il denaro contante e il denaro digitale sono complementari: la loro coesistenza offre ai consumatori una maggiore possibilità e libertà di scelta e, non da ultimo, una corretta inclusione sociale a favore di tutti quei soggetti che non vogliono o non possono aver accesso alle istituzioni finanziarie, così come stabilito dalla strategia Cash 2030 dell'Eurosistema.
"*L'evidenza empirica indica che la carenza di contante danneggerebbe sia i commercianti che i consumatori, specialmente quelli a basso reddito. Difficoltà emergerebbero in particolare per i segmenti della popolazione, quali gli anziani o le persone con un livello minore di istruzione o gli unbanked, che preferiscono o sono costretti ad utilizzare il contante. Secondo analisi recenti, una scarsità di banconote genererebbe per la collettività costi di gran lunga superiori ai benefici che deriverebbero dal contenimento delle attività illecite connesse all'utilizzo del contante." (Fonte BCE)*

Ma perché è importante garantire l'accesso al contante e quali sono le sue funzioni?
• **Il contante assicura libertà e autonomia:** detenere denaro contante non richiede l'intervento di intermediari come accade, al contrario, per i mezzi di pagamento digitali. Per pagare in contanti non è necessario alcun supporto fisico: carta, tessera o smartphone che sia.
• **Monete e banconote hanno corso legale:** i punti vendita e gli esercizi commerciali non possono rifiutare i pagamenti in denaro contante a meno che non sia stata concordata con il cliente, in precedenza, una forma di pagamento alternativa.
• **Garantisce la privacy:** le transazioni in contanti rispettano il diritto fondamentale alla protezione della privacy, dell'identità e dei dati personali.

• **È inclusivo:** il contante rende accessibile l'acquisto e il risparmio a tutti, anche alle persone che, per ragioni diverse, non dispongono di un conto corrente bancario e non hanno accesso agli strumenti digitali. In questo modo garantisce l'inclusione nell'economia reale anche delle fasce di popolazione più vulnerabili, come gli anziani o le categorie a basso reddito.
• **Pagare in denaro contante aiuta a tenere traccia delle proprie spese:** monete e banconote sono tangibili e, per questo, consentono di tenere sotto controllo la propria spesa, evitando di eccedere rispetto alle reali disponibilità.
• **È veloce:** le banconote e le monete regolano i pagamenti in tempo reale.
• **È sicuro:** il contante si è dimostrato sicuro in termini di cybercriminalità, frode e falsificazione. Inoltre, è l'unico strumento di pagamento emesso dalla Banca Centrale Europea e non comporta rischi finanziari né per il pagatore né per il beneficiario.
• **È una riserva di valore:** oltre ad essere uno strumento di pagamento, il contante rappresenta una forma di risparmio. Non a caso, nei periodi di crisi economica la domanda di denaro contante aumenta.

Quale è stato il ruolo delle società di Cash in Transit durante la pandemia?
Gli operatori di Cash in Transit hanno svolto un ruolo essenziale fin dall'inizio della crisi in quanto vi era un imperativo chiave, quello di garantire a tutti l'accesso al contante anche quando si è trattato di affrontare un drammatico aumento della domanda. Da sottolineare che, oltre a combattere con gli effetti della pandemia, si sono dovuti confrontare con un fenomeno che possiamo definire "desertificazione bancaria" , come confermato dalle più recenti pubblicazioni statistiche di Banca d'Italia (settembre 2021):
- Il numero dei soggetti bancari si è ridotto dal 2014 al 2021 da 663 a 474 (-189)
- Il numero degli sportelli bancari nello stesso periodo è passato da 30.723 a 23.480 (- 7.243)
A questo va aggiunta la conseguente riduzione degli ATM, solo in parte mitigata dall'espansione degli Independent ATM Deployer (IAD), società che hanno implementato l'istallazione di ATM indipendenti.
Tutto questo ha prodotto per i cittadini una forte riduzione della possibilità di accesso ai servizi bancari, tra i quali appunto il deposito ed il prelievo di contante.
Le società di Cash in Transit si sono prodigate per contrastare queste limitazioni, per migliorare il ciclo del contante, consentendo che continuasse a circolare senza interruzioni di approvvigionamento anche nelle zone rurali o più difficilmente raggiungibili, nel pieno rispetto delle norme di sistema, immettendo in circolo banconote in ottimo stato di conservazione e con validità legale (non contraffatte), il tutto per mantenere alto il livello di fiducia dei cittadini nei confronti della carta moneta.
Non si è trascurato poi l'aspetto della sicurezza, per i propri dipendenti e per la popolazione, implementando, con ingenti investimenti, l'utilizzo di sistemi di sicurezza passiva ed attiva, elevando il livello di sicurezza dei mezzi blindati e dei caveaux di deposito delle banconote e delle monete.
Concludendo, e prendendo spunto dalle parole di molti titolati esponenti economici e rappresentanti dell'Eurosistema, per le sue molteplici funzioni il contante svolge un ruolo fondamentale all'interno del sistema economico e finanziario, il che porta a prevedere che sopravviverà alla rivoluzione digitale, continuando ad essere utilizzato per molti anni a venire. Perché questo suo ruolo non venga messo a rischio in futuro in un'economia in rapida trasformazione, l'Eurosistema dovrà garantire da una parte un'adeguata offerta di banconote, consentendo a tutti i cittadini di avere pieno accesso al contante in base alle proprie esigenze; dall'altra, che le banconote e le monete in euro come moneta legale continuino ad essere accettate nei punti vendita e utilizzabili ovunque nell'area dell'euro, senza costi e nel rispetto della privacy.

ASSOVALORI

Nova Service e LBM Italia, un connubio che cresce e rilancia nel segmento del cash-management

intervista a Giuseppe Quartuccio, amministratore unico di Nova Service e LBM Italia

Nova Service si sta affermando nel mercato italiano come protagonista dei sistemi di trattamento delle banconote e delle monete, grazie all'altissimo livello qualitativo dei prodotti distribuiti quali Laurel, NGZ, Scan Coin, ed alla grande attenzione che riservate in ogni fase ai clienti. La vostra determinazione di crescita è sottolineata dal recente investimento nella nuova sede in via Palermo ad Assago. Ci può descrivere questa operazione nel quadro delle vostre strategie di sviluppo?
Come noto, l'acquisizione di LBM Italia da parte di Nova Service è stata molto sofferta, essendo conseguente anche alla prematura scomparsa del compianto Giuseppe Ferrara.
Abbiamo scelto di intraprendere questa strada sulla spinta del fermento nel mercato del C.I.T. ma siamo stati cauti nelle decisioni iniziali, evitando cambiamenti e cercando piuttosto di farci conoscere dai clienti e dimostrare la nostra professionalità.
Non sapevamo come gli operatori avrebbero reagito alla nostra entrata in LBM, anche in considerazione del fatto che la pandemia aveva ridotto al minimo quella che per noi è la cosa più importante, ovvero il rapporto diretto con i clienti. Fortunatamente, la risposta dell'intero mercato nei confronti del connubio Nova Service – LBM Italia è stata di alto gradimento, tanto che in un anno c'è stata una crescita esponenziale.
Proprio dal riscontro inaspettato che abbiamo ricevuto è scaturita la necessità, a fine 2021, di avere un ambiente di lavoro più adeguato alle nuove esigenze. Abbiamo dunque deciso all'inizio del nuovo anno il cambio di sede, attribuendo a questo passo un segnale di stabilità e solidità, anche perché l'immobile di via Palermo 27 ad Assago è di nostra proprietà.
La scelta dello stabile risponde alle diverse esigenze che si prospettano per il futuro, ovvero di avere da una parte uffici funzionali ma adatti ad accogliere conferenze ed incontri con i clienti; dall'altra, di disporre di spazi di logistica più ampi. Questo perché nel 2021 abbiamo registrato non solo un aumento importante delle vendite ma anche del noleggio, una modalità che richiede non solo lo stoccaggio delle macchine ma anche e, forse, soprattutto la disponibilità di ricambi e materiali di consumo, per essere il più professionali e competitivi possibile.
Altra necessità che si è creata è stata quella di portare in LBM il mondo del printing, prima estraneo all'azienda milanese, che comporta anch'esso la necessità di spazi per lo stoccaggio di macchine e ricambi per le installazioni e l'assistenza tecnica diretta.

In che modo assicurate ai vostri clienti sul territorio nazionale il servizio di assistenza capillare e puntuale che rappresenta uno dei punti di forza della vostra offerta?
Il post vendita è per noi un punto fondamentale nella relazione fornitore-cliente e l'assistenza è un nodo cruciale. Per questo abbiamo un team selezionato di tecnici, attraverso i quali gestiamo le richieste di intervento con chiusura entro 24 ore dalla richiesta nel 95,4% dei casi. Le nostre attività di assistenza coprono direttamente tutta la penisola.
Noi assicuriamo un servizio di assistenza capillare e puntuale sul territorio grazie alla struttura che in questi anni è stata sviluppata con le nostre tre sedi: la sede storica di Aprilia, dalla quale tutto è nato ed è l'attuale cuore pulsante dove viene gestita la logistica e l'assistenza

intervenendo direttamente nel centro ed in Sardegna; la sede di Messina, aperta nel 2019, dalla quale si opera nel sud, Sicilia compresa; infine, la più recente acquisizione di LBM Italia ci permette oggi di operare direttamente anche nel nord.
Tutto questo ci mette in condizione di avere una gestione diretta su tutto il territorio italiano non solo per l'assistenza tecnica ma anche per lo smistamento, in quanto ogni sede ha il proprio magazzino di ricambi e consumabili.
Ciò garantisce gli stessi tempi di intervento e consegna in ogni angolo del territorio italiano. Nella sede di Aprilia è istituito un help desk che monitora dalle ore 8 alle ore 18, dal lunedì al sabato, le richieste di assistenza, materiali di consumo, certificazioni, ecc, con immediata assegnazione alla sede e/o al tecnico di riferimento.
Altro punto cruciale è, per noi, la qualità della preparazione dello staff tecnico, condizione necessaria per mantenere alto il grado di affidabilità. Da sempre investiamo molto per far sì che i nostri tecnici abbiano accesso a corsi di formazione e di aggiornamento, siano essi organizzati presso le nostre sedi con l'intervento di preparatori delle case madri, o direttamente svolti presso le aziende, quali Laurel in Giappone, NGZ in Germania, Scan Coin in Olanda, ecc.

La vostra gamma di prodotti è stata arricchita di recente con la nuovissima linea Laurel KS, che garantisce prestazioni eccezionali. Ci può descrivere le sue caratteristiche?
Il successo di Laurel risiede, da sempre, nella dedizione verso ogni singola componente. La nuovissima linea Laurel KS è il risultato dell'evoluzione che, nel tempo, ha subito la sua antenata, la serie K.
Se già la serie K offriva prestazioni all'avanguardia, la nuova KS presenta livelli ancora più elevati: modularità dei cassetti non più fino a 12 ma bensì fino a 24 (in gruppi da quattro); struttura più verticale che incrementa la produttività; nuovo validatore ad alta tecnologia JDU-70; contazione fino a 1200 banconote/minuto. Tutto questo, assieme ad un sistema user-friendly, garantiscono prestazioni mai viste prima.
Noi vediamo nella nuova linea KS la nostra punta di diamante del settore delle selezionatrici di banconote.
Potremmo concludere affermando che la KS arriva sul connubio Nova Service – LBM Italia come la "ciliegina sulla torta" a sancire la ventata di novità e di professionalità che ha caratterizzato da subito il sodalizio tra le attività delle due società.
Siamo certi di non deludere le aspettative del mercato e di tutti i clienti che fino ad oggi ci hanno onorato della loro fiducia e fedeltà. Faremo di tutto per non deludere queste aspettative.

Contatti:
Nova Service srl
Tel. +39 06 9252446
commerciale@novaservicesrl.com
www.novaservicesrl.com

Contatti:
LBM Italia spa
Tel. +39 02 48842953
commerciale@lbm-italia.com
www.lbm-italia.com

Madama Group, un modello innovativo di sicurezza di élite

intervista a Luca Apostolico, presidente di Madama s.r.l.

Ci può parlare di Madama Group e della sua storia?
Madama Srl nasce dalla volontà di due imprenditori, Luca Apostolico e Davide Salvi, entrambi con oltre venti anni di esperienza nel settore della sicurezza pubblica e privata, di colmare una forte esigenza nel mercato privato e aziendale della sicurezza offrendo soluzioni con approccio olistico ed innovativo. Grazie all'esperienza maturata in ambito governativo e privato, oltre alla gestione sul campo delle attività operative, Madama è in grado di individuare il progetto adeguato all'esigenza del cliente.
L'obiettivo di arrivare alla corretta risoluzione di un problema con soluzioni adeguate è stato la leva per approfondire tutti i campi di attività, curando i progetti in ogni aspetto.
Il presidente Luca Apostolico, in qualità di Senior Security Manager certificato UNI 10459:2017, supervisiona in prima persona le attività di prevenzione dei rischi per i propri clienti attraverso modelli di Risk Analysis, Risk Assessment e Risk Management e nella gestione delle criticità attraverso schemi di Crisis Management, Disaster Recovery e Business Continuity.
Davide Salvi, nel ruolo di Operation Manager, si occupa della ricerca, selezione e formazione del personale addetto alle attività di security e coordina le attività operative.

Qual è la vision alla base del vostro progetto?
Crediamo che sia fondamentale essere oggettivi nello strutturare un progetto di sicurezza, mantenendo l'indipendenza dalla scelta della soluzione sia nella scelta dei prodotti che delle aziende produttrici.
Abbiamo fatto una scelta ben precisa, quella di non utilizzare soluzioni tecnologiche specifiche ma di utilizzare i prodotti più attinenti alla soluzione e, quindi, liberi da impegni di magazzino o di formazione per il personale.

Luca Apostolico e Davide Salvi

Allo stesso modo, anche l'utilizzo degli operatori avviene in funzione alla necessità oggettiva e non dal fatto che, avendo personale in carico, sia necessario fatturare ore/uomo.
In sostanza, possiamo disporre di un magazzino immaginario con qualunque soluzione e marca che il mercato offra in tutto il mondo.
Madama Group istituisce e dirige un tavolo tecnico con un pool di specialisti con esperienze verticali che, di volta in volta, vengono chiamati per svolgere il risk assessment. Operando in outsourcing a "chilometro zero", riusciamo a mantenere alta la competitività e l'efficienza nonché l'efficacia della soluzione proposta.

Quali sono le vostre attività principali?
Madama Group è organizzato in 5 dipartimenti:
1) Dipartimento Tecnologico: adibito alla progettazione, vendita, installazione e manutenzione di impianti di antintrusione, video sorveglianza, controllo accessi, impianti di rivelazione incendi, impianti di rete e soluzioni hardware e software in ambito cyber security. Realizzazione di casseforti invisibili, caveau invisibili, autorimesse sicure, panic room, serenity room e sistemi per l'anti coercizione.
2) Dipartimento Fiduciario: adibito alla fornitura di servizi per famiglie e aziende con l'utilizzo di personale non armato per attività di portierato, controllo accessi, concierge, accompagnamento Vip, ecc.
3) Dipartimento di Vigilanza e Travel Security: adibito alla consulenza in ambito di security management e alla fornitura di servizi con utilizzo di GPG in ambito Italiano e di contractor in ambito internazionale.
Il dipartimento gestisce una Centrale di controllo operativo supervisionando le attività in ambito internazionale.
4) Dipartimento di Intelligence: impegnato nella prevenzione delle infedeltà lavorative e delle infiltrazioni mafiose. Progettazione e gestione di servizi investigativi, due diligence, digital forensics.
5) Dipartimento Eventi: opera ingaggiato in qualità di security manager e delegato all'art. 8 del TULPS occupandosi di svolgere risk assessment e gestione dei piani organizzativi e operativi. Fornisce e gestisce la control room da campo capace di gestire impianti di allarme, videosorveglianza, sistemi GPS e radiocollegamenti da campo coordinando le risorse ingaggiate garantendo aggiornamenti real time agli organi governativi preposti alla gestione dell'ordine pubblico.

A quali categorie di utenti si rivolge principalmente Madama Group?
Ci rivolgiamo principalmente a multinazionali e famiglie facoltose che hanno necessità di essere accompagnati in scelte oculate sia in tempi ordinari che in quelli straordinari come durante la gestione di crisi. Siamo in grado di offrire tutti i nostri servizi in campo internazionale e con tempi di risposta competitivi rispetto alla media di mercato.

Radiolocalizzazione satellitare ovvero l'evoluzione della sicurezza

intervista a Romano Lovison, presidente ANSSAT

Ci può riassumere il quadro nazionale del comparto della localizzazione satellitare, in termini di dimensioni, numero e caratteristiche degli operatori?
Diciamo subito che la radiolocalizzazione satellitare, così come conosciuta oggi, trova le proprie origini proprio in Italia. I primi prodotti che hanno utilizzato sistemi di comunicazione cellulare (al tempo TACS) sono stati sviluppati nei primissimi anni '90 e già verso la fine del 1992 sono iniziati i primi test di funzionamento. Nel tempo, questi sistemi si sono evoluti, soprattutto nella parte di connettività e, di conseguenza, nelle nuove applicazioni e soluzioni.
All'inizio, i sistemi garantivano esclusivamente delle applicazioni di sicurezza per poi allargarsi alle applicazioni di logistica ed arrivare, quindi, alle applicazioni assicurative per la ricostruzione degli incidenti, gli stili di guida ed i parametri di utilizzo dei mezzi. Molto importanti le applicazioni di fleet management con soluzioni per la gestione predittiva delle manutenzioni, ecc.
I vari settori hanno numeri importanti, soprattutto se si pensa che il parco circolante, a fine 2021, era di circa 45 milioni di veicoli, dei quali si stima che circa il 30% abbia un sistema di radiolocalizzazione.
Ma il mercato sarà sempre più ampio in futuro e con operatori sempre più specializzati su specifici settori. Basti pensare che la localizzazione si è ampliata al mondo delle e-bike e su altri oggetti e beni che un tempo non erano proprio considerati dagli operatori.

Quali sono i servizi più richiesti dall'utenza commerciale e da quella privata?
I servizi si possono suddividere in "professional" e "consumer". Com'è naturale, i clienti aziendali sono tipicamente orientati verso i servizi professional.

Il mondo dell'autotrasporto, ad esempio, ha bisogno di soluzioni molto complesse come il servizio antirapina, da cui derivano tutte le applicazioni. Un servizio che ha consentito di ridurre un fenomeno che nel 1991, con circa 68.000 veicoli pesanti circolanti, contava oltre 1400 rapine, sino alle poche decine degli ultimi anni, con un parco circolante di circa 180.000 veicoli pesanti.
Nel tempo, i clienti hanno successivamente utilizzato il servizio per l'attività di logistica per ottimizzare il controllo gestionale della propria flotta, per rilevare e visualizzare da remoto i vari dati di telemetria del mezzo (giri motore, consumi, ecc.) oltre che per attività di scarico dati da cronotachigrafo.
Accanto a queste soluzioni, legate al mondo del trasporto, vi sono state poi le applicazioni di fleet management di importanti realtà con un consistente parco auto.
Sull'altro fronte, i privati utilizzato inizialmente questi sistemi soprattutto per la tutela della propria auto contro il furto, ma questo mercato si è poi ridotto considerevolmente a favore delle soluzioni offerte dalle compagnie di assicurazione per poter abbattere i costi assicurativi.

Infine un'ultima osservazione: sempre più case automobilistiche stanno fornendo in OEM la possibilità per il cliente di localizzare la propria auto e visualizzare altri parametri (stato del veicolo, livello carburante, ecc.). Di conseguenza, l'after-market in questo ambito sta scemando, proprio come è successo molti anni fa con le autoradio.

Quali sono le norme di riferimento sul piano legislativo e su quello tecnico?
Sul versante dei dispositivi, tutti i sistemi devono avere delle omologazioni, tra le quali due sono obbligatorie: la compati-bilità elettromagnetica CE e l'omologazione "Automotive Exx" (una E grande con un numero che individua lo stato dove è stata eseguita l'omologazione) che attesta che il sistema è idoneo ad essere installato e collegato al veicolo.
Se il sistema deve svolgere una funzione antifurto, dovrà essere omologato in conformità alla norma CEI 79/17 "Sistemi di protezione contro un impiego non autorizzato dei veicoli a motore", mentre se il sistema ha la funzionalità di black-box dovrà essere certificato in conformità alla norma CEI 79/56 "Sistemi di tipo black-box: requisiti funzionali e prove". Poi vi sono i sistemi antifurto cosiddetti "senza testimoniabilità" che vanno certificati in conformità alla direttiva 95/56/CE e/o ai Regolamenti ECE/ONU116 ed ECE/ONU 97.
Per chi volesse approfondire la questione, sul sito di ANIA si trova l'elenco dei dispositivi con le relative omologazioni.
Sul versante del servizio, se l'utente usufruisce di un servizio di centrale operativa svolto da una società di vigilanza, dovrà assicurarsi che la centrale sia autorizzata a sensi dell'art. 134 TULPS.
Non ultimo, come importanza, è l'aspetto della copertura del servizio, se solo in Italia o anche all'estero.
Se i veicoli vanno all'estero, è importante assicurarsi che non via siano blocchi di roaming sulla SIM e che la società di vigilanza abbia accordi per l'attivazione delle forze di polizia all'estero in caso di evento.

Come può fare l'utilizzatore per valutare la qualità e la serietà dei fornitori?
Innanzitutto un utilizzatore deve valutare di cosa ha bisogno. Deve valutare se ha bisogno di un sistema antirapina, antifurto, di semplice localizzazione, se può essere alimentato, dove lo installa, ecc.
Se per il privato è semplice valutare ciò, per una azienda vi deve essere un'analisi delle necessità, fatta da tutte le funzioni aziendali, accanto ad un'analisi dei rischi e delle vulnerabilità e la definizione delle misure di security per far sì che il rischio sia teso il più possibile verso lo 0. Poiché non tutte le aziende hanno queste capacità e conoscenze o un security manager in azienda, è bene che le stesse si affidino ad un consulente e a società serie e preparate e non guardino solo al prezzo per individuare l'azienda più confacente alle proprie esigenze, valutando anche il portafoglio clienti di queste aziende.

Ci può dare qualche indicazione su ANSSAT in termini di rappresentanza della categoria e di obiettivi?
ANSSAT rappresenta e raggruppa le principali aziende Italiane che si occupano di produzione di sistemi di radiolocalizza-zione e di erogazione di servizi legati alla sicurezza.
Significativa è la percentuale (circa 70/80%) dei mezzi pesanti circolanti che trasportano beni di valore, che usufruiscono del servizio professionale dei soci.
ANSSAT crede in un rapporto serio ed etico con la clientela e, per questo, ha individuato dei livelli di servizio che sono pubblicati sul sito **www.anssat.it**, liberamente scaricabili e consultabili da tutti. Obiettivo di ANSSAT e dei suoi soci è quello di fare una cultura sulla radiolocalizzazione perché molti operatori si sono affacciati sul mercato senza essere in grado di dare risposte professionali alle esigenze della clientela.

AIPS, innovazione e competenze certificate per i professionisti della sicurezza

intervista all'ing. Antonio Avolio, consigliere nazionale AIPS e coordinatore del gruppo interassociativo per la Norma UNI

In base alla sua partecipazione ai gruppi di lavoro che stanno sviluppando la nuova versione della CEI 79 e la norma UNI di prossima pubblicazione, ci può riassumere i contenuti e gli indirizzi di questi due capisaldi della qualificazione professionale del settore per i prossimi anni?

Il tema della qualificazione professionale dell'installatore inizia dal 2012 con l'allegato K della Norma CEI 79-3, dove si è dato evidenza dell'importanza delle conoscenze e delle competenze dell'installatore, in particolare quando si parla di tecnologie specifiche.

Quest'anno la Norma CEI è in revisione e si sta cercando di fare il massimo per renderla quanto più intuitiva per l'installatore e con elementi in più per il progettista nell'analisi e la valutazione del rischio.

Ad inizio 2020 era stato avviato il progetto di norma UNI 161003 con l'obiettivo di definire le competenze relative all'attività professionale dei progettisti, installatori e manutentori di impianti di allarme intrusione e rapina, videosorveglianza e controllo accessi attraverso l'individuazione di compiti e attività nonchè dei requisiti di conoscenza, abilità, autonomia e responsabilità.

Questo progetto è partito recependo le richieste del gruppo interassociativo, del quale sono con grande piacere coordinatore, con l'organizzazione nell'ambito del Gruppo di Lavoro 10 di UNI di un gruppo misto UNI-CEI dedicato alla predisposizione della norma.

Vorrei ricordare che AIPS, di cui sono consigliere nazionale, ha organizzato in occasione di Fiera Sicurezza 2021 l'evento *"Professionalità e qualificazione dell'installatore di sicurezza a tutela del mercato: il risultato del percorso interassociativo e gli spunti futuri"* con il patrocinio di UNI, al

quale hanno partecipato, assieme a me in rappresentanza di AIPS, Giulio Iucci, presidente ANIE SICUREZZA, Raffaele De Astis, presidente ASSOSICUREZZA, l'ing. Antonino Barresi di IMQ, coordinatore del Gruppo Misto UNI-CEI, Jean-François Milone di ICMQ/Cersa, e l'ing. Marco De Gregorio di UNI.

Questo incontro ha evidenziato la necessità di comunicare al mercato la valenza della norma e della certificazione corrispondente delle competenze degli installatori di sistemi di sicurezza da parte di enti terzi.

Questo è l'obiettivo sul quale si concentrerà l'attività futura di questo gruppo.

Oggi tutti concordano anche sull'opportunità di aprire il gruppo a chi ne faccia a buon titolo richiesta, alle associazioni dei consumatori e ai rappresentanti delle assicurazioni.

Quali sono gli organismi associativi che hanno promosso questi progetti? E' stata trovata coesione tra le diverse anime della categoria o ci sono istanze diverse?

AIPS che, come noto, è da sempre impegnata nella promozione della qualificazione degli installatori di sistemi di sicurezza e nel riconoscimento della professionalità, si era fatta promotrice del progetto interassociativo già in occasione di Fiera Sicurezza 2019 in occasione del convegno *"La rivoluzione della certificazione: a che punto siamo?"*.

Il tutto è stato ufficializzato ad inizio 2020 con le associazioni di settore A.I.PRO.S., A.I.P.S., ANIE Sicurezza e Assosicurezza e gli Enti di certificazione CERSA, IMQ e TÜV Italia che hanno sottoscritto un protocollo d'intesa finalizzato a promuovere uno schema condiviso di certificazione personale in una Norma tecnica UNI per le figure dei progettisti, installatori e manutentori di sistemi di sicurezza, finalizzato ad unificare i contenuti degli schemi di certificazione proprietari attualmente esistenti.

In sintesi, il progetto interassociativo si è sviluppato nel corso di successivi incontri, durante i quali le associazioni interessate hanno analizzato le norme di settore e la legislazione vigenti, condividendo l'esigenza di poter identificare in modo univoco le competenze professionali e i requisiti tecnici degli operatori del settore sicurezza, così da rispondere alla richiesta di qualificazione proveniente dal mercato.

Ad oggi devo dire che si è consolidata un'intesa di "gioco di squadra" tra le associazioni, con la disponibilità a portare avanti iniziative che possano migliorare le competenze e le conoscenze delle figure professionali e del mercato della sicurezza in generale.

Qual'è il suo percorso professionale, che l'ha portata ad occuparsi di questi temi?

Mi sono laureato in ingegneria elettronica nel 2005 e, dopo un'esperienza nel settore telecomunicazioni di circa due anni, c'è stata l'opportunità di iniziare nel 2007 una nuova esperienza lavorativa con la società del mio caro zio Bruno Maisto, la IMPEL snc.

Mio zio è stato un vero e proprio pioniere del settore, che ha iniziato l'attività specifica nel lontano 1978 credendo nelle competenze e nella formazione per differenziarsi nel mercato. Non a caso è stato uno dei primi associati nella vita iniziale di AIPS.

Dal 2007 al 2015 sono stato responsabile tecnico della sua azienda con realizzazioni di impianti antintrusione e videocontrollo per enti pubblici e privati anche di rilievo come, ad esempio, la videosorveglianza sui veicoli per il trasporto pubblico a Napoli su circa 500 mezzi.

Nel 2015 ho avviato la mia società SECURITY ENGINEERING srl, che nasce da un team di professionisti che combinano perfettamente innovazione ed esperienza pluriennale in particolare nei settori della sicurezza, dell'impiantistica elettrica e del risparmio energetico. La sicurezza è diventata oggi una priorità per ogni impresa, negozio, banca, amministrazione comunale, ente locale, abitazione privata e innumerevoli altre realtà.

L'azienda nasce come una società specializzata nella progettazione, installazione e manutenzione di impianti dedicati alla security, sempre orientata ai nuovi scenari tecnologici e capace di ampliare i propri orizzonti nei settori che portano ad un miglioramento in termini di risparmio energetico.

Nel 2010 avevo iniziato il percorso come docente all'Ordine degli Ingegneri di Napoli con i primi corsi sulla Videosorveglianza e Antintrusione, tenuti dal 2013 al 2016.

Con l'ingresso in AIPS come consigliere nazionale, ho avuto la possibilità di promuovere eventi formativi e di approfondire gli aggiornamenti normativi del settore security, con un'esperienza nella partecipazione al gruppo di lavoro in UNI dell'avv. Adarosa Ruffini "Sicurezza del Cittadino" con iniziative e studi sui "Modelli di Certificazioni Integrati".

Nel 2018 ho conseguito anche l'abilitazione come professionista in prevenzione incendi secondo il DM 5 agosto 2011, con l'iscrizione negli elenchi del Ministero dell'Interno.

Dal 2015 sono docente qualificato di Ethos Academy per l'attività formativa dei corsi sulle Norme CEI e referente tecnico/scientifico del progetto "Pillole formative", sempre in capo a Ethos Academy. Le docenze vengono svolte per corsi che sono stati validati e riconosciuti propedeutici alla certificazione degli operatori delle sale sicurezza secondo lo schema CEI /TUV Italia. Sempre in Ethos Academy, sono responsabile del team per la trasformazione dei corsi da frontale a digitale, sempre nel rispetto dello schema CEI/TUV Italia.

Ci può parlare della sua esperienza di professionista e di imprenditore della sicurezza nel Meridione e dei progetti che sta sviluppando?

Oltre alle attività imprenditoriali e associative di cui ho parlato prima, sono partner dal 2015 come referente ed esperto nella security tecnologica, di un progetto innovativo a Napoli "Exclusive Experience Store", uno spazio in cui l'eccellenza dei professionisti e delle aziende creano sinergie.

Il progetto offre una serie di servizi:

- BUSINESS HUB: è uno spazio in cui l'eccellenza dei professionisti e delle aziende creano sinergie. I prodotti e le soluzioni diventano esperienze estremamente emozionanti.

- EVENTS : Exclusive dispone di diversi spazi polifunzionali: area per esposizioni, spazi per eventi e talkshow, shooting fotografici e party aziendali.

- WORKSHOP: la sala Executive dispone di 8 comodi posti con tavolo riunione e tutte le tecnologie multimediali, mentre la sala Exclusive dispone di 24 poltrone con sistemi di video proiezione e postazione relatori per accogliere workshop, seminari e mini-congressi

- BOOK NOW: con le nostre sale riunioni è possibile ospitare i clienti e partner commerciali in una cornice lavorativa elegante e prestigiosa, prenotabile online o telefonicamente per un'offerta personalizzata.

Progetti futuri: siamo orientati ad offrire al cliente finale le migliori tecnologie e soluzioni, garantendo competenza e conoscenze approfondite delle tecnologie e degli aspetti normativi per la realizzazione di progetti e installazioni a regola d'arte.

Innovazione e sicurezza

di Tommaso Di Noia, docente ordinario di Intelligenza Artificiale presso il Politecnico di Bari e Chief Research Officer @ Wideverse

Introduzione

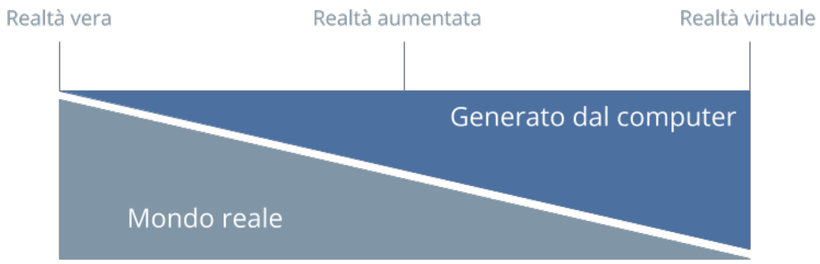
Innovazione è uno dei termini più abusati degli ultimi decenni.
Laddove prima, in un passato neanche troppo lontano, innovare poteva essere un processo virtuoso da intraprendere, ora è diventata la via necessaria da perseguire per mantenere la competitività nel proprio business.
L'opportunità di rinnovamento data da questo momento storico di ripartenza post pandemica deve essere colta come trampolino di lancio per un futuro di business sostenibile, a maggior ragione pensando all'attuale situazione internazionale.
Ma cosa è l'innovazione nel 2022?

Digital transformation e metaverso

Si parla tanto di trasformazione digitale, ma per attuare questa transizione e poterne beneficiare, è necessario comprendere le tecnologie fondanti alla base.
Il cloud e la connettività a banda larga data da fibra ottica e 5G sono le tecnologie abilitanti (e spesso nascoste) che permettono ad altre innovazioni (che invece possiamo toccare con mano) di essere alla nostra portata.
Tecnologie che devono avere alla base un rinnovamento dei processi in linea con il disegno di un futuro che rispecchi i principi di una prosperità e di una crescita che siano sostenibili per il nostro pianeta e per i lavoratori.
Anche il cosiddetto "metaverso" presentato da Mark Zuckerberg, CEO di Facebook, in cui vedremo le attività imprenditoriali sempre più immerse e connesse con mondi virtuali, è più vicino di quel che si pensi.

Le tecnologie di Realtà Virtuale, Realtà aumentata ed intelligenza artificiale

E' bene innanzitutto fare chiarezza sui confini tra realtà virtuale e realtà aumentata. Tante volte queste tecnologie ricadono insieme sotto il cappello di eXtended Reality (XR).
La distinzione più chiara l'ha fatta Google definendo il cosiddetto spettro immersivo. In figura 1, partendo da sinistra c'è la realtà vera (il mondo reale). Al centro si trova la realtà aumentata dove si può osservare un intreccio tra mondo reale e generato dal computer. Fino ad arrivare all'estremo destro dello spettro dove si trova la realtà virtuale: l'ambiente in cui si è immersi è totalmente ricostruito in computer grafica.



Che cos'è la realtà virtuale e come funziona

La realtà virtuale è una simulazione realistica e immersiva di un ambiente tridimensionale a 360 gradi, creata utilizzando software e hardware interattivi e vissuta o controllata tramite i movimenti del corpo. Le logiche classiche del gaming da cui nasce la realtà virtuale, si applicano ora a scenari come il training ed real estate.
La realtà virtuale entra a far parte della cultura popolare dall'inizio degli anni Ottanta con i libri di William Gibson, come Neuromancer, che aprono il fortunato filone letterario del cyberpunk.
La VR permette di immergersi in un ambiente completamente modellato in computer grafica e per essere fruita necessita di dispositivi e visori dedicati come quello in figura 2.

I moderni visori si basano sulla tecnologia di cui sono dotati gli smartphone che abbiamo in tasca: giroscopi e accelerometri, schermi HD per la visione stereoscopica e processori di ultima generazione per permettere alte velocità computazionali.

Che cos'è la realtà aumentata e come funziona

La realtà aumentata è una visione dal vivo di un ambiente fisico reale tramite occhiali olografici o schermi di smartphone e tablet, in cui vengono sovrapposti elementi virtuali quali suoni, immagini, video, modelli 3D, grafici o dati GPS utilizzando gli input dei sensori. La realtà aumentata è alla portata di tutti perché disponibile sui nostri smartphone e sta permeando tutti i settori, dal medicale allo shopping a quello più ludico.

Quando parliamo di realtà aumentata, degne di nota sono due categorie particolari:
- realtà assistita
- realtà mista

La realtà assistita è quella che si può provare usando visori come i Google Glass, dove il monitor su cui vengono mostrate le informazioni non copre la visuale di chi li indossa (quindi contrario alla definizione data poco prima), ma fornisce ugualmente informazioni di contesto, aumentando la nostra capacità di percepire ciò che ci circonda. E' come avere il monitor di uno smartphone poco sopra l'occhio consultabile tenendo le mani libere.
La realtà mista è invece una vera e propria rivoluzione, perché si basa sul concetto di percezione da parte del visore, dello spazio fisico. Ad esempio, visori come il Microsoft Hololens, che riconoscono pareti, pavimenti e superfici come quella di un tavolo e sopra i quali è possibile mettere veri e propri ologrammi che l'utente potrà vedere tramite le lenti del visore.

Che cos'è l'intelligenza artificiale e come funziona

L'intelligenza artificiale è una disciplina dell'informatica che studia i fondamenti teorici, le metodologie e le tecniche che consentono la progettazione di sistemi hardware e software capaci di fornire ai computer prestazioni che, ad un osservatore comune, sembrerebbero essere di pertinenza esclusiva dell'intelligenza umana. Il machine learning è una

branca dell'intelligenza artificiale che si occupa di creare sistemi che apprendono o migliorano le performance in base ai dati che utilizzano. Che si tratti di una ricerca su Amazon o di tradurre un testo, si usano algoritmi di intelligenza artificiale.

Applicazioni delle tecnologie di XR e AI per la sicurezza

Esistono diverse situazioni in cui queste tecnologie stanno già trovando applicazione e nuovi scenari che possono sembrare appartenere ad un futuro remoto, sono più vicini di quel che si pensa.

Addestramento

Che si tratti di ambito industriale, medico o militare, l'addestramento ricopre un ruolo cruciale. Maggiore è la possibilità per gli allievi di esercitarsi e provare più volte, prima saranno pronti per lavorare sul campo. Il processo di addestramento è spesso però vincolato alla scarsità delle opportunità di esercitarsi.

Basti pensare al campo medico in cui non ci sono un numero infinito di pazienti e sale operatorie o al campo militare dove i simulatori di volo sono molto costosi e disponibili solo in alcune installazioni. La realtà virtuale sta trovando grande applicazione in questo settore.

È possibile ricostruire in 3D un'intera linea di produzione o un macchinario specifico, simulando tutte le procedure operative che l'allievo deve apprendere. I costi sono molto inferiori, l'addestramento avviene in totale sicurezza e può essere ripetuto un numero potenzialmente infinito di volte.

Alla stessa maniera si possono progettare in 3D diverse ambientazioni (o ricostruire ambienti reali), come ad esempio banche, per addestrare il personale nelle operazioni di prelievo e deposito di valori. Nelle simulazioni addestrative è possibile configurare diverse situazioni di minaccia o problematiche a cui il personale deve saper rispondere.

Il vantaggio indiscusso è la possibilità di ripetere l'addestramento svincolandosi dal contesto fisico (potenzialmente difficile da riprodurre) e poter configurare simulazioni che sono facilmente aggiornabili nel tempo.

Supervisione

Sempre in ambito formativo, il training on the job sta diventando una necessità perchè bisogna rendere il più velocemente possibile gli operatori sul campo.

Grazie a strumenti come i visori di realtà aumentata, è già oggi possibile seguire in streaming le attività di un operatore da parte di un tutor che può essere seduto in una sala di controllo. La visuale del tutor è la stessa dell'operatore, questo grazie alla forma dei visori ed al posizionamento della fotocamera nella vicinanza dell'occhio.

Il tutor può cosi dare le indicazioni opportune per formare più velocemente l'operatore mentre è già in azione.

Ancora una volta l'esempio più semplice è quello del trasporto valori, in cui un tutor può supervisionare l'attività e ad esempio fare training on the job sul caricamento del denaro in un bancomat.

Supporto informativo e visione aumentata

Utilizzando i visori di realtà aumentata è possibile rendere un operatore completamente autonomo e supportarlo con informazioni di contesto a portata del suo occhio.

Si pensi ad esempio al contesto più semplice, cioè quello di navigazione indoor di uno stabile: grazie ad una mappa 3D, sarà semplice per lui dirigersi verso la sua destinazione nella maniera più veloce possibile.

Oppure grazie all'intelligenza artificiale in combinazione con le tecniche di riconoscimento delle immagini, un assistente virtuale potrà identificare elementi anomali o possibili minacce.

Una telecamera posta sul cruscotto di un furgone portavalori, con dei sistemi di intelligenza artificiale che analizzano la situazione circostante può essere un supporto di valore nello sventare minacce.

La capacità di percepire lo spazio di alcuni visori può essere di supporto in contesti in cui la precisione è di fondamentale importanza e gli ologrammi possono guidare o evidenziare all'operatore certi dettagli.

Conclusioni

Siamo agli inizi dell'epoca dell'immersive computing e del metaverso.

Le tecnologie di realtà virtuale, realtà aumentata ed intelligenza artificiale stanno entrando nel nostro quotidiano.

La tecnologia del 5G permetterà di avere in mobilità la banda necessaria a garantire la velocità necessaria per effettuare videochiamate in realtà aumentata, monitorare da remoto le attività di un operatore o di una squadra e supervisionare le loro operazioni.

Sarà possibile ridurre il numero di trasferte ed addestrare personale da remoto ed il loro operato sarà coadiuvato da assistenti virtuali integrati nei visori di realtà aumentata.

Anche i nostri veicoli diventeranno ancora più smart: il parabrezza diventerà uno schermo di realtà aumentata in grado di mostrare i dati di contesto per rendere più sicuro il lavoro.

Sotto questo aspetto, anche il lavoro di società come Niantic (creatori dei giochi in AR Ingress e Pokemon GO) che si stanno impegnando a scansionare il mondo in 3D è un passo verso nuovi modi di integrare reale e virtuale di cui può beneficiare anche l'ambito professionale e non solo quello del gaming.

Anche il mondo della sicurezza deve cogliere il valore ed il potenziale dell'utilizzo di queste tecnologie.

Realtà aumentata per formazione e sicurezza. Le proposte di Wideverse

intervista a Michelantonio Trizio, CTO di Wideverse

Si parla sempre più frequentemente di metaverso, di realtà aumentata e realtà virtuale, temi di cui si occupa Wideverse, la start-up di cui sei co-founder e partner. Puoi raccontarci prima di tutto il tuo percorso professionale e presentarci Wideverse?

Partendo da me, mi sono laureato in ingegneria informatica nel 2007 al Politecnico di Bari, dove ho fatto anche l'assistente di ricerca per qualche anno in intelligenza artificiale. Ho lavorato per aziende private come sviluppatore software, poi la voglia di mettermi in gioco mi ha spinto a frequentare una start-up school in Silicon Valley e fondare la mia prima azienda in Italia. Nel 2016 ho avviato la mia terza esperienza imprenditoriale con Wideverse, in cui ricopro il ruolo di CTO, la persona responsabile di definire tutte le tecnologie dei nostri prodotti.

Wideverse nasce dalla volontà del prof. **Tommaso Di Noia**, docente ordinario di Intelligenza artificiale al Politecnico di Bari. L'intento era, ed è tutt'ora, di trasformare la ricerca universitaria in prodotti di mercato, esplorando le nuove frontiere della realtà virtuale ed aumentata con il supporto di algoritmi di intelligenza artificiale e computer vision. L'idea è nata dopo l'organizzazione di una conferenza per sviluppatori software al Politecnico di Bari nel 2014 in cui portammo interventi sui Google Glass. Il grande interesse e l'entusiasmo che raccogliemmo durante l'evento ci convinsero ad investigare questa opportunità.

Chi sono i partner attuali?

I nostri partner principali sono aziende che fanno da system integrator e tramite i quali veicoliamo i nostri prodotti in contesti che sono prettamente b2b. Parliamo di multinazionali come Exprivia Spa e Fincons Spa, ma anche realtà del calibro di Leonardo con cui abbiamo un progetto di ricerca per l'Aeronautica Militare Italiana per il supporto alla manutenzione da remoto in realtà aumentata in ottica manutenzione e logistica 4.0.

Le sinergie che si vengono a creare sono molto interessanti e si creano dinamiche win win perché tante volte i clienti sono interessati a più tecnologie differenti in ambito 4.0.

Abbiamo anche diverse collaborazioni a vario livello con altre start up o scale up. Posso citare, ad esempio, QuestIT, azienda che possiede un motore per agenti conversazionali, quelli che brutalmente chiamiamo "chatbot". Avere un assistente virtuale inserito in applicazioni di realtà aumentata e virtuale è un vantaggio per arricchire l'esperienza degli utenti.

Quali soluzioni avete sviluppato ed a quali applicazioni sono indirizzate?

Scotty expert è il nostro prodotto principale. E' un sistema di realtà aumentata per il supporto da remoto e la gestione di procedure. Lo proponiamo come Software as a Service in cloud (SaaS) ed i nostri mercati principali adesso sono quello manifatturiero per la gestione delle manutenzioni ed il training on the job, ed assicurativo per la gestione delle pratiche dei sinistri con la possibilità di fare raccolta di evidenze in realtà aumentata.

Tramite Scotty expert i nostri clienti possono creare e gestire in totale autonomia le procedure in realtà aumentata sia con smartphone e/o tablet che con visori.

Non a caso, alcuni dei nostri principali interlocutori in azienda per questo prodotto sono spesso i responsabili della formazione, che necessitano di nuovi strumenti per addestrare il personale accelerando la curva di apprendimento ed assicurandosi che la formazione sia efficace tramite analisi dei video e dei dati dell'addestramento che include fasi di training on the job.

TourVerse invece permette a chiunque di creare un tour virtuale fatto di foto a 360° o scenari 3D. E' una piattaforma web che permette di fruire delle esperienze create sia via web che tramite visori di realtà virtuale come ad esempio gli Oculus Quest.

Showroom e addestramento sono gli scenari di riferimento. Si pensi, ad esempio alla possibilità di far addestrare un nuovo dipendente su uno scenario virtuale che riproduce una situazione di pericolo in cui può incorrere nella realtà. Poterla provare in un ambiente sicuro come quello virtuale è un vantaggio per la sicurezza e la comprensione delle problematiche dello scenario che può essere approfondito da più punti di vista.

Il nostro ultimo prodotto è selfAR che permette di aggiungere contenuti 3D in realtà aumentata ad immagini stampate ed oggetti fisici. Ad esempio, possiamo prendere una immagine presente su un bancomat ed associare in realtà aumentata lo schema di una procedura da eseguire.

Quali sono i vostri programmi per il futuro?

Si fa un gran parlare di Metaverso dopo la presentazione dello scorso settembre di Mark Zuckerberg, CEO di Facebook (ora rinominata Meta).

Il termine è preso dal romanzo cyberpunk "Snow Crash" di Neal Stephenson, pubblicato nel 1992. Nel romanzo, ambientato in un futuro molto prossimo, le persone possono incontrarsi nel metaverso, uno spazio libero, dove ci sono strade, locali, negozi, creato da programmatori indipendenti, muovendosi tramite avatar.

Le tecnologie alla base del metaverso sono quelle su cui lavoriamo fin dalla nascita di Wideverse, cioè realtà virtuale, realtà aumentata ed intelligenza artificiale (con l'aggiunta della blockchain).

Il metaverso però è ancora qualcosa di non ben definito e su cui si è appena iniziato a ragionare sia in termini di nuove applicazioni che di possibilità di applicare il concetto su mercati tradizionali come quello della sicurezza. Posso dirti che stiamo orientando sempre più le nostre tecnologie ed i nostri prodotti verso l'ambito addestrativo e formativo. Presto annunceremo alcune novità e ci aspettiamo di poter contribuire alla creazione di un mondo che sia sempre più immersivo ed in cui il passaggio tra realtà virtuale ed aumentata sia sempre più semplice.

Michelantonio Trizio è un ingegnere informatico votato all'imprenditoria innovativa ed ha come obiettivo quello di portare le tecnologie di frontiera nella vita quotidiana e lavorativa delle persone per semplificarla.
E' anche leader del GDG Bari, una community di sviluppatori appassionata di tecnologie Google, oratore, formatore ed evangelista delle nuove tecnologie.

OMNISINT presenta NEDAP AEOS, il più efficiente sistema di controllo accessi fisici

comunicato aziendale

Oggi, essere in possesso di un sistema di controllo accessi è un fattore imprescindibile per ogni impresa. Senza soluzioni adatte, le organizzazioni risultano vulnerabili a possibili accessi non desiderati ad aree protette, con rischi potenzialmente anche gravi.

Il sistema di controllo accessi **AEOS** di **NEDAP** fornito da **Omnisint** è progettato per adattarsi alle esigenze in continua evoluzione delle imprese, garantendo efficienza ed affidabilità in ogni situazione e permettendo alle organizzazioni di concentrarsi sul proprio core business, aumentando produttività e prestazioni.

Nessun'altra soluzione è in grado di far fronte alle mutevoli policy di conformità delle organizzazioni e alle possibili minacce alla sicurezza come fa AEOS, offrendo un'architettura unica, estensibile e adattabile ad ogni necessità.

AEOS è una piattaforma commerciale basata su standard aperti, le cui funzionalità sono garantite anche con una vasta gamma di lettori di terze parti, ed è altamente configurabile e personalizzabile. Utilizza un approccio unico basato su software, permettendo così di modificare le funzionalità e i livelli di sicurezza del sistema utilizzando solo la piattaforma web, rendendo più veloce ed economico l'adattamento alle mutevoli normative aziendali.

AEOS si collega facilmente con serrature fisiche già esistenti, lettori badge e altri dispositivi per migliorare il flusso di persone attraverso gli uffici o i vari edifici. È possibile integrare anche lettori biometrici o lettori badge tradizionali, serrature wireless o cablate, ascensori.

Il sistema è inoltre altamente intuitivo per permettere al personale un utilizzo immediato senza ore di formazione, con conseguente maggiore efficienza nel completamento delle attività interne.

Per raggiungere questi standard elevati, NEDAP e Omnisint collaborano con Security Specialist in tutto il mondo, creando

soluzioni all'avanguardia attraverso il "Technology Partner Program".

AEOS garantisce maggiore sicurezza ai dipendenti: il sistema è infatti totalmente protetto anche da attacchi informatici, in quanto tutte le informazioni contenute nelle installazioni sono criptate. E, per una maggiore sicurezza in campo di protezione dai cyber-attack, il sistema AEOS trasferisce e custodisce i dati negli hardware posti all'interno delle porte di accesso. In questo modo, anche in caso di decodifica non autorizzata dei dati, i lettori saranno protetti, impedendo qualsiasi intrusione.

Con AEOS aumenta l'automazione e migliora la sicurezza

Le policy di sicurezza comprendono sia procedure tecniche, sia istruzioni di lavoro per il personale addetto. Le procedure vengono applicate attraverso le funzionalità di AEOS, e la sua facilità d'uso garantisce che il personale di sicurezza sia motivato all'utilizzo.

Le attività quotidiane di routine vengono quindi automatizzate e la responsabilità delle azioni viene registrata, permettendo un aumento dei livelli di sicurezza dell'organizzazione.

Perché scegliere AEOS?

• Controllo versatile: AEOS si adatta facilmente ad ogni struttura aziendale, senza rallentare i processi

• Sicurezza end-to-end: AEOS è protetto dagli standard più elevati di cybersecurity per la protezione dagli attacchi informatici sul controllo accessi e sul furto di dati personali

• Aggiornamento costante: gli upgrade software di AEOS garantiscono il supporto necessario per l'utilizzo delle ultime tecnologie in ambito di funzionalità e sicurezza

• Elevata capacità di integrazione: dalle integrazioni delle risorse umane alla biometria e dal VMS al rilevamento delle intrusioni, AEOS ha infinite possibilità di integrazione

• Scalabilità graduale: con AEOS si può iniziare in piccolo ed espandere le funzionalità del sistema di controllo accessi gradualmente. Sia i prezzi che l'architettura sono progettati per adattarsi alle esigenze di ogni realtà

Vantaggi per gli utenti finali

Perché è preferibile investire in una piattaforma aperta ed integrata, piuttosto che in un unico sistema di sicurezza autonomo?

1. Qualità e valore: quando si acquistano separatamente i componenti del sistema di sicurezza, si può scegliere il livello di qualità che si preferisce per ogni elemento. Per alcuni elementi si potrebbe voler investire di più e per altri risparmiare acquistando versioni base.

2. Libertà di scelta: diamo la libertà di poter scegliere quali tecnologie utilizzare per ciascuna funzione, in modo da non avere vincoli verso un fornitore specifico.

3. Flessibilità: una piattaforma aperta permette di adattare rapidamente il sistema, senza compromettere la sicurezza o l'esperienza dell'utente. È possibile rispondere a nuove minacce, adottare nuove tecnologie e funzionalità e, se occorre, sostituire singole tecnologie anziché l'intero sistema.

4. Scalabilità: con una piattaforma aperta alle integrazioni come AEOS, sarà facile far crescere il sistema di controllo accessi di pari passo alla crescita aziendale. Si potranno aggiungere rapidamente nuove sedi in tutto il mondo e implementare le integrazioni necessarie a ciascuna sede.

5. Efficienza: AEOS semplifica il controllo del sistema di sicurezza per ogni ufficio o edificio e fornisce sicurezza al personale.

L'architettura completamente aperta di Nedap AEOS permette quindi una gestione omogenea della sicurezza ed un risparmio dei costi di gestione e manutenzione. Tra le sue molteplici funzioni, AEOS consente la gestione degli allarmi, il video management, la gestione dei visitatori e molteplici altre funzioni.

Proprio per queste sue caratteristiche, AEOS si rivela uno strumento prezioso presso multinazionali, piccole e medie aziende, banche, aeroporti, istituti della pubblica amministrazione, e dovunque ci sia una richiesta estesa di sicurezza e controllo delle persone, vantando già un portafoglio clienti in ognuno di questi ambiti.

omnisint
around technology

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

Parte il corso per Security Manager UNI 10459:2017 di San Giorgio

intervista a Gabriele Guarino, Presidente San Giorgio srl

San Giorgio estende il suo già ricco catalogo di proposte formative per le diverse figure della sicurezza con un corso per security manager propedeutico alla certificazione in base alla Norma UNI 10459. Quali sono gli obiettivi di un progetto così impegnativo?
L'obiettivo del corso è la formazione del Professionista della Security così come stabilito dalla normativa UNI 10459:2017. Il percorso formativo si propone di formare manager esperti nel settore della sicurezza pubblica e privata, che abbiano una buona conoscenza del business e che siano in grado di operare in modo trasversale nei processi aziendali, in uno scenario complessivo in grande evoluzione.

Come è strutturato il corso, quali sono i docenti e i costi?
Il Corso, organizzato con l'Associazione Formamente - ente di formazione con accreditamento regionale - si svolgerà in modalità webinar per 88 ore e per 32 ore in FAD a partire dal 22 marzo tutti i martedì e venerdì pomeriggio dalle 14.30 alle 18.30
E' prevista la presentazione di slides dedicate, esempi pratici, discussioni e confronto, materiale didattico fornito su supporto elettronico e su cloud, test finale alla fine di ogni giornata formativa ed esame finale.
Questo corso annovera docenti professionisti tra i maggiori esperti del settore della sicurezza pubblica e privata, quali Francesco Fantozzi, Michele Bertossi, Giovanni Campanale, Nicolay Catania, Diego Dell'Orto, Cristian Donin, Paolo Furlan, Francesco Sacerdoti, Marco Stratta, ed altri esperti qualificati.
Quanto ai costi, San Giorgio ha voluto dare l'opportunità agli interessati di partecipare con una quota molto appetibile rispetto al mercato di riferimento, pari a € 950 oltre iva.

A quali figure si rivolge in particolare?
Il corso è rivolto ai diplomati e laureati in tutte le discipline che vogliono operare nel settore della sicurezza pubblica e privata, e rappresenta un efficace metodo per valorizzare il curriculum delle figure manageriali (titolare, institore, direttore tecnico) delle società di vigilanza, logistica, handling, retail, ma anche di funzionari e dirigenti della Pubblica Amministrazione. Più in generale, di tutte le figure professionali che operano nel settore della sicurezza.

Come svilupperete gli argomenti specifici relativi ad ambiti operativi fra loro molto diversi, quali sono appunto quelli citati, istituti di vigilanza, logistica, handling, retail, PA?
Stiamo preparando dei moduli di approfondimento ad hoc con la collaborazione di esperti nei singoli ambiti operativi che proporremo all'ente di certificazione Quaser Certificazioni, nostro partner in questo percorso, per il riconoscimento di crediti formativi per il mantenimento della certificazione in base alla Norma UNI 10459 negli anni successivi. In questo modo, i security manager interessati potranno estendere nel tempo le proprie competenze in modo qualificato ed aumentare le opportunità di crescita professionale in uno scenario nel quale, come già accennato prima, si stanno delineando cambiamenti importanti per il ruolo di queste figure.

Quali sono questi cambiamenti, dal vostro punto di osservazione?
Sono cambiamenti dovuti a più fattori, alcuni maturati nel tempo, altri in rapido divenire.
Innanzitutto la sicurezza, in senso lato, è diventata sempre più una componente essenziale della maggior parte dei processi operativi delle organizzazioni pubbliche e private. Questo ha già comportato il coinvolgimento dei responsabili della sicurezza nella gestione globale delle organizzazioni, passati dalla mera attività di protezione dei beni aziendali, concepita generalmente solo come un "costo inevitabile", alla definizione ed alla mitigazione dei rischi complessivi ai quali sono esposte le organizzazioni medesime. Pertanto, con un ruolo di salvaguardia del business nel suo insieme, come del resto aveva già recepito la versione del 2017 della Norma UNI 10459.
A questo si è sovrapposta la trasformazione digitale degli ultimi anni che, tra le altre conseguenze, ha letteralmente dissolto i confini tradizionali tra sicurezza fisica e sicurezza logica ma anche tra security, safety e, più recentemente, health. Il conseguente aumento delle competenze necessarie per rispondere a queste sfide impone un'evoluzione culturale delle figure preposte, che devono "imparare" a rispondere in modo organico alle diverse minacce.
Infine, la diffusione di principi generali quali duty of care, awareness, accountability (letteralmente: obbligo di attenzione, consapevolezza, responsabilizzazione) sotto la spinta delle normative dell'Unione Europea, come ad esempio la Direttiva NIS e il GDPR, implica una nuova interpretazione del concetto di tutela delle organizzazioni, che possono trovarsi esposte a rischi di sanzioni e risarcimenti talvolta ben maggiori di quelli causati da azioni ostili volontarie o da incidenti.
La figura del "security manager" assume dunque un ruolo sempre più determinante per il buon andamento di ogni organizzazione (pubblica o privata, piccola o grande) e di questo dev'essere prima consapevole, poi "attrezzato". Chiaramente, un impegno così imponente non può trovare tutte le risposte da un semplice corso finalizzato ad una certificazione, ma ritengo opportuno sottolineare l'attenzione di San Giorgio per questi aspetti fondamentali, ai quali faremo riferimento nello sviluppo delle nostre proposte formative.

Ci può raccontare San Giorgio?
San Giorgio è una società che offre spazio a professionisti esperti in diversi ambiti per poter sviluppare le potenzialità di ciascuno, in modo da proporsi al mercato con più soluzioni per le diverse esigenze aziendali.
I nostri clienti possono avere un interlocutore completo che offre formazione e consulenza a 360°.
Oggi San Giorgio è una società accreditata e autorizzata ENAC in ordine al Dangerous Good Regulation (merci pericolose) e per l'aggiornamento degli istruttori certificati ENAC anche in ambito cybersecurity.
E' inoltre autorizzata dal Ministero dell'Interno per la formazione in materia di sicurezza sussidiaria in ambito portuale, terrestre e ferroviario e fornisce corsi di sicurezza sui luoghi di lavoro e di Maritime e Airport & Aviation security.

Mi piace infine segnalare che il nostro gruppo di formatori e consulenti, che proviene da ogni parte d'Italia, si incontra in presenza per due giorni ogni mese, scegliendo una sede diversa di volta in volta, per verificare la qualità dei servizi, dare gli aggiornamenti normativi e garantire la fondamentale "formazione ai formatori".

SAN GIORGIO

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

Premio H d’oro 2021
Categoria VIDEOSORVEGLIANZA URBANA

a cura della Redazione

Categoria: **VIDEOSORVEGLIANZA URBANA**
Azienda installatrice: **S.ET.I. - Scafati (SA)**
Denominazione e località dell’impianto: **Aggiornamento e ampliamento del sistema di videosorveglianza del Comune di Livorno con connettività IP a larga banda in fibra ottica**
Impianto realizzato: **Impianto di videosorveglianza urbano**

Nell’ambito della quindicesima edizione del Premio H d’oro, il concorso organizzato dalla Fondazione Enzo Hruby per premiare le migliori realizzazioni di sicurezza e con esse la professionalità dei più qualificati operatori del settore, la società S.E.T.I. di Scafati (SA) ha vinto il prestigioso riconoscimento nella categoria Videosorveglianza urbana con l’impianto realizzato per il Comune di Livorno.

Descrizione dell’impianto

La città di Livorno ha investito nella realizzazione di un impianto di videosorveglianza di nuova concezione, in grado di monitorare efficacemente l’intera città e reagire rapidamente a qualsiasi evento o attività sospetta.
La società S.E.T.I. ha realizzato un sistema composto da numerose telecamere IP con risoluzione 4K disposte all’interno del tessuto urbano, collegate ad un sistema di archiviazione dati e gestione delle immagini a mezzo di infrastruttura di rete in fibra ottica proprietaria.
In particolare sono state installate:

- Telecamere IP fisse che permettono di visualizzare le caratteristiche generali del sito sensibile per rilevarne fenomeni di microcriminalità e contestualizzare ogni evento significativo.
- Telecamere IP di tipo Speed Dome che permettono una visualizzazione globale.
- Telecamere IP fisse LPR che permettono la visibilità a monitor delle targhe e l’individuazione del tipo di veicoli in transito presso le postazioni.

Il centro di raccolta dati è stato ubicato nel Municipio. Il nodo di raccolta permette l’archiviazione (Storage) e l’elaborazione delle immagini mediante l’ausilio di diversi software tra cui una piattaforma di video analisi di ultima generazione che mediante applicativi di analisi video intelligente basati su rete neurale ad autoapprendimento (CNN) agevola le operazioni di monitoraggio generando degli alert e riducendo i tempi di ricerca degli eventi di interesse, generando quindi una maggiore tempestività delle operazioni di intervento e contrasto.

Caratteristiche particolari dell’opera

L’impianto di Livorno ha la peculiarità di essere uno dei pochi impianti in Italia ad essere totalmente creato su collegamenti in fibra ottica ridondata (struttura ad anello). Le 152 telecamere di cui è composto l’impianto sono dislocate nei punti nevralgici della città, e le immagini provenienti dai punti di ripresa sono arricchite da numerosi algoritmi di analisi video che consentendo la gestione di alert automatici generati da un IA (intelligenza Artificiale) coadiuvano l’intervento delle Forze dell’Ordine e degli operatori di centrale. Ogni punto di ripresa è dotato anche una telecamera di lettura targhe che consente di catturare tutti i transiti di veicoli e motocicli. L’impianto, oltre a prevedere il collegamento di 4 sale operative di diverse forze dell’ordine (Polizia Locale - Carabinieri - Polizia Di Stato - Protezione Civile) è il primo in Italia ad aver sottoscritto un protocollo operativo interforze per la contitolarità del trattamento dei dati personali derivanti dall’impiego dei sistemi di telecontrollo del territorio.

Staff e tempo impiegati per la realizzazione

6 risorse complessive - 260 giorni

Da Hanwha Techwin le telecamere della serie Wisenet X con capacità di intelligenza artificiale (AI) a bordo

comunicato aziendale

Hanwha Techwin Europe ha introdotto una nuova gamma di telecamere della serie **Wisenet X** conformi all'NDAA con capacità di intelligenza artificiale (AI) integrate, con risoluzione da 2 MP, 6 MP e 4K. La nuova gamma di prodotti, che comprende 26 telecamere di diverse tipologie, amplia le opzioni a disposizione degli operatori che vogliono migliorare il proprio sistema di videosorveglianza con il Deep Learning, riducendo il numero di falsi allarmi e lavorando in maniera più efficiente. Le capacità AI a bordo aiutano gli operatori a rilevare oggetti come persone, volti, veicoli e targhe, migliorare la qualità delle immagini e fornire dati di business intelligence.

Analisi video basata su AI Deep Learning

Grazie al Deep Learning, le telecamere riescono a soddisfare con maggiore facilità le esigenze operative in vari contesti ed in molteplici applicazioni. L'AI integrata nella gamma della serie X permette di gestire i contenuti video con maggiore facilità, comunicando agli operatori gli eventi quando necessario, e consentendo loro di individuare gli eventi e gli oggetti rilevanti con rapidità mediante la ricerca forense, nonché di fornire una business intelligence più approfondita.

La capacità di rilevamento e classificazione degli oggetti permette agli operatori di identificare con rapidità le persone, i volti, le targhe e la tipologia di veicoli (auto, autocarri, autobus e biciclette), garantendo una maggiore consapevolezza della situazione e del contesto dell'evento. Movimenti irrilevanti come quelli dovuti ad alberi, ombre e animali, che con la tecnologia di rilevamento del movimento standard sarebbero causa di falsi allarmi, vengono ignorati. Così gli operatori possono concentrarsi maggiormente sul fornire risposte a incidenti ed emergenze reali.

L'analisi basata sull'AI trova applicazione in ambiti differenti rispetto alla sicurezza, offrendo anche la possibilitá di rilevare un ventaglio di dati utili per applicazioni di Business Intelligence. Con il rilevamento degli oggetti basato su AI, le aziende possono ottenere informazioni relative a conteggi delle persone, dati sulla gestione delle code e heatmap accurate che mostrano modelli del comportamento dettagliati. La gamma offre anche il rilevamento delle intrusioni e dello stazionamento ed è completata dal supporto dei canali virtuali che consente agli operatori di registrare e monitorare contemporaneamente più aree specifiche di una scena oltre alla scena intera.

Immagini di qualità avanzata

In aggiunta a questo, la tecnologia di riduzione del rumore **WiseNRII** utilizza l'AI per identificare gli oggetti in movimento e ridurre la sfocatura in ambienti rumorosi e scarsamente illuminati. La tecnologia **Extreme WDR** sfrutta l'analisi della scena per ridurre gli artefatti di movimento fornendo immagini nitide anche in condizioni caratterizzate da elevata retroilluminazione, mentre WiseIR regola l'uscita dell'illuminazione a infrarossi sulla base dell'ingrandimento dello zoom della telecamera. WiseStreamIII riduce al minimo la larghezza di banda e lo spazio usato, ottimizzando la compressione dei dati e dei filmati. Ciò permette agli operatori di concentrarsi solo sugli oggetti e sulle aree che richiedono maggiore attenzione, con una qualità delle immagini ottimale, una larghezza di banda ridotta al minimo e requisiti di spazio di archiviazione inferiori.

Durata maggiore per prestazioni costanti

La gamma offre opzioni di telecamera dome, dome antivandalo, bullet e box con ogni dispositivo dotato di parte esterna in metallo e, nel caso delle telecamere dome, rivestimenti a resistenza elevata. Ciò consente di prolungare la durata di ogni telecamera e assicura che le immagini non siano distorte da graffi sugli obiettivi. Una valvola di sfiato consente la fuoriuscita del vapore acqueo prevenendo l'accumulo di umidità e il potenziale danneggiamento del dispositivo.

X-core e X-plus a confronto

La nuova gamma della serie X con funzioni AI è suddivisa in telecamere X-core e X-plus con la gamma X-plus che offre un design modulare che semplifica di molto le operazioni di installazione, il supporto fino a 120 fps per un'acquisizione dei movimenti senza interruzioni, una maggiore efficienza dell'illuminazione IR.

Capacità AI maggiori prestate al video

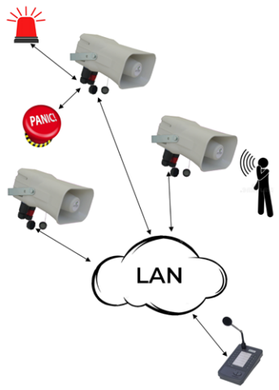
Uri Guterman, Head of Product & Marketing per **Hanwha Techwin Europe**, ha detto sulla nuova gamma della serie X: *"L'AI Deep Learning sta assumendo un ruolo sempre più fondamentale per la sicurezza considerata la maggiore quantità di video che questo reparto deve gestire. Sono orgoglioso che Hanwha Techwin Europe stia contribuendo a ridurre il numero di falsi allarmi e a integrare la business intelligence basata sull'edge e una qualità delle immagini migliorata dall'AI in una gamma più ampia di telecamere. Ciò consente di rendere gli operatori ancora più efficienti sia per la notifica di eventi in tempo reale che per la ricerca post-evento. Inoltre, rende l'AI più accessibile alle aziende che in passato erano convinte che questa tecnologia fosse troppo costosa per essere impiegata per applicazioni che non fossero high-end. Questa decisione preannuncia il futuro del video nella sicurezza".*

Hanwha Techwin Europe

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

Un punto di allarme con una tromba POE

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



Nell'ambito della diffusione sonora, le trombe e gli altoparlanti in IP con alimentazione POE costituiscono un elemento di sicuro interesse per la facilità con la quale consentono di realizzare un sistema di diffusione sonora disponendo solamente di una rete dati (LAN) anche condivisa con altri sistemi (ad esempio la TVCC).
La gamma di altoparlanti POE offerta da **ERMES** include apparati per montaggio a soffitto, a parete come anche trombe da esterno.
In particolare la tromba **SoundLAN-POE.T10C** implementa la funzione di TalkBack che permette di utilizzarla in modalità reversibile.
Infatti, oltre a riprodurre l'audio, consente di captare le voci e i suoni nelle vicinanze del punto di installazione che invia all'operatore del posto centrale, implementando così la funzione di ascolto ambientale ma consentendo anche di dialogare con la persona presente nelle vicinanze della tromba.
La **SoundLAN-POE.T10C** gestisce inoltre un pulsante di allarme esterno e pilota un lampeggiatore consentendo di realizzare un completo punto di segnalazione delle emergenze.
Attivando il pulsante, la tromba diffonde autonomamente una segnalazione sonora (o un messaggio di alert registrato a bordo), attiva il lampeggiatore associato e segnala l'evento sulla console dell'operatore del posto centrale.
Questi, a sua volta, potrà abilitare l'ascolto ambientale, diffondere un messaggio appropriato mediante il microfono della console o instaurare una conversazione con la persona presente nei pressi della tromba.
In definitiva, la **SoundLAN-POE.T10C** non è una semplice tromba POE ma un completo terminale audio di sicurezza che svolge molteplici funzioni in maniera integrata.

essecome ONLINE

n. 02/2022
Anno XLII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Tommaso Di Noia, Paolo Furlan, Federica Maria Rita Livelli, Gianluca Mauriello

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