essecome ONLINE 06/18

Periodico digitale di informazione di security & safety

2018 · ANNO XXXVIII

I SEMINARI DI ESSECOME

LINEE GUIDA

PER I CONTRATTI DI APPALTO DEI SERVIZI DI VIGILANZA E DI SICUREZZA PER IL MONDO DEL RETAIL

Milano, 26 ottobre 2018 – Hotel Hilton Milan

ANIVP · CERSA · LABORATORIO PER LA SICUREZZA · LENCHI STUDIO LEGALE · Studio Legale Associato Moro Avvocati Giuslavoristi Torino-Como

essecome · securindex.com

L'editoriale

Videosorveglianza, strumento di sicurezza o pericolo per i diritti umani?

Si estende a livello mondiale la preoccupazione per la sicurezza delle telecamere cinesi. Dopo la legge US del 13 agosto che proibisce l'acquisto di nuove telecamere e impone di smantellare quelle già installate negli uffici governativi, anche il dipartimento della difesa australiano si è impegnato a rimuoverle dalle strutture delle proprie forze armate.
Da cosa sono state provocate decisioni così drastiche da parte di amministrazioni che hanno comprato per anni vagonate di telecamere dall'imbattibile rapporto tra prezzo e qualità (delle immagini), per sorvegliare città, uffici, basi militari, aeroporti, metropolitane, tribunali, ambasciate all'estero, eccetera?
Il motivo dichiarato è quello di un pericolo per la sicurezza nazionale.
Le inchieste del Daily Mail e del Wall Street Journal del 2016 avevano svelato che il maggior produttore mondiale è controllato dallo stato cinese e avevano sollevato il sospetto che le telecamere IP possano venire utilizzate anche per convogliare in Cina le immagini di persone seguite dal governo cinese mentre si trovano in paesi occidentali, a insaputa degli interessati e degli (incauti) responsabili della sicurezza di quei luoghi.
È da supporre che il governo US e adesso quello australiano abbiano riscontrato la fondatezza di questi sospetti, agendo di conseguenza.

Fantascenza o fantapolitica? Gli esperti dicono che, almeno sul piano tecnico, non è un'ipotesi impossibile.
Come noto, le telecamere in rete sono dotate di indirizzo IP che può venire violato, come qualsiasi ogni oggetto IoT, dal pc allo smartphone, dall'impianto domotico alla stampante, eccetera.
Di conseguenza, le immagini riprese possono venire deviate, sottratte, cancellate o modificate da agenti esterni, teoricamente in qualsiasi momento.
Inoltre, la geolocalizzazione a bordo degli apparati consente di sapere dove sono posizionate le telecamere tanto ai gestori ufficiali quanto ai "gestori" sotto traccia, che possono così scegliere quali visionare per seguire le scene di loro interesse, magari in diretta.
A questo già inquietante scenario si aggiungono i più recenti sviluppi dei software di analisi video per il riconoscimento facciale, per i quali il governo cinese (ma non solo) sta investendo miliardi di dollari per tenere sotto controllo ogni angolo del paese, per individuare in qualsiasi momento in qualsiasi luogo persone, non solo dissidenti e non solo cinesi.
Ma le preoccupazioni per le telecamere cinesi non sono legate solo alla privacy dei cittadini occidentali o a questioni di sovranità nazionale: secondo la BBC, il governo cinese starebbe compiendo pesanti azioni repressive nei confronti dell'etnia musulmana Uyghurs nella regione di di Xinjiang, avvalendosi anche dei sistemi di sorveglianza realizzati dai due maggiori produttori nazionali (Hikvision e Dahua). Per questo, 17 deputati US hanno chiesto al Congresso di sanzionare questi produttori con l'espulsione dal mercato nord-americano, "per gravi violazioni dei diritti umani".

È auspicabile che queste notizie risveglino anche nel nostro paese l'attenzione in tempi brevi sull'affidabilità delle telecamere per la videosorveglianza, di chi le produce e di chi le gestisce, dal momento che stanno evolvendo da strumenti per la sicurezza dei cittadini e dei loro beni a strumenti potenzialmente pericolosi non solo per la privacy, ma anche per i diritti fondamentali dell'uomo.
Anche a casa nostra, non solo in altri paesi.

Sommario Interattivo

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

Cover Story

LINEE GUIDA PER I CONTRATTI DI APPALTO DEI SERVIZI DI VIGILANZA E DI SICUREZZA PER IL MONDO DEL RETAIL

Gli operatori della vigilanza rappresentati da ANIVP e i security manager del retail che aderiscono al Laboratorio per la Sicurezza hanno ritenuto opportuno sviluppare, con il supporto specialistico dell'organismo di certificazione CERSA S.r.l. e degli studi legali Lenchi di Vigevano e Moro di Torino, delle Linee Guida per sviluppare i contratti di appalto dei servizi di vigilanza e di sicurezza. Le Linee Guida intendono fornire sia alle aziende del retail, tra i maggiori utilizzatori di servizi di vigilanza e sicurezza, che ai loro fornitori, gli istituti di vigilanza e le imprese di servizi fiduciari, indicazioni operative utili per realizzare efficaci relazioni contrattuali in reciproca tutela, nel rispetto delle normative giuslavoristiche e di Pubblica Sicurezza.
Fra queste si ricordano il DL 25/2017 che ha sancito la responsabilità solidale del committente per gli eventuali debiti retributivi e contributivi dell'appaltatore verso i dipendenti di quest'ultimo che hanno lavorato presso il committente, e il DM 115/2014 con cui si è data attuazione al processo di qualificazione degli istituti di vigilanza stabilito dal DM 269/2010 e successivi.
I contenuti del documento sono applicabili da parte di qualsiasi categoria di utilizzatori di servizi di vigilanza e di sicurezza, in un'auspicata ottica di "sanificazione" di un mercato che, in particolare negli ultimi anni, ha visto spesso prevalere logiche solamente economiche a discapito della qualità dei servizi e della tutela dei diritti dei lavoratori.
Un fenomeno che interessa decine di migliaia di persone che contribuiscono in modo determinante e sistematico alla sicurezza dei cittadini e del territorio a supporto delle Forze dell'Ordine, che le Linee Guida si propongono di contrastare partendo dalla consapevolezza delle responsabilità delle parti contraenti.

AGENDA

14:30 - Presentazione del seminario
Raffaello Juvara - direttore essecome/securindex

14:40 - Introduzione alle Linee Guida
Giuseppe Mastromattei - Presidente Laboratorio per la Sicurezza, Marco Stratta - Segretario Generale ANIVP

15:20 - Il valore della certificazione alla Norma UNI 10891:2000 - DM 269/2010
Maurizio Grandi - Amm.re delegato CERSA

15:40 - Indicazioni per la stesura di un contratto di appalto dei servizi di vigilanza e di sicurezza
Avv. Laura Lenchi, Avv. Ezio Moro

16:20 - Sicurezza partecipata: quale ruolo per i privati nel 2018?
Autorità di Pubblica Sicurezza - Rappresentanti delle categorie di Utenti (ABI, AIPSA, Confesercenti, Laboratorio)
Rappresentanti delle categorie di fornitori di servizi di vigilanza e sicurezza

18:00 - Conclusioni (mozione finale)

Quando la security diventa una scienza

a colloquio con Paola Guerra, Fondatore e Direttore Scuola Internazionale Etica & Sicurezza Milano - L'Aquila
a cura di Raffaello Juvara

Sul piano neurologico, sono state accertate condizioni diverse tra la percezione di sicurezza (sensazione di non essere esposti a pericoli) e quella di insicurezza, tali da influire sulle reazioni degli individui in caso di emergenza?

Vi sono importanti testimonianze nel corso dei secoli - dai poemi di Erodoto alle tragedie di Eschilo, Sofocle ed Euripide, dalla medicina antica di Ippocrate alla filosofia di Platone e nei poemi didascalici di Lucrezio - dell'attenzione agli aspetti psicologici delle persone e delle popolazioni in emergenza e dei relativi comportamenti in situazioni di sicurezza e non.

Seneca (N.Q. VI, §1 e §29), per esempio, filosofo, scienziato, maestro di vita di Lucillo che potremmo definire psicologo ante litteram, rivolgendosi al discepolo, fa una breve ma modernissima trattazione degli effetti del terremoto sulla mente degli uomini causati dal sisma della Campania nel quale è "sprofondata" Pompei (5.2.62 d.C.) e scrive: *"Alcuni si sono messi a correre qua e là come forsennati e storditi per effetto della paura, che scuote le menti quand'è personale e moderata… certo nessuno prova un grande spavento senza pregiudicare un po' la sua sanità mentale, e chi ha paura è simile a un pazzo: ma la paura ben presto fa tornare in se stesse le persone, alcune invece le sconvolge con più violenza e le porta alla follia"* (Seneca, ivi, 633-634).

Le osservazioni psicologiche di Seneca conservano ancora oggi tutto il loro valore. Definiscono con acume e appropriatezza quasi diagnostica la tipologia delle risposte dei sopravvissuti al terremoto, dalle reazioni motorie "correre come forsennati" a quelle cognitive "stordimento, smarrimento", emotive "dolore, paura, terrore, panico, spavento" e mentali "le menti sono scosse, escono da sé, sconvolte con violenza e portate alla follia".

Le neuroscienze hanno dedicato molta attenzione alle basi neuronali dei processi mentali quali il linguaggio, la percezione, l'attenzione e la memoria.

La ricerca più recente si è interessata alle basi neurobiologiche delle emozioni, con un approccio che si fonda sull'idea che almeno le emozioni primarie siano il prodotto di sistemi neuronali filogeneticamente antichi e anatomicamente definiti, che si sono evoluti per consentire la sopravvivenza dell'individuo e della specie. Le neuroscienze comportamentali, cognitive classiche ed infine quelle definite "affettive" offrono un approccio interessante che prende in considerazione i processi mentali di base, le funzioni cerebrali e i comportamenti emotivi comuni a tutti i mammiferi, per localizzare i meccanismi neurali dell'espressione emotiva.

Joseph LeDoux, il neuro scienziato autore del saggio "The emotional brain" (1996), sostiene che le emozioni primarie come la paura siano governate dall'amigdala - piccola struttura a mandorla collocata nella regione del lobo temporale mediale del cervello, parte del sistema limbico - coinvolta nei sistemi della memoria emozionale e nel sistema di comparazione degli stimoli ricevuti con le esperienze passate e nell'elaborazione degli stimoli olfattivi che gestisce, in particolare, la paura.

Questo studio ha dimostrato come nei pazienti che presentano una lesione di questa formazione nervosa, la nozione di pericolo pare essere quasi inesistente. Secondo

LeDoux e Damasio, le emozioni di base come paura e rabbia prima vengono attivate dalla amigdala che reagisce ai segnali di allarme provenienti dagli organi di senso, scatenando le reazioni nell'organismo e poi vengono elaborate dalla corteccia cerebrale. La peculiarità dell'amigdala deriva dalle caratteristiche delle sue connessioni: riceve infatti numerose fibre dai recettori uditivi e visivi ed è quindi in grado di rispondere immediatamente ai messaggi che indicano una situazione di pericolo, trasformandoli in reazioni di paura o di rabbia. Pare quindi evidente come, a livello neurologico, si manifestino condizioni differenti e quindi azioni differenti tra uno stato di sicurezza e uno di insicurezza.

Il sistema limbico (e in particolar modo l'ippocampo) elabora gli stimoli provenienti dall'ambiente, al fine di costruire una rappresentazione della situazione e di organizzare risposte efficaci di evitamento degli stimoli ansiogeni. La corteccia analizza complesse informazioni, codifica memorie e apprendimenti e integrando le esperienze, dà loro un significato; il sistema limbico, invece, ha una origine filogeneticamente piu' antica, ci accomuna, per modalità di reazione, alle emozioni di altre specie animali, come ha illustrato il neuro scienziato Paul McLean (MacLean, 1990). L'amigdala svolge funzioni specifiche sia perché è un nucleo anatomicamente complesso, sia perché si trova al centro di una intricata rete di connessioni neuronali del cervello. La peculiarità dell'amigdala deriva dalle caratteristiche delle sue connessioni: riceve infatti numerose fibre dai recettori uditivi e visivi ed è, quindi, in grado di rispondere immediatamente ai messaggi che indicano una situazione di pericolo, trasformandoli in reazioni di paura o di rabbia. Queste reazioni sono molto più rapide di quelle che arrivano dalla corteccia che viene informata solo in un tempo successivo rispetto all'amigdala. Gli stimoli che generano paura vengono indirizzati verso la corteccia dopo esser pervenuti all'amigdala. Solo in un secondo momento la corteccia può analizzare, paragonare, razionalizzare: l'amigdala, dunque, reagisce prima che la corteccia sia informata di cosa stia accadendo, e questo perché l'emozione viene attivata prima del pensiero cosciente, solo successivamente interviene l'elaborazione della corteccia. I segnali provenienti dagli organi di senso raggiungono dapprima il talamo, poi arrivano all'amigdala; un secondo segnale viene inviato dal talamo alla neocorteccia. Questa ramificazione permette all'amigdala di rispondere agli stimoli prima della neocorteccia: quando valuta uno stimolo come pericoloso, l'amigdala reagisce inviando segnali di emergenza a tutte le parti principali del cervello; stimola il rilascio degli ormoni che innescano la reazione di combattimento o fuga (adrenalina, dopamina, noradrenalina), mobilita i centri del movimento, attiva il sistema cardiovascolare, i muscoli e l'intestino. Contemporaneamente, i sistemi mnemonici vengono attivati per richiamare ogni informazione utile nella situazione di paura.

In che modo le neuroscienze possono contribuire alla prevenzione ed alla gestione degli effetti di situazioni di panico collettivo, conseguenti ad eventi improvvisi come, ad esempio, i fatti di piazza San Carlo a Torino nel 2017?
Quanto è successo la sera del 3 giugno in Piazza San Carlo a Torino in occasione della finale di Champions League tra Juventus e Real Madrid ha nuovamente confermato come eventi nati come momenti di svago, nel momento in cui non si ponga la giusta attenzione alla pianificazione della sicurezza, si possano trasformare in situazioni drammatiche.
Certamente le neuroscienze possono considerarsi implicate nella prevenzione e nell'eventuale gestione di tali eventi, ma solo come importanti strumenti di conoscenza.
I professionisti devono necessariamente conoscere i meccanismi mentali relativi agli stati di shock e di panico e le reazioni individuali e di massa, se vogliono pianificare azioni preventive e gestionali efficaci.
Quindi, la risposta alla domanda è inevitabilmente un "dipende". Dipende da quali scelte vengono fatte a priori sulla formazione e sulla preparazione degli uomini della sicurezza.
La Circolare Gabrielli – relativa proprio alla gestione di questi eventi - fa appello, tra l'altro, alla collaborazione tra forze pubbliche e forze private, quale elemento essenziale per la gestione in sicurezza degli eventi.
Formazione sulle neuroscienze, professionisti di alto profilo, collaborazione tra pubblico e privato, integrazione dei ruoli: sono tutti fattori imprescindibili.

In generale, quali sono le modalità con le quali neuroscienze e scienze comportamentali (criminologia, vittimologia) possono supportare i responsabili della sicurezza pubblica?
La cultura della sicurezza sta cambiando, seppur questo mutamento sia ancora troppo lento. Di fronte a necessità sempre più complesse, è ormai assodato il bisogno di collaborazione tra ruoli per ottenere realmente dei risultati concreti. Occorre abbandonare l'idea della sicurezza associata alla sola tutela fisica. La security è una scienza, e le azioni di prevenzione e sicurezza sono il risultato prima di tutto di studio, di analisi concreta dei casi, di conoscenza, di comparazioni, di programmazione e poi anche di azioni sul campo. Criminologia, vittimologia, a seconda dei singoli casi, permettono di svolgere analisi dettagliate e puntuali, utili ad approntare misure di sicurezza efficaci. Il punto non è il pubblico o il privato, ma la preparazione del professionista e la possibilità/capacità di interazione. Lavorare in team è imprescindibile ormai.

Sicurezza partecipata: ci sono possibili termini di relazione tra pubblico e privato per prevenire o mitigare le minacce alla sicurezza, basati sulle ricerche in campo neurologico?
Certamente, desidero fare riferimento in particolare agli studi dell'equipe di Giacomo Rizzolatti dell'Università di Parma che già a metà degli anni '90 ha scoperto la presenza anche negli uomini dei "neuroni specchio". Questi sono neuroni motori che entrano in azione in tre circostanze: quando una persona compie un'azione, quando si vede la stessa azione compiuta da un'altra persona e quando l'azione è pensata, immaginata. Dagli studi più recenti, emerge che parte di questi neuroni sono presenti fin dal momento della nascita, altri si sviluppano nel corso della vita e sicuramente il loro affinamento avviene a contatto con la realtà e le esperienze.
Gli stessi modelli di apprendimento degli individui si basano fortemente sul "sistema specchio". Tutto questo ha una rilevanza significativa nel processo di formazione delle persone in materia di safety e security. La formazione del personale deve tenere conto dei modelli di apprendimento che il nostro cervello usa.
L'apprendimento, basandosi sulla costruzione equilibrata di collegamenti tra la parte teorica e quella pratica, deve migliorare la memoria della prestazione e diventare un modello mentale.
Partendo da questi assunti, è chiaro come l'allievo, per imparare, abbia necessità di ascoltare, vedere e mettere in pratica. Grazie al sistema dei neuroni specchio le azioni viste vengono trasformate in azioni possibili, mentre la mancata ripetizione delle azioni viste comporta lo svanire delle attivazioni neuronali, come se il cervello cancellasse le informazioni. Gli studi scientifici indicano inoltre che, i neuroni specchio entrano in risonanza con le emozioni del nostro interlocutore, facilitando la lettura e la comprensione delle emozioni attraverso dei *"micromessaggi"* che l'interlocutore invia. Per questo motivo è fondamentale la coerenza e la congruenza tra i segnali para-verbali e non verbali e la comunicazione verbale.
In questo quadro, per avere persone preparate a gestire emergenze in modo efficace, è chiara l'importanza di formazione teorica e pratica oltre che di simulazioni che aiutino ad apprendere e valorizzare meglio gli aspetti relazionali e la guida coerente delle azioni più adatte alla gestione delle situazioni critiche.
Parlare di sicurezza partecipata significa prevedere un'interazione tra pubblico e privato con l'obiettivo di formare professionisti che siano punti di riferimento, identificabili e affidabili nelle situazioni di emergenza. Occorrono comportamenti omogenei, professionisti pronti e preparati a collaborare, "guide" da seguire e piani d'azione studiati e gestiti da profili differenti ma complementari. Sempre di più auspichiamo quindi l'aumento delle azioni formative ed esercitative congiunte tra forze dell'ordine, operatori del soccorso e gestori di emergenze di aziende private.

Il ruolo centrale del Security Manager nel partenariato pubblico-privato per la Sicurezza Nazionale

a colloquio con Andrea Chittaro, presidente AIPSA
a cura di Raffaello Juvara

A seguito della recente scomparsa di Sergio Marchionne, alcune interpretazioni giornalistiche hanno messo in discussione il ruolo della sicurezza di FCA che, per rispettarne la privacy, non avrebbe tutelato a sufficienza gli interessi degli azionisti. Quali sono i confini tra l'assolvimento di un compito aziendale e l'etica personale che può portare, al limite, a rispettare e difendere la privacy di una persona anche andando contro gli interessi dell'azienda e dei suoi azionisti?

Ovviamente non entro nel merito di vicende specifiche. Posso però affermare che, come mi ha ricordato di recente un collega, lo stereotipo di una security da "epica di Caterino Ceresa" dovrebbe aver abbandonato non solo l'immaginario collettivo ma ancor più la quotidianità della vita aziendale. Etica, trasparenza, compliance, processi strutturati, sono i driver che indirizzano oggi, o dovrebbero farlo, l'operato dei professionisti della security aziendale propriamente intesi. E da soli sono sufficienti, a mio avviso, a rispondere alla seconda parte della domanda. Quale interesse che voglia definirsi legittimo può superare il rispetto di un codice etico o il diritto di ognuno alla protezione dei propri dati personali, a maggior ragione se "sensibili"? A mio modo di vedere nessuno.

Il responsabile della sicurezza fisica aziendale è oggi sottoposto a nuove sfide: la trasformazione digitale dei processi aziendali, l'arrivo di nuove tecnologie per la sicurezza e, di conseguenza, l'evoluzione del concetto stesso di security aziendale. Quali sono le valutazioni sue in materia e di AIPSA, l'associazione che lei presiede?

Anche in questo caso è necessario superare schemi desueti. La sicurezza fisica, del pari la sicurezza delle informazioni o "l'affascinante" ed iperenfatizzata cyber security, sono domini verticali di un sistema più articolato di gestione della sicurezza in azienda. Oggi i limiti tra spazi fisici e logici sono sempre più indefiniti, le minacce sempre più asimmetriche. Ecco perché deve affermarsi convintamente all'interno delle aziende un modello di gestione "olistico" della sicurezza, che viva di luce propria e sia dotato della necessaria autonomia rispetto alle altre funzioni. E, effettivamente, le prime "prese di coscienza" di questa esigenza cominciano a evidenziarsi, con grandi società che stanno implementando percorsi virtuosi e strumenti organizzativi coerenti con il valore di avere un centro di competenze unico per la loro sicurezza, in grado di presidiare efficacemente tutta una serie di ambiti il cui governo "parcellizzato" è sempre stato fonte di diseconomie e disfunzionalità diffuse. Questo è uno degli impegni principali che ci siamo presi come nuovo Direttivo di AIPSA in coerenza con quanto fatto dal precedente; promuovere

cultura e consapevolezza prima di tutto presso coloro che decidono come debba essere organizzata un'azienda anche dal punto di vista della sicurezza: società di consulenza strategica, Capi del personale, società di head hunting oltre ai principali decision maker ovviamente, membri di Board e Top Management. Solo se sapremo ben rappresentare, nel concreto, questo valore arriveremo a modelli consolidati nei quali una Direzione Security avrà la stessa, strutturata dignità di una Direzione Legale o HR.

Dal suo punto di vista, i security manager attuali sono adeguatamente formati rispetto alle nuove sfide? Le release della norma 10459, pubblicate dopo i necessari periodi di gestazione, possono rispondere all'evoluzione continua e rapidissima dell'attuale contesto operativo?
Già il fatto di avere una norma, seppur su base volontaristica, che definisce i requisiti professionali di chi è chiamato a svolgere un ruolo così delicato in azienda è un buon punto di partenza. Qualche passo in più andrebbe fatto sul fronte della normativa cogente. Se il D.lgs 81/2008 ha giustamente ritualizzato e rinforzato le previsioni relative alla safety non si comprende perché analogo percorso non debba essere seguito per quanto attiene la security, magari con un semplice intervento sul corpo normativo già esistente.
La valutazione del c.d "rischio di security" non è una facoltà bensì un obbligo per le figure datoriali. Che nel farlo non possono che essere supportate da coloro che possiedono le necessarie competenze in materia. Anche qui senza calarci in casi specifici, l'avere sottostimato questi particolari rischi, ad esempio in teatri internazionali complessi, ha avuto conseguenze rilevanti sia di natura legale che di ordine reputazionale per le aziende coinvolte. Il legislatore dovrà essere adeguatamente stimolato al riguardo. Ho partecipato, qualche anno fa, ad un interessantissimo studio condotto da ANMIL in collaborazione con alcune grandi aziende italiane tra le quali ENI, Snam, Saipem e Leonardo Finmeccanica, che ha messo in luce i limiti dell'attuale ordinamento, avanzando proposte di intervento concrete. Al termine della passata legislatura è stato illustrato a rappresentanti parlamentari di ogni schieramento e devo dire che ha riscosso grande attenzione. Confido che il tema potrà trovare utile riproposizione nell'attuale legislatura.

Nel rapporto con le istituzioni deputate alla sicurezza nazionale, come sta evolvendo il partenariato pubblico-privato nel nostro paese?
Devo ammettere che, rispetto agli anni passati, c'è più attenzione e proattività da entrambe le parti. Certo i modelli messi in campo hanno bisogno di ulteriori affinamenti e, soprattutto, di tradursi in un metodo di lavoro strutturato e biunivoco. La Sicurezza Nazionale non può non avere tra i propri obiettivi prioritari la tutela, in ogni contesto, dei motori dell'economia del paese. Non dimentichiamo, poi, che le più importanti reti infrastrutturali sono gestite da società

private. In questo senso, dal riconoscimento formale verso l'esterno del ruolo del security manager potrebbe derivare un contributo decisivo allo sviluppo di canali di cooperazione "trusted", trasparenti e riconosciuti sulla scorta dell'esempio di altri paesi. Su questo esistono già accordi di collaborazione di singole imprese ma anche come AIPSA stiamo lavorando alla stipula di protocolli che possano servire quali utili indirizzi per tutti. Ne abbiamo già definito uno lo scorso anno con l'Arma dei Carabinieri ed abbiamo avviato delle discussioni propedeutiche con il Dipartimento di Pubblica Sicurezza per un progetto ambizioso quanto, a mio avviso, non troppo difficile da realizzare: una sorta di albo dei responsabili delle strutture di sicurezza aziendali a disposizione delle pubbliche Autorità in caso di emergenze, crisi o comunque per qualsivoglia interlocuzione in materia. Una casa comune si costruisce dalle fondamenta e non dal tetto.

In conclusione: Mastromattei, presidente dell'associazione Laboratorio per la Sicurezza, ha lanciato recentemente con un suo articolo una provocazione, paragonando il security manager al ten. Drogo di Dino Buzzati, "intrappolato" nella Fortezza Bastiani nel deserto dei Tartari. Lei cosa ne pensa, è veramente così?
Il collega che apprezzo e stimo ha descritto con originale efficacia una condizione alla quale il security manager dovrebbe essere oramai estraneo. Certo sta a noi evitare di essere confinati o, ancor peggio, di auto confinarci all'interno delle "mura del castello" che, peraltro, sono state violate variamente nel tempo. Chi gestisce la security deve farlo, oltre che con la necessaria professionalità, con "spirito di servizio". Deve accostarsi ed approcciare le esigenze di tutte le funzioni aziendali con discrezione e capacità di farsi percepire quale supporto fattivo agli obiettivi di ognuno piuttosto che come impositore di regole stringenti e, talvolta, fini a se stesse. Deve essere in grado di affrontare il pur complesso mondo della difesa e della protezione aziendale con un imprinting "lean" che non spaventi l'interlocutore di turno. Siamo gestori di rischi e il nostro mestiere, per definizione, "evoca il fantasma del danno". Ribaltare questa percezione e trasformarla in una presa di coscienza del valore che un valido modello di sicurezza può apportare nel quotidiano del business resta uno degli obiettivi più sfidanti per il security manager.

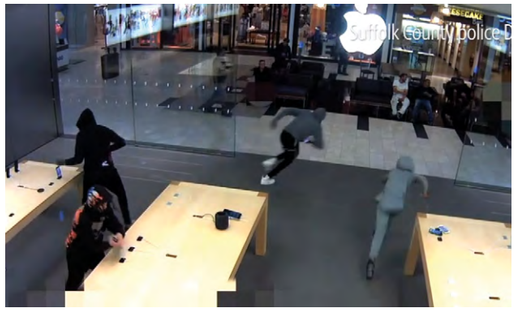
L'evoluzione globale del crimine organizzato nel Retail

di Giuseppe Mastromattei, presidente del Laboratorio per la Sicurezza

È ormai consolidato il fatto che le abitudini dei consumatori e delle metodologie di acquisto, nell'era dell'omnicanalità, siano radicalmente cambiate.
Ma questo cambiamento non ha interessato solamente i consumatori, esiste un'altra categoria che ha modificato il proprio *modus operandi*: si tratta della criminalità organizzata nel Retail.
Questo fenomeno, meglio conosciuto come "ORC" (Organized Retail Crime), è da qualche anno oggetto di approfondite analisi e studi, soprattutto nei paesi nordeuropei e nord americani.
Ma di che cosa si tratta?
Il crimine organizzato nel *Retail* è il furto su larga scala della merce esposta nei negozi con l'intento di rivenderla per ottenere un guadagno finanziario. Viene definito "organizzato" in quanto coinvolge tipicamente un'associazione criminale che impiega gruppi di individui che rubano grandi quantità di merce da un determinato, e aggiungerei pianificato, numero di negozi: operazioni criminali finalizzate ad ottenere immediata disponibilità di denaro, senza correre troppi rischi.
Infatti, la merce rubata viene, con semplicità ed in assoluta tranquillità, rivenduta immediatamente su siti web, nei mercatini e talvolta anche ad altri rivenditori. Oltre ai negozi, le *"bande ORC"* hanno come obiettivo intere spedizioni di merce caricate sui camion diretti ai punti vendita e, per rimanere al passo con i tempi, una serie di altre frodi come l'uso di carte di credito rubate o clonate (*skimming*) per ottenere merci, la modifica o sostituzione dei codici a barre per pagare prezzi inferiori e la restituzione di merce rubata per ottenere denaro o carte regalo *(return fraud*) ed altro ancora.
Il crimine organizzato nel Retail deve essere chiaramente distinto dal taccheggio ordinario, ovvero dai furti commessi da individui che cercano beni per uso personale.
Si stima che, solo in Nord America, il crimine organizzato sia costato alle aziende del Retail quasi 30 miliardi di dollari l'anno, con il 95% dei *retailer* intervistati da NRF (National Retail Federation) nel 2017[1] , che ha dichiarato di essere stato

vittima di questo fenomeno, mentre il 67% ha riscontrato che il numero di eventi collegati era cresciuto notevolmente rispetto all'anno precedente.
Ovviamente anche queste perdite contribuiscono all'aumento dei costi ed al conseguente aumento dei prezzi per i consumatori.
Ma, da quanto analizzato, non si tratta solo di un danno economico: a quanto risulta, il proliferare di queste attività criminali sta diventando anche una vera e propria minaccia per l'incolumità dei lavoratori dei negozi. Un quarto dei *retailer* intervistati, sempre nella ricerca condotta da NRF, ha dichiarato di aver constatato direttamente un aumento dell'aggressività da parte di criminali che non si è limitata alle sole minacce verbali al personale, ma anche attraverso l'utilizzo di strumenti offensivi come l'uso di spray urticanti ed altro.
Un altro obiettivo del crimine organizzato sono gli articoli come i farmaci non soggetti a prescrizione o latte artificiale, che, dopo essere stati immagazzinati spesso in modo improprio, vengono venduti dopo la scadenza o "tagliati" in quantità maggiori, creando seri rischi per la salute.
Infine, una precedente analisi sempre condotta da NRF, ha rilevato che il crimine organizzato nel Retail è un crimine definito

[1] https://nrf.com/system/tdf/Documents/retail%20library/Organized%20Retail%20Crime%20Survey%202017.PDF?file=1&title=2017%20Organized%20Retail%20Crime%20Survey



in inglese *"Gateway Crime"*, ovvero un crimine "di passaggio" con lievi conseguenze penali ma propedeutico a commettere successivamente crimini peggiori, come dimostra il fatto che il 45% di coloro che sono stati arrestati avessero anche precedenti per droga, traffico di armi ed altri crimini.
Ovviamente, considerata la tipologia del crimine, questi individui, organizzati, non si limitano ad un solo evento, ma agiscono quasi indisturbati su tutto il territorio con metodologie definite a tavolino, specifiche per ogni singolo punto vendita e per ogni marchio.
Analizzano le vulnerabilità e predispongono dei veri e propri piani criminali, ripetendoli fino a quando non vengono messe in campo soluzioni specifiche a protezione della merce messa in vendita.
Un esempio è la frode attuata attraverso il cambio del codice a barre dei prodotti laddove, in presenza di postazioni per il pagamento self service (il cosiddetto *self check out*), non sono stati predisposti adeguati controlli e misure di sicurezza. In alcuni casi sono stati riscontrati dei veri e propri "viaggi organizzati" che si sono interrotti solo quando, grazie alla collaborazione con le Forze dell'Ordine ed alla condivisione delle informazioni, è stato possibile arrestare gli autori.
Altre attività criminali, che preoccupano non per il singolo valore di ogni azione, ma per l'impressionante ripetitività, sono quelle connesse ad alcune vulnerabilità dei processi di vendita specifici per i ritorni e i cambi merce o attraverso l'utilizzo illegale e fraudolento delle "gift card".
Al singolo evento non viene dato il giusto valore che avrebbe se venisse invece considerato in scala su tutto il territorio nazionale, o meglio ancora, continentale.
Senza considerare l'aumento delle effrazioni notturne o le rapine, compiute con modalità che, a detta degli investigatori, sono state condotte con operazioni tutt'altro che improvvisate.

In una recente inchiesta de l'Espresso[2], dove si parla di crimine organizzato dedito al furto negli appartamenti in Italia, (l'articolo cita l'episodio che ha visto vittime i genitori del Ministro dell'Interno Salvini) si legge *"Una volta monopolio della piccola delinquenza comune, ora l'industria dei furti è stata conquistata dalle mafie straniere, che con il rigore di organizzazioni militari gestiscono eserciti di ladri sparpagliati in tutta Europa.*
A contendersi il mercato ci sono in particolare tre mafie internazionali. Nel nostro Paese i "signori dei furti" acquistano ville, riciclano i soldi, programmano summit criminali.
Si calcola che il giro d'affari delle razzie solo in Italia ammonti a decine di miliardi di euro all'anno.
Un business redditizio e dai rischi contenuti: quando i ladri vengono catturati, spesso scontano nelle prigioni italiane pochi mesi di detenzione e poi vengono rimpatriati nei Paesi d'origine, dove il reato associativo non viene quasi mai riconosciuto. E dunque tornano subito liberi."
Proprio quello che sta succedendo nel Retail: una vera e propria globalizzazione del crimine, dall'illecito rendimento assicurato, ma soprattutto con rischi assolutamente contenuti.
Anche se le differenze inventariali dovute a furti sono in calo, e il rapporto del Ministero dell'Interno, presentato lo scorso agosto, lo ha confermato, forse sono proprio fenomeni come il crimine organizzato nel Retail che contribuiscono a non far calare la paura tra i cittadini.
Come difenderci allora da questo preoccupante fenomeno? Al momento l'unica soluzione risiede nella capacità di rispondere attraverso una organizzazione di prevenzione capace di analizzare quanto accade quotidianamente e predisporre adeguate misure di sicurezza condivise tra sicurezza pubblica e sicurezza privata.
Ancora una volta la necessità di un concreto progetto di "Sicurezza Partecipata".

[2] http://espresso.repubblica.it/inchieste/2018/08/30/news/cosi-i-signori-dei-furti-est-la-fanno-franca-vittime-salvini-1.326377

La centralità del fattore umano nelle aziende che “fanno sicurezza”

a colloquio con Gianluca Traversa, senior Security Manager
a cura della Redazione

Nel percorso vitale delle imprese di ogni settore, il fattore determinante del successo è la “qualità”, ovvero la conformità al modello che il fondatore ha ideato per produrre un bene o un servizio che interessa una certa moltitudine di clienti. Esistono metodi per tutelare questa qualità, in particolare nelle aziende di servizi?
Nelle imprese di servizi, come in tutte le imprese, le metodologie sono molteplici. Le prime passano attraverso la formazione e l’informazione del personale operativo; le seconde attraverso metodi organizzativi sistematici (ISO 9001, 10891). Basilare è l’innalzamento del livello delle competenze di tutta l’organizzazione, per poter radicare un metodo robusto ai fine di tutelare la qualità totale dell’intera organizzazione. Spesso si intende la qualità come una caratteristica esclusiva del prodotto-servizio: per garantire la qualità, intesa come soddisfazione del cliente, occorre parlare di metodologia di organizzazione strutturata in modo trasversale rispetto tutti i processi partendo dagli stakeholders, alta direzione, process owner e personale operativo. Solo così è possibile garantire la qualità in termini di snellimento dei processi, riduzione dei costi, abbattimento degli sprechi, velocità nella progettazione ed erogazione di servizi con la massima attenzione verso il cliente. Tutto il processo precedente è una macchina sistematica ed autonoma a garantire efficienza ed efficacia da rinvestire nell’organizzazione.

Dalle sue esperienze nel settore della sicurezza, ha dedotto caratteristiche peculiari negli imprenditori che ha frequentato?
Sicuramente gli imprenditori che ho incontrato nel mondo della sicurezza sono accomunati dall’appartenenza ad una categoria ormai scomparsa di persone che credono nella

propria forza-lavoro come unica forma effettiva di sicurezza globale. Di conseguenza però non riescono a calare la vigilanza in un’attività industriale organizzata. Se si guarda il passato, possiamo notare che la possibilità di aggredire il mercato rappresentava per gli imprenditori un metodo funzionale efficiente per il raggiungimento di una buona quota di mercato. Al giorno d’oggi questo metodo presenta molte lacune poiché la pianificazione dei processi, a monte dell’erogazione del servizio, rappresenta il punto di partenza per una buona organizzazione: l’efficienza aziendale è ormai sempre più ridotta e una piccola svista può essere causa di una perdita o di un blocco dello sviluppo dell’impresa.
Voglio porre la vostra attenzione su una citazione del generale britannico Robert Baden-Powell: “Una nazione deve la sua fortuna non tanto alla forza dei suoi armamenti, quanto al carattere dei suoi cittadini”. Analogamente, un istituto di vigilanza deve la sua forza non tanto ai servizi che eroga, ma alle competenze di tutti i suoi collaboratori ed alla consapevolezza del ruolo delicato che vanno a ricoprire.

In che modo è secondo lei possibile motivare le persone, in un settore come la vigilanza, nel quale l’abbattimento dei prezzi di vendita dei servizi parrebbe impedire qualsiasi politica di incentivazione del lavoro e della professionalità?
Innanzitutto il sistema organizzativo interno degli istituti deve essere in grado di poter individuare e valutare le dispersioni di denaro, rendendo l’organizzazione più efficiente e identificando il prezzo di vendita come un’opportunità e non come un rischio. In questo contesto potrebbe essere introdotta una politica di incentivazione non necessariamente quantificabile in denaro, ma capace di motivare e consapevolizzare gli addetti alla vigilanza con competenze, attraverso l’erogazione di attività di formazione, in modo tale da accrescere la propria motivazione personale. Affidare agli addetti obiettivi aziendali per rendere più efficace il loro servizio e far emergere le personalità più brillanti in termini lavorativi, attraverso un percorso di carriera interna, sono alcuni dei mezzi che possono essere utilizzati. Ultimamente abbiamo inserito nei nostri servizi l’attività di team building anche nelle piccole organizzazioni che può essere considerato un mezzo per accrescere la motivazione personale degli addetti: il lavoro di gruppo basato sul continuo confronto di idee e la capacità dell’uomo di mettere il proprio talento al servizio degli altri sono alla base di un team funzionale e vincente in grado di migliorare e motivare le persone che fanno parte.
I risultati ottenuti con tutte le attività sopra citate hanno dato un esito positivo in tutti i nostri clienti; non ultimo la ricerca di attività ludiche da effettuare in gruppo al di fuori delle ore lavorative hanno mostrato il raggiungimento degli obiettivi lavorativi in tempi del 20% più brevi .

Quali suggerimenti o indicazioni ritiene di poter dare per compiere con successo la mutazione da istituto di vigilanza tradizionale a impresa di sicurezza in senso moderno?
Il suggerimento principale è quello di cambiare la mentalità dell’istituto tradizionale tipicamente senza livelli intermedi di responsabilità, introducendo metodi organizzativi come base, quali ad esempio la 9001, 10891 sfruttandone al massimo la potenzialità e non vedendola più come un “bollino” da affiancare al proprio nome.
Partendo da una gap analysis, si dovrebbe andare a calzare un metodo organizzativo con le sue esigenze e peculiarità. Non esistono metodi organizzativi standard. Lo standard è riferito alle normative settoriali e non deve essere concepito come metodo di partenza o fine. Innanzitutto la vigilanza, per poter essere analizzata correttamente, deve essere suddivisa in singoli processi organizzativi, non più concepita come un’unica entità. Attraverso l’introduzione degli indicatori di perfomance, ad ogni singolo processo verrà attribuito la responsabilità del proprio andamento. La trasformazione avviene attraverso la formazione di tutta l’organizzazione: la consapevolezza della necessità di cambiamento porta la direzione a divulgare le problematiche riscontrate. Solo in questo modo la vigilanza potrà iniziare a strutturarsi come industria e non come azienda artigianale. Ritengo che nel mondo di oggi non vi sia differenza nel vendere un prodotto o un servizio: cambiano semplicemente le modalità e non il fine ultimo, ovvero la massima soddisfazione del cliente, migliorando l’efficacia e l’efficienza e investendo con continuità nella ricerca e sviluppo di un settore stagnante.

Quali casi di evoluzione si possono indicare come esempi positivi, anche in settori e aree diverse?
Allemano e io come direzione vantiamo, in oltre quindici anni di attività, svariati esempi di riorganizzazione aziendale in molteplici settori, fra cui FCA per la riorganizzazione di alcuni fornitori in deriva sia in Italia che all’estero. Il nostro metodo, abbinato ai metodi organizzativi di base o specifici di settore (9001, 16949…), hanno dato risultati eccellenti. Abbiamo portato aziende padronali-artigianali a diventare aziende strutturate ed organizzate pronte a recepire nuovi clienti e mercati con il massimo dell’efficienza.
Un esempio del nostro operato riguarda un’azienda estera, caratterizzata da una forte crescita, ma non supportata dall’organizzazione interna, ed inoltre ubicata in un territorio austero come le campagne della Romania. In dieci mesi siamo riusciti a migliorare i processi e di conseguenza il prodotto. Stravolgendo completamente la mentalità di 300 risorse, l’organizzazione ha acquisito la consapevolezza di ogni singolo processo e il pieno raggiungimento della soddisfazione del cliente finale.

OPTEX

RIVELATORI PERIMETRALI DA ESTERNO

Serie BX SHIELD

La prestazione flessibile
incontra il design moderno

HESA

www.hesa.com

WISENET

DOPPIO PUNTO DI VISTA

PNM-7000VD

La telecamera multidirezionale con doppio obiettivo Wisenet P per una massima copertura dello spazio monitorato, flessibilità ed ottima qualità dell'immagine. Una soluzione ideale per il monitoraggio di ampi spazi aperti come parcheggi, centri commerciali e magazzini.

- Due obiettivi indipendenti Full HD da 2 MP offrono un angolo di visione fino a 270°
- A seconda del campo visivo da monitorare è possibile scegliere tra obiettivi da 2,4- 2,8- 3,6 o 6 mm
- Design compatto e poco invasivo: 16 cm di diametro
- Video analisi integrata: rilevamento direzione, face detection, defog, linea virtuale, comparsa/scomparsa, stazionamento e manomissione
- H.264 e Wisestream II: tecnologia di compressione all'avanguardia

hanwha-security.eu/it

Hanwha Techwin

Videosorveglianza e reti Wi-Fi tra “uso privato” e “uso pubblico”

di Angelo Carpani, libero professionista, laureato in Ingegneria elettronica esperto nella progettazione di impianti di videosorveglianza in ambito comunale

1. Introduzione

Molti Enti Locali (Comuni) utilizzano un’unica infrastruttura di rete di comunicazione per trasportare non solo le immagini delle telecamere dell’impianto di videosorveglianza comunale, ma anche per fornire un servizio di accesso alla rete internet ai propri cittadini prevedendo uno o più access point W-LAN (Wireless – Locale Area Network) in uno spazio aperto al pubblico.
Le reti in **Fibra Ottica** e le reti **Wireless** (operanti in banda *Radiolan e Hiperlan*), impiegate normalmente quali infrastrutture di rete negli impianti di videosorveglianza, rientrano tra i sistemi di comunicazione elettronica ad **“uso privato”**, intendendo con esso che la rete deve essere utilizzata soltanto per trasmissioni riguardanti attività di propria competenza, con divieto di effettuare traffico per conto terzi (art.101 del “Codice delle comunicazioni elettroniche” D.Lgs. 259/2003).

2. Quando l’uso da “privato” diventa “pubblico”

Il “Codice” distingue tra due diverse tipologie di utilizzo delle rete **Wi-Fi**[1]:
- uso privato
- uso pubblico

Se un Comune decide di utilizzare l’infrastruttura di rete di comunicazione elettronica dell’impianto di videosorveglianza anche per consentire, in uno spazio aperto al pubblico, l’accesso alla rete internet tramite tecnologia Wi-Fi, l’uso della rete da “privato” diventa “pubblico”. In questo caso non si deve quindi più fare riferimento al Titolo III del Codice *“Reti e servizi di comunicazione elettronica ad **uso privato**”* ma al Titolo II *“Reti e servizi di comunicazione elettronica ad **uso pubblico**”*.
E’ importante però sapere che **l’art.6 del “Codice” vieta espressamente a Stato, Regioni ed Enti Locali di fornire direttamente reti e servizi di comunicazione elettronica ad uso pubblico se non attraverso società controllate o collegate. Per erogare questo tipo di servizi le pubbliche amministrazioni dovranno quindi rivolgersi a operatori autorizzati ai sensi dell’art.25 del “Codice”.**

In quest’ultima situazione è necessario distinguere i seguenti casi:

• **Imprese che hanno come attività principale la fornitura di servizi di comunicazione elettronica. E’ necessaria l’autorizzazione generale,** da richiedere al Ministero dello Sviluppo Economico. Dato che questo tipo di installazione comporta l’uso pubblico, si deve preventivamente essere autorizzati ad agire come ISP (Internet Service Provider), e di conseguenza essere iscritti al ROC (Registro degli Operatori di Comunicazione) presso l’Autorità per le garanzie nelle Comunicazioni (Agcom).

• **Imprese o esercizi commerciali che non hanno come attività principale la fornitura di servizi di comunicazione elettronica.** Secondo quanto disposto dall’art.10 del D.L. 60/2013 (cosiddetto Decreto “del fare”) convertito con legge 9 agosto 2013, n.98. In questo caso l’offerta di accesso alla rete internet al pubblico tramite tecnologia WiFi non richiede alcuna autorizzazione e non prevede l’identificazione dell’utilizzatore.

Per quanto sopra esposto, si consiglia di non utilizzare la rete di comunicazione dell’impianto di videosorveglianza per offrire anche un servizio di accesso alla rete internet ai propri cittadini prevedendo uno o più access point in spazi aperti al pubblico.
In quest’ultima evenienza, l’uso della rete da “privato” diventerebbe “pubblico” con tutte le complicazioni del caso. Attenzione anche a non mettere a disposizione la propria rete dell’impianto di videosorveglianza ad imprese o esercizi commerciali che non hanno come finalità principale la fornitura di servizi di comunicazione elettronica perché, in tal caso, il Comune si troverebbe ad effettuare traffico per conto terzi, cosa vietata dall’art.101 del “Codice” quale conseguenza dell’uso privato.

3. Attenzione agli impianti di videosorveglianza che utilizzano collegamenti wireless a 17GHz.

In alcuni Comuni, a causa della “saturazione” (occupazione) dei canali radio in banda “non licenziata” *Radiolan e Hiperlan*, sono stati realizzati impianti di videosorveglianza con collegamenti wireless che operano nelle banda di frequenza a 17GHz o a 24GHz.

Questi ultimi rientrano, come gli apparati *radiolan e hiperlan*, tra le apparecchiature rispondenti alla raccomandazione della Conferenza europea delle amministrazioni delle poste e delle telecomunicazioni (CEPT) CEPT/ERC/REC 70-03.

L’adeguamento alle direttive europee, il cui obiettivo è quello di una armonizzazione dell’uso delle frequenze da parte di tutti i paesi aderenti, ha spinto il Ministero dello Sviluppo Economico alla **messa al bando delle apparecchiature che operano nella banda intorno ai 17GHz**, modificando, di fatto, il Piano Nazionale delle Frequenze con Decreto del 27 Maggio 2015:

L’immissione sul mercato di apparecchiature a corto raggio per la trasmissione dati a larga banda ad alta velocità (WAS/RLANs) operanti nella banda 17,1-17,3 GHz è consentita fino ad un anno dalla pubblicazione del presente decreto. L’impiego di tali apparecchiature è consentito fino al 31.12.2019. Tali applicazioni rientrano nel regime di “libero uso” ai sensi dell’art. 105, comma 1, lettera b) del decreto legislativo 1° agosto 2003 n. 259 e successive modifiche recante il Codice delle comunicazioni elettroniche (Nota 234).

Ciò significa che è non è più possibile immettere sul mercato nuove apparecchiature che operano in quelle bande, mentre è ancora possibile commercializzare e installare ciò che è l’esistente entro e non oltre il 31/12/2019.

A partire quindi dal 1 gennaio 2020 tutte le installazioni esistenti a 17 GHz dovranno essere spente; in caso contrario, è prevista una sanzione amministrativa (che generalmente cresce esponenzialmente con il numero di siti interessati) e il sequestro dell’impianto.

Per quanto riguarda invece la banda operante nel range di frequenze **24.000-24.250 GHz è armonizzata a livello europeo** è possibile continuare ad utilizzarla e non subirà quindi la stessa sorte del 17 GHz.

[1] Wi-Fi o WiFi è una tecnologia per reti locali senza fili che utilizza dispositivi basati sugli standard IEEE 802.11. Wi-Fi è anche un marchio di Wi-Fi Alliance, la quale consente l’uso del termine Wi-Fi Certified ai soli prodotti che completano con successo i test di certificazione di interoperabilità.

Videosorveglianza IP e cyber security all'evento The Axis Way – Smart Innovation Lab

a cura di Donato Testa, Sales Engineer di Axis Communications

Quando un sistema di videosorveglianza viene utilizzato a fini di sicurezza ha come scopo quello di proteggere persone o cose. Ma cosa succede se non è sicuro il sistema che per sua natura deve offrire protezione?

Questa domanda introduce un argomento di rilevante importanza che, il più delle volte, viene sottovalutato, disatteso oppure non considerato una priorità rispetto ad altri fattori, tra cui il costo.

Sappiamo tutti che, da quando sono state introdotte, le prime telecamere IP sono entrate a far parte di quell'ecosistema di dispositivi chiamati IoT (Internet of Things) e, come per qualsiasi altro oggetto IoT, anche per le telecamere di videosorveglianza i produttori dovrebbero adottare attenzioni sempre maggiori verso il mondo della sicurezza informatica, ancor di più per il fatto che, per loro natura, questi dispositivi catturano e rendono disponibili stream audio e video. Il più delle volte queste informazioni possono essere correlate alla privacy delle persone o ad eventi importanti e, per questo, altamente sensibili.

Diventa quindi necessario avvalersi di produttori che si impegnino ad applicare le migliori pratiche in materia di sicurezza informatica nella progettazione, sviluppo e test dei loro dispositivi, per minimizzare il rischio di difetti che potrebbero essere sfruttati in caso di attacco. Tuttavia, proteggere una rete, i suoi dispositivi e i servizi supportati richiede la partecipazione attiva dell'intera filiera: il costruttore, l'entità che realizza l'impianto (integratore di sistemi) e l'utente finale.

Focalizzandoci sui costruttori, un aspetto particolarmente importante è avvalersi della fornitura di prodotti che siano stati realizzati tramite il principio "security by design", cioè ingegnerizzati prevedendo che ogni componente software

o hardware sia stato sviluppato fin dalla progettazione, ponendo particolare attenzione al tema della sicurezza informatica. Questo, ovviamente, non mette al riparo da rischi di eventuali vulnerabilità o attacchi, ma ne mitiga gli impatti e rende maggiormente accessibili gli update di firmware e/o software per la correzione delle vulnerabilità riscontrate. A oggi ci sono vendor che riescono ad offrire gratuitamente release di update firmware fino a 10 anni per lo stesso device, come avviene per **Axis Communications** con il long-term support (LTS) che rappresenta, di fatto, un valore aggiunto considerevole.

Un altro aspetto non meno importante è che l'azienda costruttrice caratterizzi la propria produzione rifacendosi ai dettami e pratiche indicate dal **CIS, Centre for internet Security**, un'organizzazione no profit che ha come missione l'identificazione, la validazione, la promozione e la divulgazione delle migliori pratiche da mettere in atto per quanto riguarda la difesa informatica.

Quali sono gli attacchi e gli strumenti di difesa informatica e non, ai quali può essere soggetta una telecamera di videosorveglianza IP? Il sabotaggio fisico, il vandalismo e la manomissione. Per proteggere il device da queste minacce, è importante selezionare un modello resistente agli atti vandalici, installarlo nel modo consigliato dal produttore e proteggere i cavi.

Come già detto, da un punto di vista IT, la telecamera è un endpoint di rete in un contesto IoT simile a laptop aziendali, desktop e dispositivi mobili ma, a differenza di questi, non è esposta alla minaccia comune di utenti che visitano siti web o aprono allegati di posta elettronica potenzialmente dannosi, oppure installano programmi o applicazioni non affidabili.

Tuttavia, la telecamera IP è un dispositivo di rete a tutti gli effetti, con un'interfaccia propria che potrebbe compromettere l'intero sistema. Per ridurre potenziali minacce, si raccomanda infatti di non esporre una telecamera di rete come server web pubblico, consentendo l'accesso alla stessa da parte di utenti o clienti sconosciuti.

Per individui e piccole organizzazioni che non gestiscono o si avvalgono di un **VMS (Video Management System)**, il consiglio è quello di utilizzare dei software di gestione della videosorveglianza oggi sempre più disponibili gratuitamente, che supportano un numero limitato di telecamere e/o canali, ma permettono funzionalità avanzate quali registrazioni su evento e visualizzazioni live anche in remoto. I vendor più attenti caratterizzano l'utilizzo di questi software con protocolli di sicurezza avanzati, criptando la comunicazione tra client-device-PC, come avviene con **AXIS Camera Companion**. In un ambiente dove viene invece utilizzato un VMS, i client accedono sempre ai video in diretta e registrati tramite il server. Una buona pratica, se la rete o la funzionalità richiesta lo permette, è quella di posizionare il server VMS e le telecamere su una rete isolata (detta rete **DMZ - DeMilitarized Zone**), tramite isolamento fisico o virtuale, una misura comune e raccomandata, il cui intento è di ridurre l'esposizione e, di conseguenza, i rischi.

Come detto, la necessità di mantenere il sistema di videosorveglianza e quindi le telecamere IP aggiornate all'ultima release firmware è di importanza cruciale, in quanto gli update introducono non solo nuove funzionalità, ma anche tutte le protezioni alle vulnerabilità conosciute al momento del rilascio. Esistono dei software gratuiti, come ad esempio **AXIS Device Manager**, che permettono di eseguire quest'operazione in automatico, avvisando l'amministratore di sistema quando è necessario eseguire l'upgrade, un altro valido strumento che possiamo utilizzare per la gestione di realtà più o meno complesse.

Concludendo, possiamo affermare che oggi c'è bisogno di una sempre maggiore attenzione nei confronti delle problematiche connesse alla protezione di dati presenti nel mondo cyber, che impatta ancora di più nel mondo reale, cogliendo l'opportunità di utilizzare gli strumenti corretti, mitigando quelli che sono i rischi e riducendo i costi associati in caso di attacco informatico.

Questa tematica di grande interesse e attualità sarà approfondita durante l'evento **The Axis Way – Smart Innovation Lab**, una giornata interattiva alla scoperta delle soluzioni trasversali di Axis Communications, in programma giovedì 4 ottobre a Milano presso lo spazio Superstudio Più, nell'ambito della tavola rotonda dal titolo "#Cybersecurity e #GDPR nei sistemi complessi, l'integrazione e la protezione del dato" a cui parteciperanno **Maria Cupolo**, Avvocato Consulente esperto Privacy & Data Privacy Officer, **Pietro Blengino**, Componente Comitato Guida di OSSIF e **Alessandro Manfredini**, Chief Security Officer del Gruppo A2A e Vicepresidente AIPSA.

Le iscrizioni all'evento sono aperte, per maggiori informazioni a questo link è possibile consultare l'agenda completa: http://www.axis-communications.com/TheAxisWaySmartInnovationLab2018

AXIS COMMUNICATIONS

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

La Digital Transformation e il modello ERP per sicurezza fisica aziendale - 2^ parte

di Nils Fredrik Fazzini, CEO di CITEL spa

La divulgazione della consapevolezza dell'importanza del modello ERP per la gestione della sicurezza fisica aziendale è l'obiettivo degli articoli pubblicati nel 2018 da essecome a firma di **Nils Fredrik Fazzini**, CEO di **Citel spa**.
La prima parte era stata pubblicata in essecome online n. 5/2018 **(leggi)**. Il testo completo verrà pubblicato in **essecome quarterly n. 3/2018**, in uscita a ottobre (N.d.R)

Un modello derivato dal sistema informatico gestionale

Il modello ERP in campo gestionale è stato adottato dai grandi gruppi dell'informatica gestionale mondiale, che ormai vivono soprattutto di software e servizi: da IBM a SAP a Oracle; ma anche dalla piccola software house di provincia specializzata ad esempio nelle esigenze del distretto dei calzaturifici locali. Perché ERP è un modello flessibile, che può prescindere dalle dimensioni aziendali sia del produttore che dell'utente finale. Ed anche senza avere nulla a che fare con la contabilità, in quanto quello che conta sono le logiche di complementarietà piuttosto che la natura specifica del processo informatico.
È un modello distribuito ed efficiente per l'informatica gestionale perché permette di comporre catene di produttori e di soluzioni informatiche componibili secondo il progetto o il servizio. Spingendo la selezione della catena non solo alle specializzazioni applicative ma anche adeguandosi nei vari passaggi alla taglia aziendale più adatta, alla distribuzione nel territorio ed all'assistenza di vicinanza.

Il ruolo del life-long project

La necessità di garantirsi un sistema informatico evolutivo, ma allo stesso tempo in grado di preservare l'infrastruttura legacy, portano a considerare il PSIM in una chiave di sistema informatico dipartimentale gestito e sviluppato come progetto permanente. Il che ha delle implicazioni complesse che non possono rientrare in questo documento, salvo la segnalazione che tale caratteristica deve entrare in tutte le decisioni che riguardino il PSIM, le sue aspettative di vita, quelle dei fornitori chiave, oltre alle precauzioni e misure specifiche che possono essere pertinenti alla materia.
A priori, quello che si può considerare ai fini delle aspettative di vita del sistema e dell'azienda che lo produce, è l'aspettativa di vita di quest'ultima, ed anche la misura della stabilizzazione degli stakeholders al riguardo, quali i clienti ed i partner sviluppatori. In definitiva è la comunità di utenti, produttori complementari, integratori, come quella che si è costituita negli anni intorno a Centrax open-PSIM di Citel, a rendere verosimile una lunga aspettativa di vita dell'azienda a garanzia di un ***"life long project"*** che in senso lato corrisponde all'idea dell'utente di vederlo funzionare, migliorare ed evolvere senza trovarsi nella necessità di dover lanciare un progetto sostitutivo con tutte le complicazioni di legacy che comporta.
E non è quindi un caso che chi intende dotarsi di un PSIM impieghi una particolare attenzione nel verificare prioritariamente, al di là delle verifiche consuete sulla società, le referenze storiche, la customer satisfaction, le storie di integrazione che di norma riguardano la protezione degli investimenti legacy degli utenti.

Le valenze generalizzabili del paradigma ERP

Con l'adozione del paradigma ERP per la sicurezza fisica, così come avviene per la gestione aziendale, l'informatizzazione professionale dei processi dipartimentali inerenti la sicurezza fisica, può supportare anche la loro evoluzione grazie al confronto con una comunità che genera condizioni favorevoli all'innovazione di processo: da quelli tradizionali a quelli più recenti e meno definiti ma che vanno nella direzione complessiva e integrata della gestione di rischi, che tendono ad allargarsi anche a nuovi ambiti, normati in tempi relativamente recenti. Rischi aziendali ma anche professionali che possono ricadere direttamente o indirettamente nelle responsabilità del Security Manager, come quelli inerenti la resilienza aziendale, le implicazioni del GDPR, la safety del lavoratore.
Si profila quindi una prospettiva complessa che conferma – nell'interesse dell'Azienda ed a supporto del Security Manager – la necessità di puntare non solo su un modello informatizzato, ovvero un PSIM, ma anche sulla sua collocazione in un contesto di tipo ERP per la collaborazione organica e sinergica con stakeholder esperti e complementari, per la valorizzazione di una massa complessiva di User Experience adeguata a generare innovazione di processo; ma, nel caso di Citel, anche con la garanzia di continuità nei decenni e di competenza specifica generata da una massa critica unica nel settore.

CITEL

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

Sistema MACS, elettronica evoluta per una protezione perimetrale sicura e discreta

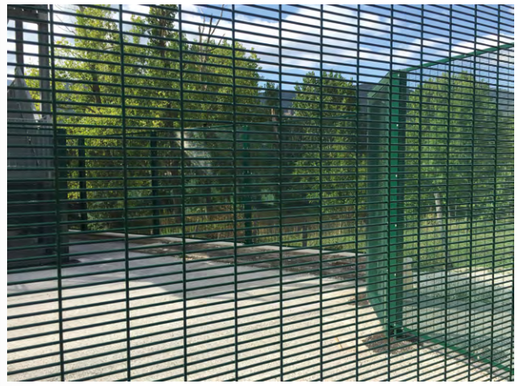
a cura della Redazione

Quando la protezione è a misura d'uomo, quando controllare e tutelare con discrezione è una necessità, allora la soluzione è il sistema **MACS** di **Nuova Defim Orsogril** (MEMS-based anticlimbing system). Questa è stata la scelta fatta, tra gli altri, anche dalla **Cooperativa Sociale Cooss Marche Onlus** per la casa di accoglienza di Serrapetrona, dove l'obiettivo principale era quello di assicurare la protezione perimetrale sia in ingresso sia in uscita con un sistema invisibile e che fosse rispettoso dell'individuo ospitato.
Per queste ragioni è stato scelto il sistema MACS applicato alla recinzione di massima sicurezza **Recintha Safety** di **Nuova Defim Orsogril** per una lunghezza di oltre 400 metri. Si è quindi puntato sulla sicurezza fisica ed elettronica con un sistema totalmente integrato, quindi completamente invisibile e capace di rilevare in maniera puntuale i tentativi di effrazione e scavalcamento, discriminando con grande precisione eventi naturali o accidentali.
MACS non è influenzabile da eventi climatici (pioggia, vento), dalla presenza di vegetazione o da azioni umane diverse dallo scavalcamento. È anche estremamente intelligente e preciso (ciascun sensore, fornisce una precisa indicazione del punto in allarme), di facile installazione si integra con sistemi di allarme già presenti. Assieme a **Recintha Safety**, con maglia antiscavalcamento e antitaglio, il sistema di fissaggio antistrappo e le elevate caratteristiche di solidità e robustezza, è una barriera invalicabile.

COOPERATIVA SOCIALE COOSS MARCHE

Siamo una cooperativa sociale che si adopera per la **cura, l'assistenza e la promozione dell'individuo.** Riconosciamo come fondamentale il diritto di ognuno di noi di avere una **giusta qualità della vita** e per questo studiamo, ci specializziamo e lavoriamo ogni giorno con professionisti del settore della salute e della cura di sé.
Ogni persona è per noi un individuo unico: la sua tutela è il nostro primo obiettivo, ecco perché il nostro motto è **"al centro del nostro Coossmo ci sei TU"**, nella convinzione che le peculiarità di ciascuno siano un patrimonio da proteggere ed esaltare.
Ci occupiamo di servizi sociali, socio-sanitari, assistenziali ed educativi, rivolti a tutti coloro che ne fanno richiesta o ne manifestano il bisogno: dal bambino all'anziano, dall'immigrato allo studente. Da sempre ci interessano la ricerca e la formazione, così come la promozione dell'integrazione e della partecipazione sociale sul territorio, prevalentemente marchigiano, con l'obiettivo di garantire occupazione lavorativa ai nostri soci.

Con il sistema **MACS (MEMS-based anticlimbing system)** si rilevano in maniera puntuale i tentativi di effrazione e scavalcamento, discriminando con grande precisione eventi naturali o accidentali.
MACS si declina nelle nostre recinzioni secondo due modalità: sia totalmente integrato sia esternamente a seconda dei modelli.
Per chi ha l'obiettivo di proteggere aree così sensibili che richiedono una massima sicurezza sia fisica sia elettronica, le soluzioni ideali sono **Recintha Safety MACS** ed **Elettra MACS** dove la sicurezza raggiunge i massimi livelli.



Inxpect MSK-101, tecnologia radar FMCW per la sicurezza antintrusione

a cura della Redazione

Una tra le ultime innovazioni tecnologiche di **TSec** è il rivoluzionario sensore di movimento Inxpect **MSK-101** basato sulla tecnologia radar **FMCW**, la stessa tecnologia radar nata in campo navale e aeronautico, di recente impiegata anche nel settore automobilistico. Quella stessa tecnologia è stata concentrata in un dispositivo per la sicurezza, un sensore che può essere usato sia all'interno che all'esterno degli edifici e rivela il movimento in maniera estremamente puntuale.

La tecnologia FMCW si differenzia dalla tradizionale microonda CW, ampiamente utilizzata nel settore della sicurezza antintrusione, per la sua caratteristica di emettere onde elettromagnetiche a frequenze modulate. Analizzando attraverso l'algoritmo proprietario alcuni fattori, come il segnale riflesso e il tempo di riflessione dell'oggetto presente nel campo di visione, il radar identifica la distanza in modo preciso e ne stima la massa e la velocità di movimento.

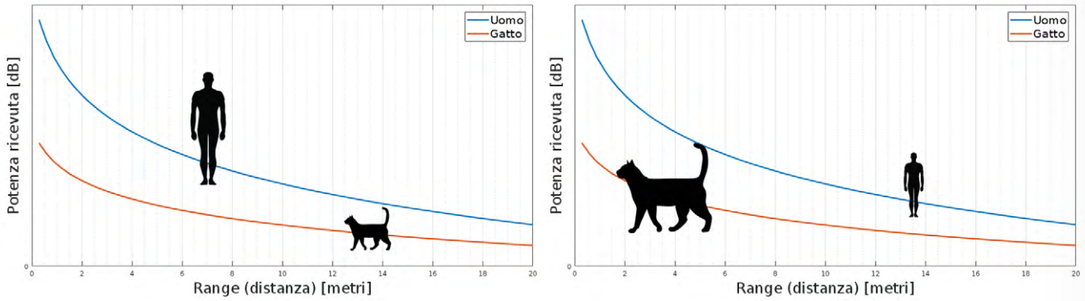
Il radar "vede" gli oggetti che sono nella sua area di rilevazione in un modo particolare, spiegabile mediante il concetto di RCS (Radar cross section).

La RCS di un oggetto è determinata in base a diverse proprietà: il materiale (più o meno riflettente), la forma dell'oggetto che influisce notevolmente sulla sua riflettività, l'angolo con cui viene visto (il radar non irradia allo stesso modo in tutte le direzioni) e la distanza a cui si trova questo oggetto.

Ad esempio, un velivolo Stealth costruito con una forma e materiali particolari, per il radar ha una RCS equivalente ad una pallina da tennis. Allo stesso modo, una biglia di ferro di due centimetri di diametro ha una RCS maggiore rispetto a una palla in spugna di un diametro di 30 centimetri. Questo perché la spugna è abbastanza trasparente alle onde elettromagnetiche, mentre il metallo ha una riflettività molto maggiore.

Grazie alla tecnologia FMCW e all'analisi accurata e puntuale della RCS, il sensore MSK-101 è in grado di discriminare il movimento di un essere umano da quello di un animale domestico, garantendo un'efficace **Pet Immunity Protection** basata sull'effettiva analisi del segnale.

MSK-101, grazie alla rilevazione precisa della distanza e alla stima della massa, discrimina il target in modo efficace.



Il livello di Pet Immunity Protection del sensore è gestibile tramite la app di configurazione.

L'applicazione permette di impostare facilmente una zona di allarme e una eventuale zona di preallarme, trascinando il cursore fino alla distanza desiderata. L'algoritmo di elaborazione del movimento fornisce all'installatore una completa flessibilità, con la possibilità di configurare aree di allarme e pre-allarme fino ad un massimo di 20m con accuratezza centimetrica, sensibilità e modalità di segnalazione alla centrale di allarme, pre-allarme, manomissione e guasto.

Un altro aspetto unico di MSK-101 è il concetto di "semi-statico", ovvero la capacità di comprendere dinamicamente quando un oggetto si muove, ma non si avvicina o allontana dal sensore stesso. La rilevazione in tempo reale da parte del sensore permette di ridurre drasticamente la possibilità di falsi allarmi in presenza di cespugli, tende, porte o finestre rimaste aperte, ecc.

Grazie alla scocca meccanica dal design ingegnoso, MSK-101 può essere installato a muro o a soffitto e, dove necessario, con il supporto di una staffa accessoria.

Il case è realizzato con criteri di progettazione IP68. La contro-piastra posteriore funge da adattatore multi-standard per le principali scatole elettriche da incasso.

A seconda dell'orientamento, il sensore può essere utilizzato per monitorare un'area ampia (orientamento orizzontale o "volumetrico") oppure per monitorare un'area perimetrale, creando una sorta di barriera di protezione per gli accessi lungo un muro o un cancello (orientamento verticale, o "a barriera").

L'ampiezza del campo coperto con orientamento orizzontale del sensore (volumetrico) è di circa 90° massimo sul piano orizzontale e di 30° sul piano verticale. Nel caso di orientamento verticale (a barriera) il campo coperto diviene una barriera larga, nel suo punto più ampio, circa 2m, e che si estende per 20m.

Grazie alla sua capacità di fornire a qualsiasi centrale di allarme segnali relativi al movimento che avvenga nel range di differenti aree completamente configurabili, MSK-101 è in grado di aumentare il livello di sicurezza di tutti i sistemi anti-intrusione. Il montaggio e la programmazione del sensore richiedono pochi minuti, in qualsiasi configurazione installativa.

Grazie alla produzione e all'ingegnerizzazione rigorosamente *Made in Italy* con controllo qualità su ogni singolo pezzo, MSK-101 e tutte le soluzioni di TSec si pongono ai vertici del mercato per la sicurezza e il contenuto tecnologico, supportando pienamente tutte le moderne esigenze installative e, allo stesso tempo, diminuendo sensibilmente i costi di installazione e di manutenzione di qualunque impianto.

TSec
TECHNOLOGY FOR SECURITY

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

Il sistema antiscasso TSEC: INERZIALI e VAS

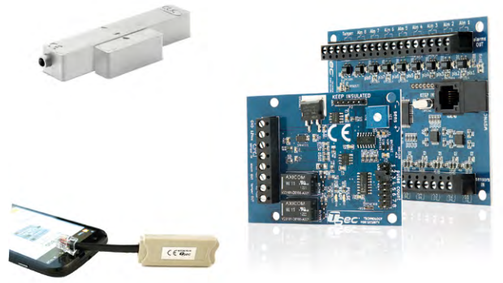
a cura della Redazione

Basato sull'analisi delle vibrazioni, la nuova architettura del sistema antiscasso **TSEC** si fonda su due principali innovazioni: da un lato una nuova tecnologia sensoristica completamente passiva e, dall'altro, l'uso di moderne tecnologie elettroniche per arrivare ad elevatissimi livelli di sensibilità, pur riducendo drasticamente la complessità della configurazione.

I sensori inerziali della serie **CLV** sono costruiti sfruttando una nuova tecnologia magnetica, dove la massa vibrante viene tenuta in equilibrio non più dalla forza di gravità ma da campi magnetici tarati in maniera minuziosa nella fase di produzione. Il sensore può, quindi, essere installato liberamente senza i vincoli di orientamento e posizionamento tipici della sensoristica a sfera tradizionale. Ciò permette di installare il sensore nelle zone e nelle posizioni più probabilmente oggetto di eventuali azioni di scasso, permettendo un ulteriore innalzamento del grado di sicurezza dell'impianto.

Le vibrazioni imposte al sensore, se sufficientemente forti da disturbare l'equilibrio magnetico, causano l'apertura del circuito elettrico. Grazie ad un progetto ingegneristico particolarmente accurato, la taratura dei campi magnetici ha permesso di realizzare un sensore la cui risposta alle vibrazioni (intervalli di tempo di apertura e ciclicità degli stessi) ricalca con molta fedeltà quella dei modelli più diffusi dei sensori tradizionali attivi.

Le schede di analisi per sensori inerziali **VAS** rappresentano quanto di più tecnologicamente avanzato oggi disponibile nel settore e sono in grado di sfruttare appieno la sensibilità dei sensori CLV. Basate su microcontrollori a 8 e 16-bit, offrono una logica di analisi completamente digitale. I modelli multicanale sono i primi sul mercato ad offrire la possibilità di gestire ciascun sensore con impostazioni di sensibilità differenziate.



La taratura avviene in maniera univoca per ogni sensore, in modo da adeguarla alla tipologia di installazione (infissi in legno, alluminio, protezione di muri, ecc.) ed alle esigenze complessive dell'impianto di sicurezza.

Ciascun canale di ingresso può anche accettare un collegamento in serie di più sensori, portando la modularità a zone di sensori anziché a sensore singolo: in questo modo è possibile realizzare impianti complessi limitando la quantità di schede di analisi da gestire, ma permettendo comunque la suddivisione per zone della sensoristica inerziale.

Nonostante la complessità del sistema, la sua configurazione risulta più semplice dei comuni sistemi che utilizzano sensori tradizionali attivi. Grazie all'innovativo sistema senza fili **Wsync**, è infatti possibile utilizzare un comune smartphone per tutte le fasi di installazione, configurazione, taratura e manutenzione del sistema.

L'accessibilità economica del sistema lo rende fruibile anche negli impianti residenziali comuni determinando un livello di sicurezza fino ad oggi impensabile per questa tipologia di realizzazioni.

TSec TECHNOLOGY FOR SECURITY

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

Mitigazione dei rischi, aumento delle opportunità nell'era digitale: le proposte di Econocom

a colloquio con Paolo Bombonati, Chief Operation Officer, Econocom Italia
a cura della Redazione

Quali sono le proposte di Econocom per supportare l'evoluzione digitale delle imprese?
Consulenza, progettazione e fornitura di risorse e beni, nonché la gestione tecnologica degli asset digitali, delle infrastrutture, delle applicazioni e delle varie funzioni di business correlate. Questi sono tutti servizi che Econocom garantisce ai propri clienti tramite una copertura finanziaria che si declina attraverso formule di canone al consumo. Siamo, infatti, in grado di analizzare e comprendere le necessità strategiche delle imprese perché diventino più competitive, offrendo una visione d'insieme, selezionando e implementando in modo indipendente le tecnologie digitali più innovative. Tutto questo viene poi offerto tramite una formula di finanziamento che permette ai nostri clienti di beneficiare di un aggiornamento costante delle soluzioni introdotte, in termini sia di software sia di hardware, a fronte di un investimento diluito nel tempo.

Avete soluzioni sviluppate in modo specifico per settori diversi come, ad esempio, il sistema bancario, il mondo del retail, il comparto manifatturiero, le PA?
Le soluzioni di Econocom rispondono alle esigenze IT e di business delle aziende che operano in diversi settori: dal retail al manufacturing, dall'utility all'education fino al banking settore bancario e alla sanità. Si caratterizzano per l'elevato livello di personalizzazione, che garantisce ai nostri clienti una maggiore forza competitiva e la massima efficienza. Offerte in modalità as-a-service, tutte le nostre soluzioni nascono da una prima fase di consulenza e analisi delle esigenze di business, per poi essere progettate ed implementate seguendo secondo i requisiti del cliente. La nostra offerta è molto ampia e varia, a partire da soluzioni di cloud ibrido in grado di offrire non solo integrazione completa tra diversi ambienti cloud ma, soprattutto, l'erogazione di applicativi aziendali e servizi innovativi e soluzioni di workplace management e di collaboration che supportano l'introduzione di progetti di smart working. A questo si affiancano una serie di progetti di innovazione digitale, che vanno dall'ottimizzazione dei processi all'integrazione degli applicativi aziendali tramite API, dalla gestione omnicanale della relazione con il cliente all'engagement in store, dall'introduzione dell'IoT alla mixed reality.

Cosa proponete in particolare per la sicurezza dei dati, una delle esigenze più sentite a seguito della digitalizzazione dei processi aziendali e l'entrata in vigore del GDPR?
Lavorando ogni giorno con tantissime aziende, Econocom è consapevole che la protezione da minacce informatiche o da incidenti che possano comportare la perdita di dati sensibili è una tematica molto sentita, sia nel settore pubblico che in quello privato. Per questo motivo, da diversi anni offriamo una serie di servizi end-to-end ai nostri clienti finalizzati proprio al monitoraggio continuo degli attacchi informatici, per permettere di rilevare rapidamente gli incidenti e ridurre al minimo la perdita e la distruzione delle informazioni aziendali. Mettiamo, inoltre, a disposizione delle aziende dei Cyber Security Specialist in grado di vigilare 24 ore su 24, 7 giorni su 7 sulle infrastrutture IT dei nostri clienti, per garantire sempre il massimo livello di sicurezza e rivedere eventualmente le politiche di sicurezza adottate. A seguito dell'introduzione del nuovo regolamento europeo sulla protezione dei dati, abbiamo quindi poi deciso di ampliare la nostra offerta adottando un approccio multidisciplinare al GDPR, per garantire ai nostri clienti un supporto completo nel processo di adeguamento dei sistemi informatici, ponendoci quindi come single point of contact per l'intera durata del progetto. Siamo, infatti, in grado di coprire tutte le attività consulenziali che vanno dall'assessment dei rischi, per verificare i processi e i modelli organizzativi adottati in azienda, fino alle attività di audit per verificare le nuove procedure adottate, offrendo piani di formazione indirizzati a sensibilizzare sul tema tutti i collaboratori aziendali. In aggiunta a questo, siamo in grado di erogare tutti i nostri servizi dalla cyber security (come pentration test e remediation) alla gestione di dati e documenti.

Come affrontate il tema della sicurezza IT correlata ai comportamenti delle persone?
Una strategia di sicurezza efficace non si può limitare all'adozione di soluzioni di protezione e monitoraggio delle infrastrutture e degli applicativi aziendali, ma deve contribuire anche ad aumentare la consapevolezza delle persone sui rischi derivabili dalle infezioni e dagli attacchi informatici. Per questo motivo, Econocom mette a disposizione dei propri clienti degli esperti di sicurezza informatica che supportino il coordinamento tra management, dipendenti e dipartimenti aziendali, per diffondere l'utilizzo di best practice, fondamentali per ridurre il rischio di perdita di dati aziendali. A questi si vanno poi ad aggiungere servizi di Security Awareness, che prevedono, tra le altre cose, corsi studiati appositamente per persone che non hanno competenze specifiche di Information Technology, ma che ogni giorno utilizzano computer o applicazioni fornite dall'azienda e che quindi possono essere vulnerabili ad attacchi informatici. Il nostro obiettivo è quello di sensibilizzare aziende e collaboratori verso comportamenti adeguati e atteggiamenti consapevoli, al fine di poter offrire un servizio completo di protezione e sicurezza, esigenze sempre più fondamentali in ogni settore di business.

econocom
asystel

CONTATTI: ECONOCOM
Tel. +39 02 336261
www.econocom.it

AXIS Device Manager, il software per una gestione on-site semplice e la protezione proattiva dei dispositivi

AXIS COMMUNICATIONS
(+39) 02 8424 5762
www.axis.com

AXIS Device Manager è uno strumento completo che consente di svolgere direttamente on-site tutte le principali attività di installazione e gestione centralizzata dei dispositivi in modo semplice e sicuro ed è la soluzione ideale per permettere a installatori di sistemi e amministratori di agevolare la protezione proattiva dei dispositivi e delle reti stesse.
Nato dall'ulteriore sviluppo della piattaforma software **AXIS Camera Management**, il software consente di gestire fino a 2000 telecamere di rete, dispositivi audio, controllo degli accessi o diverse migliaia di dispositivi in più siti e consolida la sicurezza degli apparati secondo la **"Hardening Guide"** pubblicata da Axis Communications.
Sono numerose le sue funzioni di gestione come ad esempio: assegnazione automatica degli indirizzi IP, installazione, configurazione, sostituzione e aggiornamento di singoli dispositivi, possibilità di copiare le configurazioni tra migliaia di dispositivi, connessione a più server o sistemi, punti di ripristino e impostazioni predefinite di fabbrica, aggiornamento del firmware, gestione e aggiornamento di account utente, password e certificati HTTPS e IEEE 802.1x. Il software sostituisce AXIS Camera Management e può essere scaricato gratuitamente alla pagina AXIS Device Manager.

Per maggiori informazioni su Axis Communications e la cyber security, visitare:
www.axis.com/cybersecurity

Rivelatori radio professionali da interno: BWare™ e iWAVE™ di RISCO Group

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

BWare™ e **iWAVE™** sono i rivelatori radio professionali da interno di **RISCO Group** che soddisfano i requisiti di abitazioni, uffici e piccole installazioni commerciali combinando design moderno e avanzate tecnologie di rivelazione, in grado di garantire un livello di affidabilità e sicurezza senza precedenti e, allo stesso tempo, di minimizzare i falsi allarmi grazie alla microonda in banda K.
BWare™ rappresenta la scelta ottimale per supportare la flessibilità di installazione in ogni contesto: questo sensore è infatti in grado di soddisfare le esigenze di professionisti che devono installare un sistema interamente cablato ma necessitano, comunque, di un sensore basato su tecnologia radio con lo stesso design dei modelli cablati, per rispondere a particolari esigenze di protezione di zone con architetture particolari. Conforme agli standard europei di Grado 3 (e/o Grado 2), il rivelatore BWare™ offre anche la massima sicurezza e protezione da manomissioni volontarie, grazie all'antiaccecamento con IR attivo.
Il sensore iWAVE™ DT – disponibile anche nella versione PET – è facilmente installabile attraverso una semplice staffa a parete e garantisce copertura standard grandangolo a 15m e immunità agli animali fino a 36kg.
Inoltre, la comunicazione radio bidirezionale assicura maggiore sicurezza e ridotta congestione del canale radio grazie a minori trasmissioni RF, oltre ad abilitare configurazione e diagnostica da remoto.

essecome ONLINE

n. 05 luglio 2018
Anno XXXVIII
Periodico fondato da Paolo Tura

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

HANNO COLLABORATO A QUESTO NUMERO
Angelo Carpani
Nils Fredrik Fazzini
Giuseppe Mastromattei
Donato Testa

SEGRETERIA DI REDAZIONE
redazione@securindex.com

PUBBLICITÀ E ABBONAMENTI
marketing@securindex.com

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

REGISTRAZIONE
Tribunale di Milano n. 21
del 31 gennaio 2018

GRAFICA/IMPAGINAZIONE
Lilian Visintainer Pinheiro
contatto@lilastudio.it

SENZA FILI, SENZA LIMITI.
IL VIA RADIO PER
IL PROFESSIONISTA.*

sol

** L'uso del software Sol/STUDIO e dell'app InimTech Security è riservato agli installatori in possesso di un account INIM Cloud.*

Sistema di sicurezza modulare tutto in uno 100% wireless.

Espandi le tue possibilità, con Inim Sol. Il sistema professionale completamente wireless e modulare. Una centrale ampliabile con moduli opzionali e intercambiabili per la connettività avanzata, insieme alle evolute funzionalità offerte da Inim Cloud. La app InimTech Security per installazioni in tempi record e un raffinato design per ogni spazio. Tecnologia e versatilità sulla tua stessa lunghezza d'onda. Presto presso il tuo distributore Inim di fiducia.

inim.biz

inim ELECTRONICS