Da AXIS soluzioni globali per la sicurezza nel Retail. Il bilancio del GARLF 2018

a cura della Redazione

Axis Communications affronta con sempre maggiore attenzione le tematiche relative alla sicurezza del mondo del retail, con soluzioni non solamente rivolte alla prevenzione dei reati predatori (furti, taccheggi, rapine) ma pensate con finalità più estese, come la disponibilità delle merci e la protezione dei profitti. In tal modo, si creano i presupposti per rendere la sicurezza una parte integrante del business dell'azienda, mettendo a fattor comune competenze, risorse e tecnologie. In occasione del **Global Axis Retail Leadership Forum 2018**, un appuntamento annuale per retailer da tutto il mondo organizzato da Axis quest'anno a Parigi il 12 e 13 aprile, è stato affrontato, tra gli altri, il tema della protezione dei profitti nell'era dell'e-commerce, con una valutazione dell'apporto delle tecnologie sviluppata con il confronto tra utilizzatori di categorie merceologiche diversificate ed esperti di Axis.
Abbiamo quindi chiesto a **Timo Sachsen**, Product Analyst EMEA, di sintetizzare i nuovi prodotti di Axis per il mondo del retail presentati in occasione del GARLF ed a **Steven Kenny**, Business development manager, Northern Europe, di descrivere la linee guida di Axis in materia di sicurezza dei dati in funzione del GDPR.
A **Pietro Tonussi**, Business development manager, Southern Europe, abbiamo chiesto invece un commento sull'attuale scenario di mercato ed un bilancio dell'edizione 2018 di GARLF, che ha visto per la prima volta la partecipazione del **Laboratorio della Sicurezza**, con Giuseppe Mastromattei e Federico Saini.

Pietro Tonussi, Business development manager, Southern Europe

Dal vostro punto di osservazione, quali sono le esigenze più sentite oggi dai retailer per migliorare la protezione dei profitti e la disponibilità delle merci nei PdV?
Le esigenze dei retailer sono direttamente collegate al bisogno di tenere il più possibile sotto controllo il punto vendita e, allo stesso tempo, di utilizzare soluzioni esteticamente belle e che non impattino sul layout del negozio stesso.
Dal nostro punto di vista, pensiamo che esistano prodotti che, integrati tra di loro, possano rappresentare una soluzione adatta alle esigenze di ogni singola realtà. Axis Communications ha sviluppato dei prodotti il più discreti possibile e allo stesso tempo con caratteristiche e funzionalità che permettono di raggiungere davvero l'obiettivo di tenere "tutto sotto controllo". Da sempre l'Azienda pone un'attenzione particolare anche al design, al fine di garantire alte prestazioni tecnologiche *(Multi-view, Forensic capture e risoluzione)* abbinate a soluzione estetiche all'avanguardia.
Quando si entra nello specifico della videosorveglianza, è importante anche conoscere il punto critico di un negozio e sapere che, in caso di "evento", le Forze dell'Ordine necessitano di dati, ovvero di immagini: quanto più queste sono dettagliate, tanto più sarà facile per loro identificare i responsabili dei furti. In sintesi, è necessario considerare l'utilizzabilità dell'immagine, vale a dire fare in modo che le telecamere dispongano delle qualità necessarie per acquisire immagini adeguate per le analisi forensi, specie considerando che la *loss prevention* è una problematica H24.
Grazie ai sensori multimegapixel e a opportune installazioni adeguate al layout del negozio, si può infatti ottenere una maggiore copertura (angolo di visione) e allo stesso tempo tenere sotto controllo i costi, riducendo laddove possibile il numero di telecamere. Se a questo si aggiunge la possibilità di utilizzare applicazioni intelligenti per verificare se qualcuno entra in aree private o in spazi dove il pubblico non deve esserci, allora possiamo davvero ottimizzare le soluzioni e ridurre concretamente le perdite all'interno di un negozio.
Tuttavia, è fondamentale considerare la tipologia di punto vendita in cui viene effettuata un'installazione: un supermercato potrebbe avere delle esigenze diverse rispetto al negozio fashion, perché anche la tipologia di furti è differente a seconda della categoria merceologica. Nella GDO, ad esempio, il furto dei "freschi" è difficile da rilevare attraverso il solo utilizzo delle telecamere ottiche. Per questo, abbiamo sviluppato applicazioni con alcuni dei nostri migliori partner che possono risolvere anche questa problematica, come un'innovativa soluzione che permetterà agli operatori del settore di controllare e limitare i furti di questi prodotti, utilizzando una tecnica moderna, innovativa e non invasiva come la tecnologia termica.
Sempre occupandoci di *loss prevention*, dai dati che abbiamo a disposizione risulta che gli ammanchi siano spesso dovuti anche al *delivering*. Pertanto, consentire l'accesso a queste aree attraverso un ingresso "rigoroso" tramite videocitofono, QR code e controllo accessi potrebbe ulteriormente aiutare i retailer in questa attività, attraverso un'apertura automatica e temporizzata per tenere sotto controllo anche queste situazioni delicate.
Infine anche le soluzioni audio possono essere un componente importante in tal senso, utile nel lanciare messaggi o indicazioni a chi opera in questo contesto, oltre che a valorizzare l'esperienza del cliente e favorire le vendite.

Possiamo fare un bilancio di GARLF 2018 e della partecipazione italiana a questa edizione?
Il bilancio di GARLF 2018 è assolutamente positivo anche perché in questa edizione c'è stata un'importante partecipazione da parte di una nutrita delegazione italiana tra utenti finali e, per la prima volta, anche del Laboratorio della Sicurezza che ha condiviso con noi dati e tendenze che sono emersi dalla ricerche sul settore.
Ad esempio, nel corso di quest'ultimo incontro avuto a livello mondiale con gli utenti finali, sono state discusse e affrontate soprattutto le tematiche del *loss prevention* anche in virtù di nuove tipologie di vendita come il "click and collect". Si è parlato del fatto che, oltre al punto vendita anche spazi come i box loacker debbano essere controllati in maniera adeguata con soluzioni di videosorveglianza ad hoc, così come lo devono essere quelle aree di "deposito" tipiche di questo tipo di soluzione che, sebbene in Italia debba ancora prendere piede in maniera decisa, rappresentano davvero una delle tendenze più in sviluppo del retail.

Molto importante e stimolante anche il momento in cui la delegazione ha partecipato alla tavola rotonda sul tema del crimine organizzato nel mondo del retail (ORC) durante la quale due importanti clienti finali hanno condiviso esperienze e preoccupazioni stimolando ulteriormente il dibattito sui temi più "caldi" del momento, così come quella della gestione nei supermercati della problematica del *loss prevention* e delle relative soluzioni tecnologiche a disposizione sul mercato.

Timo Sachsen, Product Analyst EMEA

Potrebbe fornirci alcune informazioni sulle ultime soluzioni Axis per il settore retail?

Telecamere panoramiche multidirezionali

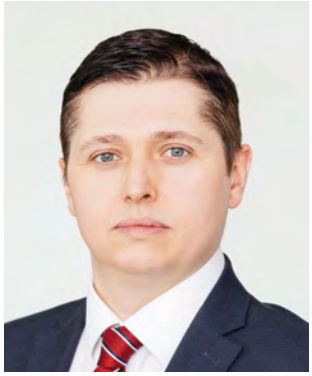
Axis ha ampliato la propria offerta di telecamere panoramiche multidirezionali, un segmento molto popolare negli Stati Uniti, ma non così tanto nel resto del mondo, per il quale si può prevedere una crescita molto più veloce rispetto ai segmenti tradizionali della videosorveglianza per questo motivo: AXIS P3717-PLE è l'ultimo componente aggiuntivo della categoria, una videocamera dotata di quattro testine sensori regolabili individualmente in un'unica unità. Ogni sensore offre una risoluzione di 1080p, per un totale di 8 Megapixel e l'uso di questo modello ridurrà i costi di installazione negli ambienti di vendita retail: invece di quattro cavi, quattro porte su uno switch e quattro licenze (*), ne verrà utilizzato solo uno per ognuno di questi (*a seconda del sistema di gestione video).

Analitiche di loitering

Le analitiche di loitering possono essere utilizzate anche in ambienti retail, solitamente vengono impiegate per rilevare comportamenti indesiderati in situazioni esterne, ad esempio per i graffiti nelle stazioni ferroviarie. All'interno di un negozio questi dati analitici possono aiutare a informare lo staff riguardo ai clienti che necessitano di assistenza. Rispetto al semplice rilevamento di movimento, che creerà un evento in un istante, gli algoritmi di loitering funzionano con un timer, quindi un evento viene creato dopo un intervallo di tempo configurato, ad esempio 60 secondi: questo aiuta a differenziare l'evento dal punto di vista della relazione tra i clienti che camminano in un'area e quelli che invece mostrano più interesse per i prodotti stessi.

Quanto è importante per voi dialogare con i vostri clienti per sviluppare dispositivi, soluzioni e applicazioni personalizzati?

Parlare e stare vicino ai clienti finali è essenziale per sviluppare i prodotti giusti. Senza un dialogo costante con i nostri clienti, non saremmo in grado di creare prodotti, sistemi e soluzioni adeguati. Il nostro dialogo è bidirezionale: cerchiamo ovviamente di capire di cosa hanno bisogno i clienti e come lavorano, ma offriamo anche una grande quantità di informazioni e servizi di formazione per consentire ai rivenditori di capire al meglio il nostro approccio e perché è diverso dalle altre offerte sul mercato. I nostri system integrator e clienti finali apprezzano il modo di fare business di Axis, perché non è solo di un processo di vendita, è più un processo di consulenza.



Steven Kenny, Business development manager, Northern Europe

Tutti oggi sono consapevoli che il rischio di crimini informatici attraverso le reti di telecamere IP è reale. In che modo i produttori possono tutelare i propri clienti?
Per le aziende produttrici di dispositivi IP è impossibile - e forse anche un po' ingenuo - pensare di riuscire a tutelare pienamente gli utenti finali dalle minacce informatiche legate all'implementazione delle loro tecnologie. Sebbene nessun produttore di tecnologie IP possa impegnarsi a garantirne la loro sicurezza al 100%, dovrebbe essere in grado di dimostrare la propria maturità informatica e il proprio supporto nella risoluzione delle minacce informatiche. Per prima cosa, ovviamente, è fondamentale il modo in cui sono state progettate le tecnologie. Il produttore è in grado di dimostrare un approccio sicuro in base al progetto *(secure by design)* o e un approccio sicuro by default? Un fornitore credibile dovrebbe incorporare la gestione della sicurezza nelle sue tecnologie, includendo le istruzioni per la modifica della password, gli indicatori di efficacia della password, la crittografia HTTPS, l'accesso remoto disabilitato fin dall'inizio e molto altro. La maggior parte delle violazioni che si sono verificate fino ad oggi avrebbe potuto essere tranquillamente evitata se fossero state scelte le tecnologie giuste con queste funzionalità di sicurezza integrate e seguendo i principi *secure by default*. Oltre alla gestione della sicurezza integrata nelle tecnologie, sono altrettanto importanti i processi e le politiche aziendali. Per coloro che si occupano di acquisti è raccomandabile verificare l'intera filiera produttiva e impegnarsi esclusivamente con le aziende che prendono sul serio la sicurezza informatica dei e nei loro dispositivi. Non solo questo, bisognerebbe assicurarsi che il vendor abbia politiche di verifiche di vulnerabilità costanti e attive e che possa mettere a disposizione guide e strumenti di sicurezza per aggiornare il firmware in modo rapido ed efficiente e modificare le password.

Pensate che il GDPR potrebbe davvero aumentare la consapevolezza dell'emergenza della protezione dei dati?
Con le recenti modifiche in materia di protezione dei dati e l'applicazione del regolamento generale sulla protezione dei dati entrato in vigore lo scorso 25 maggio, è aumentata la consapevolezza dell'importanza della sicurezza informatica a livello di consiglio di amministrazione. La sicurezza informatica deve essere considerata come un processo aziendale che comprende molti elementi, tra cui la protezione dei dati fin dalla progettazione, che devono interagire per contribuire a garantire un'adeguata protezione dei dati riservati di un'impresa. Sono ormai lontani i giorni in cui la sicurezza informatica era un problema esclusivamente di ambito IT e la protezione dei dati una questione che poteva essere affrontata in un secondo momento. Con l'aumento della domanda di dispositivi IoT collegati e, quindi, la crescita esponenziale della quantità di dati disponibili, garantire la sicurezza di queste informazioni è diventato un problema che il management deve tenere sotto controllo, soprattutto alla luce del GDPR. Troppo spesso si pensa a identificare i difetti nella sicurezza, lasciando i dati personali potenzialmente esposti a terze parti malintenzionate. Le misure sulla privacy devono quindi essere incorporate nei dispositivi IoT fin dall'inizio e in fase di progettazione. Il GDPR richiede che i produttori di tali dispositivi adottino un approccio di "protezione dei dati a partire dalla progettazione" per qualsiasi sviluppo di prodotti o servizi. Tutti i produttori di IoT devono ricordare che la sicurezza informatica e la protezione dei dati sono strettamente collegate e affinché le aziende mantengano un vantaggio sul mercato, è importante che costruiscano una relazione di fiducia con i loro fornitori. Questi ultimi devono essere in grado di dimostrare che le tecnologie, i processi e le procedure da loro utilizzate sono in linea con i principi di sicurezza IT, che sono stati valutati esternamente e che seguono linee guida come le Cyber Essentials. La valutazione dei fornitori di tecnologia all'interno della supply chain è importante oggi più che mai per proteggere i dati di un'azienda ed è l'unico modo per garantire che un'azienda stia facendo tutto il possibile per proteggere i dati personali e sensibili.

AXIS® COMMUNICATIONS