

APR 2021 – security & safety alla ripartenza degli aeroporti. Le soluzioni di Hanwha Techwin.

intervista a Fabio Andreoni, Country Manager - Italy & Greece at Hanwha Techwin Europe Ltd

Alla ripresa del traffico dei passeggeri nei voli commerciali, priorità assolute sono l'affidabilità e il rispetto delle procedure per garantire la security e la safety delle persone senza prolungare i tempi di permanenza in aeroporto. Quali soluzioni propone Hanwha Techwin per rispondere a esigenze che possono confliggere?

Le problematiche legate agli scenari che si sono creati con la riapertura del traffico dei passeggeri dopo la pausa forzata rappresentano una sfida articolata e importante anche per chi, come Hanwha Techwin, si occupa di Videosorveglianza. Da questo punto di vista, i recenti sviluppi tecnologici, che hanno visto l'implementazione di logiche di analisi video basate su algoritmi di Intelligenza Artificiale a bordo delle telecamere stesse, rappresentano un ausilio importante per garantire il rispetto delle norme e, nel contempo, non creare particolare intralcio alle normali attività all'interno di un'area passeggeri.

Esistono diverse soluzioni, ciascuna calata sulle specifiche esigenze delle varie aree.

Ad esempio, le nuove telecamere **Wisenet TNM-3620TDY**, a doppia tecnologia, termica e visibile, appositamente studiate per la misurazione della temperatura corporea, consentono di rilevare temperature in tempo reale con una precisione fino a +/-0,3°C fino a 10 persone contemporaneamente, grazie all'ausilio delle logiche di analisi video AI Deep Learning che identificano l'area relativa al volto all'interno dell'immagine. Il tutto con una rilevazione in tempo reale, in modo da non creare ostacoli o ritardi al flusso di persone.

Esistono altre possibilità, sempre utilizzando le funzioni di analisi video a bordo camera, in particolare legate alla capacità di analizzare il flusso di persone in un'area precisa, indicando in tempo reale la relativa occupazione, il numero di persone presenti e segnalando su un monitor i posti disponibili o il superamento della soglia di presenze. Un'altra funzione,



legata al distanziamento, consente anche di monitorare che la distanza tra le persone all'interno di un'area specifica venga rispettata. Esiste poi, come ulteriore ausilio, la possibilità di utilizzare le funzioni di analisi video per il rilevamento della mascherina di protezione, con algoritmi avanzati che consentono di identificare anche se la mascherina non è indossata correttamente.

Tutte soluzioni che lavorano sfruttando la capacità di analisi a bordo delle telecamere, e che danno la possibilità di utilizzare questi sensori anche per le normali funzioni di Sicurezza, tipiche di un ambiente importante come un'area aeroportuale.

Sono temuti anche attacchi hacker ai sistemi informatici ed ai dispositivi in rete degli aeroporti. In che modo si possono garantire livelli maggiori di sicurezza?

Hanwha Techwin è pienamente consapevole di avere la responsabilità di garantire che le soluzioni proposte includano accorgimenti di sicurezza informatica innovativi, che possano aiutare gli operatori aeroportuali a ridurre al minimo il rischio che i sistemi di videosorveglianza vengano violati.

Con la sicurezza informatica sempre in cima alla sua lista di priorità, Hanwha Techwin si impegna a progettare, sviluppare e realizzare prodotti e soluzioni che siano sicuri, proteggano le informazioni riservate degli utenti e rispettino le normative e gli standard internazionali sulla protezione dei dati.

Abbiamo una divisione interna, **Security Computer Engineering Response Team (S-CERT)**, totalmente dedicata all'affrontare qualsiasi potenziale vulnerabilità di sicurezza nei nostri prodotti e delle nostre soluzioni. I membri del team sono stati selezionati per la loro esperienza nell'essere in grado di identificare, analizzare e rispondere rapidamente con contromisure efficaci a qualsiasi minaccia alla sicurezza informatica. A questo proposito, Hanwha Techwin riconosce l'importanza di essere aperti e onesti con i clienti quando vengono identificate nuove minacce alla sicurezza informatica e, a questo proposito, informiamo i nostri partner di eventuali problemi il prima possibile.

Siamo orgogliosi di essere tra i produttori che sono stati invitati a partecipare allo sviluppo dello standard **Secure by Default**, con l'obiettivo di garantire che i prodotti di videosorveglianza non presentino rischi dal punto di vista della cyber security e della rete per impostazione predefinita, pronti all'uso. Inoltre, le telecamere dotate del chipset Wisenet7 sono certificate UL CAP (Cybersecurity Assurance Program). Il programma di certificazione UL CAP valuta potenziali problemi di sicurezza informatica e il livello di rischio degli hacker in relazione a dispositivi hardware e software collegabili in rete.

La strategia di sicurezza informatica di Hanwha Techwin si basa su un approccio che fa della protezione dagli attacchi informatici una caratteristica fondamentale delle nostre soluzioni di videosorveglianza che viene presa in considerazione all'inizio del processo di progettazione di un prodotto e non solo trattata come una delle tante utili funzionalità.

Non forniamo, ad esempio, prodotti che hanno password deboli preconfigurate e in cui l'utente non è tenuto ad apportare modifiche. Utilizziamo protocolli di password minimi obbligatori e auto-imposti, come il divieto di utilizzare consecutivamente la stessa lettera o numero e incoraggiare l'uso di caratteri speciali.



In particolare, le telecamere Wisenet di ultima generazione sono dotate del nostro innovativo chipset Wisenet7 che vanta un impressionante elenco di tecnologie progettate per migliorare significativamente le credenziali di sicurezza informatica delle telecamere. Questi includono la verifica dell'avvio protetto che fornisce un ulteriore livello di sicurezza tramite il "sandboxing" di diversi elementi del sistema operativo di una telecamera, il che significa che si trovano in uno spazio protetto. Wisenet7 utilizza anche un sistema operativo sicuro (OS) separato per la crittografia e la decrittografia, nonché per verificare che le app non siano state modificate o non siano contraffatte. È necessaria un'API basata su Linux separata per accedere al sistema operativo protetto, senza la quale non è possibile apportare modifiche dall'esterno di una telecamera.

Secondo le esperienze di Hanwha Techwin, quale è il livello di consapevolezza sulle problematiche legate alla cybersecurity da parte degli utenti finali, inteso come vari enti aeroportuali, e quali soluzioni stanno adottando?

Dalla nostra esperienza possiamo dire che le logiche di sicurezza informatica in ambito aeroportuale sono ben note da tempo, ed affrontate in modo completo ed approfondito da parte degli organismi responsabili. Anche il tema cybersecurity calato sullo specifico campo della Videosorveglianza è ben noto e tenuto in considerazione.