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

intervista a Giovanni Taccori, Commercial Lead Airport di Genetec Inc.

Alla ripresa del traffico passeggeri nei voli commerciali, le priorità assolute sono affidabilità e rispetto delle procedure di sicurezza, senza prolungare i tempi di permanenza. Che soluzioni propone Genetec in risposta a esigenze potenzialmente conflittuali?

Il lavoro degli addetti alla sicurezza aeroportuale è sempre più complesso. Tra sensori più intelligenti e l'aumento di dispositivi e sistemi, il volume di dati da gestire può essere schiacciante. A questo si è aggiunta la necessità di tutelare il passeggero e aiutare il personale nella gestione di ingressi e sbarchi, ad esempio impiegando linee guida per lo screening della salute dei viaggiatori. Con l'inserimento di telecamere termografiche nel sistema di controllo accessi, si potranno verificare più fattori prima di consentire l'accesso a date aree. Qualsiasi utente potrà accedere solo quando il sistema vedrà soddisfatte tutte le relative restrizioni, come una temperatura corporea minore di 37° o la mascherina correttamente indossata.

Tutto ciò rende difficile identificare le minacce tra centinaia di eventi. Le recenti soluzioni di gestione degli incidenti, come **Genetec Mission Control™**, possono smistare gli eventi che richiedono attenzione immediata e differenziare avvenimenti banali, come una porta aperta accidentalmente, dalle minacce reali, come i tentativi di effrazione. La piattaforma può analizzare gli eventi, rilevare i modelli che segnalano minacce reali, automatizzare i compiti di routine e semplificare il coordinamento delle risposte tra le parti interessate. Le procedure stanno cambiando e **Genetec Mission Control™** può aiutare a garantire il rispetto delle normative, attraverso procedure operative standard (SOP) predefinite che permettono agli operatori di rispondere in modo rapido.

Sistemi di sicurezza fisica in grado di gestire le presenze possono contribuire a limitare i contagi. Per garantire il distanziamento occorrono notifiche esatte e in tempo reale sull'affluenza alle singole aree.

L'analitica video per il conteggio persone di **KiwiVision™** garantisce esattamente questo, presentando in dashboard in modo chiaro e intuitivo la collocazione dei passeggeri. Contemporaneamente, il sistema **Security Center** tramite il suo modulo **Passenger Flow Analytic** permette di interfacciare sistemi diversi per la gestione code, beneficiando di diverse tecnologie oltre l'analisi video su telecamera (ex. LiDar o Wi-fi / Bluetooth)

Nel prossimo futuro si temono attacchi hacker ai sistemi informatici e di rete degli aeroporti. Come garantire maggiori livelli di sicurezza?

Parlando di cybersecurity, è utile dividere il problema in tre categorie: autenticazione, autorizzazione e crittografia.

L'autenticazione determina se un essere umano o una macchina è chi dice di essere e previene l'accesso non autorizzato ammettendo solo entità conosciute. Nel caso di persona fisica, avviene di solito tramite una combinazione di username e password.
L'autorizzazione verifica se l'entità autenticata ha diritto ad accedere a un dato spazio.
La crittografia (spesso sinonimo di cybersecurity nel linguaggio comune) è il processo di codifica delle informazioni per renderle leggibili solo agli utenti autorizzati. Mantiene i dati segreti, ma non impedisce di accedervi e non garantisce l'autenticità dei messaggi. È paragonabile al mettere una serratura alla porta di casa. Non si controlla chi ha accesso semplicemente mettendo la serratura, la sua forza emerge quando controlliamo chi ne possiede la chiave, tramite autenticazione e autorizzazione.
La sicurezza informatica diventa vitale nello sviluppo dei nostri prodotti e del nostro portfolio, aggiungendo nuovi livelli di protezione ad ogni release. Alcuni esempi:

• i dispositivi **StreamVault**, protetti di default, vengono forniti con tutti i controlli di sicurezza già effettuati e applicano le migliori prassi di cybersecurity al momento dell'installazione.
• l'integrità dei dati fa parte della protezione degli stessi. Per questo, abbiamo aggiunto il "video watermarking" al nostro VMS e migliorato la nostra funzionalità "firma digitale", perché assicuri l'integrità dei file e agisca come deterrente per chiunque voglia diffondere video in maniera illecita/non autorizzata.

• la gestione degli aggiornamenti del firmware è più facile che mai con il nostro nuovo **Firmware Vault**, che estrae informazioni dai siti web dei partner e invia notifiche per gestire centinaia di dispositivi e agire rapidamente quando c'è una possibile vulnerabilità. A ciò si aggiunge la capacità di gestire le password delle telecamere e la rotazione programmata per applicare facilmente le politiche di protezione delle stesse.
Da citare, infine, un paio di strumenti aggiuntivi, come il **Privilege Trouble-shooter**, che tiene traccia delle autorizzazioni e dei privilegi e garantisce che tutti abbiano accesso alle giuste funzionalità e il **Cybersecurity Score**, che permette all'operatore di lavorare su una checklist di sicurezza completa, sapendo subito cosa fare per aumentare il punteggio e rendere il sistema più resiliente e protetto da attacchi informatici.

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