# Sicurezza fisica e cibernetica negli aeroporti italiani. L'analisi di ENAV

*intervista a Francesco Di Maio, CISA CISM CRISC, C|CISO Head, Corporate Security Department - ENAV*

**Ci può fare il punto ad oggi sul livello complessivo della security del sistema aeroportuale italiano?**
L'aviazione civile italiana ha da sempre dimostrato di essere un presidio di avanguardia nei processi di sicurezza, ed applica i principi internazionali e della regolamentazione europea con grande serietà. D'altra parte, la security è parte integrante del modo di essere per il mondo aeronautico ed i security manager dei vettori aerei, degli aeroporti e degli altri operatori aeronautici cooperano attivamente tra di loro per innovare e rispondere alla domanda di sicurezza da parte dei passeggeri ed alla facilitazione dei processi di gestione, per ridurre i tempi di attesa con una risposta in termini di efficienza e qualità.

**A livello internazionale, quali sono le principali minacce che vengono attualmente percepite per la sicurezza dei voli e dei passeggeri?**
Purtroppo l'aviazione civile resta un obiettivo assai appetibile per la diversa platea di attori malevoli che si contendono la scena e non si parla solo della minaccia terroristica, che rimane a livelli consistenti per le diverse matrici ideologiche che si osservano nel campo.
Un aereo, un aeroporto, sono potenziali terminali di attacchi perché, da un lato, raccolgono numeri rilevanti di passeggeri di diverse nazionalità; dall'altro rappresentano la libertà di circolazione, non solo delle persone e delle merci ma, soprattutto, delle idee in un contesto dinamico globale.
La verità è che la minaccia si è progressivamente evoluta, passando dai tradizionali dirottamenti all'uso degli aerei come armi di distruzione di massa, richiedendo un supplemento di attenzione a tutti i livelli ed una più stretta sinergia di tutti gli attori, pubblici e privati, interessati a garantire la protezione della vita umana in volo e a terra.
A questo si affianca anche un contesto geopolitico assai dinamico, che segue una fase critica rappresentata dall'evento pandemico che ha messo a dura prova l'industria aeronautica.

Direi che oggi non esiste "una" minaccia specifica, ma esistono "più" minacce che tra di loro possono combinarsi, con attori pronti a sfruttare le vulnerabilità di punto e di sistema. Fondamentale è presentarsi preparati ad affrontare, congiuntamente, esigenze di sicurezza fisica e di sicurezza logica non dimenticando mai che il cuore del sistema è rappresentato dal fattore umano.

**In ambito cyber, quali sono le tipologie di attacchi più frequenti a livello globale e quali eventi hanno interessato il sistema nazionale?**
Negli ultimi tre anni, con un picco registrato con la crisi sanitaria globale, sono aumentati in maniera più che significativa i crimini informatici, soprattutto quelli che hanno come sfondo richieste estorsive o, comunque, finalità di natura lucrativa e predatoria, conosciuti soprattutto nella variante del "ransomware".
Nessun settore produttivo e della pubblica amministrazione, purtroppo, ne è andato esente e questo perché gli attori ostili non sfruttano tanto le vulnerabilità tecnologiche, quanto quelle legate al fattore umano, perfezionando sempre di più gli

attacchi diventati più subdoli e meno riconoscibili. Con la crisi derivante dalla guerra in Ucraina, stiamo assistendo anche ad una recrudescenza di fenomeni di attacchi, ideologicamente connotati, che mirano a creare impedimenti ai servizi che enti pubblici e privati offrono ai cittadini. Tuttavia, non sembra che, al momento, tali azioni si siano rivelate effettivamente capaci di debilitare il sistema, come invece accadde in Estonia nel 2007 o in Georgia nel 2012. Certamente sono cresciuti anche i livelli di consapevolezza nelle organizzazioni e questo è un fattore certamente abilitante i processi di difesa.

**Cosa sarebbe necessario per migliorare la prevenzione e innalzare il livello di resilienza del sistema nei confronti dei rischi cyber, anche nell'ambito del partenariato pubblico/privato?**

La parola d'ordine non può essere che una: cooperazione. Mi riferisco ad una collaborazione reale, che sostenga le organizzazioni private con una reale capacità di sostegno, nella fase di analisi del rischio, nella gestione dei processi di scambio di informazioni (quella che comunemente viene definita *threat intelligence*) che deve essere tempestiva, possibilmente automatizzata e non legata ad arcaiche modalità di tipo ministeriale-burocratico.

Le minacce corrono ad una velocità paragonabile almeno a quella degli aerei e le risposte devono essere altrettanto rapide. La comunità aeronautica italiana plaude certamente agli sforzi del Governo per elevare il livello qualitativo di questa collaborazione, ma va fatto molto di più.

Si deve operare per rendere disponibili anche agli operatori minori quegli elementi della tecnologia dell'informazione e quei processi di protezione che sono complessi, non accessibili alle organizzazioni meno strutturate, favorendo processi di aggregazione che vadano al di là della competizione tra imprese.

Noi stiamo facendo, in questo senso, la nostra parte. Con Assaeroporti abbiamo creato una community, facilitata da un programma europeo finanziato che ci siamo aggiudicati, per stabilire un "Information Sharing and Analysis Center" (ISAC) dedicato all'aviazione civile italiana ed aperto a tutta la comunità aeronautica nazionale.

Vediamo con piacere che in una delle 82 misure contenute nella Strategia Cibernetica nazionale, di recente varata dal Governo, vi sia proprio l'accento sulla necessaria cooperazione tra l'Autorità per la Cybersicurezza Nazionale e gli ISAC settoriali.

Ma ciò non basta. I security manager dialogano costantemente tra di loro anche con modalità informali, nate durante la drammatica esperienza del COVID. Vorremmo che questa partecipazione immediata, tempestiva e senza formalità possa venire sviluppata anche con i rilevanti attori pubblici, verso i quali sicuramente possiamo dare tanto.

E in aggiunta c'è il tema dei finanziamenti: la sicurezza costa, ma non è un costo. Anzi è un investimento doveroso, per i privati ma anche per l'intera comunità nazionale, perché i cittadini che viaggiano hanno il diritto di sentirsi tutelati in maniera effettiva e ricevere risposte in termini di sicurezza.

**Come valuta in generale il livello di preparazione e di responsabilizzazione sui temi della sicurezza del personale che opera nel sistema?**

L'aviazione civile è all'avanguardia in molti settori, tra i quali quelli della formazione. Per noi, in tutti i domini, sia che si tratti di controllo del traffico aereo che di aeroporti, vettori ed operatori aeronautici in generale, la formazione e la sensibilizzazione sui temi della sicurezza (nel suo complesso) è un obbligo che ha radici assai antiche.

Più di recente, si sono imposte, a livello europeo ma anche nazionale, norme vincolanti che dettano ulteriori requisiti d formazione, per esempio nei confronti degli Amministratori di Sistema, ossia coloro che hanno privilegi di accesso ai sistemi particolarmente elevati, che devono essere anche sottoposti a periodici "controlli di sicurezza rafforzati" relativi anche ai precedenti penali e di polizia.

E, in aggiunta, più norme impongono anche ai fornitori di sottostare ad un processo stringente di qualità della security, che serve ad elevare complessivamente il livello di competenze, capacità e di sensibilità verso la protezione di interessi che non sono solo dei privati, ma attengono ad un "dovere di diligenza" di natura pubblica che mira alla salvaguardia di interessi che si trovano nella fascia più alta dei valori di rango costituzionale, come la vita, l'incolumità personale, le libertà fondamentali.

Da membro di questa straordinaria comunità, percepisco lo sforzo che tutti i colleghi svolgono quotidianamente per raggiungere questi risultati di eccellenza anche oltre quanto richiesto dalla norma, per l'oggettiva sensibilità che tutti noi percepiamo come il dovere di base del nostro agire quotidiano.