Roma 6 dicembre 2017

XII CORSO DI FORMAZIONE GIURIDICO–AMMINISTRATIVA
TRASPORTO AEREO TRA INNOVAZIONE TECNOLOGICA
E INTEGRAZIONE INFRASTRUTTURALE

La nuova sfida della security aeroportuale: la cyber security

Prof. Avv. Marco Di Giugno Ph.D.
Direttore Aeroportuale Sardegna
Dottore di Ricerca in Diritto ed Economia dei sistemi produttivi, dei trasporti e della logistica
Professore a contratto di Diritto della Navigazione

In cosa consiste la Cyber Security?

*l'espressione **Cyber Security** indica un gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali non informatiche, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".*

IL PIANO NAZIONALE PER LA PROTEZIONE CIBERNETICA E LA SICUREZZA INFORMATICA (D.P.C.M. 11.04.2017)

PIANO NAZIONALE (PN)

INDIRIZZI OPERATIVI

1. Potenziamento capacità di *intelligence*, di polizia e di difesa civile e militare
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento
4. Cooperazione internazionale ed esercitazioni
5. Operatività delle strutture nazionali di *incident prevention*, *response* e *remediation*
6. Interventi legislativi e *compliance* con obblighi internazionali
7. *Compliance* a *standard* e protocolli di sicurezza
8. Supporto allo sviluppo industriale e tecnologico
9. Comunicazione strategica e operativa
10. Risorse
11. Implementazione di un sistema di *cyber risk management* nazionale

Piano Nazionale:
INDIRIZZO OPERATIVO 1

La protezione cibernetica e la sicurezza informatica nazionali, per essere efficacemente perseguite, presuppongono, in prima istanza, un'approfondita conoscenza delle vulnerabilità – non solo del fattore tecnologico ma anche di quello umano – e delle minacce cibernetiche che le sfruttano, al fine rendere le reti e i sistemi, in particolare nel caso delle infrastrutture critiche, più resilienti, assicurando, al contempo, l'efficacia del contrasto.

Piano Nazionale:
INDIRIZZO OPERATIVO 3

La formazione e l'addestramento nel settore della sicurezza informatica sono stati, fino ad oggi, orientati prevalentemente al personale specialistico che opera o che è destinato ad operare nel settore. Si pone, pertanto, l'esigenza di un'attività di promozione della cultura della sicurezza informatica diretta ad un ampio pubblico, che includa privati cittadini e personale, sia delle imprese che della Pubblica Amministrazione

Piano Nazionale:
INDIRIZZO OPERATIVO 6

La rapida evoluzione tecnologico-informatica comporta un altrettanto veloce obsolescenza delle norme che disciplinano materie correlate alle tecnologie dell'informazione e della comunicazione. Pertanto, esse necessitano di periodiche revisioni e aggiornamenti, oltre che di integrazioni, anche per creare un substrato giuridico alle attività condotte ai fini della protezione cibernetica e della sicurezza informatica e per responsabilizzare gli amministratori e gli utenti delle operazioni da questi compiute sui sistemi loro assegnati.

Piano Nazionale:
INDIRIZZO OPERATIVO 7

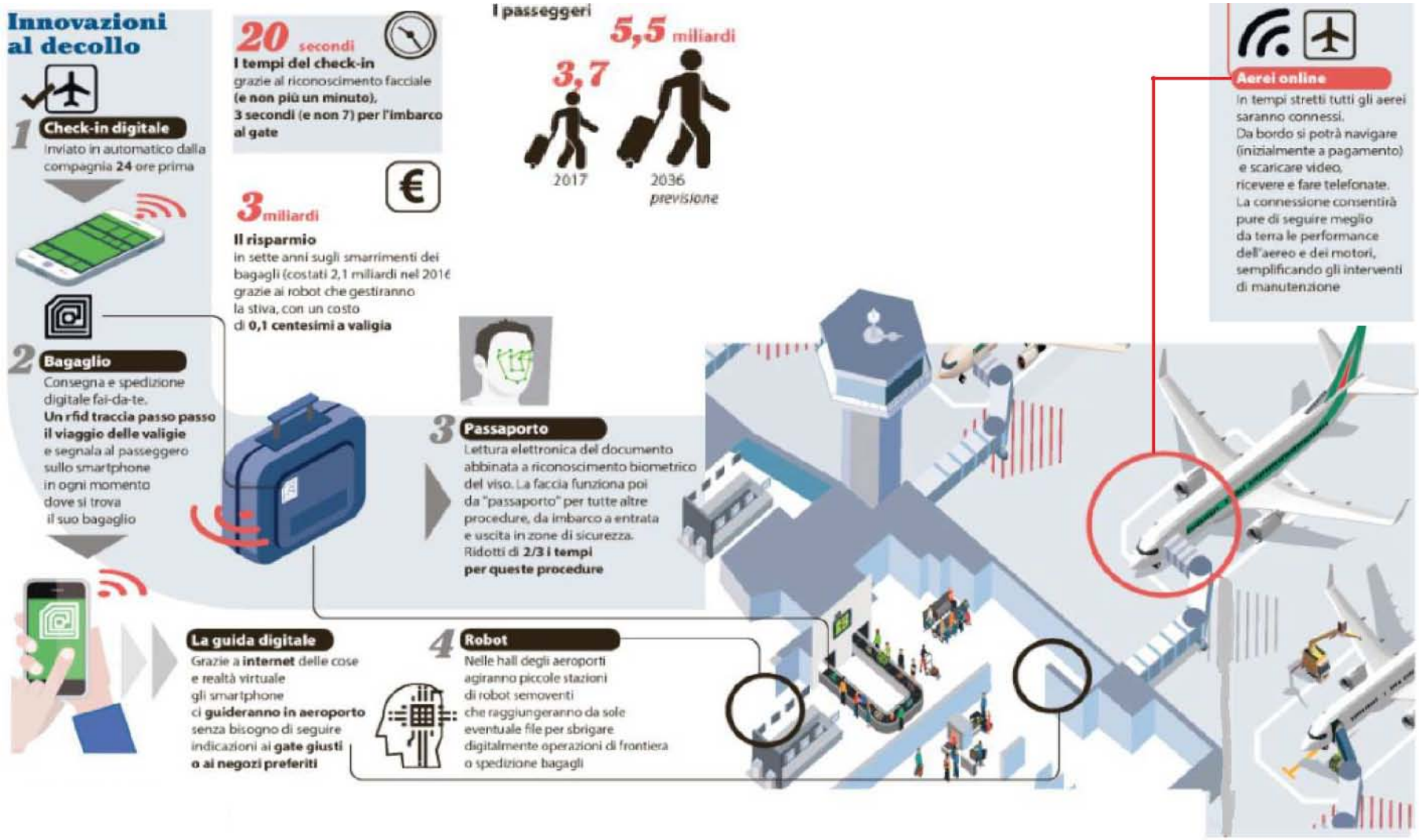
La compliance a standard e protocolli di sicurezza, elaborati sia a livello nazionale che internazionale, consente di garantire un comune ed elevato livello qualitativo nell'assicurare la protezione cibernetica e la sicurezza informatica dei sistemi e delle reti.

Cyber Security in Europa

Il 13 novembre u.s., 23 Paesi europei hanno confermato di voler incrementare la cooperazione in materia di difesa – anche in campo cyber – aderendo alla specifica Cooperazione strutturata permanente *(PErmanent Structured COoperation - PESCO)*.

La sicurezza cibernetica “è una sfida che i singoli Stati membri non possono affrontare da soli. Per affrontare minacce estremamente serie e diversificate che mettono a rischio le infrastrutture critiche e i sistemi degli Stati membri dell’Ue, abbiamo bisogno di convogliare e condividere risorse tecniche e capacità umane”.

Gli aeroporti del "prossimo" futuro



Fonte: il Corriere della Sera

Gli aeroporti del "prossimo" futuro

L'industria del trasporto aereo, alle prese con la trasformazione digitale, sta focalizzando l'attenzione su tre obiettivi:

1. proteggere business e passeggeri dagli attacchi informatici, minaccia reale in un'industria fortemente interconnessa come quella del volo;

2. ricercare sempre maggiore efficienza grazie ai servizi cloud, che consentono al contempo un contenimento dei costi

3. migliorare l'esperienza di chi vola, offrendo opzioni self-service ai passeggeri, che apprezzano indipendenza ed efficienza.

Gli aeroporti del "prossimo" futuro

Automazione dei servizi

Gli aeroporti del "prossimo" futuro

La biometria a ogni fase del viaggio: i dettagli biometrici del passeggero sono catturati tramite una scansione facciale al primo punto di contatto. Dopo il confronto del record con i documenti di viaggio – in genere il passaporto – viene creato per il passeggero un token unico e sicuro, grazie al quale il viaggiatore guadagna l'accesso nelle successive fasi del viaggio, dal check-in all'imbarco ai controlli di frontiera, tramite un semplice controllo facciale, senza mostrare altre carte

Fonte: il Corriere della Sera

Gli aeroporti del "prossimo" futuro

Track & GO

Tracciabilità dei bagagli

La "**Risoluzione IATA 753**" – a cui **tutte le compagnie aderenti all'Associazione dovranno adeguarsi entro giugno 2018** – stabilisce che tutti i bagagli trasportati in stiva debbano essere costantemente tracciati dall'inizio alla fine del viaggio: dal check-in al caricamento in stiva, fino a ogni trasferimento su un altro volo (nel caso di bagagli in transito) o all'arrivo, quando il bagaglio viene riconsegnato al passeggero.

Fonte: il Corriere della Sera

La security aeroportuale

OGGI

DOMANI

Le norme che regolano la sicurezza degli aeroporti si sono evolute sempre in risposta alla minaccia contingente, e troppo spesso solo dopo che la stessa si è manifestata.

IL RUOLO DELL'ENAC:

L'ENAC quale autorità di regolazione tecnica dell'aviazione civile ha la responsabilità di essere proattiva nel prevenire le nuove minacce