2nd Edition
CYBSEC-EXPO
THE CYBER SECURITY EVENT

CYBERSECURITY NELL'ERA DELLA NIS2: RISCHI E OPPORTUNITÀ NEL SETTORE AEROPORTUALE

2nd Edition
CYBSEC-EXPO
THE CYBER SECURITY EVENT

Applicazione Cyber Resilience Act nelle periferiche aeroportuali

Gabriele Ruggieri, Direttore BU Aviation, Custom
Matteo Boccacci, Marketing Manager Custom

Modera: Marco Labricciosa Gallese
Membro Consiglio Direttivo per il Segmento IT
Direttore Operativo, A-ICE

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

CUSTOM

EMPOWERING BUSINESS TRANSACTIONS

Applicazione delle policy Cyber Resilience Act nelle periferiche aeroportuali

Air Tech Italy
Italian Airport Industry Association

Periferiche Hardware negli aeroporti e rischi di sicurezza

✈️ Periferiche hardware comuni negli aeroporti:

- Stampanti per carte d’imbarco ed etichette bagagli, stampanti per liste passeggeri ai gate.
- Lettori barcode per carte d’imbarco
- Scanner passaporti
- Lettori biometrici
- Bilance per il peso bagagli
- Monitor FIDS (Flight Information Display Systems)
- Lettori RFID per valigie e oggetti di sicurezza

Periferiche Hardware negli aeroporti e rischi di sicurezza

⚠️ Rischi di sicurezza informatica:

- Questi dispositivi sono collegati tramite seriale, USB o Ethernet a sistemi centrali (workstation, server, cloud).
- Non possiedono misure di sicurezza autonome (come autenticazione, crittografia o antivirus).
- Sono considerati "fidati" perché fisicamente protetti e perché utilizzano firmware «dedicati» (no Windows / Linux / Android).
- Possono diventare vettori di attacco per introdurre malware o rubare dati sensibili?

✅ Protezione delle Periferiche Aeroportuali secondo il Cyber Resilience Act

1. Analisi del rischio e classificazione delle periferiche

- Identificare tutte le periferiche (lettori, stampanti, bilance, scanner, ecc.)
- Classificarle secondo la loro criticità operativa e il potenziale impatto in caso di compromissione.
- Mappare le connessioni (USB, seriale, LAN) e i protocolli usati.

2. Applicazione del principio "Secure by Design"

- Implementare protezioni a **livello firmware** delle periferiche (es. secure boot, autenticazione del firmware). ✅
- Usare **firmware firmati digitalmente** e aggiornabili solo tramite canali sicuri. ✅
- Limitare le funzioni disponibili solo a quelle strettamente necessarie (principio di minimizzazione). ⚠️

Air Tech Italy

3. Segmentazione della rete

- Isolare le periferiche aeroportuali in **reti VLAN separate**.
- Utilizzare **firewall interni** per bloccare connessioni non autorizzate.
- Abilitare solo le porte e i protocolli strettamente necessari.

4. Monitoraggio e logging

- Implementare sistemi di **monitoraggio continuo** (SIEM, IDS/IPS).
- Registrare ogni interazione con la periferica: accessi, aggiornamenti, errori.
- Correlare i log con sistemi di sicurezza centrali per **identificare attività anomale**.

5. Autenticazione e controllo degli accessi

- Ogni periferica dovrebbe richiedere **autenticazione forte** per l'accesso o la configurazione.
- Limitare l’accesso fisico e logico solo a **personale autorizzato**.
- Utilizzare certificati digitali o chiavi hardware (es. HSM o TPM) per dispositivi critici.

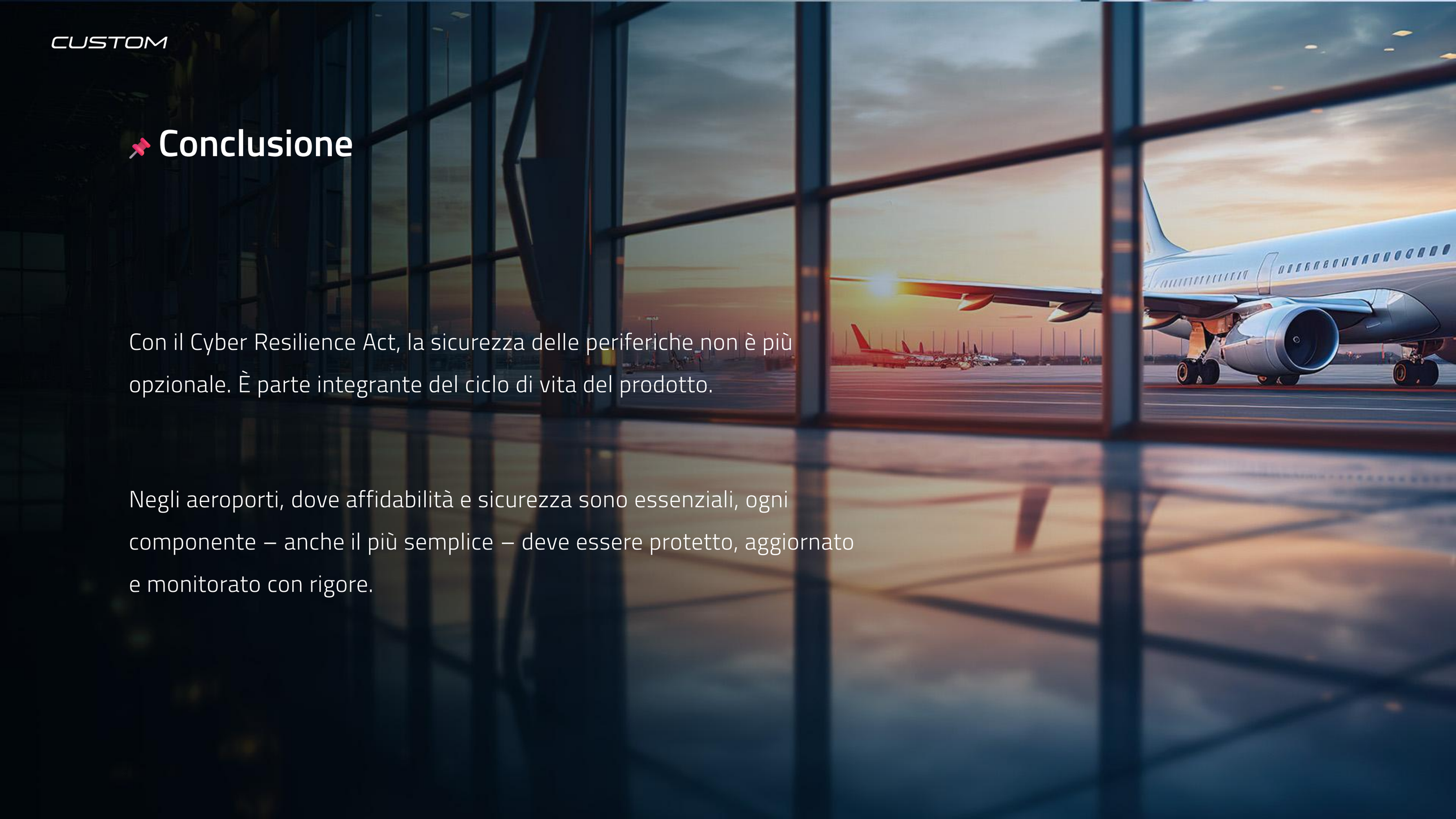
Air Tech Italy

6. Aggiornamenti di sicurezza

- Assicurare la disponibilità di **patch regolari** e tempestive.
- Automatizzare il processo di aggiornamento tramite **infrastrutture sicure di aggiornamento** (OTA o via USB firmata).
- Verificare la **conformità alle direttive CRA sui tempi di risposta alle vulnerabilità** (patch entro 24 mesi dal rilascio del prodotto e 5 anni di supporto minimo).

7. Valutazione della conformità e certificazione

- Adottare standard europei armonizzati previsti dal CRA.
- Collaborare con enti notificati per ottenere **certificazioni di sicurezza** dei dispositivi. **IATA?**
- Garantire **trasparenza** sulle vulnerabilità conosciute e sulle misure adottate.



📌 Conclusione

Con il Cyber Resilience Act, la sicurezza delle periferiche non è più opzionale. È parte integrante del ciclo di vita del prodotto.

Negli aeroporti, dove affidabilità e sicurezza sono essenziali, ogni componente – anche il più semplice – deve essere protetto, aggiornato e monitorato con rigore.

Esempi di sicurezza nell'uso di HMAC e firma digitale in applicazioni non aero

🔐 Esempio 1 – Sicurezza in un'App Gaming con HMAC-SHA256

- In una piattaforma di gaming, quando un utente vince un premio, viene generato un **QR Code sicuro** stampato offline.
- Il contenuto del QR Code include dati come:
  - ID utente
  - Premio
  - Timestamp
- Tutto viene firmato con **HMAC-SHA256** usando una chiave segreta condivisa.
- Questo previene la falsificazione del QR Code anche se la stampante **non è collegata a internet.**

Esempi di sicurezza nell’uso di HMAC e firma digitale in applicazioni non aero

🧾 Esempio 2 – Registratori di cassa e stampanti fiscali

- I moderni registratori di cassa inviano **file XML** all’Agenzia delle Entrate.
- I dati (scontrino, totale, data, ecc.) vengono **firmati digitalmente** usando chiavi RSA a 2048 bit.
- Questa firma garantisce **l'integrità e l'autenticità** delle transazioni.
- Il processo è **automatico e trasparente** per l’utente finale.

Q3X-N RT

Stampante Telematica Nativa

K3-N RT

Stampante Telematica Nativa

BIG 3 RT

Registratore Di Cassa Ethernet Telematico

Public transport and events

Aviation

550 airports and 250 airlines worldwide

Complete solutions for the Aviation sector that simplify the boarding procedures, thanks to boarding passes and luggage tags printing and reading and self-service baggage weighing systems.

Informative kiosks, recharge and deposit lockers, visualization and entertainment systems.

Some references

Airlines:

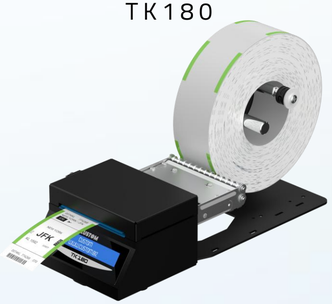
Aeroporti:

Air Tech Italy

Dedicated airlines counters

GOOD

TK180



TK180 METAL BTP RFID
ROLL HOLDER

TK180 METAL AUTOCUTTER

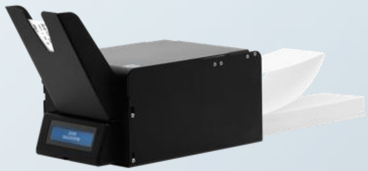
BETTER

TK202III

TK302III
ATB FRONT TRAY

BEST

TK202III METAL



TK302III METAL

TOP

TK862

Air Tech Italy

CUSTOM

EMPOWERING BUSINESS TRANSACTIONS

CUSTOM

Thank you

Air Tech Italy
Italian Airport Industry Association