CYBSEC-EXPO
2nd Edition
THE CYBER SECURITY EVENT

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

CYBSEC-EXPO
2nd Edition
THE CYBER SECURITY EVENT

Proteggere il business, senza rallentarlo

Alberto Torresan, Direttore IT, Gruppo SAVE

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

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

Proteggere il business, senza rallentarlo

CyberExpo – Piacenza, 21 maggio 2025

Air Tech Italy
Italian Airport Industry Association

Presentzione

Chief Information Officer

atorresan@grupposave.com

Chief Executive Officer

atorresan@naitec.aero

Da oltre 20 anni mi occupo di progetti IT in ambito aeroportuale, ho visto questo mercato sia dal punto di vista di cliente che del fornitore, maturando una forte competenza nei processi e sistemi del complesso mondo dell'aviazione.

CONFIDENZIALE

Informazioni generali

Gruppo degli aeroporti del Nord Est

4 Aeroporti (Venezia, Treviso, Verona e Brescia)

+ 20 Mil Pax per anno

+ 150 Destinazioni

+ 250 Mil di €

+ 1000 Dipendenti

Software house specializzata nella realizzazione di soluzioni digitali per il modo aeroportuale

+ 40 Aeroporti gestiti

+ 30 Prodotti

+ 40 Dipendenti

Proteggere il business – «ERA INTELLIGENTE»

La continua ed esponenziale evoluzione della minaccia informatica è un fenomeno in costante crescita e sempre più influenzato dall'avanzamento tecnologico e dalla digitalizzazione della vita quotidiana.

La rete internet viene utilizzata dai criminali per compiere reati di qualsiasi genere in quanto strumento agevolatore delle condotte illecite per massimizzare i profitti, in considerazione delle grandi potenzialità che derivano dai continui ed immediati scambi.

L'evoluzione degli attacchi informatici verso le infrastrutture critiche sta rimodellando il panorama delle minacce cyber, che non si limitano più alla compromissione della triade "integrità", "riservatezza" e "disponibilità" delle informazioni, ma possono estendersi fino a determinare un rischio reale per la vita delle persone.

Proteggere il business – «ERA INTELLIGENTE»

La convergenza tra sicurezza fisica, safety e sicurezza informatica è un processo in continua evoluzione che richiede un impegno costante da parte delle organizzazioni.

Gli attacchi cibernetici volti ad azioni distruttive, spionaggio e disinformazione, dovuti principalmente all'instabilità geopolitica e alle tensioni economiche, sono considerati tra i rischi globali più significativi nell'orizzonte temporale di breve e medio termine

I criminali informatici stanno adottando tecniche di attacco sempre più sofisticate grazie all'Intelligenza Artificiale

PROTEGGERE IL BUSINESS, SENZA RALLENTARLO

E’ POSSIBILE? COSA DOBBIAMO FARE?

Proteggere il business – «COSA FARE»

Fare formazione continua del personale

La cybersecurity integrata nella cultura aziendale è un aspetto cruciale per la protezione degli asset digitali e la resilienza dell'organizzazione.

Creare una cultura del rischio

Creare una organizzazione basata sulla cultura del rischio dove unisce in modo integrato Sicurezza fisica, Safety e sicurezza informatica.

Proteggere il business – «COSA FARE»

Riorganizzare, ripensare a sistemi e processi IT

Rivedere le architetture verso sistemi più resilienti, ogni progetto deve essere vagliato il rischio Cyber (soprattutto per gli impianti OT)

Portare a bordo nuovi skills interni alle direzioni IT

Implementare un sistema di difesa stratificato

Non esiste una soluzione unica per la cybersecurity aziendale, poiché ogni azienda è diversa – e diverse possono essere le minacce a cui è esposta – oggi risulta fondamentale adottare un approccio multi-livello che includa diverse tecnologie (Firewall, XDR ecc)

Proteggere il business – «COSA FARE»

Gestire gli accessi e le identità in modo seamless

Sviluppare politiche che dovrebbero rendere i sistemi di accesso semplici per gli utenti , utilizzo di MFA, single sign-on

Sviluppare una gestione della Business Continuity

E’ necessario che l’organizzazione sviluppi dei piani di Continuity del Business della soluzioni tecnologiche (DR, Backup …) e di processo (contigency plan, operation limit …) che consenta, in casi critici di non fermare il business.

Proteggere il business – «COSA FARE»

Air Tech Italy

Italian Airport Industry Association

GRAZIE !