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

Supply chain e maturità disomogenea

Luigi Ricchi, CISO, Aeroporto di Bologna

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

ORGANIZZATO DA

Air Tech Italy
Italian Airport Industry Association

Supply chain e maturità disomogenea

Aeroporto di Bologna

BLQ Innovability
Better.Living.Quality

Luigi Ricchi
Information security Manager
Aeroporto G. Marconi di Bologna Spa

membro gruppo cybersecurity - Assaeroporti

membro gruppo cybersecurity
International Airport Council Europe (ACI Europe)

membro Associso

ricchi@bologna-airport.it

Gap tra enti aeroportuali e fornitori (IT – OT - servizi)

Formazione continua
Contratti cyber-compliant
Notifica e audit previsti dalla NIS2

Gap tra enti aeroportuali e fornitori (IT – OT - servizi)

Formazione continua
Contratti cyber-compliant
Notifica e audit previsti dalla NIS2

- Flussi informativi cliente-fornitore
- Format contrattuale condiviso con Legal e HR
- Procedura aziendale di notifica e informazione interna – gestione della comunicazione

Air Tech Italy

Aeroporto di Bologna

BLQ Innovability
Better.Living.Quality

Rischi Terze Parti: Formazione continua di cyber security BOZZA

Una corretta valutazione del rischio delle terze parti comprende una comprensione delle modalità di formazione sul tema cyber security

Gli strumenti di formazione e di misurazione della consapevolezza, presenti sul mercato, sono molteplici. Per una infrastruttura critica non è accettabile avere un fornitore che non conosce lo stato della propria postura cyber, a partire dalla formazione.

Tramite check list, audit, e valutazioni delle certificazioni è possibile definire il grado di comprensione e consapevolezza delle aziende fornitrici di beni e servizi. Devo rivalutare la postura di periodo in periodo.

Facciamo domande scomode: il CEO dell'azienda e la dirigenza sono stati formati sul tema cyber security?

Rischi Terze Parti: Format contrattuale condiviso con Legal e HR BOZZA

Il rischio cyber security è un rischio aziendale, condiviso con le BU o Direzioni che guidano il business aziendale. Fra queste l'Area Legale e la gestione delle Risorse Umane possono supportare la costruzione di modelli contrattuali efficenti.

Il modello contrattuale aziendale deve contenere clausole cyber security, in cui si identifica la possibilità da parte della stazione appaltante/cliente di svolgere Audit al fine di comprendere la postura cyber del fornitore. Inoltre deve contenere regole di condivisione delle informazioni sensibili, ad esempio le dimissioni di un collaboratore nominato amministratore di sistema.

I modelli contrattuali verranno revisionati a periodi definiti come da buone pratiche dei modelli di gestione

Rischi Terze Parti: Procedura aziendale di notifica e informazione interna – gestione della comunicazione BOZZA

La procedura di notifica di un incidente informatico dovrebbe essere condivisa con le massime cariche aziendali. L'obiettivo è la conformità e la corretta comunicazione alle agenzie statali di riferimento.

La procedura di notifica deve prevedere una corretta comunicazione interna all'azienda, che permetta alle funzioni responsabili di attivarsi per l'attivazione di procedure atte al contenimento degli impatti generati dall'incidente.

Un'azienda con una buona maturità nella gestione della comunicazione, ha incaricato, prima dell'incidente, le persone che dovranno fare le comunicazioni agli organi competenti e al mercato, in caso di azienda quotata in borsa.

Aeroporto di Bologna
GRAZIE PER
L'ATTENZIONE
ricchi@bologna-airport.it
BLQ Innovability
Better.Living.Quality
STOP 2
STOP 1