Cyber Threat and risks in Aviation Security

Ali LARIBI, CPP®, CISM®, ISO xx
Cyber Security Consultant/Manager
Mobile: 0033699325372
E-mail: ali.laribi@gmail.com

Interregional Seminar ECAC-AFCAC-ACAO
« Innovation & CyberSecurity »

28-30 January 2020
Plan

- Cyber risques
- Cyber menaces visant le transport aérien
- Exemple de cyber menace
- Recommandations
Acronymes

- **ICS**: Industrial Control System
- **IIOT**: Industrial Internet of Things
- **IEC**: International Electrotechnical Commission
- **NIST**: National Institute of Standards and Technology
- **ISA**: International Society of Automation
- **CPNI**: Centre for the Protection of National Infrastructure
- **ISO**: International Organization for Standardization
- **SCADA**: Supervisory Control And Data Acquisition
- **CERT**: Computer Emergency Response Team
Baromètre des risques 2020 d’Allianz : les incidents cyber pour la première fois en tête des risques d’entreprise
Hack Motivations

Hack Motivations - December 2019

- Cyber Espionage: 11.5%
- Cyber Warefare: 3.2%
- Cyber Crime: 85.4%

Source: hackmageddon.com
CYBER MENACES visant le transport aérien?
Priorités de la cyber sécurité IT Vs OT ?
Exemple de cyber risque sur ICS/OT?
Exemple de cyber risque sur ICS/OT?

Dépôt de carburant

SAFETY

AVAILABILITY

RESILIENCE
Les Cyber risques en 2019, ICS/IIOT?

- 40% of industrial sites have at least one direct connection to the internet
- 53% of industrial sites have outdated Windows systems like XP
- 69% have plain-text passwords traversing the network
- 57% of sites are still not running anti-virus protections that update signatures automatically
- 16% of sites have at least one Wireless Access Point
- 84% of sites have at least one remotely accessible device

Source: CYBERX Report 2019
KASPERSKY ICS CERT : Cyber attaques en 2019, ICS/OT ?
Exemples de cyber attaques sur les ICS/OT
Recommandations

NIST Cyber Security Framework

- Asset management
- Business Environment
- Governance
- Risk Assessment
- Risk management Strategy

- Access control
- Awareness training
- Data Security
- Information protection
- Processes and Procedures
- Protective technology

- Anomalies and Events
- Security continuous monitoring
- Detection processes
Recommandations

Standards, Guidelines

- ISA-62443
- NIST Cybersecurity Framework SP800-53, SP800-82
- ISO/IEC 2700x
- ISO/IEC 27018
- IEC 62443
- IEC 61508
- CPNI Centre for the Protection of National Infrastructure
MERCI POUR VOTRE ATTENTION