AUTORITE NATIONALE DE L'AVIATION CIVILE
Daniel MILAN
9 décembre 2021

CYBER SECURITE DANS L'AVIATION CIVILE

Des cyber-attaques contre l'Aviation se produisent…

Mai 2009

Le Monde

Consulter le journal

ACTUALITÉS ÉCONOMIE VIDÉOS OPINIONS CULTURE M LE MAG

TECHNOLOGIES

Les ordinateurs de l'autorité de l'aviation civile américaine piratés

Des pirates auraient pu obtenir des renseignements personnels sur 48 000 employés actuels et passés de la FAA. En 2006, une attaque virale qui s'est propagée par Internet a obligé la FAA à fermer plusieurs de ses systèmes de contrôle aérien en Alaska.

Publié le 09 mai 2009 à 12h04 - Mis à jour le 09 mai 2009 à 12h04

September 5th 2018

REUTERS World Business Markets Politics TV

CYBER RISK SEPTEMBER 6, 2018 / 5:56 PM / A MONTH AGO

BA apologizes after 380,000 customers hit in cyber attack

Paul Sandle 4 MIN READ

LONDON (Reuters) - British Airways apologized on Friday after the credit card details of hundreds of thousands of its customers were stolen over a two-week period in the most serious attack on its website and app.

31 Janvier 2019

l'Opinion

Politique Economie International Opinions Dossiers Videos Blogs THE WALL STREET JOURNAL. Conférences

Intrusion

Airbus visé par une cyber-attaque

l'Opinion · 31 janvier 2019 à 07h12

L'agression visait les systèmes informatiques de la division aviation civile de l'entreprise, qui affirme qu'elle n'a eu « aucun impact »

… la menace est aussi réelle que sérieuse

La surface des cyberattaques de l'aviation augmente…

Des systèmes plus interconnectés

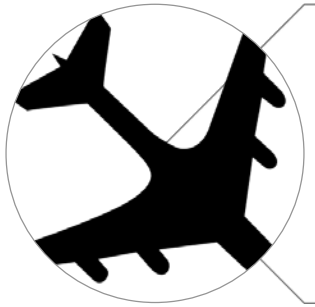
gration vers un réseau standard IP

Utilisation accrue des nouvelles technologies de l'information

Augmentation de la connectivité (*avion e-activé, services cloud, gestion totale des aéroports..)

Paysage des cybermenaces de l'aviation civile

- Deux catégories de cybermenaces:



Attaques pouvant entraîner des pertes en vie humaine ou mettre en danger la sécurité des opérations d’un aéronef.

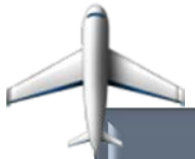
Attaques ayant des motifs criminels ou politiques entraînant des perturbations économiques pour le secteur de l'aviation

Paysage des cybermenaces de l'aviation

Quelles sont les cibles potentielles dans l'aviation civile?

Aéroports

- Systèmes informatiques internes de l'aéroport
- Contrôle de sécurité, contrôle d'accès
- contrôle des départs
- manutention des bagages



Avion

- Système de contrôle d'aéronef en vol
- Cabine (opérationnelle)
- Cabine (passagers)
- Réseau IP à bord des aéronefs
- Maintenance et ingénierie

Compagnies aériennes

- Systèmes informatiques des compagnies aériennes
- Dossiers clients et données financières
- Détails sensibles sur les revenus de l'entreprise

Gestion du trafic aérien

- Systèmes de gestion du trafic aérien
- Systèmes de Communication, Navigation et Surveillance
- Réseaux aéronautiques
- Maintenance

Exigence réglementaire

Norme 4.9.1 Chaque État contractant veillera à ce que les exploitants ou les entités définis dans le programme national de sûreté de l'aviation civile ou d'autres documents nationaux applicables déterminent leurs systèmes et données informatiques et de communication critiques utilisés aux fins de l'aviation civile et, conformément à une évaluation des risques, élaborera et mettra en œuvre, selon qu'il convient, des mesures pour les protéger des interventions illicites.

Exigence réglementaire

4.9.2 Recommandation. Il est recommandé que chaque Etat contractant veille à ce que les mesures mises en œuvre protègent comme ils se doit la confidentialité, l'intégrité et la disponibilité des systèmes et/ou des données critiques déterminées. Ces mesures devraient comprendre, entre autres, la sûreté intégrée, la sûreté de la chaîne logistique, la séparation des réseaux et la protection et/ou la limitation de toute capacité de contrôle d'accès à distance, selon qu'il convient, et tenir compte de l'évaluation des risques effectuées par les autorités nationales compétentes de l'Etat.

Elément d'orientation

- **RACI 7147**: Lignes directrices en matière de protection des systèmes d'information du domaine de l'aviation civile
- Coordination avec l'Autorité de Régulation des Télécommunication de Côte d'Ivoire (**ARTCI)**
- **ARTCI** a en son sein **le CI-CERT** (Côte d'Ivoire – Computer Emergency Response Team) qui est le centre national de veille et de réponse aux incidents de sécurité informatique , créé par le décret N°2020-128 du 29 Janvier 2020.

Entités concernées

Transmission du RACI 7147 au:

- gestionnaires d’aéroports

- Exploitants d'aéronefs

- Fournisseur de service de la navigation aérienne

- Société d’assistance en escale.

Evaluation et suivi

- Réalisation des évaluations des vulnérabilités par l'ARTCI ou autres entités compétentes
- Mise en place d'un plan d'action corrective (PAC)
- Suivi de la mise en œuvre du PAC

MERCI

FIN

dmilan@anac.ci

A.N.A.C.