REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

UNIVERSITÉ SAAD DAHLAB BLIDA 1

Institut d'Aéronautique et des Études Spatiales

Département de Navigation Aérienne

MÉMOIRE DE FIN D'ÉTUDES

Pour L'obtention du diplôme

MASTER en Aéronautique

OPTION : Opérations aériennes

Une gestion proactive des risques liés aux cyberattaques en préparation des vols dans la compagnie «Air Algérie»

Présenté par :

- Mme. **AIT HADJAM** Sarra

Dirigé par :

- Mr **KELLAL** Abdenour
- Mr **LAGHA** Mohand

Juillet 2023

TABLE DES MATIERES

RÉSUMÉ

Les cyberattaques menacent plusieurs domaines, dont l'aviation civile. Ce projet vise à étudier les risques associés à ces menaces et à analyser les mesures de cyber sécurité au sein de la compagnie aérienne « Air Algérie » lors de la préparation des vols. Tout d'abord, j'ai développé une matrice de risque liée aux événements de sûreté aérienne, ainsi qu'un programme informatique basé sur le langage "python" qui évalue les risques. Enfin, j'ai fait une évaluation des risques liés aux cyberattaques en utilisant la méthode «Bow Tie» et la matrice de risque.

ABSTRACT

Cyber-attacks threaten several areas, including civil aviation. This project aims to study the risks of these threats and analyze the cyber security measures within airline "Air Algérie" during flight preparation. First, I developed a risk matrix related to aviation security events, plus a computer program based on the "python" language that assesses risk. Finally, I did cyber-attacks risks assessment using the “Bow Tie” method and the risk matrix.

ملخص

تهدد الهجمات الإلكترونية عدة مجالات، بما في ذلك مجال الطيران المدني. يهدف هذا مشروع إلى دراسة مخاطر هذا التهديد، وتحليل إجراءات الأمن السيبراني داخل شركة الطيران "الخطوط الجوية الجزائرية" أثناء التحضير للرحلات. أولاً، قمت بتطوير مصفوفة مخاطر تتعلق بأحداث أمن الطيران، بالإضافة إلى برنامج كمبيوتر يعتمد على لغة البرمجة "بايثن" الذي يقوم بتقييم المخاطر. واخيرا، أجريت تقييمًا لمخاطر الهجمات الإلكترونية باستخدام طريقة ربطة العنق واعتمادا على مصفوفة المخاطر.

REMERCIEMENTS

En tout premier lieu, je remercier le bon **Dieu**, le tout puissant, qui m'a donné la force, la volonté, le courage et la patience, pour faire face à toutes les difficultés et les obstacles durant toutes mes années d'étude.

Mes profonds remerciements et ma plus grande gratitude vont à **Mr. KELLAL** et **Mr. LAGHA,** mes promoteurs, pour leur disponibilité, la confiance et l'autonomie qu'ils m'ont accordée, et leurs précieux conseils qui m'ont permis de mener à bien ce travail.

J'adresse mes sincères remerciements aussi à **Mr. ADJILI**, **Mme. MEZAACHE** et tout le personnel de la Direction de Sureté, sans oublier **Mr. NEMDIL** et les ingénieurs de la sous-direction ENGENRING, pour leurs aides et disponibilités.

Mes remerciements vont également au **jury** pour leur présence, leur lecture attentive de ce mémoire, ainsi que pour leurs remarques lors de la soutenance afin d'améliorer mon travail.

Afin de n'oublier personne, mes vifs remerciements s'adressent à tous ceux qui m'ont aidée de près ou de loin, à réaliser ce modeste mémoire.

DÉDICACES

Du fond de mon cœur, je dédie ce travail à tous ceux qui me sont chers.

A Ma **chère mère « MALIKA »**, mon soleil qui ne s'arrête jamais de briller, ma lumière et ma raison de vivre, « tout au long de ma vie, j'ai essayé de chercher des solutions face aux troubles de cette vie, mais à chaque fois mes pas me guident toujours vers toi, tu es mon guide dans l'existence».

A Mon **cher père « FARID »**, le symbole de la force, l'épaule solide, l'homme de ma vie et l'exemple que je veux suivre, « tout ce que tu fais devient l'étendard de mes actions, je suis si fière d'être ta fille ».

Chers parents, vous comptez à mes yeux bien plus que tout au monde, aucune dédicace ne saurait exprimer mon amour éternel, mon respect, ma fierté, et ma considération pour les sacrifices que vous avez consenti pour moi.

A Ma Chère Sœur : **« SIHEM »**, son Mari **« KARIM »**, et ses petits-enfants **« LINA »** & **« RACHID »**

Vous êtes ma source de bonheur et ma joie de vivre. Ma vie ne serait jamais aussi spéciale et extraordinaire sans votre présence et votre amour. Je suis si chanceuse de vous avoir à mes côtés.

A ma deuxième famille : Mes chère grand-mères **« YAYA »** & **« Seti »**, Mes cher oncles «**HACENE**» &

« NADJIB » et leurs familles, Mes **chère tantes**, Mes cousines adorées **« NIHAD »** & **« NANI »**, **« WASSILA »** & son mari **« MUSTAPHA »**, **« AMEL »** & son mari **« NACIM »**, Mes chers cousins **« AMINE »**, **« OUSSAMA »**, **« IMAD »** et **« RACHID »**

Aucun langage ne saurait exprimer mon respect et ma considération pour votre soutien et encouragements. Que Dieu le Tout Puissant vous garde et vous procure santé et bonheur.

A **« AMAYAS »** qui m'a soutenu tout au long de ce mémoire

A Mes meilleures amies **ACHWAK**, **SARAH**, **SADJIA**, et **NESSRINE**

En témoignage de l'amitié qui nous unit et des souvenirs de tous les moments que nous avons passés ensemble, je vous dédie ce travail et je vous souhaite une vie pleine de santé et de bonheur.

LISTE DES ABREVIATIONS

ABREVIATION	SIGNIFICATION
A/D	Aérodrome.
AFM	Airplane Flight Manual.
ASDA	Accelerate-Stop Distance Available (Distance utilisable pour l'accélération-arrêt).
CAP	La circulation aérienne publique.
CD	Disque Compact.
DACM	Direction de l'Aviation Civile et Météorologique.
DGSN	Direction Générale de la Sureté Nationale.
DME	Distance Measuring Equipment (Équipements de mesure de distance).
DOA	Direction des Opérations Aériennes.
DPF	Direction de Police des Frontières.
EASA	European Union Aviation Safety Agency.
EFB	Electronic Flight Bag.
FAA	Federal Aviation Administration.
FIR	Flight Information Region (Région d'information de vol).
FMC	Flight Management computer.
FMS	Flight Management System.
IATA	Association International de Transport Aérien.
IOSA	IATA Operational Safety Audit.
ISARP	IOSA Standards and Recommended Practices.
ISM	Manuel des normes d'IOSA.

LDA	Landing Distance Available (Distance utilisable à l'atterrissage).
METAR	METeorological Aerodrome Report.
MMD	Masse maximale au décollag.
NDB	Non Directional Beacon (Balise non directionnelle).
NOTAM	Notice To AirMen (avis aux navigateurs aériens).
OACI	Organisation de l'Aviation Civile International.
PCMCIA	Personal Computer Memory Card International Association.
PCN	Pavement Classification Number (Le numéro de classification de la chaussée).
PNCQSAC	Programme National de Contrôle Qualité en Sureté de l'Aviation Civil.
PNFSAC	Programme National de Formation en Sureté de l'Aviation Civil.
PNSAC	Programme National de Sureté de l'Aviation Civil.
PSE	Programme de Sureté Exploitant.
QFU	La direction magnétique d'une piste par rapport au Nord magnétique.
QNH	Pression Barométrique Corrigée au niveau moyen de la mer.
RSFTA	Réseau du Service Fixe des Télécommunications Aéronautiques.
RWY	RunWay.
SARPs	Standards and Recommended Practices.
SeMS	Security Management System.
SID	Standard Instrument Departure (Départ standard aux instruments).
SMS	Safety Management System.

SSLIA	Service de Sauvetage et de Lutte contre l'Incendie d'Aérodrom.
STAR	Standard Terminal ARrival (Arrivée Terminale Standard).
SWY	StopWay.
TAF	Terminal Aerodrome Forecast (Prévisions d'aérodrome terminal).
TEMSI	TEMps Significatif.
TODA	Take-Off Distance Available (Distance utilisable au décollage).
TORA	Take-off Run Available (Distance de roulement utilisable au décollage).
TWY	TaxiWay.
UE	Union Européen.
USB	Universal Serial Bus (bus informatique avec une transmission des données en série).
V1	La vitesse au-delà de laquelle le décollage ne doit plus être interrompu.
V2	Vitesse de sécurité au décollage à 35 pieds du sol en bout de piste.
VR	Vitesse de rotation.
V_{MBE}	Maximum Brake Energy (La vitesse maximale à partir de laquelle un avion peut initier un décollage interrompu et rester dans les limites de chaleur du système de freinage).
VOR	VHF Omnidirectional Range.

LISTE DES FIGURES

LISTE DES TABLEAUX

TERMINOLOGIES LIÉE A LA SURETÉ

Les termes qui sont définis dans le Vocabulaire de l'aviation civile internationale (Doc 9713) et dans les Annexes sont employés ici conformément aux définitions et aux usages de ces documents. Des termes différents sont parfois utilisés à l'échelle mondiale pour désigner des installations, services, procédures et autres notions qui concerne l'exploitation et la planification des aéroports. Dans ce mémoire, on s'est efforcé d'employer autant que possible les termes dont l'usage est le plus répandu à l'échelle internationale.

Actes d'intervention illicite : Actes ou tentatives d'actes de nature à compromettre la sécurité de l'aviation civile et du transport aérien incluant, sans s'y limiter :

— la capture illicite d'un aéronef ;

— la destruction d'un aéronef en service ;

— la prise d'otages à bord d'un aéronef ou sur un aérodrome ;

— l'intrusion par la force à bord d'un aéronef, dans un aéroport ou dans l'enceinte d'une installation aéronautique ;

— l'introduction à bord d'un aéronef ou dans un aéroport d'une arme, d'un engin dangereux ou d'une matière dangereuse, à des fins criminelles ;

— l'utilisation d'un aéronef en service dans le but de causer la mort, des blessures corporelles graves ou des dégâts importants à des biens ou à l'environnement ;

— la communication d'informations fausses de nature à compromettre la sécurité d'un aéronef en vol ou au sol, de passagers, de navigants, de personnel au sol ou du public, dans un aéroport ou dans l'enceinte d'une installation de l'aviation civile. [1]

Analyse du risque : L'analyse est le processus consistant à classer des faits en utilisant des méthodes, des outils ou des techniques spécifiques. [2]

Attaque : Une atteinte à la sécurité d'un bien. [1]

Atténuation des risques : Processus d'intégration de défenses ou de contrôles préventifs pour réduire la gravité et/ou la probabilité de la conséquence prévue d'un danger. [2]

Audit de sûreté : Examen approfondi de l'application de tous les aspects de la mise en œuvre du programme national de sûreté de l'aviation civile. [1]

Autorité compétente de sûreté de l'aviation : Autorité désignée par un État, au sein de son administration, et chargée de l'élaboration, de la mise en œuvre et de l'application du programme national de sûreté de l'aviation civile. [1]

Blessure fatale : est définie comme une blessure aboutissant à la mort dans trente jours après l'accident. [2]

Blessure grave : Toute blessure que subit une personne au cours d'un accident et qui :

a) Nécessite l'hospitalisation pendant plus de 48 heures, cette hospitalisation commençant dans les sept jours qui suivent la date à laquelle les blessures ont été subies ;

b) Se traduit par la fracture d'un os (exception faite des fractures simples des doigts, des orteils ou du nez) ;

c) Se traduit par des déchirures qui sont la cause de graves hémorragies ou de lésions d'un nerf, d'un muscle ou d'un tendon ;

d) Se traduit par la lésion d'un organe interne ;

e) Se traduit par des brûlures du deuxième ou du troisième degré ou par des brûlures affectant plus de 5 % de la surface du corps ;

f) Résulte de l'exposition avérée à des matières infectieuses ou à un rayonnement nocif. [2]

Blessure mineure (secondaire) : est une blessure qui exige un traitement médical, mais qui ne peut être classifié comme une blessure sérieuse. Il n'exige pas de traitement médical et/ou l'hospitalisation pendant plus de 48 heures. [2]

Conséquence : L'impact ou l'effet de la perte ou de résultat du scénario. [3]

Contrôle de sûreté : Mesures établies visant à empêcher l'introduction d'armes, d'explosifs ou d'autres engins, articles ou substances dangereux qui peuvent être utilisés pour commettre un acte d'intervention illicite. [1]

Culture sûreté : Est un ensemble de normes, de croyances, de valeurs, d'attitudes et d'hypothèses inhérentes au fonctionnement quotidien d'une organisation et reflétées par les actions et les comportements de toutes les entités et du personnel de l'organisation. [3]

Cyber -Attaque : C'est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques. [2]

Cyber -Security : L'ensemble des technologies, des contrôles et des mesures, ainsi que des processus et des pratiques conçus pour garantir confidentialité, intégrité, disponibilité et protection globale des systèmes, réseaux, programmes, appareils, informations et données contre les attaques, les dommages, l'accès non autorisé, l'utilisation et/ou l'exploitation. [2]

Danger : Une condition, objet ou activité qui a le potentiel de causer des blessures, des dommages à l'équipement ou aux structures, une perte de matériel, ou une réduction de la capacité à exécuter les fonctions assignées. [2]

Destruction complète d'un avion : Signifie, que les dégâts portés à l'avion ont causé le démantèlement structurel sévère de composants majeurs par l'impact, l'explosion ou le feu et l'avion est apparemment au-delà de la restauration. [2]

Défenses : Mesures d'atténuation spécifiques, contrôles préventifs ou mesures de rétablissement mises en place pour empêcher qu'un danger se réalise ou s'accroisse jusqu'à une conséquence indésirable. [2]

Dégâts mineurs (secondaires) à un avion : signifient les dégâts exigent la réparation provisoire ou permanente immédiate, mais qui est facilement réparable. [2]

Dégâts substantiels à un avion : signifient des dégâts qui affectent défavorablement la résistance structurelle, l'exécution ou les caractéristiques de vol d'un avion et qui exigerait normalement la réparation majeure ou le remplacement du composant affecté. [2]

Différence entre sureté et sécurité : La sécurité se concentre sur la prévention des accidents et des défaillances involontaires, tandis que la sûreté vise à prévenir les actions malveillantes et intentionnelles. Ces deux concepts sont importants dans

différents domaines pour assurer la protection globale des individus, des systèmes et de l'environnement.

Évaluation de risque : Processus de détection des dangers et d'évaluation systématique des risques associés. [3]

Les Expositions : sont des erreurs non inhérentes au logiciel, au micro logiciel, au matériel ou au composant de service qui l'exposent au risque d'être exploité, telles que des erreurs de configuration, des ports ouverts et des informations d'identification faibles.

Gestion des risques : Processus visant à déterminer les risques, évaluer leurs implications, et faire un plan d'action et évaluer les résultats. [3]

Matrice de risque : Une matrice de risque est un outil d'évaluation des risques qui permet de classer les risques en fonction de leur probabilité et de leur gravité. Cette méthode peut également être appliquée pour évaluer les risques de sûreté.

Menace : Appelée également facteur contributif. Actions, omissions, événements, conditions ou une combinaison de ceux-ci, qui ont conduit à un événement indésirable ou à un accident. [2]

Menaces terroristes : Les compagnies aériennes sont des cibles privilégiées des terroristes en raison de leur visibilité et de leur impact potentiel sur un grand nombre de personnes. Les attaques terroristes peuvent prendre différentes formes, comme des détournements d'avions, des attentats à la bombe ou des attaques à l'arme à feu. [2]

Prédictive : Recherche dans l'activité opérationnelle normale, d'évolutions non souhaitées dans la conduite des opérations, pour identifier de futurs problèmes potentiels. [2]

Proactive : Anticipation des problèmes par la détection des dangers potentiels à travers le traitement du retour d'expérience et l'analyse des activités quotidiennes de l'entreprise. [2]

Programme de sûreté : Mesures écrites adoptées pour assurer la protection de l'aviation civile internationale contre des actes d'intervention illicite. [1]

Réactive : Analyse des événements. [2]

Risque : Probabilité qu'un acte d'intervention illicite soit exécuté avec succès contre une cible donnée, en se basant sur une évaluation de la menace, de la conséquence et de la vulnérabilité. [2]

Scénario de la menace : Identification et description d'un acte crédible d'intervention illicite comprenant une cible, des moyens et des méthodes d'attaque (mode opératoire), et l'adversaire. [2]

Sécurité : État dans lequel les risques liés aux activités aéronautiques concernant, ou appuyant directement, l'exploitation des aéronefs sont réduits et maîtrisés à un niveau acceptable. [2]

Sureté : Protection de l'aviation civile contre les actes d'intervention illicite. Cet objectif est réalisé par une combinaison de mesures ainsi que de moyens humains et matériels. [1]

Sûreté aéroport : Inclus le contrôle et la gestion du système de permis d'accès (badge ou laissez-passer) pour les zones à accès réglementé, l'inspection /filtrage et la fouille manuelle des équipages, et de leurs bagages de cabine et de soute, lors de leur accès en zones contrôlées réglementées de l'aéroport, ainsi une inspection filtrage des bagages de cabine et de soutes au niveau de l'aérogare.

Ces taches sont effectuées par la DGSN. [3]

Sûreté passagers et bagages : Les passagers, les diplomates et d'autres personnes privilégiées, les passagers à mobilité réduite et cas médicaux sont soumis ainsi que leurs bagages de cabine à une inspection filtrage, de même que les passagers malades, ces passagers bénéficient des sièges qui sont les plus appropriées à leurs besoins. [3]

Le personnel au sol de DGSN empêchera l'embarquement de tout passager ou groupe de passagers dont le comportement est suspect, en vols c'est à la discrétion du CDB, en coordination avec le chef de cabine. [3]

Sûreté d'aéronefs : Des mesures de sûreté sont appliquées pour empêcher toute tentative d'acte de malveillance par l'introduction d'armes, ou d'explosifs susceptibles d'être utilisé pour commettre un acte d'intervention illicite : avant, pendant l'embarquement et durant le vol. [3]

Une liste de vérification pour chaque type d'aéronef est éditée et distribuée aux effectifs concernés. Cette dernière est destinée aux équipages de conduite, et aux personnel au sol (DOS/DS) concerné par cette mission et les taches y afférentes.

La compagnie Air Algérie est responsable de la protection de ses aéronefs lorsqu'ils ne sont pas en service et qu'ils se trouvent dans une zone privative (ateliers, hangars…etc.). [3]

Les Vulnérabilités : sont des failles dans les logiciels informatiques, les micros logiciels, le matériel et les composants de service qui peuvent être exploitées par un acteur malveillant pour obtenir un accès non autorisé et mener une cyberattaque.

INTRODUCTION GÉNÉRALE

« Croire que le transport aérien est à l'abri de la cyber menace revient à se voiler la face. C'est un sujet sérieux auquel nous devons nous attaquer »

‘’A affirmé en 2016, Patrick Ky, directeur de l'Agence Européenne de Sécurité Aérienne AESA’’.

Grâce à l'intégration continue et rapide de nouvelles technologies, le secteur de l'aviation devient de plus en plus interconnecté et dépendant des systèmes informatiques.

Le système aéronautique mondial, est l'un des systèmes de technologies de l'information et des communications (TIC) le plus complexes et le plus intégrés au monde, est une cible potentielle pour les cyber-attaques de grande envergure.

Cependant, l'évolution rapide des technologies s'accompagne de celle des menaces nombreuses et variées, il peut s'agir de vol de données de passagers, de blocage de systèmes opérationnels, de modifications des informations, de brouillages des communications ou encore de prises de commande de logiciels ou d'aéronefs à distance par des acteurs malveillants. Les attaques peuvent affecter les infrastructures aéroportuaires, les aéronefs ou les systèmes de navigation aérienne, à travers des failles des systèmes de sécurité informatique ou par l'intermédiaire d'une menace interne. Certains sont intentionnelles d'autre ne sont que des dommages collatéraux : une attaque sur un système d'exploitation pourrait toucher les ordinateurs de compagnies aériennes. Si les mesures de Cyber-Sécurité appropriées ne sont pas mises en place pour faire face à cette menace évolutive, l'aviation civile peut être en danger.

Reconnaissant la nature multiforme et multidisciplinaire du Cyber-Sécurité, et notant que les cyber-attaques peuvent simultanément toucher une vaste gamme de domaines et s'étendre rapidement, il faut impérativement élaborer une vision commune et définir une stratégie mondiale de Cyber-Sécurité. La vision OACI de la Cyber-Sécurité mondiale est que le secteur de l'aviation civile est résilient aux cybers

attaques et qu'il reste sûr et fiable au niveau mondial, tout en continuant à innover et à croître.

Les préparations des vols sont également visées par les cyberattaques. A cet effet j'ai réalisé ce projet, dont les objectifs sont les suivants :

- Faire une matrice de risque liée aux évènements de sureté pour la compagnie aérienne «Air Algérie », et un programme informatique en langage Python qui fait l'évaluation des risques.
- Etudie les différents cas de cyber attaques ciblant le domaine de la préparation des vols.
- Analyser les mesures de cyber sécurité au niveau d'Air Algérie.
- Evaluer les risques des cyberattaques en utilisant la méthode BOW TIE.

Ce projet est structuré en quatre chapitres afin de fournir une analyse complète. Le premier chapitre présente un aperçu de la compagnie aérienne "Air Algérie" et de sa direction de sureté, où j'ai passé mon stage de fin d'études. Le deuxième chapitre examine le cadre réglementaire national et international en matière de sûreté de l'aviation civile. Le troisième chapitre fournit des informations générales sur la gestion des risques, les méthodes d'évaluation des risques, les menaces lis à la sûreté aérienne, ainsi qu'une présentation de la matrice des risques. Il met également en évidence le programme python dont j'ai mentionné dans les objectifs. Enfin, le quatrième chapitre se concentre sur l'évaluation des risques liés aux cyberattaques.

CHAPITRE I

PRÉSENTATION DE LA COMPAGNIE {AIR ALGÉRIE}

I.1. INTRODUCTION

AIR ALGERIE (code IATA : AH, code OACI : DAM), est une société par actions (S.P.A), elle tire son expérience de son ancêtre la CGT (Compagnie Générale de Transport).

Air Algérie est chargée d'assurer les services aériens de transport public réguliers ou non réguliers, nationaux ou internationaux de personnes, de marchandises, de courrier et de travail aérien, dans le cadre du plan national de développement économique et social.

Dans ce chapitre je vais vous donner un aperçu sur la compagnie ainsi que sa direction de sureté.

I.2. HISTORIQUE D'AIR ALGÉRIE

Air Algérie a été créée en 1974 et son réseau était principalement en France. Son siège social était situé à Paris et ses opérations étaient limitées au territoire algérien et à la France.

En 1963, la compagnie générale des transports aériens est passée sous la tutelle du ministère des transports et elle est devenue un instrument privilégié du gouvernement pour la politique du transport aérien en Algérie.

En 1970, le gouvernement algérien a acquis 83% des actions de la compagnie, en rachetant celles détenues par des sociétés étrangères autres qu'Air France. Le 15 décembre 1974, Air Algérie est devenue une entreprise entièrement nationale en rachetant les 17% d'actions restantes.

En 1975, la compagnie aérienne a absorbé les activités de la société de travail aérien (S.T.A) et a été désignée comme "société nationale de transport et travail aérien" par une ordonnance promulguée en février 1979.

Au fil des années, Air Algérie a ouvert de nouvelles bases, élargi ses lignes et effectué des ventes d'aéronefs pour s'adapter aux demandes du marché. [5]

I.3. RESEAUX D'AIR ALGÉRIE

AIR ALGÉRIE dispose d'un réseau de 77 destinations dont :

44 destinations à l'international desservant 27 pays :

- 10 en France,
- 18 en Europe,
- 09 Maghreb - Moyen orient,
- 05 en Afrique,
- 02 lignes long-courrier vers le Canada et la Chine.

Et 32 destinations sur le réseau national. [6]

I.4. MISSIONS D'AIR ALGÉRIE

- Attribuer des conventions et des accords pour exploiter les réseaux internationaux et domestiques en vue d'assurer le transport des personnes, fret, bagages, et courriers quel que soit sa nature : régulier ou non (saisonnier, charter) …
- L'avitaillement des avions dans des conditions fixées par le ministère du transport (l'entretien, la réparation, la révision et toute autre opération de maintenance des aéronefs et équipements pour son compte et le compte des tiers).
- La vente et l'émission de titres de transport pour son compte ou pour le compte d'autres entreprises de transport
- Assurer la réparation, la révision, la maintenance, l'entretien, l'achat et la location des aéronefs. [7]

I.5. MOYENS D'AIR ALGÉRIE

Pour que chaque compagnie aérienne maintienne son haut niveau de production, elle s'appuie sur une armée de travailleurs et une flotte importante. AIR ALGERIE fait partie des grandes compagnies du monde, elle est basée sur les :

I.5.1. MOYENS HUMAINS

Air Algérie compte un effectif de 9327 employés ; les catégories de son personnel se répartissent comme suit :

- 8140 personnels au sol.
- 502 personnels navigants techniques.
- 685 personnels navigants commerciaux.

Sachant que tous son personnel est de nationalité algérienne. [6]

I.5.2. MOYENS DE PRODUCTION / FLOTTE

Air Algérie dispose de 55 Avions répartis comme représente le Tableau 1 :

Tableau I.1 : Flotte d'Air Algérie. [6]

Avions	Modèle	Nombre
Avions passagers	A330-200	08
	B737-800	24
	B737-600	05
	ATR72-500	10
	ATR72-600	03
Avions convertibles PAX/Cargo	ATR72-500	02
	B737-700C	02
Avion-cargo	*B737-800 BCF*	*01*

I.6. LA DIRECTION DE SURETÉ

L'organisation de la direction de la sûreté s'inscrit dans le cadre de la protection optimale des biens et des personnes, prévention des risques relatifs aux actes d'intervention illicites tels que définis par la convention OACI/DACM (PNSAC).

La sûreté est une fonction organique et permanente, placée sous l'autorité d'un Directeur de la sûreté nommé par le Président Directeur général. Son fondement

légal est justifié par les dispositions de l'ordonnance 95-24, de septembre 1995. Sur le plan de la réglementation internationale elle assure les missions de sûreté conformément à l'annexe17, de l'OACI les différentes recommandations de l'IATA et les exigences des pays desservis.

Au plan national, ses prérogatives prennent source dans le Programme national de la Sûreté de l' Aviation civile (PNSAC).

Cette Direction permet de :

- Identifier les rôles et les responsabilités en matière de sûreté :
- Piloter la fonction sûreté aérienne et la sûreté interne
- Évaluer les besoins de protection
- Communiquer, informer, sensibiliser et former aux procédures de sûreté ;
- Mesurer et évaluer la performance du système de management de la sûreté mis en place.
- Contrôle des performances du système de gestion de la sûreté. [8]

I.7. CONCLUSION

‘’Assurer la sureté’’ dans le transport aérien est l’une des priorités de la compagnie aérienne. Surtout face à l’augmentation exponentielle du transport aérien et à l’augmentation des actes malveillants dans le monde.

D’après ce chapitre on conclut que la Direction de Sureté et un pilier essentiel dans l’organisme de la compagnie aérienne (Air Algérie).

CHAPITER II

LE CADRE RÉGLEMENTAIRE INTERNATIONAL ET NATIONAL DE LA SURETÉ DE L'AVIATION CIVILE

II.1. INTRODUCTION

Le cadre réglementaire de l'aviation civile est un ensemble de règles, de normes et de procédures établies par les autorités compétentes pour la sécurité, l'efficacité et la gestion de l'aviation civile dans un pays donné. Ces réglementations sont conçues pour régir divers aspects de l'aviation, tels que la conception et la certification des aéronefs, la formation et les qualifications des pilotes, les opérations aériennes, la navigation, la sécurité des passagers et des équipages, la protection de l'environnement, la sureté aérienne, et bien d'autres encore.

Ce chapitre englobe le cadre réglementaire national et international de l'aviation civile, ainsi que les exigences de la compagnie aérienne dans le domaine de la sureté aérienne et la vision de l'OACI sur le cyber sécurité.

II.2. CADRE RÉGLEMENTAIRE INTERNATIONAL

II.2.1. ORGANISATION DE L'AVIATION CIVILE INTERNATIONALE

Une organisation créée le 7 décembre 1944, lors de la Convention de Chicago relative à l'aviation civile internationale, et officiellement devenue une agence spécialisée des Nations Unies en 1947. L'OACI a pour objet « d'assurer la coopération internationale et la plus grande uniformité possible des réglementations et normes, procédures et organisations relatives aux questions d'aviation civile dans le monde ». A ce jour, l'OACI gère plus de 12 000 SARPs ventilées dans les 19 Annexes à la Convention de Chicago. Le Comité d'intervention de l'OACI et du transport aérien a conduit son Conseil le 22 mars 1974 et adopter les Normes et pratiques recommandées contenues dans l'Annexe 17 de la Convention de Chicago, qui ont jeté les bases du Plan de sûreté de l'aviation civile de l'OACI. Suite aux attentats du 11 septembre 2001, le règlement n° 2320/2002 d'application directe, a été adopté pour protéger l'aviation civile d'actes d'intervention illicite et pour jeter les bases d'une interprétation commune de l'Union européenne de l'annexe 17 des États membres de la Convention de Chicago. Ce règlement a été remplacé par le nouveau règlement n° 300/2008 en mars 2008. [9]

Il s'appuie sur les principes suivants :

- ➔ Chaque État membre est responsable de la sûreté des vols quittant son territoire, conformément au principe de la responsabilité de l'État hôte défini par l'OACI ;
- ➔ Tous les passagers, les membres du personnel et les bagages sont inspectés et filtrés avant l'embarquement.

Ce règlement impose aux exploitants aéroportuaires l'obligation de mettre en œuvre des mesures de sûreté sur le site aéroportuaire en plus des mesures à prendre par les compagnies aériennes et les entreprises dans la zone réservée.

La plupart des règles de sécurité de l'aviation civile sont établies par des autorités internationales et européennes. [11]

II .2.1.1. ANNEXE 17 : Sûreté

L'annexe 17 établit les premières définitions dans l'industrie telle que contrôle, agent habilité et zone de sûreté réglementée. Zones d'exclusion de sûreté et conseils sur les principaux problèmes de sûreté, notamment :

1. Mesures et procédures visant à empêcher tout accès non autorisé à l'aérodrome.
2. Élaboration de programmes de formation.
3. Isolement des passagers soumis à un contrôle de sécurité.
4. Inspection des aéronefs à la recherche d'armes dissimulées ou d'autres dispositifs dangereux.
5. Transport de prisonniers.
6. Transport de bagages enregistrés par les forces de l'ordre.
7. Contrôle du fret et du courrier.
8. Incorporation des considérations de sécurité dans la conception des aéroports.
9. Vérification des antécédents des employés de l'aviation.
10. Rapprochement des passagers et des bagages.
11. Mesures de sécurité pour les fournitures et les opérateurs de restauration.

Et, après 2001 :

1. Normes de contrôle d'accès.

2. Nouvelles normes pour le contrôle des passagers, des bagages à main et des bagages enregistrés.
3. Personnel de sécurité à bord des avions.
4. Protection du cockpit. [12]

II.2.1.2. DOC 8973 : Manuel de Sûreté de l'Aviation Civile

Le Manuel de sûreté de l'aviation a été conçu pour aider les États à promouvoir la sécurité et la sûreté de l'aviation civile. Il a pour objet d'assister les États dans la prévention des actes d'intervention illicite et, s'il y a lieu, dans la riposte à de tels actes, par la mise en œuvre des éléments ci-après :

- Cadre juridique et supervision de la sûreté ;
- Conception, infrastructure et équipement des aéroports ;
- Recrutement, sélection, formation et certification ;
- Procédures et application de mesures de sûreté.

Le Manuel de sûreté de l'aviation contient des éléments d'orientation sur la manière dont les États peuvent se conformer aux normes et pratiques recommandées de l'Annexe 17. Bien que les méthodes de conformité indiquées soient fondées sur des pratiques et des procédures généralement acceptées et courantes dans l'aviation civile internationale, elles ne sont pas les seules voies. D'autres façons de se conformer aux normes et aux pratiques recommandées décrites dans l'Annexe17 peuvent être tout aussi appropriées. [1]

II.2.1.3. L'OACI et la Cyber-Sécurité

La vision OACI du cyber sécurité mondiale est que le secteur de l'aviation civile est résilient aux cyberattaques et qu'il reste sûr et fiable au niveau mondial, tout en continuant à innover et à croître.

Cette vision peut être réalisée comme suit :

- Reconnaissance par les États membres des obligations que leur impose la Convention relative à l'aviation civile internationale (Convention de Chicago) d'assurer la sécurité, la sûreté et la continuité de l'aviation civile, en tenant compte de cyber sécurité ;

- Coordination du cyber sécurité de l'aviation entre les autorités des États afin d'assurer l'efficacité et l'efficience de la gestion mondiale des risques de cyber sécurité ;
- Engagement de toutes les parties prenantes de l'aviation civile à développer plus avant la cyber résilience, en assurant la protection contre les cyberattaques qui peuvent influer sur la sécurité, la sûreté et la continuité du système de transport aérien.

La stratégie s'aligne sur d'autres initiatives de l'OACI liées à la cybernétique et coordonnées avec les dispositions correspondantes en matière de gestion de la sécurité et de la sûreté. Les objectifs de la stratégie seront atteints grâce à une série de principes, de mesures et d'actions dont le cadre repose sur sept piliers, à savoir :

- Coopération internationale
- Gouvernance
- Législation et règlements efficaces
- Politique de cyber sécurité
- Partage de l'information
- Gestion des incidents et planification d'urgence
- Renforcement des capacités, formation et culture de cyber sécurité [4]

II.3. CADRE RÉGLEMENTAIRE NATIONAL

II .3.1. DIRECTION DE L'AVIATION CIVILE ET MÉTÉOROLOGIQUE

La Direction de l'Aviation Civile et Météorologique est une direction centrale du Ministère des Transports, elle-même subdivisée en deux directions : celle de l'aviation civile et celle de la météorologie.

→Elle est chargée de :

- L'étude, la coordination, la synthèse et le contrôle des travaux liés au développement de son domaine d'activité ;
- Assurer la sûreté, la sécurité, et la régularité de la navigation aérienne dans l'espace aérien national ;
- Préparer les plans de développement des infrastructures et des matériels aéronautiques ;

- ❖ Elaborer les cartes aéroportuaires et suivre leur mise en œuvre ;
- ❖ Certifier les aérodromes et les prestations des services de navigation aérienne
- ❖ Définir les conditions de l'assistance météorologique de l'ensemble des usagers ;
- ❖ Constituer une banque de données relative à la DACM et d'en assurer le suivi.

→En liaison avec d'autres structures concernées elle est chargée de :

- ❖ Superviser la formation et le perfectionnement dans les métiers et les professions de l'aviation civile et de la météorologie ;
- ❖ Préparer et suivre les accords internationaux, bilatéraux et multilatéraux relatifs à l'aviation civile et la météorologie ;

→Elle comprend quatre (4) sous-directions :

- ❖ La S/D des infrastructures aéroportuaires,
- ❖ La S/D de la régulation des transports aériens,
- ❖ La S/D du contrôle de la sécurité et de la navigation aérienne,
- ❖ La S/D de la météorologie.

La DACM est responsable de l'élaboration et de la mise à jour de Programme National de Sureté de l'Aviation Civile (PNSAC) en concertation avec les services de la Direction de Police des Frontières (DPF), et les services de la Direction Générale de la Sureté National (DGSN), ainsi que toutes les parties concernées. [11]

II .3.2. <u>DIRECTION GÉNÉRALE DE LA SURETÉ NATIONALE</u>

La direction générale de la sûreté nationale (DGSN), est l'autorité chargée de coordonner la mise en œuvre des contrôles de sûreté au niveau des aéroports ouverts à la circulation aérienne publique (CAP).

La DGSN a pour missions :

- ➢ De coordonner la mise en œuvre des mesures de sûreté relatives du au PNSAC, PNCQSAC et PNFSAC.

- L’établissement des moyens de coordination des activités entre les différents organismes concernés par le PNSAC, PNCQSAC et PNFSAC ou qui en sont responsables.
- L’évaluation et communication à l’Autorité Chargée de l’Aviation Civile des informations concernant les menaces visant la sûreté de l’aviation civile.
- La communication à l’Autorité Chargée de l’Aviation Civile de tout acte d’intervention illicite visant la sûreté de l’aviation civile.
- La proposition à l’Autorité Chargée de l’Aviation Civile de suggestions, notamment la réévaluation des mesures et procédures de sûreté à la suite d'un acte d'intervention illicite et prise des dispositions nécessaires pour corriger les insuffisances. [11]

II.4. LES RECOMMENDATIONS

II .4.1. INTERNATIONAL AIR TRAFIC ASSOCIATION

II.4.1.1. Définition

L'IATA correspond à l'association internationale des transporteurs aériens. Il s'agit d'une importante organisation commerciale regroupant nombreuses compagnies aériennes volontaires, originaires de tous pays du monde entier.

Cette organisation n'a rien à voir avec l'OACI qui est une organisation intergouvernementale officielle à caractère obligatoire (Les membres de l'OACI sont des Etats, tandis que ceux de l'IATA sont des transporteurs).

IATA a été créée pour succéder à l’International Air trafic Association qui résidait à La Haye depuis 1919. A ses débuts, l'association comprenait 31 pays membres avec 57 compagnies aériennes. Après plus de 60 ans d'existence, aujourd'hui, IATA comprend 230 compagnies aériennes qui sont devenues membres sur 126 pays dans le monde entier. Ce chiffre représente les 95% de toutes les compagnies aériennes mondiales. [13]

I.4.1.2. But et objectif

L'objectif de l'IATA est de promouvoir la sécurité des vols, améliorer les services, élaborer des standards commerciaux, pour le bénéfice des passagers.

Elle se bat pour les intérêts des compagnies aériennes mondiales, en luttant contre les éventuelles réglementations ou charges inadaptées. Si l'objectif principal de l'association est de représenter ces compagnies aériennes, leurs missions sont nombreuses au profit des compagnies de transport aériennes et également au profit de l'environnement.

IATA travaille ainsi pour aider les compagnies aériennes à préserver leurs intérêts. [13]

II.4.2. IATA OPERATIONNEL SAFTY AUDIT

L'IOSA (IATA Opérationnel Safety Audit) est une certification sécurité touchant 8 domaines opérationnels, visant la gestion de la sécurité, sûreté, des compagnies aériennes. Le registre IOSA compte maintenant 308 transporteurs, dont 224 sont membres de l'IATA.

La check liste IOSA développée afin de mettre en œuvre les bonnes pratiques recommandées de l'industrie du transport aérien.

Le manuel des normes de l'IOSA (ISM) est la seule source de critères d'évaluation à utiliser par les auditeurs lorsqu'ils effectuent un audit, il est publié en vue de fournir les normes et les pratiques recommandés de l'IOSA (ISARP), les documents d'orientation associés et d'autres informations nécessaires à un opérateur pour se préparer avec succès à un audit. L'ISM peut également servir de guide à tout opérateur souhaitant structurer ses systèmes de gestion et de contrôle opérationnels conformément aux dernières normes industrielles.
Ce document se compose de huit sections, à chaque section est associé un identifiant de trois lettres (entre parenthèses ci-dessous) comme suit :

- Section 01 : système d'organisation et de gestion (ORG) ;
- Section 02 : opérations de vol (FLT) ;
- Section 03 : contrôle opérationnel et répartition des vols (DSP) ;
- Section 04 : ingénierie et maintenance des aéronefs (MNT) ;
- Section 05 : opérations en cabine (CAB) ;
- Section 06 : opérations d'assistance en escale (GRH) ;
- Section 07 : opérations de fret (CGO) ;
- Section 08 : gestion de sûreté (SEC)

Les exigences de sûreté publiée dans les annexes de l'OACI constituent la principale source des spécifications contenues dans les ISARPs. [14]

II.5. LES PROGRAMMES DE SURETÉ

II.5.1. LE PROGRAMME NATIONAL DE SURETÉ DE L'AVIATION CIVILE {PNSAC}

Le programme National de Sûreté de l'Aviation Civile (PNSAC) a été élaboré conformément aux dispositions de la loi 98-06 fixant les règles générales relatives à l'aviation civile, modifiée et complétée, notamment son article 16 qui exige de l'autorité chargée de l'aviation civile d'élaborer ou de faire élaborer un programme national de sûreté de l'aviation civile, qui compte l'ensemble des mesures et des actions destinées à assurer la protection de l'aviation civile contre les actes d'intervention illicite. Ceci étant en conformité avec les normes et pratiques recommandées de l'annexe 17 - sûreté - à la convention relative à l'aviation civile internationale, qui impose à chaque Etat membre d'établir et de mettre en œuvre un programme national de sûreté de l'aviation civile, et de s'assurer que toutes les personnes impliquées le connaissent et l'appliquent. [15]

II.5.1.1. Objectifs et applicabilité du Programme

L'objectif de PNSAC est d'énoncer la politique de l'État en matière de sûreté de l'aviation civile, de préciser l'organisation, les procédures et pratiques pour riposter rapidement à toute menace, et de récapituler les références réglementaires relatives à la sûreté de l'aviation civile, décrit l'organisation des services de l'Etat, leurs missions et leurs responsabilités, précise les mesures et les moyens de sûreté, décrit les dispositions applicables en matière de contrôle qualité, et les sanctions encourues en cas de manquement.

Ce programme est conçu pour satisfaire aux normes et pratiques recommandées de l'Annexe 17 à la Convention relative à l'aviation civile internationale, ainsi qu'aux dispositions connexes relatives à la sûreté de l'aviation et figurant dans les Annexes 2, 6, 9, 10, 11, 13 ,14 et 18 de l'OACI.

Les mesures visant à assurer la protection contre les actes d'intervention illicite prévues par le PNSAC sont applicables à tous les services aériens, de transport

public, réguliers, non réguliers, internationaux, intérieurs, de travail aérien, d'aviation légère et les services aériens privés, ainsi à tout aéroport, aérodrome et hélistation, aux prestataires de services aéronautiques et toutes les autres entités qui ont un rôle dans la sûreté de l'aviation civile et dans la mise en œuvre dudit programme. [15]

II.5.2. PROGRAMME DE SURETÉ ÉXPLOITANT {PSE}

II.5.2.1. Objectif

Produit de l'application de la règlementation nationale et internationale en matière de Sûreté de l'Aviation Civile, des normes et exigences supplémentaires en la matière, le programme de sûreté est le reflet de l'organisation et des dispositions actuelles en matière de sûreté au niveau de l'entreprise Air Algérie.

Le programme de sûreté englobe et formalise l'ensemble des procédures de sureté des différentes structures opérationnelles de l'entreprise, des programmes de formation spécifique de sureté et de contrôle qualité sûreté, en réponses aux situations et/ou actes portant et/ou pouvant porter atteinte à la sûreté des passagers et des aéronefs ainsi qu'aux installations aéroportuaires.

Il constitue ainsi un système de gestion de la sûreté, étendu et orienté vers une évolution pertinente et permanente des dispositions de sûreté en fonction de l'évolution de la règlementation, des facteurs humains, organisationnels, techniques et du développement des activités. [3]

II.5.2.2. Domaines d'application

Le présent manuel est applicable à l'ensemble des activités opérationnelles au sein de l'entreprise Air Algérie et/ou ayant un lien avec ses dernières tels que les fournisseurs et sous-traitants externes.

Il permet ainsi aux différentes structures de la compagnie, ainsi qu'aux sous-traitants de répondre aux normes exigées en matière de sureté.

Les mesures de sûreté décrites dans ce programme ayant pour objective d'assurer la protection contre les actes d'interventions illicites, sont appliquées de la même manière pour les vols domestiques et les vols internationaux.

Ce programme décrit fidèlement les exigences normatives, législatives, et règlementaires (nationale et internationale). Il assure notamment l'implémentation et la diffusion des mesures de sureté opérationnelles, et ce conformément à la procédure de gestion des documents du système SMQ D''AIR ALGERIE, en vigueur.

II.6. CONCLUSION

Dans ce chapitre on voit qu'au niveau international, l'organisation principale responsable de l'établissement de normes et de réglementations pour l'aviation civile est l'Organisation de l'aviation civile internationale (OACI), et au niveau national, chaque pays a son propre organisme de réglementation de l'aviation civile.

Il faut savoir que les réglementations de l'aviation civile évoluent constamment pour s'adapter aux nouvelles technologies, aux défis de sécurité et aux préoccupations environnementales. Il est donc essentiel pour les acteurs de l'aviation civile de se tenir informés des réglementations en vigueur et de s'y conformer pour assurer un fonctionnement sûr et efficace du secteur.

Enfin, on conclut que le cadre réglementaire est indispensable pour assurer la sureté dans le transport aérien (passager et/ou de fret).

CHAPITER III

GESTION DES RISQUES LIÉE A LA SURETÉ AÉRIENNE

III.1. INTRODUCTION

La gestion des risques liée à la sûreté aérienne est une préoccupation majeure dans le domaine de l'aviation. Ce chapitre se concentre sur l'identification et l'analyse des menaces auxquelles sont confrontées les compagnies aériennes, ainsi que la gestion des risques dans le domaine de la sûreté aérienne. Pour assurer la sureté il faut évaluer les risques selon une méthode précise, et utiliser une matrice de risque qui est un outil d'évaluation largement utilisé dans la gestion des risques.

Dans ce chapitre vous allez trouver une matrice de risque liée aux évènements de sureté spéciale pour l'exploitant Air Algérie, ainsi qu'une exécution d'un programme en python qui fait l'évaluation des risques.

III.2. LES MENACES LIÉE A LA SURETÉ D'UNE COMPAGNIE AÉRIENNE

La sureté est une préoccupation majeure pour les compagnies aériennes, et il existe plusieurs menaces qui peuvent cibler leur sûreté, notamment :

Actes de terrorisme **:** les actes terroristes peuvent viser des aéroports, des avions ou des passagers, mettant en danger la sécurité de la compagnie aérienne et de ses clients.

Sabotage interne : des employés malveillants peuvent tenter de saboter les avions, les équipements ou les installations de la compagnie aérienne.

Piratage informatique : les cyber-attaques peuvent perturber les systèmes informatiques de la compagnie aérienne.

III.2.1. MENACE INTERNE

Une menace interne pour une compagnie aérienne peut être représentée par un employé ou un groupe d'employés qui se livrent à des actes malveillants. Ces actes peuvent inclure le sabotage des avions, le vol de propriété intellectuelle ou de données sensibles, la vente de billets d'avion illégaux, la falsification de documents, ou même des actes de terrorisme.

Il est important pour les compagnies aériennes de prendre des mesures pour réduire les risques liés aux menaces internes en effectuant des vérifications de

sécurité approfondies lors de l'embauche d'employés, en surveillant les activités des employés et en établissant des politiques et des procédures claires en matière de sécurité pour tous les employés. La formation régulière des employés sur la sécurité peut également aider à réduire les risques liés aux menaces internes.

Voici quelques exemples de menaces internes :

Sabotage **:** un employé mécontent ou mal intentionné peut saboter un avion, un équipement ou une installation, causant des dommages importants et mettant en danger la sécurité des passagers.

Vol de données sensibles : un employé malveillant peut voler des informations confidentielles de la compagnie aérienne, telles que des données de carte de crédit ou des informations de voyage, et les utiliser à des fins illégales.

Complicité dans des activités criminelles : un employé peut être complice de trafic de drogue ou de contrebande, en aidant des criminels à passer des marchandises ou des personnes à travers les contrôles de sécurité de l'aéroport.

Négligence ou non-respect des procédures de sécurité : un employé peut enfreindre les règles de sécurité de la compagnie aérienne, par exemple en ne vérifiant pas correctement les bagages ou en permettant à des passagers non autorisés d'accéder à des zones restreintes de l'aéroport.

III.2.2. CYBER ATTAQUE

La sécurité et la sûreté du système aéronautique mondial sont ciblés par la cyber-attaque qui est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.[2]

Une cyber-attaque contre une compagnie aérienne peut avoir des conséquences importantes, car les compagnies aériennes dépendent largement de la technologie pour leurs opérations et la gestion de leurs données. Voici quelques exemples de conséquences d'une cyber-attaque pour une compagnie aérienne :

Perturbations des opérations : une cyber-attaque pourrait perturber les systèmes informatiques utilisés pour la réservation des billets, la gestion des vols, la communication entre les équipes, etc.

Vol de données sensibles : une cyber-attaque pourrait entraîner le vol de données sensibles telles que les informations personnelles et les détails de paiement des clients, ce qui pourrait compromettre la sécurité de ces derniers.

Perte de réputation : une cyber-attaque pourrait nuire à la réputation de la compagnie aérienne, en particulier si elle est incapable de réagir rapidement et de rassurer les clients quant à la sécurité de leurs données.

Coûts financiers importants : une cyber-attaque peut entraîner des coûts élevés pour la compagnie aérienne, tels que les coûts de restauration des systèmes, les coûts liés à la communication avec les clients et les coûts de mise en conformité avec les réglementations en matière de protection des données.

III.3. GESTION DES RISQUES

La notion de risque est toujours associée aux notions de responsabilité, dommages, événements indésirables, gravité. Mais la définition retenue est celle du Management de risques de projets : «le risque est un danger ou inconvénient possible ou probable dont on peut mesurer l'occurrence et la gravité »

Le terme évaluation des risques est utilisé pour décrire l'ensemble du processus ou de la méthode qui permet :

- De cerner les dangers et les facteurs de risque qui pourraient causer un préjudice (identification des dangers).
- D'analyser et d'examiner le risque associé au danger (analyse du risque et examen du risque).
- De déterminer des moyens appropriés pour éliminer le danger ou pour maîtriser le risque lorsque le danger ne peut pas être éliminé (maîtrise du risque).

Une évaluation des risques consiste en une inspection approfondie du lieu de travail en vue d'identifier entre autres les éléments, situations et procédés qui peuvent causer un préjudice, en particulier à des personnes. Une fois que le risque a été

cerné, il faut analyser et évaluer la probabilité et la gravité du risque. Il faut ensuite déterminer quelles mesures adopter afin d'empêcher le préjudice de se concrétiser.

III.3.1. AVANTAGES DE LA GESTION DES RISQUES

Les évaluations des risques sont très importantes puisqu'elles font partie intégrante d'un bon plan de gestion de la sureté et de la sécurité au travail. Elles contribuent à :

- Sensibiliser les personnes aux dangers et aux risques.
- Déterminer qui est exposé à des risques (employés, personnel d'entretien, visiteurs, entrepreneurs, membres du public, etc.).
- Déterminer si un programme de gestion est nécessaire pour un danger particulier.
- Déterminer si les mesures de maîtrise des risques en place sont appropriées ou s'il faut en instaurer d'autres.
- Hiérarchiser les risques et les mesures de maîtrise de ces derniers.
- Satisfaire les obligations juridiques, le cas échéant. [17]

III.3.2. LES MODES DE LA GESTION DES RISQUES

Dans la gestion des risques on trouve trois modes :

- **Le mode réactif :** rapport des évènements/incidents qui se sont produits.
- **Le mode proactif :** Analyses des évènements/incidents récurrents, étude de la tendance.
- **Le mode prédictif :** Prévision des menaces potentielles, suite d'une évaluation du risque. [3]

III.3.3. CONCEPT DE LA GESTION DES RISQUES

Le concept de la gestion des risques est basé sur :

- COMPRENDRE LE RISQUE :

Nommer correctement les menaces pour de mieux comprendre les sources ou les mécanismes du risque et ainsi évaluer la perte due aux conséquences.

- IDENTIFICATION DES RISQUES :

L'identification des risques est un exercice de collecte de données basée sur une combinaison des méthodes réactives, proactives, prédictives.

- ANALYSE DES RISQUES :

C'est d'analyser les risques on fonction de leurs probabilités et sévérités pour faire sortir l'index de risque

- LA DOCUMENTATION DES RISQUES :

La documentation des risques est une étape essentielle du processus d'identification des menaces ainsi qu'un indice de la maturité d'un système de gestion de risque. [17]

III.3.4. PROCESSUS DE LA GESTION DES RISQUES

Le processus de la gestion de risque comprend les 3 étapes suivantes :

- L'analyse du risque (probabilité et gravité de l'occurrence).
- L'évaluation du risque (acceptabilité de risque).
- Le contrôle du risque. (Atténuation de risque). [17]

III.3.5. COMMENT PLANIFIER UNE ÉVALUATION DES RISQUES ?

En général, pour planifier une évaluation des risques il faut déterminer :

- Quelle sera la portée de l'évaluation des risques (p. ex. les éléments à évaluer, les lieux physiques où se déroulent les activités de travail ou le type de dangers en cause).
- Les ressources nécessaires (formation d'une équipe pour l'évaluation des risques, détermination des sources de renseignements, etc.).
- Quels types de mesures serviront à l'analyse des risques (p. ex. le degré de précision de l'échelle ou des paramètres requis pour fournir l'évaluation la plus pertinente possible).

- ❖ Qui sont les intervenants concernés (gestionnaires, superviseurs, travailleurs, représentants des travailleurs, fournisseurs, etc.).
- ❖ Quels lois, règlements, normes ou codes s'appliquent dans votre province ou territoire et quelles sont les politiques et procédures organisationnelles à respecter. [16]

III.3.6. LES OBJECTIFS DE L'ÉVALUATION DES RISQUES

L'objectif du processus d'évaluation des risques consiste à examiner les dangers, puis à éliminer ces dangers ou à réduire le degré de risque en ajoutant des mesures de maîtrise des risques, au besoin.

Le but est de tenter de répondre aux questions suivantes :

- ❖ Que peut-il arriver et dans quelles circonstances ?
- ❖ Quelles sont les conséquences possibles ?
- ❖ Quelle est la probabilité que les conséquences possibles se produisent ?
- ❖ Est-ce que le risque est maîtrisé efficacement, ou faut-il prendre d'autres mesures ? [16]

III.3.7. COMMENT DÉFINIT-ON LES RISQUES ?

Pour être certain de détecter tous les risques, il faut :

- ❖ Vérifier tous les aspects du travail.
- ❖ Tenir compte des activités inhabituelles, telles que l'entretien, la réparation.
- ❖ Examiner les registres des accidents/incidents/quasi-accidents.
- ❖ Intégrer les personnes qui travaillent « hors site », soit à la maison, à un autre endroit, sur la route, chez le client, etc.
- ❖ Examiner comment le travail est organisé ou effectué (tenir compte de l'expérience des personnes qui effectuent le travail, des systèmes utilisés, etc.).
- ❖ Vérifier les conditions inhabituelles prévisibles (p. ex. incidence possible sur la procédure de maîtrise des risques qui pourrait la rendre inefficace lors d'une urgence, d'une panne de courant, etc.).

- ❖ Déterminer si un produit, une machine ou un équipement peut être modifié, de façon intentionnelle ou non (p. ex. un dispositif de protection pouvant être retiré).
- ❖ Examiner les risques pour les visiteurs ou pour le public.
- ❖ Tenir compte du type de personnes en cause, en sachant que le degré de risque peut différer. [16]

III.3.8. LES CATEGORIES DES RISQUES

Les risques auxquels vous pourriez être confronté appartiendront pour la plupart aux catégories suivantes :

Risque opérationnel : les risques opérationnels sont des erreurs de processus ou de procédure, comme une mauvaise planification ou un manque de communication entre les équipes.

Risque financier : ces risques concernent l'ensemble des événements entraînant des pertes de bénéfices pour l'entreprise.

Risque technique : les risques techniques sont en lien avec la technologie de l'entreprise. Il peut s'agir par exemple de failles de sécurité, de pannes de courant et de connexion internet ou de dommages matériels.

Risque externe : les risques externes échappent totalement à votre contrôle : inondations, incendies. D'autres catégories de risques seront à prendre en compte selon votre secteur d'activité. Si vous avez par exemple des clients gouvernementaux, vous devrez réfléchir plus particulièrement aux risques juridiques, et si votre entreprise vend un bien matériel, aux risques liés à la fabrication. [18]

III.3.9. L'ÉVALUATION DES RISQUES DE SURETÉ

L'évaluation des risques de sûreté est essentielle dans de nombreuses industries, telles que l'industrie nucléaire, l'industrie pétrolière et gazière, l'aviation, les transports en commun, la construction, etc. L'objectif de l'évaluation des risques de sûreté est de minimiser les risques pour les personnes, les biens et l'environnement en identifiant les mesures de prévention et d'atténuation appropriées.

L'évaluation des risques de sûreté est essentielle pour garantir la sécurité et la fiabilité des installations et des systèmes, ainsi que pour assurer la protection des travailleurs, de l'environnement et du public. Elle permet également de déterminer les mesures de prévention et d'atténuation nécessaires pour minimiser les risques.

L'évaluation des risques de sûreté doit être effectuée par des professionnels qualifiés et expérimentés dans le domaine concerné, en utilisant des outils et des méthodes appropriés.

III.4. SYSTEME DE GESTION DE SURETE {SeMS}

III.4.1. DÉFINITION DU SeMS

- **Se : Security = Sûreté**

Protection de l'aviation civile contre les actes d'intervention illicite.

Cet objectif est réalisé par une combinaison de mesures ainsi que de moyens humains et matériels.

- **M : Management = Gestion**

Affectation des ressources.

- **S : System = Système**

Un ensemble organisé de procédures et de processus.

D'où le SeMS : un ensemble organisé de procédures et de processus, basé sur une distribution déterminée des ressources qui permet la protection de l'aviation civile contre les actes d'intervention illicite. [19]

III.4.2. OBJECTIFS DU SeMS

Le SeMS a pour objectif d'identifier et de gérer les risques de sûreté, assurée, que l'efficacité des mesures de sûreté prises pour gérer les risques. D'une autre façon, il vise à atténuer les risques liés aux actes d'intervention illicite contre l'aviation civile.

Il s’appuie sur :

- ❖ La mise en œuvre et conformité effectives des mesures de sûreté ;
- ❖ La durabilité des mesures qui soient proportionnées et réalistes à long terme ;
- ❖ La coopération et partage des informations avec les parties prenantes au processus de sûreté en local ou à l’international ;
- ❖ Le renfort, la coopération et le partage des informations entre les parties prenantes au processus de sûreté ;
- ❖ Le développement d’une culture métier et de compétences humaines en sûreté ;
- ❖ Une surveillance proactive de l’évolution de la menace avec l’avancée de la technologie.

Les SeMS par conséquent est considérés comme un outil efficace permettant d’évaluer la performance des mesures de sûreté d’une façon continue et proactive.

Pour atteindre les objectifs de sureté assignés et énumérés plus haut le SeMS de la compagnie s’appuie sur un ensemble d'éléments corrélés :

1. Une culture de la sureté
2. Un système documentaire pour la bonne mise en oeuvre (Manuels : PSE-PFS /Processus/Procédures).
3. Une organisation adaptée
4. Une politique engagée,
5. Une formation adaptée et conforme aux exigences et standards nationaux et internationaux
6. Évaluation, analyse et gestion des risques.
7. Surveillance continue du système. [19]

III.4.3. ÉLÉMENTS DU SeMS

Le SeMS devrait comprendre les éléments suivants :

- ➢ Engagement et responsabilité de la direction ;
- ➢ Ressources ;
- ➢ Gestion de la menace et des risques ;
- ➢ Suivi de la performance. Compte rendue et amélioration continue ;

- Intervention en cas d'incident ;
- Programme de formation sue les SeMS ;
- Communication.

Ces éléments sont applicables aux entités chargées de mettre en œuvre des mesures de sûreté de l'aviation, ou à toute autre entité jouant un rôle dans la protection de l'aviation civile contre les actes d'intervention illicites. [19]

III.5. MÉTHODES D'ÉVALUATION DES RISQUES

Il existe différentes méthodes d'évaluation de risque selon le domaine d'application et les objectifs visés. Voici quelques-unes des méthodes courantes d'évaluation de risque :

Analyse des modes de défaillance et de leurs effets (AMDE) : Cette méthode consiste à identifier les modes de défaillance potentiels d'un système, les conséquences de ces défaillances et la probabilité de leur survenue.

Analyse des arbres de défaillances (AAD) : Cette méthode consiste à identifier les événements qui pourraient entraîner une défaillance du système et à construire un arbre logique des causes et des effets pour évaluer la probabilité d'occurrence d'une défaillance.

Analyse des risques opérationnels (ARO) : Cette méthode évalue les risques associés aux activités et processus opérationnels d'une organisation. Elle se concentre sur les risques liés aux processus, aux personnes, à la technologie et à l'environnement.

Analyse des risques industriels (ARI) : Cette méthode évalue les risques associés aux activités industrielles telles que la production chimique, pétrolière et gazière, l'exploitation minière et la production d'électricité.

Analyse des risques financiers (ARF) : Cette méthode évalue les risques financiers tels que le risque de crédit, le risque de marché et le risque opérationnel associé aux activités financières d'une organisation.

Analyse des risques informatiques (ARI) : Cette méthode évalue les risques associés à l'utilisation des systèmes d'information tels que les attaques de pirates informatiques, les erreurs de programmation et les pannes de matériel.

Analyse de la sécurité physique (ASP) : Cette méthode évalue les risques associés à la sécurité physique des bâtiments et des infrastructures, tels que le vol, le vandalisme et les catastrophes naturelles.

Il faut savoir que ces méthodes ne sont pas exhaustives et qu'il existe d'autres méthodes d'évaluation de risque. Le choix de la méthode dépend des objectifs spécifiques de l'évaluation de risque et des caractéristiques du système ou de l'activité évaluée.

Dans ce projet la méthode d'évaluation de risque adaptée est la « BOW TIE » et je vais la présenter dans le titre ci-dessous.

III.5.1. LA MÉTHODE D'ÉVALUATION DES RISQUES « BOW TIE »

La méthode d'évaluation de risque BOW TIE (ou nœud papillon en français) est une méthode de gestion des risques visuelle, qui permet de représenter et de visualiser clairement les liens entre les différentes causes et conséquences potentielles d'un événement dangereux, pour mieux comprendre ses risques associés, ainsi que les mesures de prévention et d'atténuation de ces derniers. Elle est souvent utilisée dans des industries à haut risque telles que la production pétrolière et gazière, l'industrie chimique et l'aviation, mais elle peut être également appliquée dans d'autres domaines où la gestion des risques est essentielle.

La méthode BOW TIE permet de : réduire la probabilité d'occurrence d'un événement dangereux, minimiser ses conséquences, faciliter la communication des risques aux parties prenantes et d'élaborer des plans d'urgence en cas de survenance.

La méthode BOW TIE se compose d'un diagramme en forme de nœud papillon comme représente la Figure03, où le centre représente l'événement indésirable, que l'on cherche à prévenir, et les deux ailes représentent, les mesures préventives à mettre en place en amont (sur la partie gauche du diagramme), ainsi que les mesures correctives à mettre en place en aval (sur la partie droite du diagramme). La partie gauche de la BOW TIE représente les causes potentielles de l'événement, ou

les scénarios de défaillance. La partie droite représente les conséquences potentielles de l'événement, ou les scénarios de répercussions. [20]

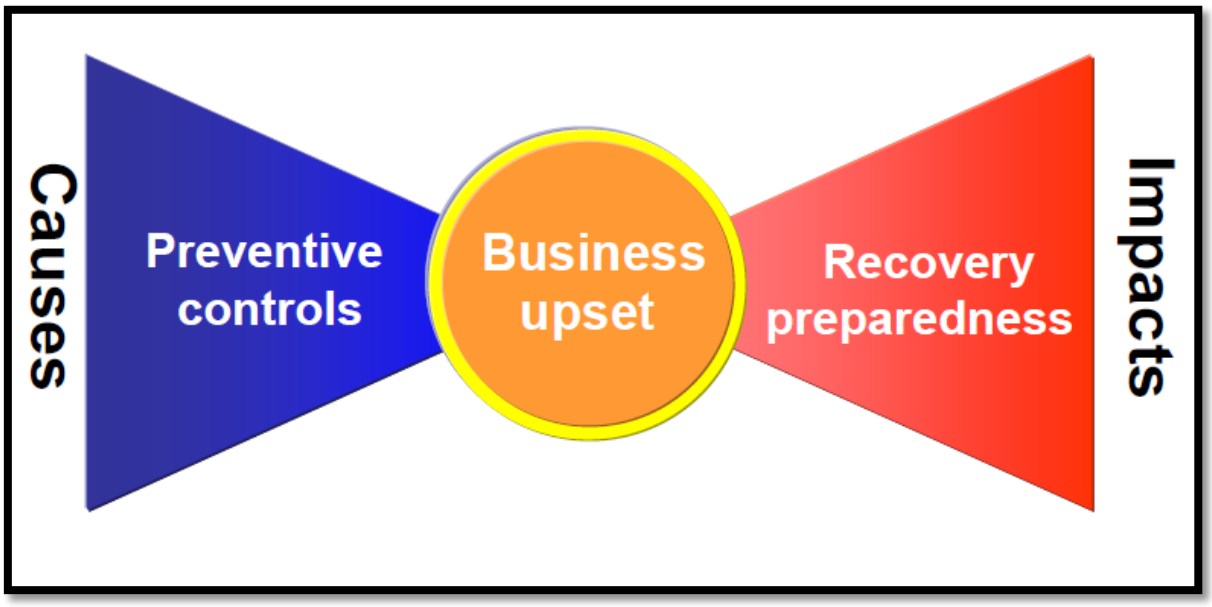


Figure III.1 : Diagramme 01 de la BOW TIE. [20]

III.6. MATRICE DE RISQUE

Une matrice de risque est un outil d'évaluation des risques qui permet de classer les risques en fonction de leur probabilité et de leur gravité. Cette méthode peut également être appliquée pour évaluer les risques de sûreté.

La matrice de risque pour la sûreté est présentée sous la forme d'un tableau à deux dimensions. L'axe horizontal représente la probabilité d'occurrence du risque, tandis que l'axe vertical représente la gravité des conséquences du risque.

La probabilité peut être classée en plusieurs catégories, telles que faible, moyenne ou élevée. La gravité des conséquences peut également être classée en plusieurs catégories, telles que mineure, modérée, majeure ou catastrophique.

La probabilité d'occurrence est souvent évaluée en fonction de la fréquence des événements passés similaires, de l'expérience et de l'expertise des travailleurs impliqués, et des facteurs environnementaux et techniques.

La gravité du risque peut être évaluée en fonction de la probabilité d'impact sur la sécurité des travailleurs, sur l'environnement, sur le public, sur les équipements et sur la production.

Cette matrice est souvent utilisée dans l'évaluation des risques de sûreté pour aider à hiérarchiser les risques et à déterminer les mesures de prévention et d'atténuation nécessaires.

En utilisant la matrice de risque pour la sûreté, les risques peuvent être classés en quatre catégories :

Risques élevés : ces risques ont une probabilité d'occurrence élevée et une gravité élevée. Ils nécessitent une attention immédiate et des mesures de prévention et d'atténuation urgentes.

Risques moyens : ces risques ont une probabilité d'occurrence moyenne et une gravité moyenne. Ils nécessitent des mesures de prévention et d'atténuation pour réduire leur probabilité et leur gravité.

Risques faibles : ces risques ont une probabilité d'occurrence faible et une gravité faible. Ils peuvent être gérés par des mesures de prévention et d'atténuation courantes.

La matrice de risque pour la sûreté peut être adaptée en fonction des besoins spécifiques de l'entreprise et des caractéristiques des risques évalués. [18]

III.6.1. ÉCHELLE DE GRAVITÉ

Lorsque vous créez un modèle de matrice des risques, vous devez commencer par définir votre échelle de gravité. Celle-ci correspondra aux colonnes de la matrice et mesure la gravité des conséquences de chaque risque. Dans une matrice 5 × 5, elle compte cinq niveaux :

Négligeable (1) : le risque aura peu de conséquences s'il se produit.

Mineur (2) : les conséquences du risque seront faciles à gérer.

Modéré (3) : les conséquences du risque mettront du temps à être atténuées.

Majeur (4) : les conséquences du risque seront importantes et pourront engendrer des dommages à long terme.

Catastrophique (5) : les conséquences du risque seront véritablement néfastes et il sera probablement difficile de s'en remettre. [18]

III.6.2. ÉCHELLE DE PROBABILITÉS

Vous devrez ensuite définir votre échelle de probabilité, laquelle correspondra aux lignes de votre modèle de matrice des risques. Cette échelle estime la probabilité que chaque risque se produise réellement.

Très probable (5) : ce risque se produira très certainement à un moment ou à un autre du projet.

Probable (4) : il y a de fortes chances que ce risque se produise.

Possible (3) : ce risque pourrait se produire, mais pas nécessairement. Que la chance soit avec vous.

Peu probable (2) : il y a peu de chances que ce risque se produise.

Très improbable (1) : il y a très peu de chances que ce risque se produise. [18]

III.6.3. ACCEPTATION DE RISQUE

Lorsqu'on représente un risque dans notre matrice en fonction de sa probabilité et de sa gravité, on peut alors déterminer son degré d'impact. Celui-ci répond à un code couleur, allant du vert au rouge, et est évalué sur une échelle de A -> C.

Faible donc c'est **C** : ces événements ont peu de chances de se produire, mais dans le pire des cas, ils n'auraient pas de graves conséquences sur votre entreprise. Pas besoin d'en faire votre priorité dans votre plan de gestion des risques. Mais il faut les contrôler

Moyen donc c'est **B** : Il suffit de prendre les mesures nécessaires pendant la phase de planification pour les prévenir et atténuer leurs effets. Ces derniers ne doivent pas être pris à la légère, sans pour autant devenir une priorité absolue.

Élevé donc c'est **A** : attention ! Ces risques peuvent mettre en péril votre entreprise si vous n'en tenez pas compte pendant la phase de planification. Comme ces risques aux conséquences graves sont susceptibles de se produire, ils doivent être prioritaires dans votre plan de gestion des risques.

Une matrice des risques 5 × 5 est idéale pour mener une analyse plus détaillée. En effet, une fois vos risques représentés dans votre modèle de matrice, celle-ci présentera un spectre de couleurs plus étendu vous permettant de savoir en un clin d'œil à quel degré d'impact correspond chacun de vos risques (élevé, moyen ou faible).

On peut bien évidemment modifier les éléments de la matrice afin de mieux les adapter aux besoins de l'entreprise, tout comme la taille et la terminologie de la matrice des risques. Il faut suivre 5 étapes essentielles pour faire une matrice de risque comme le montre la Figure 04 [18] :

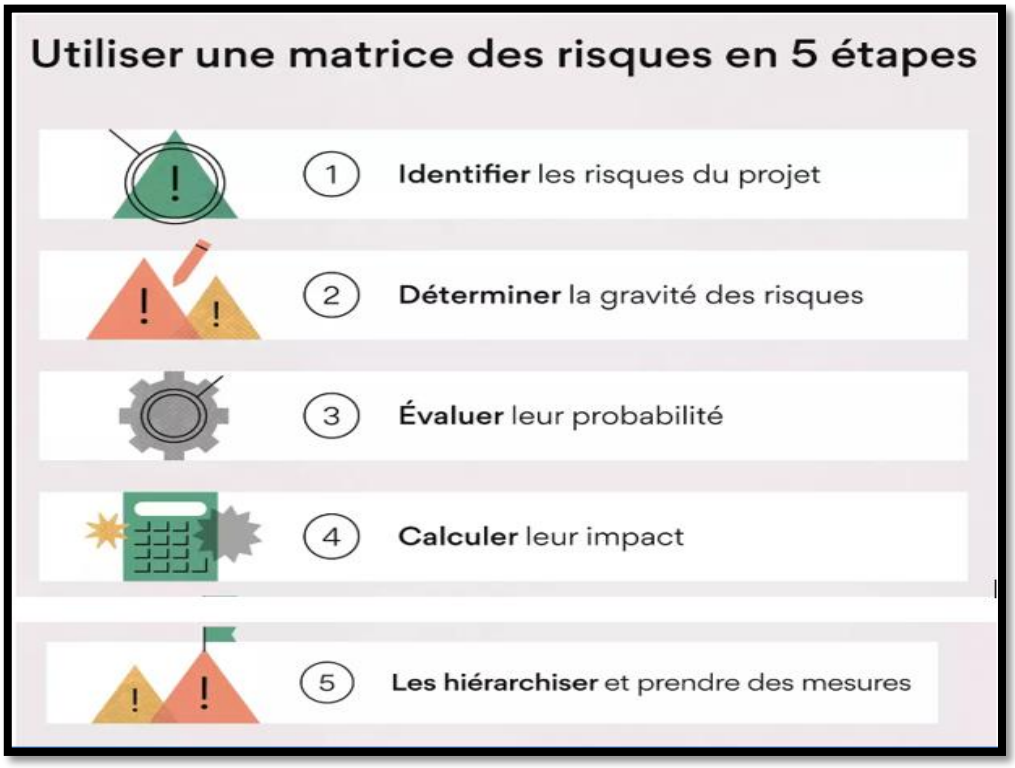


Figure III.2 : La matrice en 5 étapes. [18]

III.7. LA MATRICE DE RISQUE D'AIR ALGÉRIE {ÉVENEMENT DE SURETÉ}

Pour assurer la sureté et la protection des passagers, des équipages, du personnel au sol et du public contre des actes d'intervention illicite dans l'aviation civile.

Air Algérie a mis en place un système d'identification et d'évaluation des risques associés aux menaces qui s'adapte au mieux à toutes les situations et occurrences. Ce système est basé sur une matrice des risques.

Lors de l'analyse des risques, l'indice de risque est fondé sur l'évaluation des deux facteurs suivants :

- La probabilité qu'un évènement se produira.
- La sévérité de la conséquence de cet évènement.

III.7.1. PROBABILITE DE L'ÉVÈNEMENT

Le tableau 02 suivant présente l'échelle de probabilité pour les évènements de sureté.

Tableau III. 1 : Échelle de probabilité de la matrice de risque d'Air Algérie.

Probabilité			
Niveau de probabilité	Signification	Occurrence/N[b] de vol (74000 vol /an)	N[b] de fois dans l'industrie/an
P5-> Extrême	Se produit fréquemment	> 3 fois	> 3 fois
P4-> Elevé	Très probable (Il se produit souvent)	3 fois	3 fois
P3-> Medium	Probable (Déjà arrivé)	2 fois	2 fois
P2-> Faible	Rarement arrivé	1 fois	1 fois
P1-> Négligeable	Improbable (jamais arrivé)	Jamais	Jamais

III.7.2. SÉVÉRITÉ DE L'ÉVÈNEMENT

Le tableau 03 ci-dessus présente l'échelle de sévérité pour les évènements de sureté

Tableau III. 2 : Échelle de sévérité de la matrice de risque d'Air Algérie.

Sévérité	
Niveau de Sévérité	Dégâts humains / Dégâts matériel / Perte financière / Réputation de la compagnie/ Effet d'impact environnemental
S5 -> Extrême	Nombreux morts ≥3 / Destruction complète d'un avion / >10M$ ou entre 10M$- 5M$ / Impact international / Concentrés ou À retardement (à long terme)
S4 -> Elevé	Un ou deux morts et/ou Des personnes ont des blessures fatales ou des blessures graves / Dégâts substantiels à un avion / entre 5M $ - 500k $ / Impact national / Impact temporaire immédiate
S3 -> Medium	Des personnes ont des blessures mineures /Dégâts mineurs (secondaires) à un avion / entre 500k 10k$ / Impact dans l'entourage de la compagnie / Impact local
S2 -> Faible	Nuisance ou une panique entre les passagers / Dommage mineurs au système / entre 10k $ - 5k$ / Impact au sein de l'entreprise / Impact réversible
S1-> Négligeable	Pas de blessés / Aucun dommage / entre 0 $ -5k$ / Pas d'impact / Pas d'impact

III.7.3. LA MATRICE DE RISQUE

RISQUE = PROBABILITÉ + SEVERITE.

Tableau III. 3 : Matrice de risque d'Air Algérie.

G / P	S5	S 4	S 3	S 2	S 1
P5	10	9	8	7	6
P 4	9	8	7	6	5
P3	8	7	6	5	4
P2	7	6	5	4	3
P1	6	5	4	3	2

	S5	S4	S3	S2	S1
P5	A	A	A	A	B
P4	A	A	A	B	B
P3	A	A	B	B	C
P2	A	B	B	C	C
P1	B	B	C	C	C

Après avoir classé les risques par ordre de gravité, l'index d'évaluation du risque est utilisé pour déterminer le niveau de risque et les mesures à prendre.

III.7.4. SEUILS D'ACCEPTABILITÉ

Le tableau suivant représente comment atténuer le niveau risque lors de la gestion des risque ainsi que les décisions à prendre.

Tableau III. 4 : Seuils d'acceptabilité des risques.

Niveau de risque	Risque	Atténuation de risque	Niveau de prise de décision
A	Elevé	Niveau de risque inacceptable : La partie des opérations concernée (destination, type avion, système, procédure…) doit être interrompue immédiatement et ne peut reprendre qu'une fois les mesures de contrôle effectives. Approbation de la haute direction requise. Un plan d'actions doit être mis en œuvre afin de ramener le niveau de risque en « Faible ».	Plan d'actions développé immédiatement Actions implémentées aussitôt que possible et validées en comité de sureté.

B	Moyen (Acceptable Avec atténuation)	Niveau de risque tolérable sous réserve que des mesures soient mises en œuvre dans des délais acceptables afin de diminuer le niveau de risque. Des mesures de réduction du risque doivent être identifiées et implémentées afin de rejoindre le niveau « C : Faible ». Si un niveau de risque acceptable n'est pas atteint dans le délai imparti, une décision de dérogation du top management est nécessaire.	Plan d'actions développé sous 1 semaine et validé en comité de sureté. Actions implémentées sous 1 mois.
C	Acceptable	Niveau de risque acceptable nécessitant une surveillance renforcée. Des données doivent être collectées de manière continue afin de consolider l'évaluation du risque et éviter toute dégradation en risque inacceptable. Un renforcement des mesures existantes et l'implémentation de mesures supplémentaires doivent être considérés.	Plan d'actions développé sous 1 mois. Actions implémentées sous 3 mois.

III.7.5. ATTENUATION DU RISQUE

Après avoir identifié les risques qui ont besoin d'être atténués, et pour :

1. Éliminer le risque, où
2. Réduire le niveau du risque, ou la gravité des conséquences ou la probabilité d'occurrence de ce risque, où
3. Éviter l'exposition au risque.

La direction de la sureté adopte les démarches suivantes :

- ❖ Déclenche un point sureté aux fins d'évaluer le risque et établir « Registre d'identification et d'évaluation du risque »
- ❖ Interpelle les autorités pour une collaboration en cas de nécessité.
- ❖ Renforce le contrôle sur l'application des procédures de sûreté par des inspections ou des audits.
- ❖ Mobilise la direction concernée par le risque identifié (exp : le chef d'escale/direction/représentants).
- ❖ Mobilise les agents de sûreté pour mettre en œuvre les actions préventives adaptées pour l'atténuation des risques.
- ❖ Met des barrières additives de prévention.

III.7.6. L'ÉXÉCUTION DU PROGRAMME

J'ai réalisé un programme qui fait l'évaluation des risques, ce programme est basé sur le langage ''Python''. Les Figures ci-dessus vous présentent quelques exécutions pour calculer le niveau de risque.

Dans L'interface graphique les abréviations représentent :

- ❖ NM : Nombre de Morts.
- ❖ BL : Blessures.
- ❖ PN : Panique.
- ❖ AC : Aircraft (état d'aéronef).
- ❖ X : Les couts financière.
- ❖ IMP : Impact sur la réputation.
- ❖ IMP2 : Impact environnemental
- ❖ OC : Nombre de fois d'Occurrence dans la compagnie / an (les deux dernières années).
- ❖ OC2 : Nombre de fois d'occurrence dans l'industrie / an (les autres compagnies durant les dernières années).

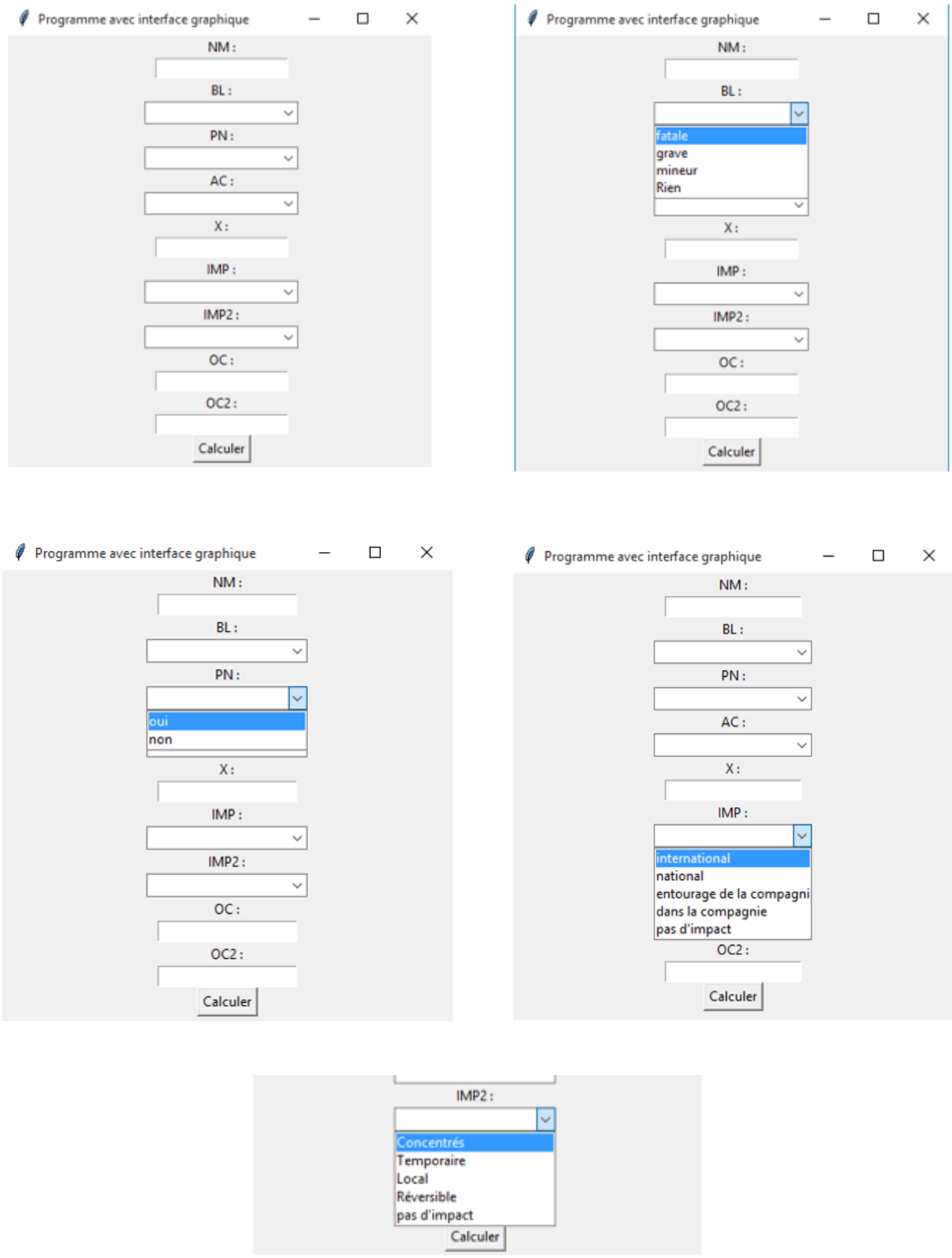


Figure III.3 : Interface graphique du programme.

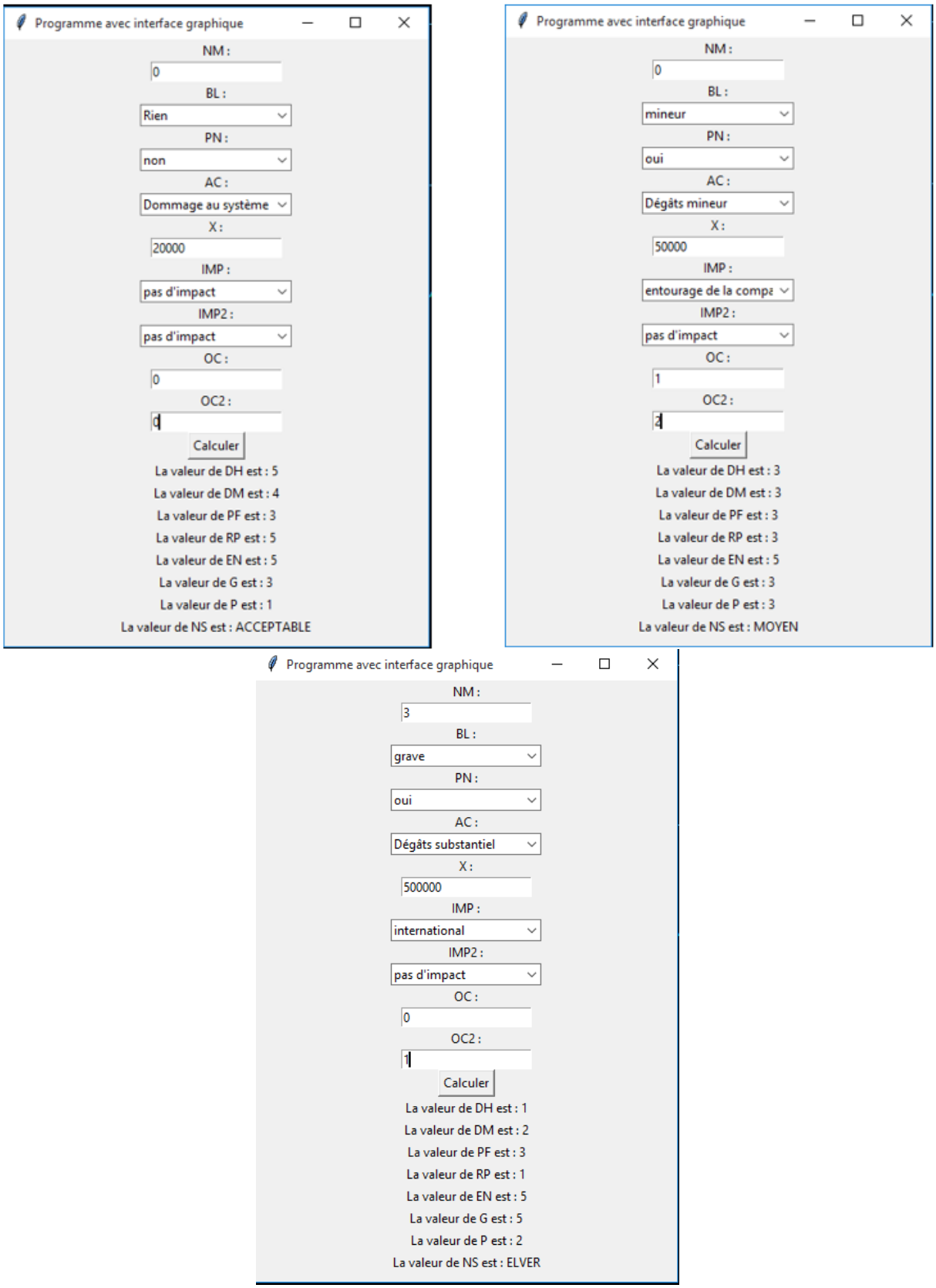


Figure III.4 : Exécution du programme.

III.8. CONCLUSION

A la fin de ce chapitre, on conclut que la gestion des risques liée à la sûreté aérienne est une tâche complexe mais essentielle pour garantir la sureté des vols. Grâce à l'analyse des risques et à l’approche proactive, il est possible de réduire les vulnérabilités et de prévenir les incidents de sureté aérienne. Cependant, il est important de rester vigilant et de continuer à innover pour faire face aux menaces émergentes et assurer la sûreté aérienne à long terme.

CHAPITER IV

ÉVALUATION DES RISQUES LIES AUX CYBER ATTAQUES CIBLANT LA PRÉPARATION DES VOLS

IV.1. INTRODUCTION

Pour assurer la sureté informatique dans une compagnie aérienne et spécialement le domaine de la préparation des vols, il faut connaître les potentiels des cyber attaquants, imaginer toutes les malveillances possibles, et mettre en place des systèmes proactifs et réactifs contre les cas de cybers attaques. Pour ce là je me suis déplacée vers la sous-direction engineering dans la direction des opérations aériennes (DOA), pour analyser et diagnostiquer les vulnérabilités visant les logiciels et les outils informatique utiliser lors de la préparation des vols. Et concernant les mesures de cyber sécurité mise par Air Algérie pour protéger son système informatique je me suis déplacée vers la direction sécurité informatique (DSI) pour avoir des informations.

Dans ce chapitre je vais faire une évaluation des risques liés aux cybers attaques ciblant la phase de préparation des vols

IV.2. LA PRÉPARATION DES VOLS

Afin d'effectuer un vol sûr et efficace, des multiples opérations sont mises en place, en commençant par la demande de fiabilité du vol jusqu'au plan de vol. Et dans cette partie je vais vous présenter comment préparer un vol ?

La séquence de préparation du vol débute par une demande de fiabilité (Destination, charge offerte autorisée, temps de vol, le type d'avion approprié et la quantité de carburant nécessaire) qui est adressée soit par le service commercial de la compagnie (vol commercial) soit par le service cargo (vol cargo) à la direction Programme, qui à son tour transmet la demande à la Direction des Opérations Aériennes pour l'étude de fiabilité.

Lorsque la demande parviendra à la Direction des Opérations Aériennes, la Sous-Direction (S/D) ENGENRING s'en chargera, et elle est divisée en quatre départements et chaque département a ses propres tâches.

- Département Navigation Route et Aérodrome.
- Département Performances et Monitoring.
- Département Documentations.
- Département Flight Dispatcher.

IV.2.1. DÉPARTEMENT NAVIGATION ROUTE ET AÉRODROME

Les Ingénieurs de ce département font l'étude d'admissibilité d'A/D de destination :

- Le téléchargement par SKYBOOK des : NOTAM (Des informations sur la FIR et l'Aérodrome de destination), TAF, METAR, TEMSI, SIGMET (Des bulletins météo sur A/D de destination).
- Le téléchargement par eLink des informations sur : le PCN des RWY et TWY, les dimensions des RWY et TWY, et des informations sur le SSLIA.
- Vérifier la disponibilité du service de contrôle aérien (La circulation d'aérodrome)

Puis lorsque l'A/D de destination est adéquat ils choisissent les A/D de (départ, dégagement au départ et dégagement à l'arrivée) ensuite ils déterminent la route et l'altitude de sécurité entre aérodrome de départ, d'arrivée et de dégagement en utilisant le JetPlanner PRO :

- Tracer sur la carte 1/500 000 le trajet
- Choisir des repères caractéristiques chacun à environ 10 à 15 minutes de vol
- Noter le ou les points culminants du parcours ou l'altitude de sécurité
- Déterminer les routes magnétiques aller-retour
- Mesurer et noter la distance en chaque repère
- Calculer la durée de chaque tronçon
- Mesurer et noter les flanquements des balises VOR si possible
- Noter l'ordre d'utilisation des fréquences
- sans oublier de tenir en compte le passage des FIR

A la fin lorsque la route est prête ils envoient une Note de Services (NS) aux autres départements.

IV.2.2. DÉPARTEMENT PERFORMANCES ET MONITORING

Lorsque la Note de Service arrive aux ingénieurs de ce département ils font le calcul des performances de décollage / atterrissage et ils préparent les fiches limitations par le :

- ❖ Calcul de MMD (Masse Maxi au Décollage).
- ❖ Calcul des limitations (Piste {TORA, TODA, ASDA, LDA} – Obstacle – 2ém Segment – V_{BE} (Brake energie).
- ❖ Calcule des vitesses (V_1 (vitesse de décision), V_R, V_2).
- ❖ Faire une étude du chargement et vérifier si le centrage se situe dans la plage de sécurité.

Pour calculer les limitations il faut savoir les données sur :

- ✓ Aérodrome A/D :
  - QFU
  - Longueur de piste
  - Slope : la pente de piste
  - Etat de piste : DRY or WET or SNOW or ICE
- ✓ Météorologie :
  - Wind : intensité et direction
  - Température
  - Pression : QNH
- ✓ Avion :
  - Flaps : Volet
  - Moteur : Turbo prop, Turbo réact
  - Anti-Ice : OFF or ON
  - Air Con : OFF or ON

IV.2.3. DÉPARTEMENT FLIGHT DISPATCHER

Les ingénieurs de ce département quand ils reçoivent la NS ils font le

- ❖ FIX ROUTING des A/D (départ, dégagements, arrivée) et des AIRWAYS (routes aériennes) dans la plateforme de JetPlanner PRO

pour que le jour J (le jour du vol) les TNAO vont les trouver facilement et les utiliser dans le plan de vol.

- ❖ Téléchargement des NOTAM de tous les A/D motionné dans la route.

IV.2.4. DÉPARTEMENT DOCUMENTATIONS

Les ingénieurs de ce département sont chargés de la documentation c'est-à-dire placé tous les documents et les manuels nécessaires au vol à bord ainsi que leurs mis à jour

Les Documents et les manuels qui sont obligatoirement à bord :

- ❖ Fiches limitations (Mise à jour tous les 28 jours)
- ❖ Fiches de percé (liée aux procédures d'approche pour chaque A/D)
- ❖ C COM : Cabin Crew Operatings Manual
- ❖ F COM : Flight Crew Operatings Manual
- ❖ AFM : Airplane Flight Manual
- ❖ QRH : Quick Reference Handbook
- ❖ MMEL : Master Minimum Equipment Liste (c'est un extrait du MEL {Minimum Equipment Liste, qui est envoyé par le constructeur}, il est fait par la compagnie selon ses Avions, et approuvé par EASA / FAA)
- ❖ W&B : Weight and Balance Manual
- ❖ FPPM : Flight Planning Performance Manual
- ❖ Certificat d'immatriculation
- ❖ Certificat de navigabilité valide 3 ans
- ❖ Certificat d'examen de navigabilité valide 1 an
- ❖ Rapport de masse et centrage
- ❖ Certificat acoustique EASA
- ❖ Licence de station d'aéronef
- ❖ Attestation d'assurance
- ❖ Carnet de route sauf pour les vols locaux
- ❖ Plan de vol si déposé
- ❖ Le dossier de vol lors du chaque vol

Les 4 Manuels d'exploitation :

- MANEX A : Généralité et Fondement

- MANEX B : Exploitation Avion
- MANEX C : Routes et Aérodromes
- MANEX D : Documentations

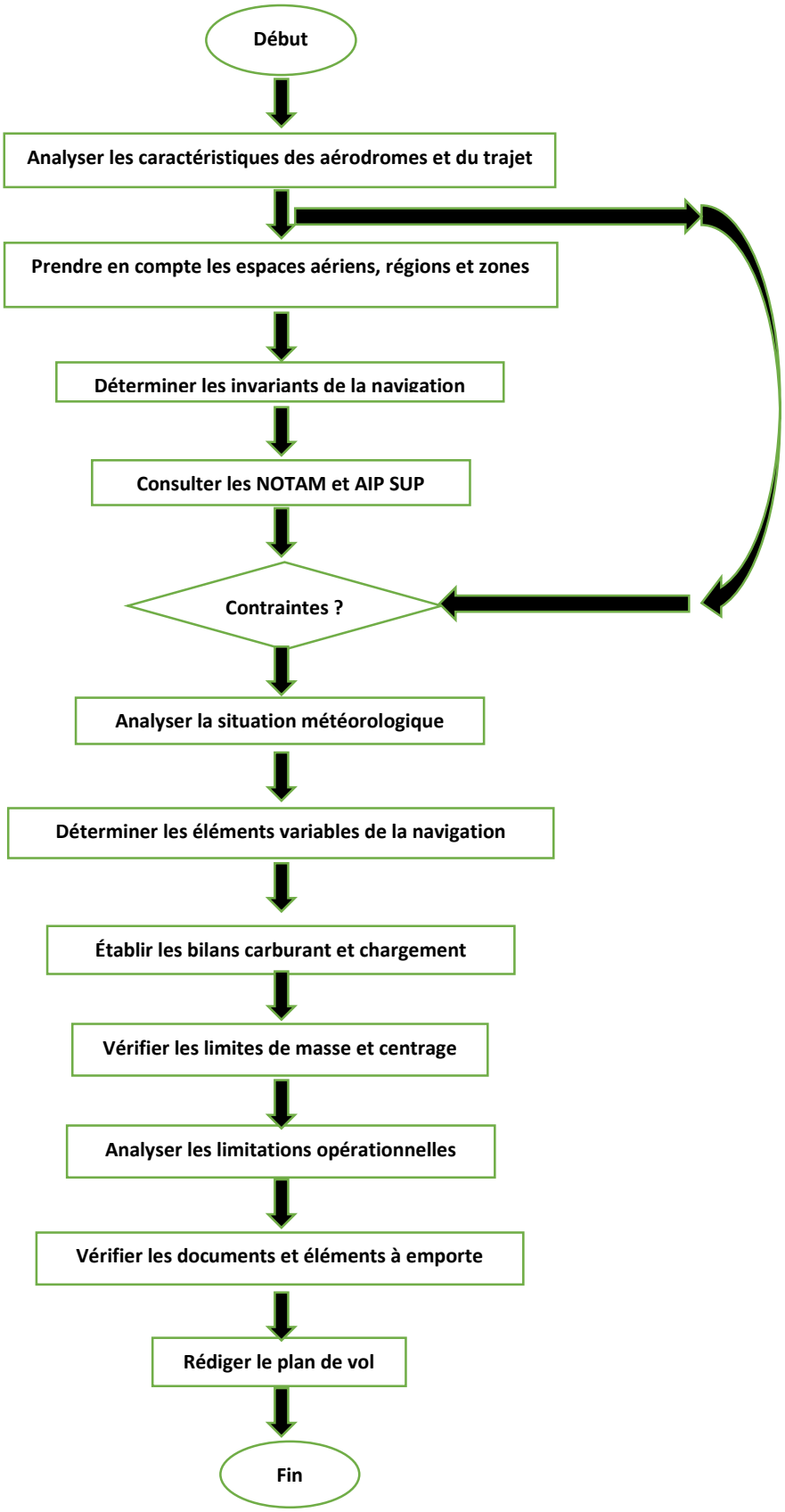
IV.2.5. LE JOUR J « LE JOUR DU VOL »

Les techniciens de flight dispatcher préparent le dossier de vol en utilisant le JET PLANER PRO, SKAYBOOK, RSFTA…etc.

Le Dossier de vol :

- ❖ FEUILLE D'INSTRUCTION ET STATISTIQUE
- ❖ HIL / MEL / CDC
- ❖ PLAN DE VOL TECHNIQUE (JET-PLAN)
- ❖ NOTAMS
- ❖ PLAN DE VOL ATC
- ❖ DOSSIER METEO
- ❖ BULLETIN PRÉVISIONNEL DE CHARGEMENT
- ❖ CARTON DE DÉCOLLAGE ET ATTERRISSAGE
- ❖ DEVIS DE POIDS ET CENTRAGE

IV.2.6. L'ORGANIGRAMME DE LA PRÉPARATIONS DES VOLS



IV.3. LES LOGICIELS ET LES OUTILS INFORMATIQUES UTILISER PAR AIR ALGÉRIE LORS DE LA PRÉPARATION DES VOLS

Dans une compagnie aérienne moderne, les logiciels et les outils informatiques jouent un rôle essentiel pour garantir des opérations sûres et efficaces. Un des principaux logiciels utilisés est le système de gestion des opérations aériennes, qui englobe différentes fonctionnalités telles que la planification des vols, la gestion des équipages, la gestion des réservations et la gestion des ressources. Ce système permet de coordonner tous les aspects liés aux vols, des horaires de départ et d'arrivée aux informations sur les passagers. Ainsi que les ingénieurs et les pilote utilisent des outils informatiques lorsqu'ils préparent les vols.

Air Algérie fait partie des compagnies moderne, et dans ce titre je vais vous présenter les logiciels et les outils informatiques utilisé.

IV.3.1 LES LOGICIELS SUR ORDINATEURS

- **Jet Planner PRO**

JetPlanner PRO est un logiciel utilisé par les compagnies aériennes pour générer les plans de vol techniques, c'est un serveur indépendant qui a une base de données sur laquelle Jeppssen fait des amendements chaque 28jours, les compagnies aériennes créent une base de données propre à elles où les équipements, la flotte, les aérodromes de dégagement et toutes les informations concernant la compagnie sont enregistrées, et mise à jour par les administrateurs.

L'interface de gestion de vol complète de Jeppesen est conçue pour un flux de travail configurable afin de gérer les opérations de vol assignées pour inclure la planification, la libération et les tâches après le vol. JetPlanner permet à l'utilisateur de définir le niveau d'automatisation qu'il souhaite intégrer dans son flux de travail, y compris le flux de travail manuel, partiel ou entièrement automatisé.

JetPlanner Pro est une solution logicielle puissante et à jour qui permet aux planificateurs de vol et aux répartiteurs de faire leur travail efficacement et d'optimiser au mieux leurs opérations aériennes. Parmi ses avantages :

- ✓ Exploite le moteur JetPlan éprouvé pour produire des itinéraires optimisés en termes de temps, de coût ou de carburant

- ✓ Dispose d'une interface utilisateur moderne optimisée pour la planification de vol automatisée, manuelle et ad hoc
- ✓ Exploite la suite de services de données de Jeppesen, y compris les NOTAM et la météo
- ✓ Dispose d'un protocole de messagerie robuste permettant l'intégration avec des systèmes tiers
- ✓ Utilise une automatisation avancée qui permet aux planificateurs de vol de se concentrer sur des tâches complexes et de grande valeur
- ✓ A accès aux informations de navigation Jeppesen dans le monde entier qui sont la référence dans l'industrie

❖ **ELink**

ELink, fournit par Jeppesen, il nous offre une application simple et intuitive pour rechercher, visualiser, organiser et imprimer les cartes en route et terminales, le texte du manuel des voies aériennes et les lettres de révision. Parmi ces avantages :

- ✓ Accédez aux principales informations de navigation au monde à tout moment et en tout lieu
- ✓ eLink Online permet d'accéder aux cartes via Internet, tandis qu'eLink pour Windows offre une visualisation hors ligne des cartes sur PC
- ✓ Les deux versions prennent en charge les solutions de navigation numérique, rationalisant le processus de gestion de la révision des cartes de navigation et augmentant l'efficacité opérationnelle

❖ **SkyBook**

SkyBook est le logiciel d'opérations de vol fournit par « bytron aviation systems » dont vous avez besoin pour créer une compagnie aérienne entièrement numérique et connectée.

skybook est une solution de bout en bout, fournissant à vos opérations aériennes un processus de répartition automatisé. Améliorer l'efficacité en coordonnant tous les facteurs techniques, y compris ;

- ✓ Planification de vol
- ✓ Mises à jour météo
- ✓ Cartes ETOPS et traçage d'itinéraire
- ✓ Suivi des vols et gestion des retards

- ✓ Gérez de manière transparente toutes les données EFB et de vols envoyés au pilote, à l'équipage et à l'équipe des opérations. La répartition des vols fournit les bonnes données, au bon endroit, au bon moment.
- ✓ Informations sur le briefing de vol
- ✓ Vérifiez instantanément les METAR, TAF et NOTAM
- ✓ Données de vol en temps réel, surveillance et alertes

Skybook fournit un dossier d'information de premier ordre en se concentrant sur les informations les plus importantes pour le poste de pilotage.

- ❖ **Airport Manager « NAVDATA »**

La base de données Jeppesen Aviation contient plus de 18 600 aéroports et 2,6 millions d'enregistrements de données. Elle est utilisée par les compagnies aériennes, les services de vol d'entreprise et presque tous les principaux fabricants d'avionique dans le monde, Jeppesen NavData offre :

Couverture : Seul Jeppesen offre une couverture mondiale, avec un accès à plus de 7 000 aéroports

Contenu : il fournit également des données sur les obstacles et le terrain, ainsi que des services de données personnalisables pour de nombreuses plates-formes et fabricants différents.

Précision : Seuls les documents sources originaux sont analysés par rapport aux données complètes et détaillées disponibles dans leurs systèmes. Ces données sont ensuite traitées à travers les milliers de règles métier de notre base de données inégalée

Qualité : Processus qualité DO-200B conforme aux certificats FAA LOA 1 et EASA DAT

Configuration : NavData est adapté spécifiquement à vos besoins - ou vous pouvez le configurer vous-même. Aucune autre solution n'offre la flexibilité de Jeppesen NavData

❖ PEP : Performance Engineer's Program

C'est un logiciel fourni par Airbus, il se compose d'une base de données de performances à basse vitesse et d'une base de données de performances à haute vitesse avec leurs programmes respectifs. Pour préparer les fiches limitations.

Les programmes de performances à basse vitesse consistent en un programme de calcul de cartes de décollage et d'atterrissage (TLC) qui permet de calculer les :

- Performances de décollage et d'atterrissage réglementaires,
- Performances de décollage non certifiées prenant en compte les données de piste et les conditions météorologiques,
- Ainsi que le programme de tabulation et d'interpolation (TAB), délivré avec l'AFM (Aircraft Flight Manual), qui permet la lecture, l'édition et interpolation des tables répertoriées dans l'AFM.

Les programmes de performances à grande vitesse sont le programme de calcul des performances en vol (IFP) qui permet de calculer :

- Les performances des aéronefs.
- performances pour chaque phase de vol

Le programme de surveillance des performances de l'avion (APM) qui permet d'analyser les performances de croisière de l'avion à partir des données enregistrées pendant les périodes de vol stabilisées.

❖ FODM : Flight Operations Documentation Manager

Il permet de customiser les données envoyé par Airbus (Doc XML) pour qu'elles soient appropriées à la compagnie

❖ BPS : Boeing Performance Software

C'est un logiciel fourni par Boeing, il permet de calculer :

- Performances de décollage et d'atterrissage réglementaires,
- Performances de décollage non certifiées prenant en compte les données de piste et les conditions météorologiques
- Les performances des aéronefs.
- performances pour chaque phase de vol

Afin de préparer les fiches limitations.

Nb : Jeppesen envoie des fichiers LPC pour les avions Airbus, et des fichiers OPT pour les avions Boing, pour mettre à jour les données des A/D sur le PEP et le BPS chaque 28 jrs, et pour savoir quelle sont les A/D mise à jour il envoie également le fichier Jeppesen-Revision

- **FOS : Flight Operating Software**

C'est un logiciel fourni spéciale pour les avions ATR, il fait le même travail que PEP et le BPS.

IV.3.2 LES OUTILS INFORMATIQUES

1) Les Ordinateurs

Lors de la préparation des vols chaque Ingénieur utilise son ordinateur de travail personnel.

2) L'EFB : Electronic Flight Bag

C'est une plate-forme informatique sur IPÄD qui vise à réduire ou remplacer les papiers souvent dans le bagage à main du pilote, y compris le manuel d'exploitation et des graphiques. En outre, l'EFB peut accueillir spécialement des applications logicielles pour automatiser d'autres fonctions normalement exercées à la main, comme les calculs de performances au décollage. Donc l'EFB est une gestion de l'information électronique qui permet aux équipages d'effectuer des tâches de gestion de vol plus facilement et plus efficacement avec moins de papiers.

Les dispositifs d'EFB sont capables d'afficher une variété de données de l'aviation ou d'effectuer des calculs de base (calcul des performances du décollage, croisière, atterrissage, et en cas de panne moteur, calcul du devis de masse et centrage, optimisation de la charge offerte...)

L'EFB est nommé par rapport au sac de voyage traditionnel du pilote, qui est typiquement un sac lourd contenant des documents que les pilotes portent dans le cockpit. D'autre part, il doit assurer le niveau de sécurité obtenu avec l'utilisation de la documentation papier ; le niveau de sécurité doit être maintenu et amélioré, c'est-à-dire pour avoir l'approbation d'éliminer les documents à bord des aéronefs l'un des conditions les plus essentielles est l'évaluation de risque lie à l'utilisation de l'EFB.

La compagnie Air Algérie a adopté le projet de l'EFB en 2016 en gardant toujours la version papier ; les EFB installés dans le cockpit, certains sont fixes sur avion, mais d'autres sont portables et peuvent donc être connectés à internet. L'administration du système EFB est faite par un administrateur EFB qui est désignée par l'exploitant.

L'EFB permet l'installation d'applications de performances et le téléchargement de toute la documentation requise (MEL, FCOM, AFM, QRH…) et de ses mises à jour afin de réaliser les vols en toute facilité et sécurité avec la précision requise. On citera :

- FSW « FLY SMART WITH AIRBUS » : pour Airbus ;
- OPT « ON BOARD PERFORMANCE TOOL » : pour Boeing ; et
- SPS « SINGLE-POINT PERFORMANCE SOFTWARE » pour l'ATR

Les outils de performance embarquée permettent à l'équipage de conduite et au personnel au sol de la compagnie aérienne d'effectuer en temps réel des calculs de masse et centrage et de décollage et d'atterrissage pour toutes les cellules avion actuelles. En utilisant les conditions actuelles des passagers, du fret, des conditions météorologiques et des pistes, il réduit les coûts de maintenance en empêchant l'usure du moteur et augmente les revenus en optimisant la capacité des passagers et du fret.

Les données de mis à jour envoyés par Jeppesen pour les outils de performance embarquée sont customisés selon les besoins de la compagnie par :

- PAADMIN → pour Airbus
- OPT Administrateur → pour Boing
- FOS → pour ATR

3) Le transfert des données de vol via USB, CD, PCMCA

Pour transférer les données de vol vers **le FMS** ou les ou mettre à jour (chaque 28jrs), la personne chargée de cette tâche utilise des supports numériques tels que les USB, CD, PCMCIA (PC card).

- USB → pour A330
- CD → pour B737
- PCMCIA → pour ATR

Ces données sont téléchargées du PC par des lecteurs.

4) Le FMS : Flight Management System

Le FMS est un élément principal de l'avionique d'un avion moderne, il permet de réduire la charge de travail de l'équipage dans la planification des vols, la gestion des performances, le pilotage de l'avion à travers le pilote automatique et le contrôle de la poussée des réacteurs, de mesurer les paramètres de vol et d'effectuer la navigation.

Le FMS est donc en mesure de contrôler la totalité du vol, du décollage à l'atterrissage en effectuant tous les calculs utiles à travers les FMC (Flight Management Computeur). Il fournit également toutes les informations du vol sur les écrans appropriés.

Tous les FMS sont munis d'une base de données nécessaire notamment pour la construction et le suivi du plan de vol, dans la zone où l'avion est sensé voler. Cette base de données contient :

- Des plans de vol préalablement établis - Balises de navigation VOR, VOR/DME, DME, NDB
- Way-points (points de report)
- Airways (routes aériennes)
- Holding (attente)
- Contraintes (altitude ou/et de vitesse)
- Aéroports et leurs différentes pistes
- Départs standards SID (Standard instrument departure)
- Arrivés standards STAR (Standard Instrument Arrival)
- Et d'autres renseignements concernant les installations au sol.

Et elle est mise à jour tous les 28 jours, par l’administrateur (ingénieur d’étude aéronautique), pour assurer l’intégrité des données utilisées, la conformité avec la réglementation et la politique compagnie. L’administrateur est chargé de :

- Télécharger les logiciels mise à jour par le constructeur ;
- Décoder les données existants (les procédures des aérodromes, Air way...) ;

- Transférer ces données codées sur CD/ USB/ PCMCIA pour mettre à jour le FMS de chaque avion.

IV.4. LES DIFFÉRENTS TYPES DES CYBER ATTAQUES

Aujourd'hui, nous pouvons tous être victime d'une attaque informatique, que nous soyons une entreprise ou une personne tierce, nous disposons tous d'informations confidentielles, qui peuvent être la cible d'une attaque.

Certaines attaques informatiques ont comme objectif d'infecter l'ordinateur, on parle alors de machine zombie. Une infection informatique est le fait qu'un ordinateur soit contrôlé/utilisé par une personne malveillante à l'insu du propriétaire.

Une infection peut dans certains cas être faite pour utiliser la puissance combinée de milliers d'ordinateurs infectés. Il existe deux utilisations de cette puissance :

- Une attaque puissante : certaines attaques informatiques nécessitent une grande puissance pour pouvoir être efficace (Denial of Service attack (DoS)).
- Cryptominage : la puissance combinée est utilisée pour miner la monnaie virtuelle. Ceci permet aux mineurs d'éviter de devoir acheter d'autres ordinateurs pour miner, ils empruntent illégalement ceux des autres.

Dans ce titre je vais donc analyser les différentes attaques informatiques existantes. Cette liste n'est pas exhaustive, il existe énormément de menaces au niveau informatique, les menaces listées sont les plus courantes et celles dont nous en entendons le plus parler dans les news ou les journaux. [21]

IV.4.1. SOCIAL ENGINEERING

L'ingénierie sociale est une attaque utilisée pour collecter des informations sur des cibles potentielles ou les pousser à faire des transactions/paiements. L'ingénierie sociale se base sur une faiblesse commune de tous les systèmes d'informations existants : le facteur humain.

L'ingénierie sociale est donc le principe d'exploiter des faiblesses psychologiques sociales pour obtenir des informations ou de l'argent d'une personne, le contact est fait via différents moyens : téléphone, réseaux sociaux,

messagerie, rencontre personnelle, etc… C'est une attaque qui demande peu de connaissances techniques et est souvent utilisée pour la récolte d'informations ou sur des cibles psychologiquement faibles (personnes âgées/handicapées). [21]

IV.4.2. L'ACQUISITION DE MOT DE PASSE

L'acquisition de mot de passe est le fait qu'une personne malveillante va tenter de deviner le mot de passe d'un utilisateur avec l'aide de certaines informations.

En effet, malgré les différents avertissements concernant la composition d'un mot de passe, la majorité des personnes cherchent à avoir un mot de passe qui soit facile à se rappeler ce qui le rend donc facile à deviner. Nous avons tous différents comptes sur différents sites et il est parfois difficile de se rappeler de tous nos mots de passe, ce qui pousse les personnes à avoir le même mot de passe pour des comptes différents. Tous ces éléments créent un danger pour l'utilisateur, si le mot de passe est simple et est le même pour différents comptes, il suffit de deviner ce dernier pour pouvoir accéder à toutes les données.

Cette attaque vise tout le monde, le but est tout simplement d'obtenir des informations/accès et par la suite de s'enrichir avec les informations obtenues. [21]

IV.4.3. SQL INJECTION

Le langage SQL. SQL (Structured query language ou langage de requête structurée) est un langage informatique permettant l'exploitation des bases de données relationnelles, il permet de faire des manipulations sur les données par des requêtes : la lecture, la modification, l'ajout et la suppression de ces dernières.

SQL Injection est donc une attaque qui exploite la syntaxe SQL, il s'agit d'injecter dans une requête SQL du code supplémentaire pour provoquer une manipulation des données de la base de données.

Les principales cibles de ce type d'attaques sont les entreprises disposant de base de données. Plus l'entreprise est grande et importante, plus il y a de risques que cette dernière soit prise pour cible. En effet, plus il y a de clients plus il y a de données à vendre ou à utiliser et plus l'importance de l'entreprise est grande, plus les données ont de la valeur. [21]

IV.4.4. CROSS-SITE SCRIPTING (XSS)

Certains sites (internet) permettent aux utilisateurs d'intéragir avec le site en récupérant les inputs qui feront alors partie du site. Comme exemple, les sites avec des photos et articles qui permettent aux utilisateurs de commenter grâce à des interfaces/formulaires.

Le cross-site scripting est le fait d'exploiter une faille pour y injecter un contenu malveillant provoquant alors d'autres actions que celles déjà existantes sur la page. La faille peut être via un message par un forum ou par de la manipulation d'URL.

Il existe deux types de failles XSS :

- XSS réfléchi / non permanent : ce type de failles sont présentes lorsque les données fournies par un utilisateur sont utilisées par le serveur pour produire une page de résultat avec son URL. Ces URLs sont utilisées avec l'ingénierie sociale pour forcer un utilisateur à cliquer sur une URL piégée.
- XSS Stocké / permanent : ce type de failles sont présentes lorsque les données fournies par un utilisateur sont stockées sur un serveur (base de données, fichiers, etc…).

Elles sont dangereuses car permanentes et permettent donc d'atteindre un grand nombre de victime.

Les cibles de ces attaques sont les entreprises disposant d'un site internet. En effet, plus un site internet a de visiteurs/clients, plus le risque d'une attaque potentielle est élevé. [21]

IV.4.5. MALWARE

Malware vient de l'anglais « malicious software » qui signifie logiciel malveillant. Un malware est développé dans le but de nuire ou de récolter des informations d'un système. Il existe différentes familles de malware qui ont chacune leur manière de fonctionner et des objectifs divers.

IV.4.5.1. Virus

Un virus est un automate auto réplicatif, c'est-à-dire qu'il peut fabriquer par autonomie une copie de lui-même en utilisant les ressources de son environnement. Tout comme leurs versions biologiques, les virus sont conçus pour se propager, ils

se répandent par tous les moyens d'échange de données numériques : réseaux, disques durs, clefs USB, etc…

Un virus est conçu pour rester indéfiniment caché, on dit alors qu'il s'exécute en arrière-plan, il peut faire un certain nombre d'actions dans l'appareil hôte :

- Supprimer des données, soit pour effacer ses traces, soit pour nuire au système.
- Endommager le système ou le ralentir.
- Installation de malware.
- Chiffrer des données pour demander une rançon.

Selon la manière dont est codé un virus, il sera et agira différemment :

- Le virus classique : il est attaché à un programme ou existe sous forme d'exécutable, une fois exécuté, il infecte l'appareil et se répand en se dupliquant sur d'autres exécutables. De plus certains virus contiennent une « charge utile », une charge utile est une action qui s'exécute après un certain temps qui supprime ou modifie des fichiers du système. Le virus mutant : il s'agit d'un clone d'un virus existant qui a été réécrit par d'autres programmeurs afin d'en modifier le comportement et la signature.
- Le virus polymorphe : vu que les antivirus détectent la signature des virus pour les repérer, le virus polymorphe dispose d'une fonction de chiffrement et de déchiffrement de leur signature qui leur permet de changer de signature après chaque exécution pour rester invisible aux yeux de l'antivirus.
- Le rétrovirus ou bounty hunter : il s'agit d'un virus qui a la capacité de modifier les signatures des antivirus afin de les rendre obsolètes/inefficaces.
- Le virus de boot : il s'installe dans le secteur de démarrage de l'appareil (Master boot record), il va prendre la place d'un programme de démarrage et sera ainsi exécuté lors du démarrage de l'appareil.
- Le macro virus : il utilise les macros des logiciels pour s'exécuter, notamment les logiciels de la suite Microsoft Office (Word, Excel, Powerpoint, etc…) qui disposent de macros grâce à un langage de

script commun : VBScript. Ainsi il est exécuté lors des macros et peut contaminer des fichiers. [21]

IV.4.5.2. Ver (Worm)

Un ver est un malware, il est similaire au virus car il a comme objectif de se propager et est auto réplicatif. Cependant, tandis que le virus a besoin d'un programme hôte pour se reproduire, le ver utilise les ressources de son environnement pour se multiplier et se propager.

Pour se propager, le ver utilise le réseau. Si le ver se trouve sur le réseau, il peut se propager sur les appareils connectés au réseau sans que l'utilisateur ne doive faire quoique ce soit. Par exemple, un ver peut envoyer une copie de lui à tous les contacts d'un carnet d'adresse, puis il envoie une copie de lui à chaque personne du carnet d'adresses des destinataires, etc. Le ver est utilisé pour :

- ✓ Infecter l'ordinateur (machine zombie)
- ✓ L'envoi de multiples requêtes à un serveur.
- ✓ Cryptominage. [21]

IV.4.5.3. Cheval de Troie (Trojan)

Le cheval de Troie vient de l'histoire de la Grèce antique lors de la guerre de Troie. L'histoire raconte que les Grecs ont offert aux Troyens un cheval de bois géant comme cadeau, les Troyens ont amenés le cheval de bois dans la ville comme un symbole de victoire. Cependant, des soldats grecs étaient cachés dans le cheval et ont attendu la nuit pour pouvoir ouvrir les portes de la ville et ainsi permettre à l'armée d'y entrer et d'obtenir la victoire. Voilà pour le mythe, mais qu'est-ce qu'un cheval de Troie en informatique ?

Un cheval de Troie n'est déjà pas un virus mais un malware qui a l'apparence d'un logiciel légitime, il contient dans son code une fonctionnalité malveillante et dans certains cas le logiciel remplit normalement le rôle pour lequel il a été installé. C'est lors de l'installation du logiciel que le cheval de Troie va installer le code malicieux qu'il transporte.

Les chevaux de Troie contiennent des parasites et ne sont pas auto réplicatifs, ils peuvent également ouvrir des portes du système aux personnes malveillantes. [21]

IV.4.5.4. Logiciel espion (Spyware)

Initialement, les logiciels espions étaient des logiciels utilisés pour espionner ou récolter des informations sur un ordinateur. Ces logiciels sont plus répandus qu'on ne le pense, on peut par exemple les trouver :

- Dans un cadre scolaire : il est utilisé lors des épreuves sur ordinateur pour pouvoir voir les écrans des étudiants et ainsi vérifier si ces derniers ne trichent pas.
- Dans le cadre familial : il est utilisé par les parents afin de s'assurer que les enfants ne fassent pas n'importe quoi avec l'ordinateur et n'aillent pas n'importe où sur le net.
- Dans le cadre professionnel : il est utilisé par l'employeur afin de surveiller les employés.
- La police : il est utilisé pour pouvoir suivre des activités criminelles.
- Lors d'attaque informatique : il est utilisé pour siphonner les données des utilisateurs.
- Commerciale : il est utilisé pour suivre la navigation internet d'utilisateurs pour faire de la publicité ciblée.

S'il s'agit d'un logiciel légitime installé par le propriétaire, ces logiciels ne sont pas dangereux. Cependant, s'il s'agit alors d'un malware qui s'est installé sans que le propriétaire du système ne s'en rende compte, alors le logiciel est dangereux car selon sa nature il transmettra des données confidentielles à la personne malveillante. Le logiciel espion utilise internet comme moyen de communication pour pouvoir transmettre les données récupérées à la personne malveillante.

Le type d'informations récupérées dépendra du logiciel espion et de sa conception :

- Enregistreur d'URL internet : ce logiciel mémorise tous les sites et pages visités, il peut être utilisé par la police, les parents (contrôle parental) et en milieu professionnel et parfois, dans un but commercial pour faire de la publicité ciblée.
- Attrapeur d'écran : il enregistre une capture d'écran à chaque fois que l'état de ce dernier change. Il est notamment utilisé au milieu scolaire lors d'épreuve sur ordinateur.

- ❖ Enregistreur d'email et de chat : il effectue une copie du texte de tous les emails entrants et sortants et dans le cadre d'un chat, de tous les messages.
- ❖ Enregistreur de frappe (keylogger) : il enregistre dans un fichier texte toutes les frappes faites sur le clavier (recherche Google, mot de passe, nom d'utilisateur, etc…). Bien souvent ces logiciels sont conçus pour détecter les URLs et s'activent seulement si cette dernière est importante : e-banking, site de ventes, etc….

À noter qu'à partir du moment que le logiciel espion enregistre des données sur votre ordinateur, il est alors possible de pouvoir récupérer et lire ces dernières. Si le logiciel est légitime, il vous sera sûrement demandé un mot de passe pour pouvoir y accéder, mais dans le cadre d'un malware, les informations seront directement transférées à la personne malveillante et l'accès vous sera bloqué. [21]

IV.4.5.5. Cible des malwares

Personne n'est à l'abri d'un malware. Les cibles varient seulement selon l'objectif recherché par la personne malveillante. En effet, si cette dernière souhaite obtenir de la puissance pour une attaque informatique plus importante (voir Denial of Service attack (DoS)), elle cherchera à propager le malware à travers des personnes tierces peu importe de qui il s'agit.

Si la personne malveillante cherche à récolter des informations sur une entreprise, elle cherchera sûrement à infecter un poste de travail quelconque dans l'entreprise (peu importe la hiérarchie de la personne) afin de pouvoir se répandre et ainsi obtenir les informations souhaitées. [21]

IV.4.6. DANIAL OF SERVICE ATTACK (DoS)

Le principe de cette attaque est de rendre indisponible un service en lui envoyant un nombre important de requêtes afin de saturer le serveur. Il faut savoir qu'un serveur a une capacité limitée de communication, si une personne malveillante parvient donc à envoyer des paquets/requêtes à répétition, le serveur peut alors commencer par ralentir et finalement crasher.

Figure IV.1 : Structure d'une attaque par déni de service [21]

Avec l'évolution technologique, aujourd'hui nous avons des serveurs plus performants et il devient difficile d'exécuter une attaque DoS. Cependant, il existe une alternative de plus grande ampleur que l'attaque par déni de service : Distributed Denial of Service attack (DDoS) ou attaque par déni de service distribuée. Le principe reste le même qu'une attaque par déni de service. Cependant, les cibles sont de plus grand réseau et demande alors une plus grande puissance pour pouvoir saturer ces derniers. L'attaque implique donc l'utilisation de la puissance combinée d'un grand nombre de machines infectées. Les personnes malveillantes souhaitant faire ce genre d'attaque doivent donc infecter des machines de nombreuses personnes. Lors de ces attaques, les propriétaires des machines ne sont pas conscients que leur ordinateur a été infecté et qu'ils ont participé indirectement à une attaque.

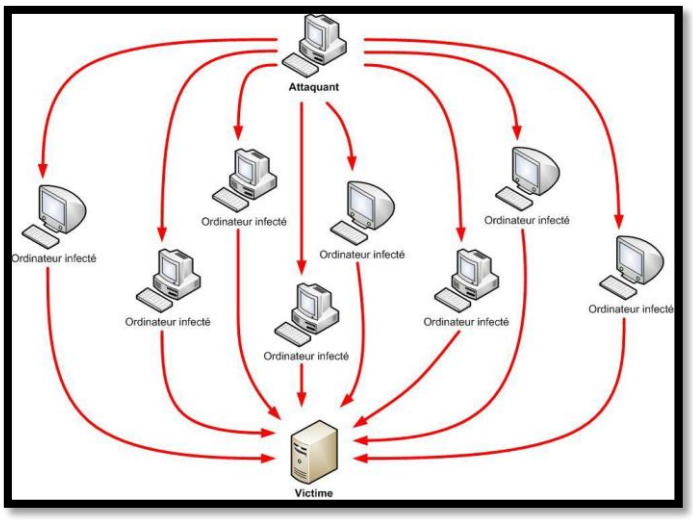


Figure IV.2 : Structure d'une attaque par déni de service distribuée [21]

Une attaque DDoS peut donc bloquer, temporairement ou durablement, un site web ou une plateforme d'e-commerce. De manière moins visible de l'extérieur, elle peut altérer le fonctionnement d'une application ou d'un serveur de messagerie, et empêcher la distribution des courriels dans une entreprise, par exemple.

Pour conduire une attaque DDoS, un hacker fait appel à un botnet, c'est-à-dire un « réseau zombie » de terminaux infectés, qui reçoivent tous l'instruction d'envoyer des requêtes au même service ou serveur. L'essor des objets connectés, faiblement sécurisés, mais disposant d'une large bande passante, démultiplie la surface d'attaque potentielle.

Une attaque DDoS peut avoir un impact sur votre activité, et donc des répercussions financières particulièrement graves : au-delà de l'arrêt partiel ou total de l'activité, il faut intégrer le coût de la surconsommation de bande passante, les frais de remise en service, et l'altération de l'image de la société auprès de ses clients. Enfin, les auteurs de l'attaque peuvent exiger une rançon pour la faire cesser. D'après une autre étude de Netscout, les attaques DDoS pourraient coûter plus de 550 millions d'euros par.

Les cibles des attaques par déni de service sont souvent des grandes entreprises/sites. Ils sont souvent pris pour cible par des groupes de pirates pour des raisons d'idéologie et de politique. [22]

IV.4.7. RANSOMWARE

Les ransomwares sont des logiciels d'extorsion qui peuvent verrouiller votre ordinateur et demander une rançon en échange du déverrouillage de celui-ci.

Dans la plupart des cas, l'infection par ransomware se présente comme suit. L'application malveillante commence par accéder à l'appareil. Selon le type de ransomware, c'est l'ensemble du système d'exploitation ou des fichiers individuels qui sont chiffrés. Une rançon est alors demandée aux victimes en question. Pour minimiser le risque d'attaque par ransomware, il est conseillé d'utiliser des logiciels de haute qualité, comme les logiciels de Kaspersky.

Les ransomwares : un élément de la famille des applications malveillantes

Les malwares sont le résultat d'un mélange des mots « malveillant » et « application » en anglais. Le terme « malware » couvre donc l'ensemble des applications malveillantes qui peuvent être dangereuses pour votre ordinateur. Il s'agit entre autres des virus et des chevaux de Troie.

IV.4.8. Phishing, spear-phishing et whaling

Dans la vraie vie, si une personne venait à sonner à votre porte en se présentant comme un représentant d'une entreprise auquel vous êtes le client tout en vous demandant de l'argent ou une signature pour X ou Y raisons, il y a de très fortes chances que vous ne le croyez pas non ? Aujourd'hui avec internet et l'anonymat qu'il fournit, la personne ne vient plus sonner à votre porte mais prend contact avec vous via différents réseaux afin d'obtenir de l'argent et/ou des informations. Cette méthode s'appelle le phishing qui vient du mot anglais « fishing » qui signifie pêcher. Le phishing est donc une pratique qui consiste à viser un « poisson » (nous tous), lui envoyer un appât et espérer que ce dernier morde à l'hameçon dans le but de récupérer des informations ou d'infecter son appareil.

Chaque jour, il y a des milliers de personnes qui se font piéger et révèlent leurs informations personnelles/confidentielles (nom d'utilisateur, mot de passe et données) à de mauvaises personnes ou se font infecter.

- Phishing : phishing cible tout le monde, le principe du phishing et d'envoyer énormément de mails et d'espérer que parmi toutes les personnes ciblées, quelques-unes mordent à l'hameçon, personne n'est à l'abri du phishing.
- Spear-phishing : il cible également tout le monde mais de manière plus précise et avec des informations complémentaires pour tromper plus facilement la victime (nom, adresse, etc…).
- Whaling : il cible le gros poisson, un chef d'entreprise, directeur, chef de banque, etc…

IV.4.9. VECTEURS DES MENACES

Maintenant que nous en savons plus sur les menaces informatiques d'aujourd'hui, il est important de comprendre par quels moyens certaines sont transmises. Pour ce faire, voici le tableau 6 qui permet d'avoir un aperçu sur les différents vecteurs et leurs menaces. [21]

Tableau IV. 1 : Vecteurs de menaces.

Menaces	Vecteurs	Explication
Social engineering	Téléphone Messagerie Rencontre personnelle	L'attaque nécessite que la personne malveillante prenne contact avec la victime afin de pouvoir manipuler cette dernière.
Acquisition de mot de passe	Réseaux sociaux	Cette attaque nécessite de récupérer des informations sur la victime par différents moyens pour deviner le mot de passe.
Phishing, spear-phishing et whaling	Messagerie	L'attaque nécessite l'envoi d'un grand nombre de mails (phishing) ou de mails ciblés (spear-phishing) ou de mail précis (whaling) en espérant que les victimes répondent à l'arnaque.
SQL Injection	Serveur avec base de données utilisant le langage SQL	L'attaque nécessite une base de données utilisant le langage SQL afin d'en exploiter la syntaxe.
Cross-site scripting	Serveur	L'attaque nécessite que la victime ait un serveur.
Malware (virus, vers, cheval de Troie, Spyware)	Messagerie Logiciel Navigation internet	Ces différents parasites peuvent être exécutés par un script attaché à une pièce jointe d'un email. Certains logiciels qui semblent légitimes viennent avec des Malwares. La navigation sur des sites douteux/inconnus peut permettre à certains Malwares d'infecter

	Branchement direct	l'appareil. Dans certains cas, le branchement d'un appareil non infecté à un appareil infecté peut infecter ce dernier (clef USB, disque dur externe, ordinateur).
Denial of Service attack	Serveur	L'attaque nécessite que la victime ait un serveur fournissant une ressource.

IV.5. CYBER-SÉCURITÉ AU NIVEAU D'AIR ALGERIE

Avant de parler sur les mesures de cyber-Sécurité au niveau d'Air algérie, il faut définir c'est quoi une cyber-Sécurité.

Cyber : Tout ce qui concerne l'utilisation des technologies et d'informatique.

Cyber-Sécurité : la cyber-Sécurité consiste à réduire le risque des cybers attaques par des moyens physiques ou des mesures de cyber défense dans le cadre de l'utilisation des systèmes d'informatique.

La sécurité informatique fait référence à des propriétés d'un système informatique qui s'expriment en termes de disponibilité, d'intégrité et de confidentialité. Ces critères de base sont réalisés par la mise en œuvre des fonctions et services de sécurité, tels que ceux de contrôle d'accès ou de détection d'incidents par exemple. Des services de sécurité liés à l'authentification (notions d'authenticité et de véracité) ou encore à la non-répudiation, à l'imputabilité, ou à la traçabilité contribuent à protéger des infrastructures numériques.

Ci-dessus vous trouvez les mesure de cyber-Sécurité pour chaque type de cyber attaque.

1) Attaque par le piratage de compte : Vole de données

Mesures de prévention :

- Sensibilisation :

Exemple d’un message de sensibilisation pour les employeurs AH par email :

Nous souhaitons vous rappeler de l’importance de la sécurité de la messagerie professionnelle. En tant qu’outil de communication officiel, la messagerie est une cible potentielle pour les cybercriminels et les personnes malveillantes qui cherchent à extorquer des informations sensibles et/ou une usurpation d’identité

Pour la sécurité de votre compte, veuillez :

- ❖ Dans le cadre de l’exercice de vos activités professionnelle, utiliser exclusivement la messagerie professionnelle d’Air Algérie (...@airalgerie.dz)
- ❖ Ne jamais utiliser la messagerie AH pour des raisons personnelles (création de comptes sur les réseaux sociaux, envois de mails personnel ou s’inscrire sur des newsletters etc...),
- ❖ Dans le cadre de l’exercice de vos activités professionnelle Ne jamais utiliser votre messagerie personnelle,
- ❖ Ne jamais faire suite aux e-mails provenant de sources inconnues,
- ❖ Vérifier toujours les adresses sources et les noms de domaines,
- ❖ Ne jamais cliquer sur des liens ou télécharger des fichiers joints aux e-mails provenant de sources inconnues,
- ❖ Ne jamais transférer ou répondre à ces e-mails,
- ❖ Utilisez des mots de passes complexe en combinant majuscule, minuscules, chiffres et caractères spéciaux,
- ❖ Changer régulièrement vos mots de passe,
- ❖ Ne jamais communiquer ses mots de passe à une tierce personne,
- ❖ Ne pas partager d'informations sensibles ou confidentielles par e-mail,
- ❖ Tenir votre système d’exploitation et antivirus à jour,
- ❖ Signaler toute expiration de licence antivirus ou toute éventuelle infection virale,
- ❖ Signaler immédiatement toute activité suspecte sur votre machine et changer immédiatement le mot de passe.

- Faire des formations en présentiel pour sensibiliser le personnel.
- Double authentification pour chaque compte.

- Masse mailing : le mass mailing est d'envoyer le même e-mail à un grand groupe de contacts en même temps. Il répète le message de votre entreprise et vous aide à rester dans la tête de vos contacts. Il est utilisé pour tester le personnel de l'entreprise.

2) Attaque par D DOS :

Mesures de prévention :

- Protection Anti-DDOS :

Un système de protection anti-DDoS permet de protéger un site web, une application, un réseau ou un datacenter contre les attaques par déni de service. Il remplit deux missions principales. Tout d'abord, il analyse en continu et en temps réel les paquets de données qui transitent sur le réseau IP. Puis, en cas d'attaque, il détourne les éléments non-légitimes du trafic entrant, pour ne laisser passer que le trafic légitime.

Un anti-Ddos fait généralement appel à un ensemble de composants systèmes et logiciels pour inspecter et isoler le trafic malveillant et n'autoriser que les requêtes d'accès légitimes. Il convient à ce stade de distinguer les anti-DDoS cœur de réseau et les anti-DDoS sur site.

- Cloudflare : Un réseau mondial conçu pour le cloud.

Le réseau mondial de Cloudflare est conçu pour sécuriser l'ensemble des équipements que vous connectez à Internet de manière privée, rapide et fiable. Sécurisez vos sites web, API et applications Internet. Protégez vos réseaux d'entreprises, vos employés et vos appareils. Rédigez et déployez du code qui s'exécute à la périphérie du réseau. Cloudflare garantit également la sécurité en protégeant les propriétés Internet contre les activités malveillantes telles que les attaques DDoS, les bots malveillants et autres intrusions funestes.

3) Attaque par Phishing , les logiciels malveillants ou l'injection de code : fuites de données.

Mesures de prévention :

Vous pouvez utiliser des outils de sécurité standard pour vous protéger contre la perte et la fuite de données. Par exemple, un système de détection d'intrusion

(IDS) peut alerter sur les tentatives d'accès à des données sensibles. Un logiciel antivirus peut empêcher les attaquants de compromettre les systèmes sensibles. Un pare-feu peut bloquer l'accès de toute partie non autorisée aux systèmes stockant des données sensibles.

Si vous faites partie d'une grande organisation, vous pouvez vous tourner vers des outils ou des solutions DLP désignés pour protéger vos données. Vous pouvez également utiliser les outils du centre d'opérations de sécurité (SOC) pour vous aider avec **DLP**. Par exemple, vous pouvez utiliser un système SIEM (Security Information and Event) pour détecter et corréler les événements susceptibles de constituer une fuite de données.

- DLP (Data Loss Prevention)

La prévention des pertes de données (DLP) est la pratique consistant à détecter et à prévenir les violations de données, l'exfiltration ou la destruction indésirable de données sensibles. Les organisations utilisent DLP pour protéger et sécuriser leurs données et se conformer aux réglementations.

Le terme DLP fait référence à la défense des organisations contre la perte de données et la prévention des fuites de données. La perte de données fait référence à un événement au cours duquel des données importantes sont perdues pour l'entreprise, comme lors d'une attaque par ransomware. La prévention des pertes de données se concentre sur la prévention du transfert illicite de données en dehors des limites organisationnelles.

Les organisations utilisent généralement DLP pour :

- ❖ Protégez les informations personnelles identifiables (PII) et respectez les réglementations en vigueur
- ❖ Protéger la propriété intellectuelle essentielle pour l'organisation
- ❖ Obtenez une visibilité des données dans les grandes organisations
- ❖ Sécurisez la main-d'œuvre mobile et appliquez la sécurité dans les environnements Bring Your Own Device (BYOD)
- ❖ Sécuriser les données sur les systèmes cloud distants.

4) Attaque lors de la recherche internet ou l'utilisation Web

En informatique, un fichier log permet de stocker un historique des événements survenus sur un serveur, un ordinateur ou une application. Ce "journal" présenté sous la forme d'un fichier, ou équivalent, liste et horodate tout ce qui se passe.

Ce fichier log est protégé par le SIME (Security Information and Events Managment).

Mesures de prévention :

- Security Information and Events Managment (SIEM) :

La gestion des informations et des événements de sécurité (SIEM) est un ensemble d'outils et de services offrant une vue globale de la sécurité des informations d'une organisation.

Les outils SIEM fournissent :

- ❖ Visibilité en temps réel sur les systèmes de sécurité de l'information d'une organisation.
- ❖ Gestion du journal des événements qui consolide les données de nombreuses sources.
- ❖ Une corrélation d'événements recueillis à partir de différents journaux ou sources de sécurité, à l'aide de règles si-alors qui ajoutent de l'intelligence aux données brutes.
- ❖ Notifications automatiques d'événements de sécurité. La plupart des systèmes SIEM fournissent des tableaux de bord pour les problèmes de sécurité et d'autres méthodes de notification directe.

5) Attaque par les Malware et les Ransomware

Mesure de prévention :

- Endpoint Detection and Response (EDR) :

La détection et la réponse aux terminaux (EDR), également connue sous le nom de détection et réponse aux menaces sur les terminaux (ETDR), est une solution intégrée de sécurité des terminaux qui combine une surveillance et une collecte continues en temps réel des données des terminaux avec des capacités de réponse et d'analyse automatisées basées sur des règles. Le terme a été suggéré par Anton Chuvakin de Gartner pour décrire les systèmes de sécurité émergents qui

détectent et enquêtent sur les activités suspectes sur les hôtes et les terminaux, en utilisant un degré élevé d'automatisation pour permettre aux équipes de sécurité d'identifier et de répondre rapidement aux menaces.

Les principales fonctions d'un système de sécurité EDR sont les suivantes :

- ❖ Surveillez et collectez les données d'activité des terminaux qui pourraient indiquer une menace
- ❖ Analyser ces données pour identifier les modèles de menace
- ❖ Répondez automatiquement aux menaces identifiées pour les supprimer ou les contenir, et informez le personnel de sécurité
- ❖ Outils d'investigation et d'analyse pour rechercher les menaces identifiées et rechercher les activités suspectes.

- Protection contre les ransomwares :
  - ❖ Ne cliquez jamais sur des liens dangereux : évitez de cliquer sur les liens contenus dans les messages de spam ou sur des sites Web inconnus. Si vous cliquez sur des liens malveillants, un téléchargement automatique peut être lancé, ce qui peut entraîner l'infection de votre ordinateur.
  - ❖ Évitez de divulguer des informations personnelles : si vous recevez un appel, un message texte ou un email d'une source non fiable vous demandant des informations personnelles, n'y répondez pas. Les cybercriminels qui préparent une attaque par ransomware peuvent essayer de collecter à l'avance des informations personnelles, qui sont ensuite utilisées pour adapter les messages de phishing à la victime. En cas de doute sur la légitimité du message, contactez directement l'expéditeur.
  - ❖ N'ouvrez aucune pièce jointe douteuse : les ransomwares peuvent également s'introduire dans votre appareil à travers les pièces jointes d'un email. Évitez d'ouvrir toute pièce jointe à l'aspect douteux. Pour vous assurer que l'email est digne de confiance, prêtez une attention particulière à l'expéditeur et vérifiez que l'adresse est correcte. N'ouvrez jamais de pièces jointes qui vous invitent à exécuter des macros pour les visualiser. Si la pièce jointe est infectée, son ouverture entraînera l'exécution d'une macro malveillante qui permettra à l'application malveillante de prendre le contrôle de votre ordinateur.

- ❖ N'utilisez jamais de clés USB inconnues : ne connectez jamais de clés USB ni d'autres supports de stockage à votre ordinateur si vous ne savez pas d'où ils proviennent. Il se peut que des cybercriminels aient infecté le support de stockage et l'aient placé dans un lieu public pour inciter quelqu'un à l'utiliser.
- ❖ Maintenez vos programmes et votre système d'exploitation à jour : la mise à jour régulière des programmes et des systèmes d'exploitation contribue à vous protéger contre les applications malveillantes. Lorsque vous effectuez des mises à jour, assurez-vous de bénéficier des derniers correctifs de sécurité. Cette mesure complique la tâche des cybercriminels qui souhaitent exploiter les vulnérabilités de vos programmes.
- ❖ Utilisez uniquement des sources de téléchargement connues : pour minimiser le risque de téléchargement de ransomwares, ne téléchargez jamais de logiciels ni de fichiers multimédias à partir de sites inconnus. Faites confiance aux sites vérifiés et dignes de confiance pour effectuer des téléchargements. Les sites Web de ce type sont reconnaissables aux certificats numériques. Assurez-vous que la barre d'adresse du navigateur de la page que vous visitez indique « https », et non « http ». Un bouclier ou un symbole de cadenas dans la barre d'adresse peut également indiquer que la page est sécurisée. Faites également preuve de prudence lorsque vous téléchargez quoi que ce soit sur votre appareil mobile. Vous pouvez faire confiance à la boutique Google Play Store ou à l'App Store d'Apple, en fonction de votre appareil.
- ❖ Utilisez des services VPN sur les réseaux Wi-Fi publics : une mesure de protection judicieuse contre les ransomwares consiste à utiliser consciencieusement les réseaux Wi-Fi publics. Lorsque vous utilisez un réseau Wi-Fi public, votre ordinateur est plus vulnérable aux attaques. Pour rester protégé, évitez d'utiliser un réseau Wi-Fi public pour effectuer des transactions sensibles ou utilisez un service VPN sécurisé.

6) Attaque due aux Téléchargements

Mesures de prévention :

- Un Firewall (Pare-feu) :

Est un appareil de sécurité réseau qui surveille et filtre le trafic réseau entrant et sortant en s'appuyant sur des politiques de sécurité préalablement établies par l'entreprise. Celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données.

- Common Vulnerabilities and Exposures :

CVE, abréviation de vulnérabilité et exposition communes, est une base de données de vulnérabilités et d'expositions de sécurité informatique divulguées publiquement.

CVE fait également référence aux vulnérabilités et expositions individuelles auxquelles un identifiant CVE unique (ID CVE) est attribué et ajoutés à la base de données (liste CVE). Un enregistrement CVE est publié pour chaque CVE afin de fournir gratuitement des détails sur la vulnérabilité au public.

- CHMOD :

CHMOD (abréviation de change mode) est un appel système d'Unix (norme POSIX) ainsi que la commande correspondante qui permet de changer les permissions d'accès d'un fichier ou d'un répertoire.

7) Attaquer par clés USB

La clé USB reste un outil pratique pour travailler au quotidien. Elle peut cependant facilement être infectée par un virus alors apprenez à la protéger.

Mesures de prévention :

- Acheter une clé USB sécurisée

Une clé USB sécurisée est une clé qui utilise des micropuces dans ses composants pour protéger le lecteur flash par un mot de passe. Certaines marques proposent des clés USB qui nécessitent l'écriture physique d'un code PIN pour pouvoir accéder à la clé USB. Elles peuvent contenir des fonctions telles que l'effacement des données si le mot de passe ou le code PIN n'est pas correctement écrit un certain nombre de fois. Le prix de ces clés est plus élevé que celui des clés qui n'ont pas cette fonction, mais il est préférable d'acheter ces clés USB qui vous permettent de protéger son contenu par un mot de passe.

- Utiliser un outil tiers

Vous pouvez également utiliser des outils et des logiciels tiers pour protéger par mot de passe un lecteur USB sur Windows 10. Vous pouvez installer différents logiciels qui peuvent vous aider à crypter les données en toute sécurité sur votre clé USB en vous fournissant un code PIN ou un mot de passe que vous devez taper avant d'accéder au contenu de votre clé USB. Quelques-unes des applications tierces incluent, mais ne sont pas limitées à :

- ❖ Gilisoft USB encryption
- ❖ Rohos Mini drive
- ❖ USB Safeguard
- ❖ USB secure
- ❖ DiskCryptor
- ❖ VeraCrypt

N'importe lequel de ces logiciels et beaucoup d'autres peuvent être utilisés pour protéger le lecteur flash par mot de passe.

IV.6. L'ÉVALUATION DES CYBER ATTAQUES

Dans ce titre je vais faire une évaluation des risques des cybers attaques (voir IV.4), lors de la préparation des vols (voir IV.2 et IV.3), en utilisant la méthode BOW TIE présentée dans le chapitre III (voir III.5.1) et la matrice de risque que j'ai développé, ainsi que le programme (voir III.7).

Lorsqu'on dit la méthode BOW TIE, c'est-à-dire :

Identifier : L'évènement indésirable, Les différentes menaces et causes

Contrôler : Les barrières de prévention.

Définir : Les barrières d'atténuation et récupération.

Evaluer : Les conséquences.

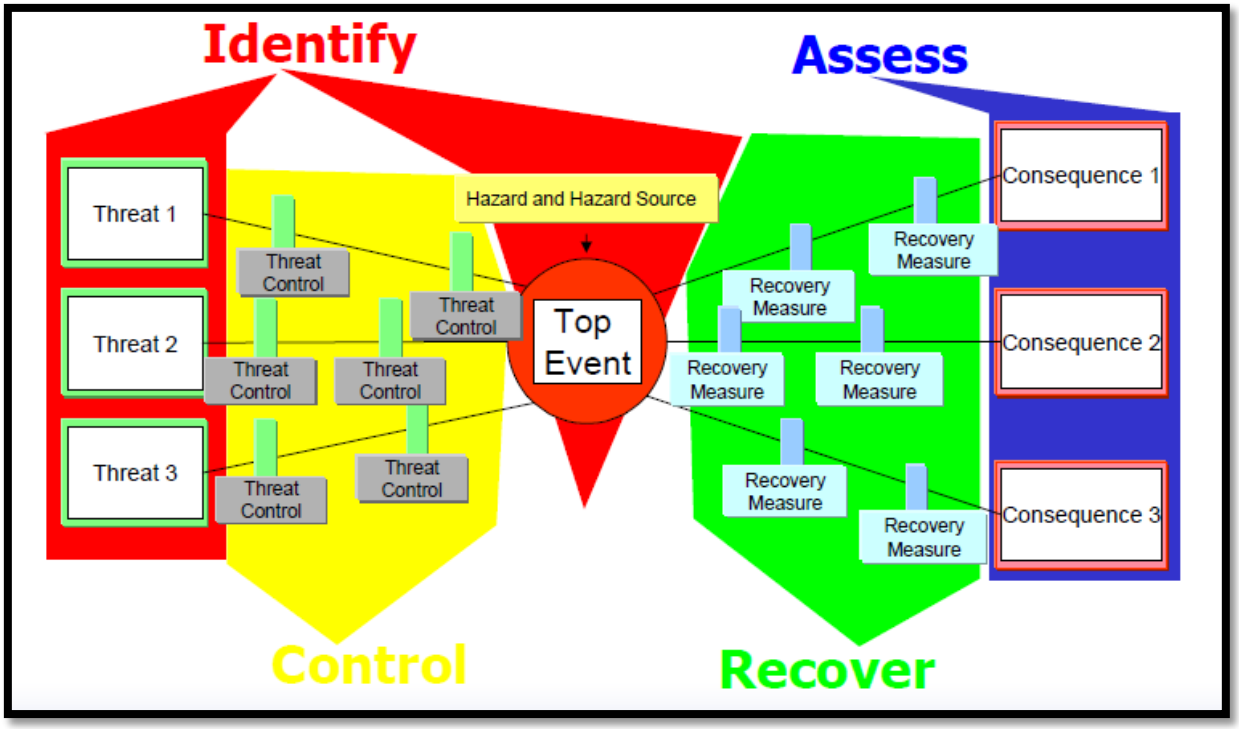


Figure IV.3 : <u>Diagramme 2 de la BOW TIE.</u>

<u>Objet d'évaluation</u> : Les systèmes informatiques et les outils technologique critiques dans les opérations aériennes.

<u>Directions concerné</u> : Direction des opérations aériennes, et la direction de sureté.

<u>Evènement indésirable commun</u> : Cyber attaque des systèmes informatiques et les outils technologiques dans la préparation des vols.

- Systèmes de planification de vol et données utilisées
- Systèmes de répartition et données utilisées
- Systèmes et données de calcul des performances des aéronefs
- EFB : Electronic Flight Bag (sac de vol électronique)
- Systèmes de navigation

Le tableau ci-dessus représente 2 évènements indésirables présentés selon la méthode BOW TIE.

Tableau IV. 2 : BOW TIE sous forme d'un tableau.

Menaces	Causes	Barrières de prévention	Evènement indésirable	Barrières de récupération	Conséquences
- Fuite de donnés -Transférer des fausses données - Sabotage ou modification de la base de données des applications de calcule des performances - Sabotage ou modification des cartes électroniques et documentation	- Acquisition des mots de passes - Malware -Attaque DDOS ou DOS -Ransomware -Phishing (Hamçonnage visant l'obtention de renseignements confidentiels) -Injection SQL	-Anti-SPAM -Sensibilisation -Blocage de liens frauduleux via pare-feux. -Anti- Virus -Logiciels de monitoring -Procédure et logiciels de détection de vulnérabilités -Code reviewing par l'équipe de développement -Accès authentifié par empreinte digitale -Registre et traçabilité des accès -Masse mailing de sensibilisation au personnel - Authentification à deux facteurs	**Accès non autorisé aux logiciels**	-Calcul de performance en utilisant les abaques des performances constructeur. -Disponibilité de toute la documentation opérationnelle en format papier à bord. -Application des Procédures d'urgence par l'équipage. Déclanchement de la procédure urgence compagnie ERP (Fiche Étude Risque). -Réinitialisation des accès. -Changement de mot de passe. Cryptage des données.	-Perte de données -Données inexploitables -Aéronefs non exploitables (blocage des systèmes software -Perte de l'aéronef (position de l'appareil, destruction de l'aéronef) -Déroutement de l'aéronef –Atteinte à l'image de la compagnie –pertes financières -Altération de l'exploitation normale de l'aéronef et perturbation des programmes des vols

-Défaillance et/ou Sabotage de l'équipement (IPAD) EFB	- Acquisition des mots de passes - Malware	-sensibilisation du personnel -Anti- Virus -Vérification mutuelle de l'intégrité des résultats donnés par les applications de calcule de performance (CDB/FO) -Accès sécurisé au Lieu de stockage et de maintenance de l'équipement (IPAD) -Chaque membre d'équipage de conduite dispose de son propre tablette -Tout équipement représentant des défaillances est considéré H/S	**Utilisation non autorisée d'EFB Ou attaque d'EFB**	-Calcul de performance en utilisant les abaques des performances constructeur -Disponibilité de toute la documentation opérationnelle en format papier à bord	-Perte de données -Données inexploitables -Altération de l'exploitation normale de l'aéronef et perturbation des programmes des vols

Après l'identification des conséquences, maintenant je vais les évaluer en utilisant la matrice de risque et le programme développé (voir III.7)

Tableau IV. 3 : L'évaluation.

Conséquences	Probabilité	Gravité	Niveau de risque
-Perte de données	P2	G2	Acceptable
-Données inexploitables	P2	G2	Acceptable
-Aéronefs non exploitables (blocage des systèmes software	P3	G3	Moyen
-Perte de l'aéronef (position de l'appareil, destruction de l'aéronef)	P2	G5	Elevé
-Déroutement de l'aéronef	P2	G5	Elevé
−Atteinte à l'image de la compagnie	P2	G4	Moyen
−pertes financières	P2	G3	Moyen
-Altération de l'exploitation normale de l'aéronef et perturbation des programmes des vols	P2	G4	Moyen

IV.7. CONCLUSION

A la fin de ce chapitre on conclut que la phase des préparations des vols n'est pas à labri des risques de cyber attaque, et la Méthode BOW TIE, elle est très utile pour présenter ces risques. Pour évaluer ces derniers il est nécessaire d'utiliser la matrice de risque afin de définir leurs niveaux.

On conclut également que la cyber sécurité porte bien sur la protection d'équipements informatiques, afin de les surveiller ou d'en prendre le contrôle, de plus elle concerne les usages défensifs de ces systèmes.

CONCLUSION GÉNÉRALE

Mon étude touche à sa fin, ce qui me permet maintenant de répondre à la question initialement posée : Est-il possible de gérer les risques liés aux cybers attaques ciblant la phase de préparation des vols ?

Tout d'abord, l'efficacité de la sûreté de l'aviation civile ne peut résulter que d'un engagement conjoint de tous les acteurs concernés, d'où la nécessité de définir entre eux un cadre réglementaire commun au quotidien dans la mise en œuvre des mesures de sûreté.

Les compagnies aériennes sont le secteur le plus vulnérable aux cyberattaques. C'est pourquoi la cyber sécurité est devenue un pilier de la stabilité et du développement du transport aérien commercial, ce qui nécessite que la culture de cyber sécurité doit être diffusée et renforcée auprès des prestataires de services.

Ensuite, afin d'étudier les risques de sûreté, notamment les cyber attaques, il est nécessaire de s'appuyer sur une méthode d'étude des risques efficace (dans mon étude j'ai utilisé la méthode BOW TIE) et une matrice des risques pour les évaluer.

Au final, on conclut que les risques liés aux cybers attaques peuvent être gérés de manière proactive, même à la phase de préparation des vols.

RÉFÉRENCES BIBLIOGRAPHIQUES

[1] MANUEL DE SURETÉ DE L'AVIATION, Doc 8973, Douzième édition, 2020

[2] MANUEL DU SYSTEME DE GESTION DE LA SÉCURITÉ ÉDITION N° : 03, 2022

[3] PROGRAMME DE SURETÉ, P.S.E, 07 EDT, REV 01,2022

[4] OACI -- Objectif stratégique de sûreté et facilitation -- Stratégie de cyber sécurité de l'aviation -- Octobre 2019.

[5] « Présentation d'Air Algérie- Rapports de stage- Lahiba26 » sur etudier.com, 28 mai 2013 (Consulté le 02/08/2023 à 10 :38).

[6] MANUEL QUALITE AIR ALGÉRIE Edition : 05

[7] MANEX A. Edition N°02 DOA sous-direction Engineering Air Algérie

[8] MANUEL D'ORGANISATION-DIRECTION DE LA SURETE Edition : 03

[9] France OACI -- L'OACI en quelques lignes — 26 mai 2022 https://oaci.delegfrance.org/L-OACI-en-quelques-lignes (Consulté le 23 juin 23 à 17 :14).

[11] ETUDE DE LA GESTION DES RISQUES CYBERSECURITE POUR L'EXPLOITANT AIR ALGERIE DANS LE CADRE DE SeMS -- Présenté par : REGUIEG MANAL - CHIBANE MANEL -- En vue de l'obtention du diplôme de Master en Aéronautique -- Spécialité : Navigation Aérienne --Option : OPERATIONS AERIENNES -- UNIVERSITE SAAD DAHLEB BLIDA 1 – IAES -- 2021 – 2022.

[12] ANNEXE 17 Onzième édition, mars 2020

[13] AUDIT IOSA SELON ISM6 Appliqué sur la compagnie Tassili Airlines, Auteur(s) : BENACHOUR, Mohamed Anis -- MOUSSERATI, Mohamed Oussama ; Date de publication : 2012, Editeur : université Blida 1

[14] IOSA 14 sept 2021 IOSA standard Manual

[15] Programme Nationale de Sureté d'Aviation Civile ALGERIE, Version n° : 5, Mai 2019

[16] Danger et risque - Évaluation des risques www.cchst.ca (Consulté le 25/06/2023 à 23 :48).

[17] La Gestion des Risques, concepts et méthodes, Révision 01 du 28 janvier 2009– CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS.

[18] Modèle de matrice des risques : évaluer efficacement les risques d'un projet pour assurer sa réussite (exemples inclus). 23 février 2023 asana.com/fr/resources/risk-matrix-template

[19] Security Management System Manual 2017, Copyright IATA

[20] Practical HSE Risk Management – An Introduction to the Bow-tie Method / Presentation to the International Conference for Achieving Health & Safety / Best Practice in Construction, Dubai, UAE, 26th- 27th February 2007 / By Gareth Book, Risktec Solutions Ltd.

[21] Analyse sur les différentes cyberattaques informatiques – Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES par : "Kevin CACCIAPAGLIA" – Carouge, le 3 septembre 2018 – Haute École de Gestion de Genève (HEG-GE) – Filière : Informatique de gestion.