« Cybersécuriser » l'aviation, un enjeu essentiel

Par Yannick ASSOUAD
Directrice générale adjointe du Groupe Thales

Nous vivons dans un monde de plus en plus connecté, et l'aviation ne fait pas exception. Que ce soit dans le cockpit, dans la cabine ou au sol, la connectivité apporte une toute nouvelle dimension à la sécurité des vols, à l'efficacité opérationnelle des compagnies aériennes, ainsi qu'au confort et au plaisir des passagers. Cependant, ces nouvelles capacités s'accompagnent de préoccupations critiques en matière de cybersécurité, qui doivent être intégrées au cœur de la conception des nouveaux produits et systèmes, et tout au long de leur cycle de vie opérationnel. Dans cet article, Yannick Assouad, EVP Avionique du Groupe Thales, détaille ces enjeux de cybersécurité associés à l'essor du numérique dans l'aviation, présente le cadre réglementaire en devenir, et souligne l'importance capitale pour les acteurs du secteur aéronautique de livrer des équipements qui sont "*cybersecure by design*".

La cybersécurité est désormais un enjeu qui nous concerne tous, dans nos sphères personnelles comme professionnelles. Nous sommes aujourd'hui conscients des risques bien concrets associés au monde virtuel qui alimente notre quotidien par le biais d'applications et de systèmes connectés : des comptes réseaux sociaux piratés, des coordonnées bancaires usurpées, des données personnelles volées… mais il ne suffit pas d'avoir connaissance de ces dangers ; il faut prévenir, se protéger, adopter les bonnes pratiques, et savoir comment réagir en cas de faille, voire contrecarrer les attaques. Le secteur de l'aéronautique dans son acception la plus large, et à une échelle toute autre, doit également faire face à ces menaces.

C'était l'objet du rapport de référence sur la cybersécurité dans l'aviation, publié en 2019 par l'Atlantic Council et soutenu par Thales : l'industrie aéronautique récolte les fruits de la numérisation des quinze dernières années, mais cette évolution engendre aussi de nouveaux risques, notamment des vulnérabilités sociales et techniques qui n'avaient jamais été prises en compte auparavant. Comme le mentionne également le rapport, « toute perturbation peut rapidement avoir des répercussions internationales, causer d'importants préjudices financiers et de réputation, et potentiellement compromettre la sécurité ».

Dans cet écosystème de l'aviation, où les différents acteurs sont tous très interdépendants et de plus en plus interconnectés, la cybersécurité implique non seulement la protection des informations sous forme de données numériques, mais aussi les réseaux, sites web, services, ordinateurs et portails associés, qui partagent et permettent l'accès aux données.

L'ère de l'aviation connectée

Évoquons ici l'impact du numérique dans l'aviation, à savoir un des principaux leviers du renouveau du secteur à la suite de la crise liée à la pandémie, aux côtés des efforts engagés en matière de réduction de l'impact climatique du transport aérien.

Au sol, les opérations de l'ensemble de la chaîne aéronautique nécessitant le recours au numérique sont de plus en plus nombreuses. Dans les aéroports, tous les services sont connectés pour faciliter l'expérience des passagers et réduire la charge de travail des opérations aériennes. Les centres d'exploitation des compagnies aériennes sont de plus en plus numérisés, qu'il s'agisse des systèmes de gestion des équipages, des systèmes d'exploitation des vols ou des systèmes de gestion des passagers. Les centres de maintenance des avions sont devenus de véritables nœuds logiciels, les mises à jour des systèmes et des contenus circulant en permanence. Enfin, la gestion du trafic aérien dépend de capacités de communication, de navigation et de surveillance en temps réel, qui sont de plus en plus connectées.

Au-dessus de nos têtes, les avions sont devenus des pôles de communication et de données mobiles, qui devraient générer 98 millions de téraoctets de données d'ici 2026, selon le rapport de référence "MRO Big Data" de la firme Oliver Wyman (2016). Pour être plus efficaces, les systèmes du cockpit sont de plus en plus connectés à des sources du monde ouvert. Par exemple, afin d'optimiser les profils et les trajectoires de vol, les systèmes de gestion de vol de nouvelle génération de l'avion capitalisent sur les données météorologiques et de trafic en temps réel. De plus, au lieu de s'appuyer sur des supports papier et des dossiers à l'ancienne, les pilotes utilisent

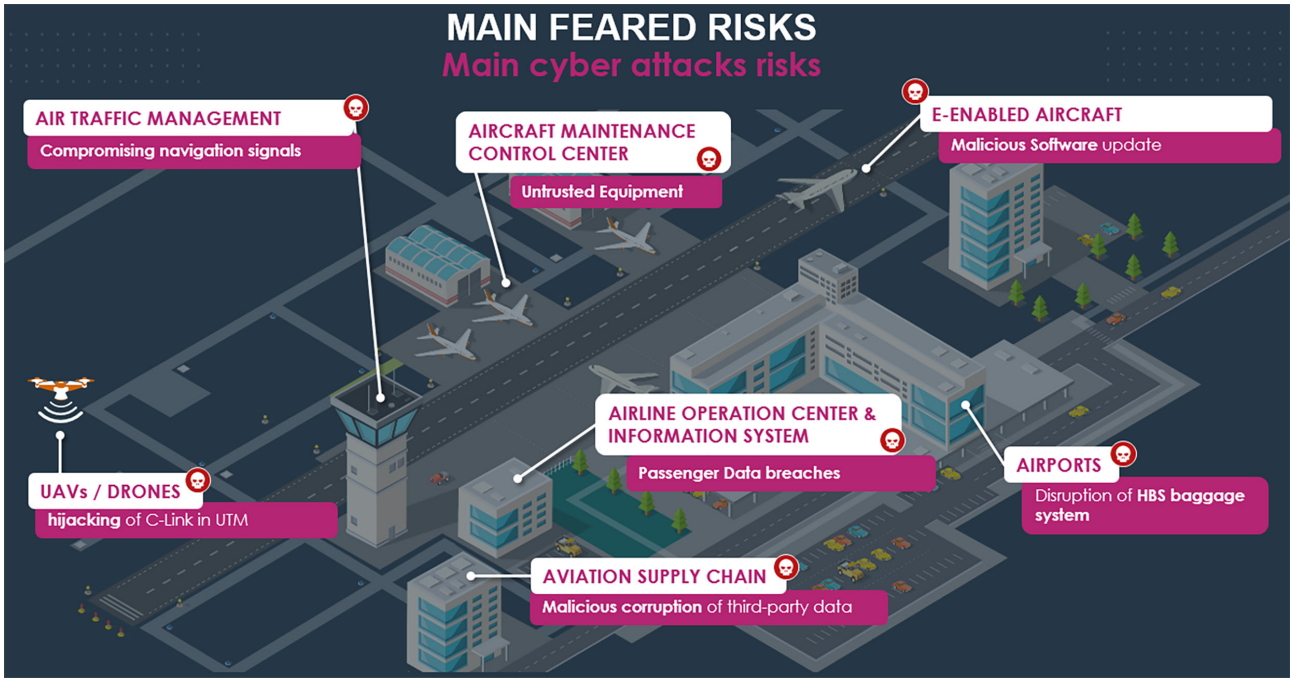

Figure 1 : Les principaux risques de cyberattaques (Source : Thales).

désormais des bagages de vol électroniques (ou *electronic flight bags*), qui fournissent une multitude de ressources et d'applications utiles, connectées et mises à jour en permanence pour optimiser les opérations.

Enfin, côté cabine, les systèmes de divertissement et de connectivité à bord offrent aux passagers non seulement un moyen de s'occuper, mais également une large gamme de services qui peuvent être personnalisés par les compagnies aériennes en fonction du profil du passager, de la destination et du type de voyage, ainsi que des capacités de connectivité et de communication qui permettent au passager de se sentir aussi bien dans les airs qu'au sol !

Un cadre réglementaire en devenir

Les autorités aéronautiques, notamment l'ICAO (l'Organisation de l'aviation civile internationale), l'EASA (l'Agence européenne de la sécurité aérienne) ou la FAA (Federal Aviation Administration, américaine), pilotent la normalisation des règles de cybersécurité pour le domaine aérien, sur la base des conclusions de groupes de travail composés d'opérateurs et d'industriels. Ces avancées permettent la mise en place d'un cadre global pour les systèmes de gestion de la sécurité de l'information.

Au sein de l'ICAO, les travaux effectués donnent lieu à des normes et à l'identification de meilleures pratiques, à l'élaboration de procédures et de documents d'orientation (*guidance materials*), à des cellules de veille pour s'assurer que le cadre du droit aérien international soit adapté pour faire face aux cyberattaques contre l'aviation civile, à des exercices de sensibilisation aux différentes instances de l'aéronautique civile aux enjeux de la cybersécurité, ou encore au déploiement d'initiatives de renforcement des capacités en matière de cybersécurité aérienne et de soutien à la mise en œuvre à l'intention des États et de l'ensemble de la communauté aéronautique.

Plus généralement, le secteur dans son ensemble est extrêmement actif dans ce domaine. Par exemple, l'ASD (Aerospace, Security and Defence Industries Association of Europe) dispose elle aussi d'un groupe de travail sur la cybersécurité dont l'objectif est de fournir des documents de synthèse de prise de position (*position papers*) sur les stratégies de cybersécurité dans l'aviation, et des organisations telles que l'EASA et l'EUROCAE (Organisation européenne pour l'équipement de l'aviation civile) coordonnent un certain nombre de comités consultatifs techniques dans des domaines tels que la formalisation d'orientations pour des procédures homogènes de gestion des risques, et l'identification des risques et des menaces pour la sécurité et leur impact sur le domaine aéronautique. Il va sans dire que Thales joue un rôle important dans tous ces développements.

L'atout essentiel du "*cybersecure by design*"

Pour des acteurs industriels comme Thales, cela signifie qu'il est essentiel de fournir des produits et des systèmes « cyberconçus », "*cybersecure by design*", c'est-à-dire résistants aux multiples risques réels de cyberattaques : vol de données, brouillage, injection de messages modifiés, signaux compromis (*spoofing*), corruption et actions malveillantes, etc. De fait, notre priorité est de garantir la sécurité et la résilience commerciale de ceux qui utilisent nos systèmes, qu'il s'agisse d'acteurs au sol (gestion du trafic aérien, d'aéroports, des opérations d'une compagnie aérienne) ou dans les airs (à bord des aéronefs).

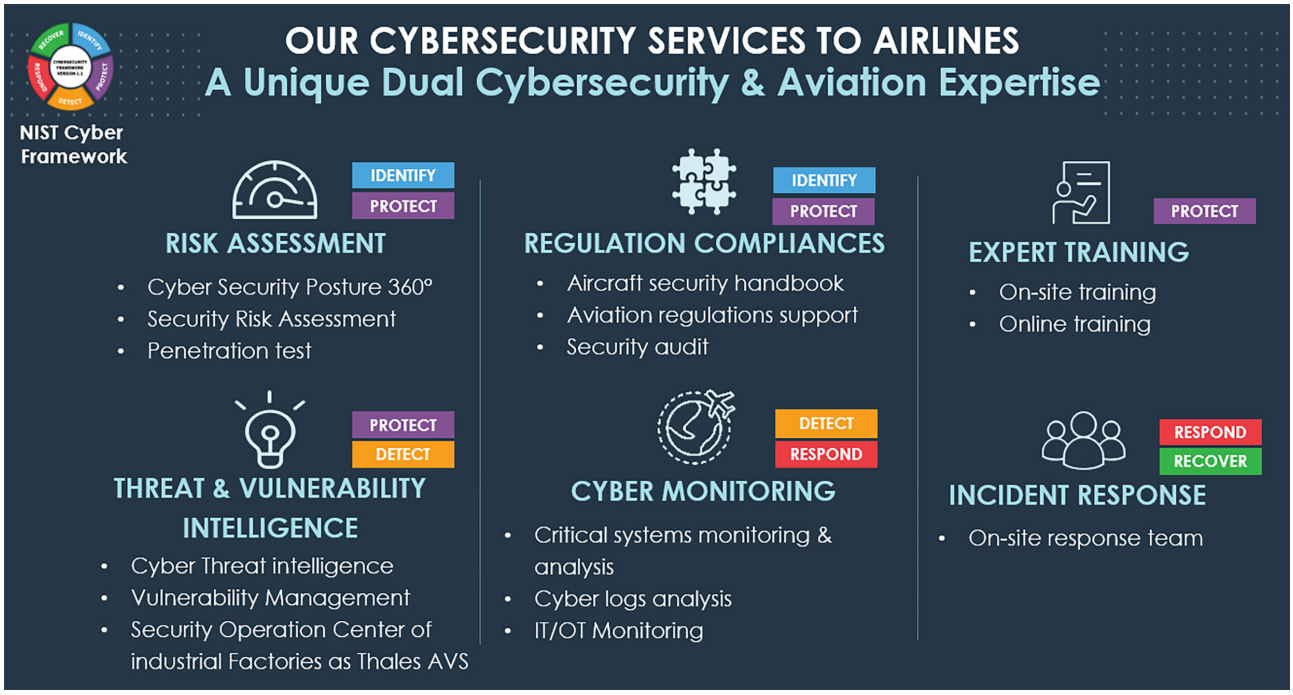

Figure 2 : Les services proposés par Thales (Source : Thales).

Nous avons intégré nativement la cybersécurité dans nos processus d'ingénierie et de fabrication en anticipant la conformité aux normes aéronautiques de cybersécurité telles que ED203-A/D0-256a, et en mettant en œuvre le cadre cybersécurité du NIST (National Institute of Standards and Technology) du ministère américain du Commerce – le cycle Identifier-Protéger-Détecter-Réagir-Reprendre – pour nos solutions.

Le fait que Thales fasse partie de la chaîne de confiance de l'aviation signifie également que nous sécurisons nos livraisons de produits contre les modifications malveillantes en apportant des preuves de leur authenticité tout au long de leur cycle de vie, et en travaillant activement pour aider nos fournisseurs à être cyber-résilients.

Un exemple probant est notre produit FlytLINK Aviocast, qui offre des échanges de données en monde ouvert depuis le cockpit *via* une passerelle cybersécurisée, et qui peut être installé sur les flottes actuelles. Avec ce produit, nous sommes pionniers dans le déploiement automatisé des corrections de vulnérabilités cyber sur le terrain, ce qui réduit les coûts de maintenance et renforce la sécurité. Cela illustre la manière dont nous fournissons une protection de bout en bout, du cockpit à la cabine et aux systèmes au sol, créant ainsi une chaîne de données critiques sécurisée pour les opérations de vol.

Un autre cas d'école est la suite avionique de cockpit FlytX. Le matériel (écrans et interfaces homme-machine) comme le logiciel ont été dotés de capacités cybersécurisées dès la conception, que ce soit d'ailleurs pour un usage dans l'univers civil ou militaire. Lorsque nous parlons des principaux atouts de FlytX, nous soulignons des qualités telles que sa compacité, son orientation vers l'équipage, ses capacités de personnalisation et son statut de connexion permanente et complète. Évidemment, les aspects de cybersécurité concernent principalement cette dimension « connectée », en tant que moyen de s'assurer que ces systèmes robustes ne comportent aucun angle mort, malgré les échanges constants avec des applications et des sources de données du monde ouvert... et c'est dans ce domaine que nous avons pleinement appliqué notre expertise interne en matière de cybersécurité.

Concrètement dans ce cas de figure, les serveurs de connectivité associés authentifient la légitimité des utilisateurs et des demandes, et les données sont filtrées pour être identifiées comme entièrement conformes et correctement formatées. Cette approche cybersécurisée dès la conception signifie que FlytX – ainsi que son « cerveau de navigation », le système de gestion de vol PureFlyt – est déjà totalement aligné sur les règles actuelles et à venir portant sur la cybersécurité de l'aviation.

Dans un contexte de menaces en constante évolution, Thales a aussi mis en place des unités dédiées pour répondre aux incidents de cybersécurité des clients (PSIRT, *product security incident response team*), qui peuvent être complétées par des services de surveillance de la « cybersanté ». Enfin, une offre structurée a également été conçue pour permettre à nos clients compagnies aériennes de faire de la cybersécurité une partie intégrante de leurs opérations. Cela va de l'élaboration d'une stratégie de cybersécurité et de son intégration dans leurs activités quotidiennes à la gestion d'une crise, en passant par l'engagement et la sensibilisation des opérateurs et des pilotes, ainsi que par le suivi permanent des principales menaces, pour une adaptation efficace des investissements en matière de cybersécurité.

Une approche dynamique et proactive

C'est en adoptant ce type d'approche dynamique et proactive au cœur de notre écosystème que nous pourrons collectivement porter l'aviation connectée vers de nouveaux sommets, tout en veillant à ce que les opérations de vol, les systèmes au sol et à bord, et l'expérience des passagers soient cyber-avérés, résilients et sécurisés. Je vous souhaite donc de bons vols en toute sécurité… et en toute cybersécurité !

Bibliographie

COOPER P. (2019), "Aviation cybersecurity: Scoping the challenge", Atlantic Council.

EASA, "Developing cybersecurity regulations in aviation & part-IS", https://www.easa.europa.eu/community/topics/developing-cybersecurity-regulations-aviation-part

HOYLAND T., SPAFFORD C. & MEDLAND A. (2016), "MRO Big Data – A lion or a lamb?", Oliver Wyman / Marsh & McLennan Companies, https://cavok.oliverwyman.com/content/dam/oliver-wyman/cavok/files/FINAL_MRO_Survey_2016_web.pdf

IATA, "Compilation of cybersecurity regulations, standards, and guidance applicable to civil aviation", https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regs.pdf

ICAO, "Aviation cybersecurity", https://www.icao.int/aviationcybersecurity/Pages/default.aspx