La force de la communauté en cybersécurité : l'exemple de l'aviation - Suite de l'ouvrage "Sécurité numérique & Aéronautique" (*Collection CyberCercle - Regards Croisés, 2022*)

Eric VAUTIER
DSI adjoint - RSSI Groupe - Groupe ADP
Senior advisor - CyberCercle

Près de trois ans après la publication du Regards croisés sur la sécurité numérique de l'aéronautique, il nous a semblé intéressant de le rouvrir pour opérer une forme de "droit de suivi", en toute humilité, sur les sujets qui avaient été exposés. L'idée n'est pas de distribuer des bons ou des mauvais points, mais d'analyser ce qui a été fait, ou pas, et d'en tirer des enseignements pour l'action à venir.

Le CERT Aviation France

Considéré, dixit la conclusion de la contribution du Directeur Général de l'Aviation Civile, comme "un outil [à] coconstruire par l'aviation civile pour l'aviation civile", le CERT Aviation France a vu le jour en novembre 2022, matérialisant l'engagement pris par la DGAC un an plus tôt. Constitué autour d'un noyau dur de membres fondateurs, le CERT Aviation France a pour mission principale d'accompagner les acteurs du secteur dans leur montée en maturité en sécurité numérique, que ce soit en matière d'anticipation, de protection ou de réaction à des incidents.

Via les associations représentant les compagnies aériennes, les aéroports, les industriels et les prestataires de service de l'aviation, le CERT Aviation France possède plus de 700 "bénéficiaires" de services essentiels en matière de cybersécurité - réponse à incidents 24 heures sur 24, surveillance continue de leurs sites Web, formations, etc. – contribuant ainsi au renforcement de la posture cyber de ces entreprises.

Mais la vraie valeur ajoutée est la capacité à faire appel à la solidarité de l'écosystème en cas de besoin. Une parfaite illustration en est le traitement en mode crise du bug Crowdstrike de juillet 2024. A peine quelques semaines plus tôt, le CERT Aviation France avait initié ses briefings quotidiens en prévision de la période des Jeux Olympiques de Paris. Même si la plupart des acteurs de l'aviation n'étaient pas directement touchés, la mise en commun des bonnes pratiques des acteurs plus rôdés a permis à ceux qui étaient directement impactés de mieux réagir - partage technique – et de mieux informer les entités qu'elles impactaient indirectement – partage d'information.

Depuis, les JOP se sont déroulés sans encombre, mais ce briefing quotidien perdure et permet à tout l'écosystème de "prendre la température" – l'état de la menace – grâce au partage des incidents recensés par les uns ou les autres.

Vers l'ISO27AERO ?

Dans sa contribution, Stéphanie Buscayret, alors CISO de Latécoère, appelait de ses vœux la création d'un référentiel de sécurité spécifique à l'aviation

"de portée mondiale, auditable depuis tous les pays, reconnu par tous les organismes publics et privés".

L'intérêt d'un tel référentiel est évident : simplification des engagements contractuels par le biais d'un questionnaire unique quel que soit le donneur d'ordre et réduction du coût de remplissage par les fournisseurs, comparaison facile entre pairs de l'aviation et constitution d'un catalogue cohérent de solutions de sécurité adaptées au secteur.

Cité en exemple dans l'article, l'entité BoostAerospace, créée conjointement par Airbus, Dassault Aviation, Safran et Thales, en avait déjà constitué un, nommé AirCyber. Il y a trois ans, AirCyber était circonscrit au périmètre des fournisseurs des quatre sociétés fondatrices et comptait une centaine de membres (sur 7000 possibles).

A nouveau, le principe de communauté a joué à plein : des associations hors de l'écosystème Airbus ont commencé à s'y intéresser, des discussions se sont engagées, incluant notamment Boeing, l'autre acteur incontournable du secteur, pour déterminer si ce référentiel pouvait passer à l'échelle et être diffusé mondialement. Un consensus a mis quelques mois à être atteint et BoostAerospace a rendu AirCyber *open source* durant l'année 2024, permettant ainsi sa reconnaissance par l'Aviation-ISAC, société américaine à but non lucratif dédiée au partage d'informations de cybersécurité, charge à leurs membres de l'intégrer à leurs contrats.

Un premier palier important avait été franchi, au moment où BoostAerospace atteignait les 300 membres. Mais certaines réticences persistaient, principalement dues au fait qu'il s'agissait de la propriété d'une société fortement liée à Airbus. Et une fois de plus, des échanges constructifs ont commencé à dégager le chemin vers un standard indépendant de toute entité commerciale : la création d'un comité de normalisation et d'un schéma d'accréditation d'auditeurs qualifiés sont en bonne voie, avec la contribution active d'Eurocontrol, dont le statut assure la neutralité idéale pour mener ces débats. Combien de temps faudra-t-il pour aboutir au résultat ? Difficile à dire, mais les acteurs de bonne volonté avancent, laissant envisager des progrès réguliers.

Je conclurai en observant le chemin parcouru et le pragmatisme de la méthode : d'un référentiel interne avec ses défauts à un standard universel, au travers d'une démarche *bottom-up* en mode intelligence collective.

Tirer les leçons de la Part-IS ?

Dans sa contribution, Patrick Ky, alors Président de l'EASA, cite l'ESCP, l'entité montée en 2019 par l'EASA pour conduire la *rulemaking task 720* [je laisse sciemment le vocabulaire anglais]. Les travaux se voulaient un modèle de concertation pour créer la réglementation en matière de cybersécurité de la sécurité aérienne : l'Agence conviait les compagnies aériennes, les aéroports, les constructeurs, les mainteneurs et les autorités nationales pour que chacun s'exprime sur cette, à l'époque, troisième réglementation européenne en matière de cybersécurité dans l'aérien, après la NIS et la règlementation sur la cybersécurité dans la sûreté. Très rapidement, les "invités", dont je faisais partie, ont compris que les travaux ne seraient pas collaboratifs. Les demandes de cohérence avec les autres textes ? Balayées : l'EASA se considérait au-dessus des autres et la loi serait un *lex specialis* qui ferait référence. Le fait que les entités les plus matures étaient calées sur l'ISO 27001 ? Idem, l'EASA allait expliquer à tous dans un texte réglementaire, la "Part-IS", une nouvelle manière d'implémenter la cybersécurité. Les craintes que ledit texte soit trop détaillé pour être à même de tenir dans le temps ? Idem : l'EASA aller assurer la veille technologique par le biais d'*Acceptable Means of Compliance*.

La raison ? L'Agence avait un calendrier à tenir – un peu décalé par la pandémie, évidemment – et a souhaité s'y tenir coûte que coûte, au détriment de la concertation.

Le résultat ? Publiée en 2021, la Part-IS est une politique de sécurité suffisamment désalignée avec

l'ISO 27001 pour compliquer la vie de tous les RSSI concernés, et six ans plus tard, à quelques mois de l'entrée en vigueur de la réglementation, l'EASA a encore publié des propositions d'amendement des AMC, compliquant à la fois la tâche des entités devant mettre en œuvre les mesures dans un délai court et celle des entités chargées de les auditer. L'histoire n'est pas encore finie, attendons la suite…

Vous devez avoir trouvé dans cette description des points communs avec le processus de transposition de la Directive NIS 2 dans notre pays. Mais, pour la NIS 2, les "AMC", ie les décrets et les arrêtés, ne sont pas encore publiés, ce qui laisse la chance à une transposition, au global, plus collaborative, pourquoi pas en confiant la responsabilité de leur rédaction aux ministères en charge des secteurs concernés. On éviterait peut-être ainsi des textes inadaptés dont l'interprétation nous détournerait finalement de la mise en place des mesures nécessaires pour assurer la sécurité numérique de nos entreprises.