# Audit de la protection des infrastructures critiques – Mise en œuvre des exigences minimales dans le domaine du service de la navigation aérienne

## Skyguide

## L'essentiel en bref

Les infrastructures critiques (IC) assurent l'approvisionnement de la Suisse en biens et services indispensables. Pour protéger ces IC, il faut garantir un fonctionnement aussi permanent que possible. Dans ce contexte, la résilience des technologies de l'information et de la communication (TIC) ou la protection des infrastructures critiques (PIC) contre les cybermenaces revêtent une grande importance. Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale de PIC (2018–2022). L'aviation civile et les services de la navigation aérienne en font aussi partie. Sur mandat de la Confédération, Skyguide assure les services civils et militaires de la navigation aérienne en Suisse et dans les régions limitrophes. La Confédération est l'actionnaire majoritaire de Skyguide.

Le Contrôle fédéral des finances (CDF) a vérifié le respect par Skyguide des exigences minimales en matière de protection des TIC contre les cyberattaques. La « norme minimale pour améliorer la résilience informatique » recommandée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) pour les exploitants d'IC a été appliquée. Cette norme couvre essentiellement les cinq thèmes : identifier, protéger, détecter, réagir et récupérer et propose des mesures concrètes à mettre en œuvre.

Skyguide traite ces cinq thèmes de manière systématique. Le niveau de sécurité minimal recommandé par la norme n'est actuellement pas encore complètement atteint. La plupart des travaux nécessaires à cet effet ont déjà été identifiés et lancés. L'audit du CDF a toutefois identifié un potentiel d'optimisation supplémentaire.

**La gestion de la sécurité de l'information doit être opérationnelle**

Un système de gestion de la sécurité de l'information (ISMS) est un élément fondamental de la sécurité de l'information. L'ISMS définit des règles, des procédures, des mesures et des outils qui permettent de gérer, de contrôler, de garantir et d'optimiser la sécurité de l'information.

Skyguide est en train de mettre en place un ISMS conforme aux exigences de l'Office fédéral de l'aviation civile. Lors de l'audit, celui-ci n'était pas encore finalisé et sa mise en œuvre doit être assurée.

**Les droits d'accès, la gestion des vulnérabilités et la mise en œuvre cohérente des directives doivent être améliorés**

Pour réduire les risques de sécurité, un utilisateur ne devrait disposer que des autorisations dont il a impérativement besoin pour effectuer son travail. Skyguide applique ce « principe

du moindre privilège ». Cependant, les droits d'accès attribués ne sont pas vérifiés régulièrement. Ainsi, il n'est pas garanti que les autorisations soient adaptées après des modifications des tâches d'un utilisateur (par exemple, changement de service ou de fonction).

Les administrateurs disposent d'autorisations étendues qui leur permettent de modifier ou même de désactiver les mesures de sécurité des systèmes. En conséquence, les administrateurs sont les premières cibles d'attaque. Les administrateurs doivent être régulièrement sensibilisés et formés à la sécurité informatique. Ce n'est pas encore systématique.

Skyguide a mis en place une analyse de vulnérabilité automatisée pour recenser les vulnérabilités techniques de son matériel et de ses logiciels. Cependant, les développeurs et les responsables d'applications doivent encore être mieux formés à l'utilisation des résultats des analyses. Les vulnérabilités doivent impérativement être recensées et catégorisées de manière centralisée pour pouvoir les éliminer ensuite de façon contrôlée.

Lors d'un contrôle aléatoire, le CDF a constaté qu'après des modifications de directives, les paramètres concernés dans un système existant n'avaient pas été adaptés aux nouvelles valeurs. Skyguide doit s'assurer, dans le cadre du processus de changement formel, que tous les systèmes sont adaptés aux nouvelles exigences.

**L'absence de géoredondance pourrait entraîner de longues interruptions de service**

Les systèmes pour les services de la navigation aérienne sont disponibles de manière redondante, mais ne sont pas physiquement installés dans différents lieux. En conséquence, si un site entier tombe en panne, le service est interrompu et le service de la navigation aérienne n'est plus assuré dans toute la Suisse. De plus, il n'existait pas encore de plan de gestion de la continuité des affaires ni de rétablissement après un sinistre pour un tel scénario, de sorte que Skyguide est actuellement mal préparé à un tel incident.

**Une optimisation de la gestion des fournisseurs est nécessaire**

Skyguide a externalisé l'exploitation d'importantes parties de son infrastructure TIC à des prestataires de services. Cela augmente la complexité des modifications apportées aux systèmes et nécessite une excellente communication et collaboration afin de prévenir les pannes de système. De même, les réactions aux pannes de système doivent être très bien préparées. Différents incidents ont montré qu'il existe encore un potentiel d'optimisation dans ce domaine.

Skyguide doit aborder les risques liés aux chaînes d'approvisionnement avec tous les prestataires de services critiques.

**Texte original en allemand**