Audit de la sécurité informatique
RUAG MRO Holding SA

L'essentiel en bref

Le 21 mars 2018, le Conseil fédéral a décidé de regrouper les unités d'affaires de l'ancienne entreprise RUAG, actives presque exclusivement pour l'armée suisse, dans une nouvelle société du groupe RUAG MRO Holding SA (MRO CH), respectivement sa filiale RUAG SA. Il s'agissait de dissocier ces unités du reste du groupe RUAG (RUAG International) qui réalise des activités tant civiles que militaires au niveau international. Avec cette décision, le Conseil fédéral entendait améliorer la sécurité informatique et assurer à l'armée une fourniture de prestations robuste, transparente et optimisée en termes de coûts. Tout en s'acquittant de sa mission ancrée dans la loi – garantir l'équipement de l'armée – MRO CH devrait avoir la possibilité de poursuivre son développement dans d'autres domaines d'activité.

La scission concernait aussi les technologies de l'information et de la communication (TIC) de RUAG. Le Département fédéral de la défense, de la protection de la population et des sports s'est vu confier la responsabilité des TIC de RUAG SA. Toute l'infrastructure et les systèmes TIC ont été réorganisés et les données reprises dans le périmètre de sécurité de la Base d'aide au commandement de l'armée (BAC). En conséquence, les normes de sécurité informatique de la Confédération doivent être remplies. Le projet de dissociation générera des coûts à hauteur de 81 à 86 millions de francs, selon une estimation de septembre 2020. Sur les 57 millions dépensés jusqu'à fin septembre, 34 millions sont imputables à la scission des TIC. Le projet concerne près de 2500 collaborateurs de MRO CH sur plus de 20 sites en Suisse.

Le présent audit s'est concentré sur la sécurité des systèmes TIC, soit sur le transfert contrôlé au sein de RUAG SA et dans le périmètre de sécurité de la BAC.

L'audit a montré que le transfert des systèmes et des données s'est, dans une large mesure, bien passé, même si les projets subséquents ne sont pas terminés. La gouvernance informatique et l'organisation en matière de sécurité informatique sont adéquates, mais d'importants travaux d'ajustement restent nécessaires. La collaboration avec la BAC fonctionne, mais n'est pas encore bien huilée.

Succès de la scission des TIC malgré la complexité du projet et les retards

Après la scission des TIC (première étape), les services standard de la BAC devraient être utilisés. Par conséquent, les employés de RUAG SA ont reçu de nouveaux appareils de bureautique de la BAC. Prévu pour le 1er janvier 2020, le déploiement n'a pas pu être respecté pour diverses raisons. La migration a été reportée à Pâques 2020. Fin avril 2020, le changement de système *(cut-over)* a pu être finalisé, la première étape de la scission a été achevée à la fin juin 2020. Les objectifs du projet ont été atteints.

Le transfert des données constituait un sérieux défi. Pour exclure toute propagation de maliciels, il n'était pas permis de copier les données directement des systèmes de l'ancienne entreprise RUAG dans ceux de la BAC. Les données ont donc été transférées dans une zone de quarantaine de la BAC via une ligne de données spécialement créée où elles ont fait l'objet d'une analyse antivirus, avant d'être transférées dans les nouveaux systèmes.

MRO CH a lancé un autre projet pour nettoyer les données de ses anciens systèmes dans le cadre de la seconde étape du processus de dissociation. Il consiste à effacer les données à caractère militaire et confidentielles des anciens systèmes ou à les rendre illisibles. Il est crucial qu'un tel nettoyage inclue les archives et les copies de sauvegarde. Le projet est mené en étroite collaboration avec RUAG International. Le nettoyage des données est placé sous la responsabilité de RUAG SA, qui en est propriétaire.

Dans cette seconde étape, qui se poursuivra jusqu'à la fin de 2021, il s'agit aussi de mettre en sécurité l'infrastructure scientifique et technique. La responsabilité et l'exploitations incombent à RUAG SA.

La nouvelle organisation de sécurité de RUAG SA est structurée de manière efficace

L'organisation de sécurité de RUAG SA est adéquate. L'implication de responsables de la sécurité dans différents domaines assure un échange constant d'informations. Les divers secteurs sont bien coordonnés et les échanges avec la direction sont garantis. Des échanges réguliers avec l'organisation de sécurité de la BAC sont établis.

La mise en place d'un système de gestion de la sécurité de l'information avec les activités d'audit contribuent à une sécurité de l'information sur le long terme. La gestion des risques et la gestion de la continuité des activités sont en cours de réalisation. La seconde ne deviendra opérationnelle qu'en 2023. RUAG SA devrait trouver ici une solution plus rapide, au moins pour ses principaux processus d'affaires.

Besoins d'amélioration ponctuels au niveau de la sécurité d'exploitation

L'exploitation des systèmes de RUAG SA est du ressort de la BAC depuis la migration. Les contrôles de sécurité sont effectués par le Centre des opérations de sécurité *(Security Operations Center)*. Lors de l'intégration des systèmes dans leur nouvel environnement, aucun contrôle de conformité en matière de sécurité à large échelle n'a été réalisé. Cela représente un risque important, surtout pour les applications reliées à Internet. La BAC devrait effectuer de tels contrôles de conformité en matière de sécurité de manière systématique.

Depuis que sa gouvernance incombe à l'administration fédérale, RUAG SA est soumise aux directives de la Confédération. Ainsi, il a fallu demander pour certaines applications des dérogations à la protection de base des TIC. Ces dernières devraient être supprimées autant que possible ou, à défaut, formalisées.

Les recommandations émises par le CDF dans ses précédents rapports sont pour la plupart mises en œuvre

Les recommandations du CDF des rapports 18517 et 19418 ont été en bonne partie suivies, dans la mesure où elles concernent MRO CH. Des organisations de projet ont été mises en place pour les deux recommandations encore en suspens au moment de l'audit et les travaux sont en cours. La mise à jour des documentations de sécurité (recommandation 19418.002) était réalisée à 60 % et devrait être terminée d'ici fin 2020. Lors du transfert de l'infrastructure scientifique et technique dans un périmètre de sécurité (recommandation 19418.003), l'architecture cible et les prestations ont été définies. Le centre de calcul requis est opérationnel, et le projet devrait être achevé d'ici fin 2021.

Texte original en allemand