Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

RUAG. Sécurité informatique – Situation en 2021

Rapport du 18 février 2022 de la Commission de gestion du Conseil national

Avis du Conseil fédéral

du 30 mars 2022

Madame la Présidente,
Mesdames, Messieurs,

Conformément à l'art. 158 de la loi sur le Parlement, nous nous prononçons comme suit sur le rapport du 18 février 2022 de la Commission de gestion du Conseil national concernant la sécurité informatique de RUAG en 2021.

Nous vous prions d'agréer, Madame la Présidente, Mesdames, Messieurs, l'assurance de notre haute considération.

30 mars 2022

Au nom du Conseil fédéral suisse:

Le président de la Confédération, Ignazio Cassis
Le chancelier de la Confédération, Walter Thurnherr

Avis

1 Contexte

Le 22 février 2022, la Commission de gestion du Conseil national (CdG-N) a publié son rapport «RUAG. Sécurité informatique – Situation 2021»[1], dans lequel elle aborde en particulier la protection des données militaires et d'autres données sensibles au sein des unités de l'entreprise RUAG. Elle revient aussi sur la communication du Conseil fédéral, ainsi que du Département fédéral de la défense, de la protection de la population et des sports (DDPS) et du Département fédéral des finances (DFF) en tant que représentants du propriétaire.

Dans son rapport, la CdG-N mentionne une émission de la télévision suisse alémanique qui a révélé que des pirates informatiques seraient parvenus à s'introduire dans le réseau de RUAG International Holding SA (RUAG International) et qu'il existerait toujours de nombreuses connexions avec RUAG MRO Holding SA (RUAG MRO) rendant possible aussi un accès à des données sensibles de l'armée.

La CdG-N est parvenue à la conclusion que, contrairement à ce qu'annoncé dans l'émission télévisée, il n'y avait aucune preuve tangible d'un piratage de RUAG International au printemps 2021. À la suite des analyses que l'entreprise a immédiatement menées, de graves lacunes de sécurité ont toutefois été identifiées. Comme des mesures ont immédiatement été prises et soumises à des tests de résistance rigoureux menés par un cabinet externe, la commission est de l'avis que RUAG International a réagi de manière conforme. La CdG-N recommande néanmoins des mesures supplémentaires pour continuer à réduire le risque de fuites de données.

Par ailleurs, la CdG-N s'est penchée sur la question de savoir si le DFF et le DDPS ont bien défendu les intérêts de la Confédération dans le cadre de cet incident et si le Conseil fédéral et le DDPS en particulier l'ont informée correctement et en toute transparence sur l'état d'avancement du processus de dissociation et sur la sécurité informatique au sein de RUAG. Elle est d'avis que les deux départements ont réagi de manière adéquate à l'émission télévisée. Par contre, elle estime que la communication au sujet de la dissociation et de la cybersécurité aurait dû être plus transparente à son égard.

La CdG-N formule deux recommandations en tout. Elle invite le Conseil fédéral se prononcer sur son rapport et ses recommandations d'ici au 30 mars 2022.

1 FF **2022** 491

2 Avis du Conseil fédéral sur la mise en œuvre des recommandations du 18 février 2022

Le Conseil fédéral se prononce comme suit sur les recommandations:

Recommandation 1: Protection des données militaires et des autres données sensibles

La CdG-N demande au Conseil fédéral de prendre les mesures nécessaires pour que RUAG International ne dispose plus de données militaires ou d'autres données sensibles après l'effacement prévu des données (pas même dans des archives ou des sauvegardes). La question se pose de savoir si la suppression doit être contrôlée par des experts externes. Il convient par ailleurs d'examiner s'il serait opportun de demander un contrôle supplémentaire de la situation des données avant chaque vente de parties de RUAG International.

En préambule, force est de relever que l'un des principaux objectifs du processus de dissociation était d'assurer que seule RUAG MRO Holding SA (RUAG MRO) ait accès aux données de l'armée pertinentes en matière de sécurité. La migration de la majorité de ces données s'est effectuée en avril 2020 lors de la première étape de la dissociation des systèmes informatiques (*cut-over*). Grâce à la migration dans le périmètre de sécurité de la Base d'aide au commandement (BAC), RUAG MRO a profité d'une norme élevée de sécurité et commencé son activité aussi indépendamment que possible du réseau de RUAG International.

Le Conseil fédéral précise dans ce contexte que les données d'intérêt sécuritaire de l'armée sont aujourd'hui traitées uniquement par RUAG MRO. Les données qui étaient encore enregistrées sur d'anciens systèmes de RUAG International n'ont plus été traitées. Elles ont été recherchées de manière ciblée et effacées une à une dans le cadre d'un autre projet, où les systèmes ont été passés manuellement en revue. Le Contrôle fédéral des finances (CDF) a décrit la procédure en détail dans son rapport d'audit[2] en 2021. Il a évalué l'ampleur et déterminé le caractère sensible des données concernées. II est notamment arrivé à la conclusion que la procédure de suppression des données sur les systèmes de RUAG International est adéquate.

Le Conseil fédéral est conscient des risques d'une potentielle fuite de données sensibles. Pour cette raison, le DFF et le DDPS accompagnent de près le projet de dissociation dans toute sa complexité. Les services propriétaires avaient demandé tant à RUAG MRO en tant que propriétaire des données et responsable de leur nettoyage qu'à RUAG International de prendre un maximum de précautions dans le nettoyage des données. Un certain séquençage n'a toutefois pas pu être évité. Ainsi, il n'a pas été possible de procéder au nettoyage définitif des données avant le changement de système (*cut-over*). Ensuite, après leur migration, les données pertinentes en matière de sécurité ont été systématiquement classifiées et nettoyées. Les données des copies de sauvegarde, des archives, des répertoires personnels (*shares*), des boîtes aux lettres

2 CDF (2021): audit du 22 février 2021 de la sécurité informatique de RUAG MRO Holding SA (nº d'audit 20431): www.efk.admin.ch > Publications > Sécurité & environnement > Défense & armée > Sécurité informatique – RUAG MRO Holding SA.

électroniques et des répertoires de transfert (*transfer shares*) ont été saisies et nettoyées.

RUAG MRO a en outre commandé un audit externe dans le but de vérifier l'autonomie et les fonctionnalités des systèmes informatiques dissociés. Quant au CDF, il a de plus indiqué dans son programme annuel 2022 qu'il allait poursuivre l'examen de la cybersécurité de RUAG MRO[3].

RUAG International a engagé un nouveau chef de la sécurité de l'information, qui a pour mission de garantir la gestion rigoureuse des données à chaque désinvestissement. Les services propriétaires ont dans ce contexte demandé à RUAG International de faire vérifier par des spécialistes externes, avant chaque vente de ses parties, si elle a pris toutes les dispositions appropriées pour éviter que des données sensibles soient involontairement transmises.

En outre, il est établi que la vente de secteurs d'activité de RUAG International permettra de réduire la complexité des systèmes informatiques, et donc le risque de fuites des données.

Le Conseil fédéral estime avoir ainsi pris des mesures efficaces pour protéger les données militaires et les autres données sensibles et considère donc la première recommandation comme réalisée.

Recommandation 2: Communication plus transparente

La CdG-N invite le Conseil fédéral à prendre des mesures adéquates pour que, à l'avenir, le Conseil fédéral ainsi que les services propriétaires du DFF et du DDPS informent les commissions de haute surveillance de manière plus transparente et plus rapide des difficultés rencontrées lors de la dissociation de RUAG et, en particulier, dans le cadre du développement de RUAG International.

Le Conseil fédéral s'efforce toujours d'assurer la transparence dans les échanges d'informations avec les commissions de haute surveillance et s'y applique scrupuleusement. Dans ce contexte, il signale que, dans son rapport de 2020 sur la réalisation des objectifs stratégiques par BGRB Holding SA (RUAG)[4], l'avancement des travaux a été présenté en détail et de manière explicite, en particulier concernant les défis posés par la dissociation de RUAG, comme en témoigne la mise en œuvre détaillée de l'objectif stratégique 2.1.3, à travers lequel le Conseil fédéral attend de la société de participation financière «qu'elle poursuive rapidement les travaux restants en lien avec la dissociation des activités de la société et qu'elle les termine d'ici à fin 2021 au plus tard».

Le transfert des systèmes informatiques de RUAG MRO dans le périmètre de sécurité de la BAC en avril 2020 et la division du patrimoine pratiquement simultanée qui l'a accompagné, avec la répartition des actifs et des passifs à la suite de la séparation

3 Programme annuel 2022 du Contrôle fédéral des finances, p. 12.: www.efk.admin.ch > Publications > Communication institutionnelle > programmes annuels > Programme annuel 2022.

4 Conseil fédéral (2020): rapport du Conseil fédéral du 19 mars 2020 concernant la réalisation des objectifs stratégiques 2020 par BGRB Holding SA (RUAG) (confidentiel).

opérationnelle et juridique de RUAG MRO et de RUAG International, ont constitué les principales étapes de la dissociation. Les travaux de nettoyage et les projets restants, comme le *rebranding*, constituent depuis septembre 2020 une étape secondaire de la dissociation, car d'une part ils sont d'importance moindre par rapport à la nécessité d'exécuter les travaux pour l'armée dans un environnement télématique sûr et d'autre part la dissociation est achevée pour l'essentiel depuis le milieu de l'année 2020.

On peut affirmer aujourd'hui que la dissociation de RUAG a été menée à bien. Le CDF l'a confirmé en indiquant au point 2.1 de son rapport d'audit que «les objectifs du projet ont été atteints tant sur le plan qualitatif que quantitatif»[5].

Le Conseil fédéral prend acte de la demande des CdG de communiquer de manière transparente et rapide au sujet des défis de RUAG. Il entend se montrer précis quant aux développements d'importance pour la Confédération dans son rapport sur les objectifs stratégiques de cette entreprise et dans toutes ses communications la concernant.

Le Conseil fédéral accordera encore plus d'attention à la demande de communication transparente émise par la CdG-N. Dès lors, il estime avoir donner suite aux deux recommandations.

5 Cf. note 2