Prüfung der Informatiksicherheit
RUAG MRO Holding AG

Das Wesentliche in Kürze

Am 21. März 2018 hat der Bundesrat beschlossen, die fast ausschliesslich für die Schweizer Armee tätigen Geschäftseinheiten der damaligen RUAG in einer neuen Konzerngesellschaft RUAG MRO Holding AG (MRO CH), resp. deren Tochtergesellschaft RUAG AG, zusammenzuführen. Diese Teile sollten von der übrigen RUAG (RUAG International), die international zivile und militärische Geschäfte tätigt, entflochten werden. Der Bundesrat verfolgte mit diesem Entscheid das Ziel, die Informatiksicherheit zu erhöhen und eine robuste, transparente und kostenoptimierte Leistungserbringung für die Armee sicherzustellen. Die MRO CH sollte ihre gesetzlich verankerte Zweckbestimmung – die Sicherstellung der Ausrüstung der Armee – weiterhin erfüllen und gleichzeitig die Möglichkeit haben, sich in den übrigen Geschäftsgebieten weiterzuentwickeln.

Die Entflechtung betraf auch die Informations- und Kommunikationstechnik (IKT) der RUAG. Es wurde entschieden, die IKT für die RUAG AG in die Verantwortung des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport zu geben. Die komplette IKT-Infrastruktur und die -Systeme wurden im Sicherheitsperimeter der Führungsunterstützungsbasis der Armee (FUB) neu aufgebaut und die Daten übernommen. Entsprechend müssen die IKT-Sicherheitsvorgaben des Bundes erfüllt werden. Das Entflechtungsprojekt verursacht Stand September 2020 voraussichtlich Kosten in der Höhe von 81–86 Millionen Franken. Von den bis Ende September aufgelaufenen Gesamtkosten von 57 Millionen sind 34 Millionen Franken der IKT-Entflechtung zuzuordnen Das Projekt betraf rund 2500 Mitarbeitende der MRO CH an über 20 Standorten der Schweiz.

Bei der vorliegenden Prüfung steht die Sicherheit der IKT-Systeme im Fokus und zwar hinsichtlich der kontrollierten Überführung zur RUAG AG und in den Sicherheitsperimeter der FUB.

Die Prüfung hat gezeigt, dass die Überführung der Systeme und Daten, trotz offener Nachfolgeprojekte, weitestgehend erfolgreich abgelaufen ist. Die IKT-Governance und -Sicherheitsorganisation sind zweckmässig aufgestellt, müssen aber noch umfangreiche Nacharbeiten leisten. Die Zusammenarbeit mit der FUB funktioniert, ist aber noch nicht eingeschliffen.

Erfolgreicher Abschluss der IKT-Entflechtung trotz hoher Komplexität und Verzögerungen

Nach der IKT-Entflechtung (erster Arbeitsschritt der Entflechtung) sollten künftig die Standardservices der FUB beansprucht werden. Aus diesem Grund wurden die Mitarbeitenden der RUAG AG mit neuen Büroautomationsgeräten der FUB ausgerüstet. Der für den 1. Januar 2020 geplante Übergang in die neue Umgebung konnte aufgrund verschiedener Umstände nicht eingehalten werden. Die Migration erfolgte daher verspätet an Ostern 2020. Per Ende April 2020 konnte der IT-Cutover abgeschlossen werden und per Ende Juni 2020 wurde der erste Arbeitsschritt der Entflechtung abgeschlossen. Die Projektziele wurden erreicht.

Eine grosse Herausforderung stellte der Datentransfer dar. Um die Verschleppung von Malware auszuschliessen, durften keine Daten direkt von den Systemen der alten RUAG zur FUB kopiert werden. Daher wurden diese über eine eigens dafür eingerichtete Datenleitung

in einen Quarantänebereich der FUB transferiert, dort auf Malware gescannt und danach auf die neuen Systeme übertragen.

Für die Bereinigung der Daten auf den alten Systemen hat die MRO CH im Rahmen des zweiten Arbeitsschritts der Entflechtung ein weiteres Projekt lanciert. Hierbei sollen die militärisch relevanten und vertraulichen Daten auf den Altsystemen gelöscht oder unkenntlich gemacht werden. Dabei ist es von grosser Wichtigkeit, dass auch Archive und Datensicherungen im Fokus der Bereinigung stehen. Das Projekt erfolgt in enger Zusammenarbeit mit der RUAG International. Die RUAG AG ist als Dateninhaberin für die Bereinigung verantwortlich.

Die Technisch Wissenschaftliche Infrastruktur (TWI) wird ebenfalls im Rahmen des zweiten Arbeitsschritts bis Ende 2021 in einen sicheren Zustand überführt. Die Verantwortung und der Betrieb liegen bei der RUAG AG.

Die neue Sicherheitsorganisation der RUAG AG ist zielführend aufgebaut

Die Sicherheitsorganisation der RUAG AG ist zweckmässig aufgestellt. Durch die Einbindung von Sicherheitsbeauftragten in den Fachbereichen ist ein durchgängiger Informationsaustausch gewährleistet. Die unterschiedlichen Teilbereiche sind gut aufeinander abgestimmt und der Austausch mit dem Management ist sichergestellt. Ein regelmässiger Austausch mit der Sicherheitsorganisation der FUB ist etabliert.

Der Aufbau eines Informationssicherheitsmanagementsystems inklusive der Audittätigkeiten tragen zu einer nachhaltigen Informationssicherheit bei. Das Risikomanagement und das betriebliche Kontinuitätsmanagement sind im Aufbau. Letzteres soll erst 2023 operativ werden. Hier sollte die RUAG AG, mindestens für die wichtigsten Geschäftsprozesse, eine raschere Lösung erarbeiten.

Einzelne Aspekte in der Betriebssicherheit müssen verbessert werden

Der Betrieb der Systeme der RUAG AG ist nach der Migration in der Verantwortung der FUB. Die Sicherheitsüberwachung erfolgt durch deren Security Operations Center. Bei der Einbindung der Systeme in die neue Umgebung wurden keine flächendeckenden Sicherheitskonformitätsprüfungen durchgeführt. Dadurch besteht, insbesondere bei Anwendungen mit Zugang zum Internet, ein erhebliches Risiko. Die FUB sollte diese Sicherheitskonformitätsprüfungen konsequent durchführen.

Mit dem Übergang in die Governance der Bundesverwaltung unterliegt die RUAG AG den Vorgaben des Bundes. Daher mussten für gewisse Anwendungsfälle Ausnahmen zum IKT-Grundschutz beantragt werden. Diese gilt es, wo möglich, abzubauen oder andernfalls noch zu formalisieren.

Die Empfehlungen der EFK aus früheren Berichten sind weitgehend umgesetzt

Die Empfehlungen der EFK aus den Berichten 18517 und 19418 wurden, soweit sie die MRO CH betreffen, weitgehend umgesetzt. Für die zum Prüfzeitpunkt noch offenen zwei Empfehlungen wurden Projektorganisationen aufgebaut und die Arbeiten sind am Laufen. Die Bereinigung der Sicherheitsdokumentationen (Empfehlung 19418.002) weist einen Erfüllungsgrad von 60 % auf und soll per Ende 2020 abgeschlossen werden. Bei der Überführung der TWI in einen sicheren Perimeter (Empfehlung 19418.003) wurden die Zielarchitektur und die Serviceleistungen spezifiziert. Das erforderliche Rechenzentrum ist in Betrieb. Das Projekt soll bis Ende 2021 abgeschlossen werden.