Fragen Rundschau, 12.05.2021

Einleitung
Der Bundesrat hat im März 2018 die Entflechtung von RUAG beschlossen und das zeitliche Vorgehen festgelegt. Die dazu notwendigen Arbeiten wurden so priorisiert, dass einerseits die physische und rechtliche Trennung zwischen RUAG MRO und RUAG International erfolgen konnte und andererseits eine verbesserte Sicherheit durch die Integration eines Grossteils der Informatik von RUAG MRO in den Sicherheitsperimeter des VBS (Verteidigung) erlangt werden konnte. Dieser erste entscheidende Arbeitsschritt konnte mit dem IT-Cut-Over im Mai 2020 beendet werden.

In einem zweiten Arbeitsschritt erfolgt die Ablösung der Technisch-Wissenschaftlichen Infrastruktur (TWI), die Entflechtung von RUAG Real Estate und die geordnete Datenbereinigung zwischen den beiden Subholdings von RUAG. Die Priorisierung und zeitliche Staffelung der Arbeiten zur Entflechtung waren notwendig, weil deren Komplexität zu hoch und die eigene Kapazität zu gering waren, um sie alle mit dem ersten Arbeitsschritt im Mai 2020 abschliessen zu können.

Diese zeitliche Staffelung wurde unter anderem in den Strategischen Zielen des Bundesrats für die BGRB Holding AG 2020 – 2023 vom Oktober 2019 (BBl 2020 961) aufgezeigt.

Nahezu alle Arbeiten des zweiten Arbeitsschrittes sind sicherheitsrelevant und notwendig, um die Sicherheitsstandards des Bundes und die Empfehlungen der EFK umsetzen zu können. Um die mit der Staffelung der Arbeiten verbundenen Sicherheitsrisiken möglichst rasch zu eliminieren, zielen die komplexen Arbeiten des zweiten Arbeitsschrittes auf einen Abschluss per Ende 2021.

Zur Entflechtung allgemein:
Herzstück der Entflechtung aus "IT-Optik" bildet die Migration und Integration der Informatiksysteme von RUAG MRO in den Sicherheitsperimeter der Armee. Dieser Schritt wurde im April 2020 mit dem sog. Cut-Over erfolgreich vollzogen. Die noch zu unternehmenden Folgearbeiten sind nahtlos angelaufen; der Eigner wird darüber regelmässig orientiert.
Dementsprechend spricht auch der Bund nach wie vor im Zusammenhang mit RUAG / BGRB von "Entflechtung", siehe z.B. hier: Bund nimmt Einsitz in den Verwaltungsrat von RUAG (admin.ch)

Mit der vom Bundesrat beschlossenen Entflechtung des RUAG-Konzerns entstanden per 1. Januar 2020 zwei Unternehmen, die organisatorisch vollständig voneinander getrennt sind. Weil diese Unternehmen aber beide noch RUAG in ihrem Namen tragen, ist die Unterscheidung essenziell wichtig: einerseits gibt es die RUAG International Holding AG, andererseits die RUAG MRO Holding AG. Im Folgenden werden die beiden der Einfachheit halber als "RUAG International" und als "RUAG MRO" bezeichnet.

Allgemeine Recherchefragen

- **Ist es richtig, dass vom alten Ruag-Netzwerk Verbindungen zu Polycom, Swisstopo, Zoll, NCSC, Fedpol, Armasuisse, NDB, FisH, Flieger Flab führen?**
  - Grundsätzlich ist zwischen dem Netzwerk von RUAG International und demjenigen von RUAG MRO zu unterscheiden. Beide Netzwerke befinden sich heute in getrennten Umgebungen. Das RUAG MRO-Netzwerk ist in den Perimeter der Führungsunterstützungsbasis der Armee (FUB) integriert.
  - Bei der Technisch-Wissenschaftlichen Infrastruktur (TWI) von RUAG MRO gibt es keine Verbindungen zu den aufgeführten Bereichen von VBS und EFD.

- RUAG International hat Netzwerk-Verbindungen zu verschiedenen Kunden im Rahmen der üblichen Geschäftstätigkeiten etwa zum Zoll.

- **Ist es richtig, dass es diese Verbindungen heute immer noch gibt?**
  - Siehe Antwort auf Frage 1.

- **Hat die Ruag eine Gesamtübersicht der Querverbindungen in andere Netzwerke?**
  - Sowohl RUAG MRO als auch RUAG International verfügen über eine vollständige Übersicht aller Querverbindungen in andere Netzwerke.

Hack 2016 und dessen Aufarbeitung bis heute

- **Experten sagen, dass beim Hack 2016 der Nachrichtendienst betroffen war, möglicherweise Operationen von Agenten im Ausland, die Geheimarmee AAD10, aber auch das Zeugenschutzprogramm des Fedpol. Was sagen Sie dazu?**
  - Wir verweisen auf die damalige Medienmitteilung: Cyber-Angriff auf die RUAG: Weiterer Schaden konnte abgewendet werden | RUAG

- **Das Sicherheitsprogramm «Impact» hatte zum Ziel, das Netzwerk nach dem Hack sicherer zu machen. Mehrere Insider sagen, der Hack sei nicht sauber aufgearbeitet worden. Stattdessen seien beim «Aufräumen» Server geklont, Daten 1:1 kopiert und alte Rechner neu aufgesetzt worden. Was sagen Sie dazu?**
  - Die Daten von RUAG MRO sind mit der Entflechtung in den Sicherheitsperimeter des VBS, d.h. den Perimeter der Führungsunterstützungsbasis der Armee (FUB) migriert worden. Dabei wurden sämtliche Systeme neu aufgebaut und ausschliesslich auf Sicherheitsrisiken geprüfte Daten in den FUB-Perimeter transferiert. Die neue IT-Infrastruktur hat somit heute den gleichen Schutz wie die Systeme des VBS. Die FUB erbringt als Service-Provider Dienstleistungen der ICT-Grundversorgung. Für den proaktiven Schutz von IT-Infrastruktur und Daten sorgen zusätzlich die Dienstleistungen des Security Operations Center (SOC) der FUB.
  - Im Zuge des Datentransfers bei der Entflechtung wurden sämtliche Daten von RUAG MRO einem intensiven, mehrstufigen Prüfverfahren unterzogen, nach den geltenden Vorgaben analysiert, die Data Ownership verifiziert und entsprechend klassifiziert. Für die Überprüfung und den Transfer von ITAR-relevanten Daten wurden zusätzliche Sicherheitsvorkehrungen zur Einhaltung der gesetzlichen Vorgaben getroffen. Militärisch-klassifizierte Daten wurden protokolliert, inventarisiert und durch entsprechende Schutzmassnahmen vor unbefugtem Zugriff und Data Leakage geschützt.

- **Anscheinend wurde «Impact» 2019 unvollendet abgebrochen. Was sagen Sie dazu?**
  - Das Projekt wurde nicht abgebrochen, sondern ging aufgrund veränderter Rahmenbedingungen, wie dem geplanten Outsourcing und der Cloud-Migration bei RUAG International in ein Folgeprogramm namens Apollo über. Das Programm Impact wurde 2019 durch EY und ETH auditiert.

- **Im vertraulichen EFK-Bericht 2018 heisst es, dass vertrauliche Daten unverschlüsselt im Netz liegen. Gemäss mehreren Quellen ist das heute noch so. Was sagen Sie dazu?**
  - Zum Zeitpunkt des EFK-Berichtes 2018 hatte die Entflechtung noch nicht stattgefunden.

- Mit der Überführung in den FUB-Perimeter wurde für RUAG MRO der Sicherheitsstandard der Armee übernommen.
- Die heutige Sicherheits-Umgebung der FUB bildet einen sehr hohen Schutz gegen unerlaubtes Eindringen. Für den proaktiven Schutz von IT-Infrastruktur und Daten von RUAG MRO sorgen zusätzlich die Dienstleistungen des Security Operations Centers (SOC) der FUB.
- RUAG International hat ebenfalls ein umfassendes Schutzkonzept, um Angriffe proaktiv zu monitoren und abzuwehren.

- **Laut mehreren Quellen und Ruag internen Dokumenten fehlt der Überblick über den enormen Datenbestand bis heute. Bei der Ruag International, aber auch bei der MRO Schweiz. Was sagen Sie dazu?**
  - Das ist falsch.
  - RUAG MRO verfügt über einen vollständigen Überblick der eigenen Datenbestände. Im Zuge der Entflechtung wurden sämtliche Daten von RUAG MRO nach den geltenden Vorgaben analysiert, die Data Ownership verifiziert und die Daten bei Bedarf neu klassifiziert.
  - RUAG International führt und dokumentiert ebenfalls das eigene Daten-Inventar aller Applikationen inklusive der Klassifizierung.

- **Laut mehreren Quellen hat der «Brain-Drain» bis heute zu einem gravierenden Know-How-Verlust geführt, der bei der Datenbereinigung auch heute noch ein Problem darstellt. Was sagen Sie dazu?**
  - Bei RUAG MRO bewegte sich die Fluktuation innerhalb der IT auf sehr tiefem Niveau, ein Brain-Drain hat nicht stattgefunden. Die Datenbereinigung konnte erfolgreich durchgeführt werden.
  - Bei RUAG International kam es aufgrund des IT-Outsourcings und der strategischen Transformation zu einem Stellenabbau in der IT. Die Datenbereinigung war zu keinem Zeitpunkt davon betroffen.

Sicherheitsprobleme an den IT-Systemen der Ruag

- **Mehrere Experten sagen, Schadsoftware könnte praktisch das ganze System verschlüsseln. Was sagen Sie dazu?**
  - Beide Unternehmen haben zahlreiche Massnahmen getroffen, um die Auswirkungen eines Angriffs zu minimieren, unter anderem mit adäquater Security-Software.

- **Die Ruag wurde 2019 aufgrund der Sicherheitsdefizite an den Systemen mehrfach gewarnt. Uns sagen mehrere Experten, dass auch heute niemand den Gesamtüberblick über das Ruag Netzwerk hat. Dass der Schutzgrad nicht höher ist als zur Zeit des Hacks 2016. Was sagen Sie dazu?**
  - Diese Aussage ist falsch.
  - RUAG MRO hat einen vollständigen Überblick über das eigene Netzwerk. Durch den Neuaufbau der kompletten Infrastruktur in der FUB-Umgebung entspricht der heutige Schutzgrad von RUAG MRO jenem des VBS.
  - RUAG International hat nach der Entflechtung ebenfalls stark in die IT- und Informationssicherheit investiert. Das Unternehmen setzt dabei auf drei Ebenen an: Mensch, Prozess und Technologie. In allen Bereichen wurden extensive Fortschritte gemacht und das Unternehmen verfügt heute über einen Schutz, der kontinuierlich an den wachsenden Anforderungen und Bedrohungen aktiv ausgerichtet wird.

- **Ruag und der Bundesrat kommunizierten 2020 die erfolgreiche Entflechtung. Uns liegen Ruag interne Dokumente vor, die zeigen: das stimmt nicht. Die Ruag Real Estate gehört noch zur IT-Landschaft der Ruag International.**

- Die RUAG Real Estate AG wird wie geplant und gegenüber dem Eigner kommuniziert, im Rahmen des "Arbeitsschritt 2" der Entflechtung bis Ende 2021 auf eine vollständig neue Infrastruktur migriert.
- Die IT von RUAG Real Estate AG wurde nicht in den Sicherheitsperimeter der Armee transferiert. Für Immobilien gilt ein anderer Schutzbedarf als für das Kerngeschäft. Dennoch wird auch dieser Teil angepasst und bis Ende 2021 auf eine vollständig neue Infrastruktur migriert.

- **Mehrere Quellen sagen: Die Ruag-Daten seien bei der Entflechtung 1:1 zur Ruag International kopiert worden – mit der Anweisung, jeder Teil (MRO Schweiz und Ruag International) nehme sich, was er brauche und lösche den Rest. So könnte ein «Schläfer», der sich nach wie vor im System verstecke, mitkopiert worden sein. Auch in den Perimeter des FUB. Was sagen Sie dazu?**
  - Diese Aussage ist falsch. Die Daten wurden klar nach der Auftrennung der Geschäfte zugeteilt. Es gab kein Prinzip der 'Selbstbedienung'.
  - Die Daten von RUAG MRO sind mit der Entflechtung in den Sicherheitsperimeter des VBS, d.h. den Perimeter der Führungsunterstützungsbasis der Armee (FUB) transferiert worden. Dabei wurden sämtliche Systeme neu aufgebaut sowie ausschliesslich Daten, welche mit der dedizierten Scaninfrastruktur der FUB überprüft wurden, in den FUB-Perimeter transferiert. Zudem wurden alle Applikationen vollständig in der neuen Umgebung neu installiert und nicht kopiert.

- **Die technisch wissenschaftliche Infrastruktur (TWI) gehört eigentlich zu MRO Schweiz, müssten entflochten werden. Sie befinden sich aber immer noch in der Systemlandschaft der Ruag International. Das widerspricht der Entflechtung. Was sagen Sie dazu?**
  - Die Technisch-Wissenschaftliche Infrastruktur (TWI) wird, wie geplant und dem Eigner gegenüber kommuniziert, im Rahmen Folgearbeiten bis Ende 2021 auf eine vollständig neue Infrastruktur migriert.
  - Hier handelt es sich um Infrastrukturen, die nicht einer IT-Standard-Funktionalität entsprechen und teilweise dezentral angewendet werden. Bei den TWI handelt es sich deshalb um eigene, abgeschottete Netzwerke.
  - Die Migration erfolgt schrittweise.

- **Laut uns vorliegenden Dokumenten betrachtet auch die Ruag die TWIs als «erhöhtes Sicherheitsrisiko». Man habe keinen Überblick über die IT-Infrastruktur, den Datenbestand und den Querverbindungen in fremde Netzwerke. Was sagen Sie?**
  - RUAG MRO hat einen vollständigen Überblick über alle TWI und hat zwecks weiterer Steigerung des Schutzniveaus sowohl in technischer als auch in prozeduraler Sicht für jede einzelne TWI eine Referenz-Architektur definiert und verabschiedet, welche auch entsprechende Kontrollmechanismen im Sicherheitsbereich umfasst. Die TWI werden grundsätzlich in abgeschotteten Netzwerken verwaltet.

- **Ruag International verfügt 1:1 über den alten Datenbestand des Ruag Netzwerks. Von Ruag International ist es nach wie vor möglich, in den nationalen Teil des Netzwerks zu kommen. Was sagen Sie dazu?**
  - Sämtliche Daten von RUAG MRO auf der Umgebung von RUAG International wurden bereinigt, gelöscht oder dauerhaft anonymisiert. Die Rückbauarbeiten der Firewall-Infrastruktur sind abgeschlossen und die Verbindungen alle gekappt.

- **Ruag International hat die IT nach Indien ausgelagert. Experten erachten das als Sicherheitsproblem, weil:**
  - Diese Aussage können wir so nicht stehen lassen. Viele IT-Experten sind sich einig, dass IT-Outsourcing das Sicherheitsniveau erhöht, weil grosse Provider

jederzeit aufgrund ihrer Grösse und ihrer Ressourcen in der Lage sind, die neusten Sicherheitsvorkehrungen zu etablieren – besser, als dies mit internen Mitteln möglich wäre.

- **die Entflechtung des Konzerns entgegen öffentlichen Verlautbarungen noch nicht abgeschlossen ist und das Netzwerk dadurch durchgängig ist**
  - Diese Aussage ist falsch. Die Netzwerke sind komplett getrennt. TechMahindra als der Outsourcing-Partner von RUAG International hat keinerlei Zugriff auf das Netzwerk von RUAG MRO.
- **die Schweiz mit dem Outsourcing die Kontrolle von womöglich sensiblen Daten ins Ausland abgibt**
  - Die Kontrolle sensibler Daten ist immer in der Hoheit von RUAG International. Der Zugriff auf sensible Daten ist auf ein Minimum beschränkt und unterliegt höchsten Sicherheitsanforderungen, Mitarbeitende mit Fernwartungszugriff werden regelmässig überprüft.
- **mit den indischen Administratoren nicht die nötige Sicherheitsüberprüfung gemacht worden ist**
  - Das ist falsch.
- **im Netz ITAR-relevante und möglicherweise vertrauliche/geheime Daten liegen**
  - Im öffentlich-zugänglichen Netz liegen keinerlei ITAR-relevante Daten. Im geschützten Firmennetzwerk liegen ITAR-Daten. RUAG International verfügt über modernste Trade-Compliance-Standards, um überhaupt operieren zu können in den bestehenden Geschäftssegmenten. Die Mitarbeitenden, die mit ITAR-Daten hantieren, werden regelmässig geschult und es finden regelmässige Compliance-Assessments durch eine zentral geführtes Trade Compliance Organisation statt. Entsprechende Berechtigungen stellen sicher, dass Mitarbeitende des IT-Outsourcing-Partners keinen Zugriff haben.

- **Es wird befürchtet, Tech Mahindra könnte theoretisch über die nicht entflochtene Ruag Real Estate Überwachungskameras oder Zutrittssysteme von Armee relevanten Gebäuden «übernehmen» und manipulieren. Was sagen Sie dazu?**
  - Die Real Estate-Systeme wie Kamera und Zutrittssystem sind in separaten Netzwerksegmenten angesiedelt, auf die nur Mitarbeitende von RUAG Real Estate Zugriff haben.

- **Uns liegt ein Ruag internes Dokument vor, das zeigt, dass im Netz der Ruag International noch heute militärisch klassifizierte Daten liegen. Dies bestätigt der vertrauliche EFK-Bericht vom Februar 2021. Was sagen Sie dazu?**
  - Im Rahmen des 2. Arbeitsschritts der Entflechtung wurden bereits alle Daten von RUAG MRO, die sich noch auf Systemen der RUAG International befanden bereinigt, anonymisiert bzw. gelöscht. Dies betrifft u.a. das gesamte SAP-Umfeld, Mailboxen, File-Server und Daten, die in relevanten Applikationen direkt gehalten werden.
  - RUAG International arbeitet nach wie vor in geringem Ausmass für militärnahe Kunden oder Lieferanten, diese Daten sind entsprechend klassifiziert und geschützt abgelegt.

- **Im Netzwerk findet man etwa Pläne der Triebwerkdaten der FA/18. Auf die könnten Cyber-Terroristen zugreifen und sie manipulieren. Was sagen Sie dazu?**
  - Ja, wir haben Daten der F/A-18 in unserem Bestand. Der Hersteller ist einer unserer Kunden des Aerostructures Segment von RUAG International. Sensitive Daten sind bei uns mit Zugriffsbeschränkungen zusätzlich geschützt. Alle ITAR-relevanten Daten sind zudem so beschränkt, dass nur internes Personal in der Schweiz darauf zugreifen kann.

Aktueller Stand des Netzwerks

- **Gemäss unseren Informationen sind im April 2021 Unbefugte ins Netzwerk der Ruag International eingedrungen, hatten u.a. Zugriff auf Ordner-Strukturen von internationalen Programmen der Ruag Space. (Anmerkung Redaktion: Die Rundschau wird in ihrer Berichterstattung weder sensible Daten noch Wegweiser zum Innern des Netzwerks exponieren).Was sagen Sie zum Vorfall?**
- **Was sagen Sie dazu, dass mutmasslich sensible Daten ungenügend geschützt sind?**

  - Unsere Systeme sind nach neusten Erkenntnissen geschützt und werden aktiv an den wachsenden Anforderungen und Bedrohungen ausgerichtet. Wir haben keinerlei Hinweise auf einen Hack des Netzwerks von RUAG International. Das uns vorliegende Bildmaterial der Rundschau ist für unsere IT-Experten kein schlüssiger Beweis eines effektiven Zugriffs. Dennoch gehen wir den Hinweisen nach und nehmen sie ernst. Das Unternehmen analysiert derzeit die Hinweise in einer Taskforce, wird allenfalls entsprechende Massnahmen umsetzen und weiter in die Prävention und Sensibilisierung der Mitarbeitenden investieren. Zudem behält sich das Unternehmen eine Strafanzeige vor.

Verantwortlichkeiten

- **Gemäss mehreren Insidern waren von der Geschäftsleitung, über den Verwaltungsrat der Ruag bis zum CdA Thomas Süssli, BR Viola Amherd und VBS-Generalsekretär Toni Eder über die zahlreichen Schwachstellen des Netzwerkes informiert. Wieso wurde es gegenüber der Öffentlichkeit anders dargestellt?**
  - Das ist falsch. Die NZZ hat bereits Ende 2019 über die hohe Komplexität berichtet: Ruag: Cyberangriff hält Experten auch nach Jahren noch auf Trab (nzz.ch)

- **Gemäss mehreren Quellen und internen Ruag-Dokumenten wusste die gesamte Spitze der Ruag (MRO Schweiz, International, Beteiligungsgesellschaft) sowie der Spitze des VBS (Generalsekretär T. Eder), dass die Entflechtung Probleme bereitet und nicht abgeschlossen ist. Wieso wurde es gegenüber der Öffentlichkeit (und auch der Politik) anders dargestellt?**
  - Der Eigner ist zu jeder Zeit und aktuell über den Stand der Entflechtung informiert worden. Bis Sommer 2020 präsidierte das VBS einen gemeinsamen Steuerungsausschuss von VBS, Armee und RUAG. Der Eigner wird zudem regelmässig im Rahmen der BGRB-Berichterstattung über die Entflechtungsthemen, den Programmfortschritt und über allfällige Risiken informiert.
  - Die Entflechtung ist unternehmerisch abgeschlossen. Die IT von RUAG MRO wurde an Ostern 2020 in den FUB-Perimeter überführt. RUAG MRO und RUAG International werden rechtlich als getrennte Unternehmen geführt. Sowohl die Kunden wie die Mitarbeitenden wurden klar zugeordnet. Dass es noch Abschlussarbeiten gibt, war immer transparent.