Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksicherheit RUAG – Situation 2021

Bericht der Geschäftsprüfungskommission des Nationalrates

vom 18. Februar 2022

Das Wichtigste in Kürze

Die Geschäftsprüfungskommission des Nationalrates (GPK-N) leitete im vergangenen Jahr eine Prüfung zur Informatiksicherheit bei RUAG ein. Sie klärte dabei die Frage, ob der Bund als Eigner angemessen auf den mutmasslichen Hackerangriff reagiert hatte, der im Mai 2021 bekannt wurde. Zudem prüfte sie, wie es um die Informatiksicherheit von RUAG International und RUAG MRO steht, welche Verflechtungen zwischen den beiden Unternehmen bestehen und welche Risiken damit verbunden sind. In diesem Zusammenhang interessierte sie auch die Frage, ob die Geschäftsprüfungskommissionen (GPK) von den zuständigen Departementen und vom Bundesrat in den letzten Jahren transparent und korrekt über den Stand der Entflechtung und die Informatiksicherheit bei der RUAG informiert wurden.

Im Rahmen ihrer Untersuchung prüfte die GPK-N verschiedene Unterlagen und hörte die zuständigen Personen von Seiten des Bundes – insbesondere den Vorsteher des Eidgenössischen Finanzdepartements (EFD) und die Vorsteherin des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) –, von Seiten RUAG sowie Vertreter der Eidgenössischen Finanzkontrolle (EFK) an.

Die GPK-N kam zum Schluss, dass die zuständigen Bundesstellen grundsätzlich angemessen auf den mutmasslichen Angriff reagiert haben. Sie begrüsst auch, dass RUAG International selber rasch die nötigen Massnahmen einleitete und externe Experten beauftragte, um die Vorwürfe gründlich zu prüfen. Dabei zeigte sich, dass es keine erhärteten Belege für den mutmasslichen Hackerangriff auf RUAG International im Mai 2021 gibt. Ungeachtet dessen führte die mediale Berichterstattung bzw. die anschliessenden Untersuchungen dazu, dass RUAG International auf schwerwiegende Mängel in der Informatiksicherheit aufmerksam wurde und in der Folge verschiedene Massnahmen einleitete. Für die Kommission ist unverständlich, dass die Mängel nicht früher erkannt wurden und RUAG International ihre Informatik nicht schon früher von einer spezialisierten Firma testen liess. Sie ist der Ansicht, dass solche Tests periodisch stattfinden sollten, im Interesse der Unternehmen, aber auch im Interesse des Bundes als Eigner. Sie fordert den Bundesrat bzw. das EFD aus zuständiges Departement daher auf, eine solche Vorgabe an RUAG International zu prüfen.

Die letzten bestehenden Verbindungen zwischen RUAG International und RUAG MRO sollten gemäss den Verantwortlichen bis Ende 2021 getrennt und die Entflechtung damit vollständig abgeschlossen sein. Für die GPK-N ist dabei von höchster Bedeutung, dass die beiden Unternehmen gemeinsam dafür sorgen, dass auf den Systemen von RUAG International keine sensitiven Daten und insbesondere Daten der RUAG MRO verbleiben. Da nicht ausgeschlossen werden kann, dass sich solche Daten in Archiven und Backups befinden, daher bei der Löschung übersehen und bei einem Verkauf von Teilen von RUAG International in fremde Hände gelangen könnten, sollten aus Sicht der GPK-N zusätzliche Massnahmen geprüft werden. Möglich wäre insbesondere eine zusätzliche und gezielte Datenprüfung vor jedem Verkauf. Die GPK-N wird diese Frage mit den zuständigen Stellen im EFD und im VBS klären. Ebenso wird sie weitere Auskünfte sowie eine Bestätigung der Löschung der Daten auf den Systemen von RUAG International verlangen.

Die Information über den Stand der Entflechtung in den vergangenen Jahren erachtet die GPK-N als zu wenig transparent. Sie lädt den Bundesrat daher ein, sicherzustellen, dass er bzw. das EFD und das VBS mit ihren Eignerstellen die Oberaufsichtskommissionen künftig transparenter und zeitnah über allfällige Herausforderungen bei der Entflechtung der RUAG informieren, insbesondere auch im Zusammenhang mit der Weiterentwicklung von RUAG International.

Bericht

1 Einleitung

2016 wurde bekannt, dass die RUAG von einem Cyberangriff betroffen war. Die Geschäftsprüfungskommission des Nationalrates (GPK-N) hat sich danach vertieft mit der Aufarbeitung dieses Vorfalls beschäftigt und Empfehlungen an den Bundesrat gerichtet.[1] Als Folge des damaligen Angriffs entschied der Bundesrat im Juni 2017, die damalige RUAG aufzuteilen und die Teile, die hauptsächlich für die Armee tätig sind (heutige RUAG MRO Holding AG), von den übrigen, international ausgerichteten Geschäftsbereichen (heutige RUAG International Holding AG) zu trennen. Diese beiden Subholdings sind unter der Dachgesellschaft BGRB (Beteiligungsgesellschaft Rüstungsbetriebe) Holding AG zusammengefasst, welche vollständig in Bundesbesitz ist.

Mit der organisatorischen Entflechtung verbunden war auch das Ziel einer kompletten Trennung der Informatiksysteme. Die Daten und Systeme der RUAG AG, welche Teil der RUAG MRO Holding AG ist und für die Armee tätig ist, sollten in den Sicherheitsperimeter der Führungsunterstützungsbasis der Armee (FUB) migriert und so die Informatiksicherheit erhöht werden. Die RUAG selber startete nach dem Cyberangriff das Projekt «Impact», um ihr Netzwerk nach dem Hackerangriff sicherer zu machen. Dieses wurde später von der RUAG International fortgeführt und abgeschlossen.

Im Mai 2021 berichtete die Rundschau des Schweizer Fernsehens[2], es sei Hackern gelungen, in das Netzwerk von RUAG International einzudringen. Dies sei besonders gefährlich, da von diesem Netzwerk nach wie vor zahlreiche, nicht oder ungenügend gesicherte Verbindungen in andere Netzwerke und insbesondere zu Systemen der RUAG MRO bestünden.

Die GPK-N beschloss in der Folge, Abklärungen zur Informatiksicherheit von RUAG International und RUAG MRO durchzuführen und dabei auch die Vorwürfe in Zusammenhang mit dem mutmasslichen Hackerangriff zu prüfen. Im Fokus der Abklärungen standen dabei die Fragen, ob die Informatiksicherheit von RUAG International und RUAG MRO genügt, welche Verflechtungen zwischen den beiden Unternehmen noch bestehen und welche Risiken damit verbunden sind. Zudem prüfte die Kommission, ob der Bund als Eigner angemessen auf den mutmasslichen Hackerangriff reagiert hatte und ob die Geschäftsprüfungskommissionen (GPK) von den zuständigen Departementen und vom Bundesrat in den letzten Jahren transparent und korrekt über den Stand der Entflechtung und die Informatiksicherheit bei der RUAG informiert wurden.

Um die erwähnten Fragen zu klären, hörte die Subkommission Vertreter von RUAG International und RUAG MRO, die Vorsteherin des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) und den Vorsteher des Eidgenössischen Finanzdepartements (EFD) sowie weitere zuständige Personen im VBS

1 Bewältigung des Cyberangriffs auf die RUAG: Berichte der GPK-N vom 8. Mai 2018 (BBl **2018** 4575) und vom 19. Nov. 2019 (BBl **2020** 2549).
2 Rundschau, SRF 1, ausgestrahlt am 19. Mai 2021.

und EFD an. Denn das VBS ist verantwortlich für die Steuerung und Kontrolle der BGRB Holding sowie für die Geschäfte im Bereich der RUAG MRO, während das EFD die Federführung bei Geschäften der RUAG International innehat.

Weiter behandelte die Subkommission Berichte der Eidgenössischen Finanzkontrolle (EFK), welche verschiedentlich Prüfungen zur Informatiksicherheit bei RUAG, RUAG MRO und RUAG International durchführte, und liess sich von der EFK auch direkt über deren Erkenntnisse und Einschätzungen informieren.

2 Informatiksicherheit und Stand der Entflechtung

2.1 Informatiksicherheit RUAG International

Die Vertreter von RUAG International betonten gegenüber der zuständigen Subkommission, dass weder die eigenen Experten noch eine externe Firma[3] die in der «Rundschau» gezeigten Vorgänge nachvollziehen konnten, man habe keinen Nachweis für einen unbefugten Zugriff auf die Systeme von RUAG International gefunden.

Die externen Experten befassten sich bei ihrer Prüfung aber nicht nur mit den Vorwürfen der «Rundschau», sondern sie sollten die Systeme unabhängig davon gründlich testen und dabei auch «mit krimineller Energie und Kreativität» Lücken und Mängel finden. In diesem Rahmen wurden gemäss dem CEO von RUAG International einige ernstzunehmende Sicherheitsmängel identifiziert, denen mit Sofortmassnahmen und längerfristigen Massnahmen begegnet wurde. Zu den identifizierten Mängeln gehören gemäss RUAG International insbesondere Versäumnisse in Schulung und Ausbildung sowie Software- und System-Upgrades, die nicht rechtzeitig durchgeführt wurden. Es habe sich dabei nicht um dieselben Schwachstellen gehandelt, welche bei früheren Prüfungen[4] identifiziert worden waren. Der CEO räumte ein, dass man diese Schwachstellen früher hätte erkennen müssen. Als Konsequenz davon trennte sich RUAG International vom Verantwortlichen für die Informatiksicherheit (Chief Information Security Officer) und nahm organisatorische Anpassungen vor.

Die zuständige Subkommission liess sich im Rahmen ihrer Abklärungen auch über die aktuelle Prüfung der Informatiksicherheit bei RUAG International durch die EFK informieren.[5] Die EFK stellte dabei fest, dass verschiedene Massnahmen zur Verbesserung der Informatiksicherheit umgesetzt oder noch in Umsetzung begriffen sind. Sofern diese wie geplant umgesetzt werden, führe dies zu einer wesentlichen Erhöhung der Informatiksicherheit. Weiter hielt die EFK fest, dass RUAG International

3 Es handelt sich dabei um die Firma SEC Consult.
4 Prüfungen der EFK, der ETH Zürich («Sicherheitsaudit Projekt IMPACT», 2019) und der Firma EY («IMPACT Audit Follow-up», 2019).
5 Im Rahmen dieser Nachprüfung erhob die EFK ab Juni 2021 den Stand der Umsetzung von früheren Empfehlungen zur Informatiksicherheit. Zugleich sollte die Prüfung die Risiken hinsichtlich eines möglichen Abflusses sensitiver Daten bei einem Verkauf von RUAG Ammotec einschätzen.

mittlerweile die ITAR-Daten[6] systematisch erhoben habe, eine darüber hinaus gehende Inventarisierung weiterer sensitiver Daten stehe aber noch aus. Damit bestehe ein «schwer einschätzbares Restrisiko», dass bei einem Verkauf von Unternehmensteilen unerkannte sensitive Daten in falsche Hände gelangen, falls diese nicht vorher erkannt und gelöscht werden (vgl. Absatz 2.3).

Was den aktuell diskutierten Verkauf von RUAG Ammotec[7] betrifft, gab die EFK Entwarnung: Da die Informatik von Ammotec schon seit 2014 weitgehend von jener von RUAG International getrennt sei und Ammotec keinen Zugriff auf RUAG-Daten – und damit auch auf ITAR-Daten – habe, schätzt die EFK das Risiko, dass bei einem Verkauf heikle Daten abfliessen, als klein ein.

Gemäss den Vertretern von RUAG International hat die beauftragte externe Firma ebenfalls geprüft, inwiefern sich die geplanten Verkäufe von einzelnen Unternehmensteilen auf die Informatiksicherheit auswirke. Dabei sei sie zum Schluss gekommen, dass die Komplexität der Informatik dadurch kleiner werde. Damit werde eine die Überwachung der Systeme einfacher und die Informatiksicherheit eher höher.

Ein Thema, das die zuständige Subkommission im Rahmen ihrer Abklärungen auch aufnahm, betraf die Auslagerung von Informatikdienstleistungen der RUAG International an den indischen IT-Dienstleister Tech Mahindra. Die Vertreter von RUAG International erläuterten, dass die Firma für die RUAG International und viele andere Grosskonzerne Infrastruktur- und Unternehmensdienstleistungen erbringe. Sie habe keinen Zugriff auf sensitive Daten, insbesondere auf ITAR-Daten. Auch verfüge RUAG International heute über keine militärischen Daten mehr, diese seien bei der RUAG MRO bzw. im Sicherheitsperimeter der FUB. Die EFK befasste sich ebenfalls mit dieser Auslagerung und kam zum Schluss, dass diese mit der nötigen Sorgfalt geplant und umgesetzt wurde bzw. die nötigen Vorkehrungen getroffen wurden, um heikle Daten zu schützen.[8]

2.2 Informatiksicherheit RUAG MRO

Auch die Vertreter der RUAG MRO hielten zu den Medienberichten vom Frühling 2021 fest, dass sie keine unberechtigten Zugriffe feststellten konnten. Überhaupt habe man seit dem Hackerangriff von 2016 keine kritischen Vorfälle mehr registriert. Die wesentlichen Daten und Systeme von RUAG MRO seien im Rahmen der Entflechtung in den Perimeter der FUB überführt worden und damit heute gleich geschützt wie die Informatik der Armee.

6 Dabei handelt es sich um Daten und Informationen, welche den «International Traffic in Arms Regulations» unterliegen, einem Regelwerk der USA über den Handel mit Waffen sowie Rüstungs- und Verteidigungsgütern.
7 RUAG Ammotec produziert vor allem Munition und gehört zu RUAG International.
8 Die EFK wies im Rahmen der Verwaltungskonsultation darauf hin, dass ihre diesbezügliche Prüfung vor der Löschung der MRO Daten bei RUAG International abgeschlossen wurde. Daher werde im entsprechenden Bericht die Löschung der Daten der MRO Schweiz bei RUAG International noch als Pendenz ausgewiesen, welche aber bis Ende 2021 erledigt sein sollte.

Sie wiesen darauf hin, dass die Informatik der Technisch-Wissenschaftlichen Infrastrukturen (TWI)[9] und der RUAG Real Estate, welche zur RUAG MRO gehören, nicht zum militärischen Kernbereich gehört und daher nicht in den Perimeter der FUB migriert wurde. Hierzu würden aber Folgearbeiten laufen, welche auch einer Verbesserung der Informatiksicherheit dienen sollen. Diese Arbeiten sollten bis Ende 2021 abgeschlossen sein.

Die EFK hielt gegenüber der Subkommission fest, dass sich die Informatiksicherheit von RUAG MRO seit 2016 «deutlich verbessert» habe. Das Risiko einer Gefährdung der Systeme von RUAG MRO Schweiz von aussen oder über die RUAG International sei heute klein. In ihrem Bericht vom Februar 2021 zur Informatiksicherheit der RUAG MRO[10] kommt die EFK zum Schluss, dass die Informatikentflechtung trotz der hohen Komplexität und Verzögerungen erfolgreich abgeschlossen sei und ihre früheren Empfehlungen dabei im Wesentlichen umgesetzt worden seien. Sie sieht allerdings noch Verbesserungspotential bei der Betriebssicherheit sowie Risiken bei der Bereinigung von Archiven und Datensicherungen (vgl. Absatz 2.3).

2.3 Stand der Entflechtung

Wie bereits oben erwähnt, hielten die Verantwortlichen der RUAG MRO, aber auch die Verantwortlichen des Generalsekretariates VBS (GS VBS) gegenüber der Subkommission fest, dass inzwischen sämtliche sicherheitsrelevanten Daten der RUAG MRO in den Sicherheitsperimeter der FUB migriert wurden. Bei dieser Migration wurden umfangreiche Vorkehrungen getroffen, um zu gewährleisten, dass bei der Migration keine Schadsoftware in die Systeme der FUB gelangt. Aktuell laufen noch verschiedene «Restarbeiten». Diese betreffen den Rückbau der nicht mehr benötigten Systeme und die Datenbereinigung bei RUAG International sowie die Systeme der TWI[11] und die Informatik von RUAG Real Estate (diese werden nicht in den FUB-Perimeter integriert).

Gemäss RUAG MRO und RUAG International sind diese Arbeiten schon weit fortgeschritten: Die Datenbereinigung sei im 2. Quartal 2021 abgeschlossen worden und der grösste Teil der Informatik von RUAG International sei rückgebaut worden. Auch bezüglich Real Estate und der TWI seien die Arbeiten am Laufen und sollten bis Ende 2021 abgeschlossen werden. Zu den Zuständigkeiten für den Rückbau der Systeme und die Bereinigung der Daten hielten die Vertreter der beiden Subholdings fest, dass diese Arbeiten in enger Absprache zwischen RUAG International und RUAG MRO erfolgen. Konkret würden die Daten und Systeme von der RUAG MRO geprüft, diese erteile dann den Auftrag zum Löschen oder Abschalten. Die RUAG International führe dies aus und bestätige die Löschung bzw. Abschaltung. Der Datenbestand und insbesondere die sensitiven Daten, die vor der Entflechtung bei RUAG International

9 Dezentrale IT-Infrastrukturen für spezifische Geschäftsanwendungen, die mit Maschinen und Prüfgeräten bzw. spezifischen Applikationen ausgestattet sind und nicht aus der FUB heraus betrieben bzw. bereitgestellt werden können.
10 Bericht der EFK vom 22. Febr. 2021, veröffentlicht.
11 Vgl. Fussnote 9.

bestanden, seien per Ende Mai 2021 gelöscht worden. Eine Ausnahme seien die Daten, die in den Systemen von Real Estate und TWI noch vorhanden sind; diese würden auf Ende 2021 gelöscht.

Die Verantwortlichen gaben an, dass die RUAG – RUAG MRO und RUAG International – heute eine vollständige Übersicht über ihre Daten, Server und Archive habe. Dies sei eine Voraussetzung für die Migration der militärischen Daten in den FUB-Bereich gewesen und auch für die jetzt noch laufenden Arbeiten.

Die EFK beurteilt die Situation kritischer als die Vertreter der RUAG-Subholdings. In ihren Berichten zur Informatiksicherheit bei RUAG MRO und bei RUAG Holding[12] und in ihren Ausführungen gegenüber der zuständigen Subkommission wies sie darauf hin, dass bei der Datenbereinigung gewisse Risiken bestehen, denen RUAG die nötige Aufmerksamkeit schenken sollte. Insbesondere erachtet es die EFK als zentral, dass bei der Löschung der Daten von RUAG MRO auf den Systemen von RUAG International auch geprüft wird, welche Archive und Datensicherungen bestehen, und ob diese auch Daten enthalten, die gelöscht werden müssen. Die EFK bezweifelt, dass die RUAG diesbezüglich eine vollständige Übersicht hat.[13] Ebenso stellte sie fest, dass RUAG International zwar die ITAR-relevanten Daten erhoben und klassifiziert hat, nicht aber weitere sensitive Daten. Die fehlende Komplettübersicht über Archive, Backups und sensitive Daten könnte dazu führen, dass bei einem Verkauf von Unternehmensteilen heikle Daten abfliessen. Die EFK hat die RUAG MRO und RUAG International[14] daher aufgefordert, dieser Problematik die nötige Aufmerksamkeit zu schenken und sie wird voraussichtlich auch eine Prüfung betreffend die Löschung der Daten durchführen.

2.4 Bewertung der GPK-N

Auf der Basis ihrer Abklärungen kam die GPK-N zum Schluss, dass es keine erhärteten Belege für den mutmasslichen Hackerangriff auf RUAG International im Mai 2021 gibt. Ungeachtet dessen führte die mediale Berichterstattung bzw. die anschliessenden Prüfungen dazu, dass RUAG International auf schwerwiegende Mängel in der Informatiksicherheit aufmerksam wurde und verschiedene Massnahmen traf. Aus Sicht der Kommission hat RUAG International nach dem Vorfall angemessen reagiert und seine Informatiksicherheit einem gründlichen Härtetest durch eine externe Firma unterzogen. Nicht verständlich ist für die Kommission aber, weshalb diese Mängel nicht bereits früher erkannt wurden und warum RUAG International ihre Informatik nicht schon früher von einer spezialisierten Firma testen liess. Die GPK-N ist der Ansicht, dass ein solcher Test periodisch wiederholt werden sollte, einerseits im Interesse

12 Berichte der EFK vom 22. Febr. 2021 (veröffentlicht) und vom 21. Okt. 2019 (nicht veröffentlicht).

13 Gemäss der Rückmeldung der RUAG MRO im Rahmen der Verwaltungskonsultation kann ein Restrisiko, dass Datenträger nicht erfasst bleiben, nicht vollständig ausgeschlossen werden. Dieses sei allerdings sehr klein, es liege «im Promille-Bereich».

14 Die Verantwortung für die Löschung der sicherheitsrelevanten Daten auf den Systemen von RUAG International ist eine geteilte. Die RUAG MRO ist nicht aus der Verantwortung entlassen, bis die Daten, die sie für ihre Arbeit übernommen bzw. in den Perimeter der FUB migriert hat, bei RUAG International gelöscht sind.

der Firma (Schutz ihrer Geschäftsgeheimnisse), andererseits aber auch im Interesse des Bundes als Eigner. Sie fordert den Bundesrat bzw. das EFD daher auf, zu prüfen, ob eine entsprechende Vorgabe an RUAG International möglich und sinnvoll wäre, um die Eignerinteressen im Hinblick auf einen möglichen Verkauf zu wahren.

Was den Stand der Entflechtung betrifft, geht die GPK-N davon aus, dass diese per Ende 2021 vollständig abgeschlossen ist. Von besonderer Wichtigkeit ist dabei, dass RUAG MRO und RUAG International gemeinsam dafür sorgen, dass auf den Systemen von RUAG International keine sensitiven Daten und insbesondere Daten der RUAG MRO verbleiben. Die GPK-N wird diesbezüglich im kommenden Jahr weitere Auskünfte bzw. eine Bestätigung der Löschung verlangen.

Aufgrund der Befunde der EFK, wonach heikle Daten möglicherweise auch in Archiven und Backups versteckt sind, deswegen bei der Löschung übersehen werden und bei einem Verkauf in fremde Hände gelangen könnten, stellt sich für die GPK-N aber auch die Frage, ob zusätzliche Massnahmen nötig sind. Insbesondere wäre zu prüfen, ob der Bund als Eigner RUAG International verpflichten sollte, vor jedem Verkauf einer Einheit eine zusätzliche und gezielte Datenprüfung vorzunehmen oder in Auftrag zu geben. Diese sollte sämtliche Daten inventarisieren und analysieren, ob sich darunter noch sensitive Daten der RUAG MRO, ITAR-Daten oder andere heikle Daten befinden. Die GPK-N bzw. die beiden GPK werden diese Frage im kommenden Jahr mit dem Bund als Eigner bzw. den zuständigen Eignervertretern im EFD und VBS klären.

Empfehlung 1: Schutz von militärischen und anderen sensitiven Daten

Die GPK-N fordert den Bundesrat auf, die nötigen Massnahmen zu treffen, um sicherzustellen, dass RUAG International nach der geplanten Löschung der Daten tatsächlich über keine militärischen oder andere sensitiven Daten mehr verfügt (auch nicht in Archiven oder Backups). Dabei stellt sich die Frage, ob die Löschung allenfalls durch externe Experten überprüft werden sollte. Ebenso ist zu prüfen, ob es zweckmässig wäre, vor jedem Verkauf von Unternehmensteilen von RUAG International einen zusätzlichen Check der Datensituation zu verlangen.

3 Reaktion des Eigners

3.1 Massnahmen von EFD und VBS

Die Abklärungen der Subkommission zeigten, dass das VBS am 12. Mai 2021 (also rund eine Woche vor der Ausstrahlung der Sendung) eine schriftliche Anfrage der Rundschau zum mutmasslichen Angriff erhielt und umgehend das EFD informierte. Die Vorsteherin des VBS betonte gegenüber der Subkommission denn auch mehrmals, dass der mutmassliche Angriff RUAG International betroffen habe, für welche das EFD zuständig sei. Ungeachtet dessen nahm gegenüber der Rundschau dann aber

nicht das EFD bzw. diese beiden Departemente gemeinsam Stellung, sondern lediglich das VBS.[15]

Die Vorsteherin des VBS und der Vorsteher des EFD gaben aber an, dass die beiden Departemente sich in Bezug auf Fragen zu RUAG International und RUAG MRO eng abstimmen, insbesondere zur Vorbereitung der Sitzungen des Verwaltungsrats der BGRB Holding AG. Dort nehmen seit dem 1. April 2021, wie von der GPK-N bereits seit längerem gefordert[16], die Direktorin der Eidgenössischen Finanzverwaltung (EFV) und der Generalsekretär des VBS Einsitz. Der Bundesrat will damit die Entflechtung und Privatisierung von RUAG International enger begleiten.[17]

Der Vorsteher des EFD gab an, dass der mutmassliche Hackerangriff und Fragen zur Informatiksicherheit an den Sitzungen des Verwaltungsrates der BGRB Holding vom 18. Mai 2021 und vom 1. Juni 2021 behandelt wurden. Das EFD und VBS haben darüber hinaus keine eigenen Abklärungen eingeleitet, sondern stützen sich bei der Bewertung der Situation vor allem auf die Auskünfte von RUAG International sowie der von dieser beauftragten externen Firma.

Das EFD gab gegenüber der GPK-N auch an, dass es aufgrund der öffentlichen Berichterstattung über den mutmasslichen Hackerangriff keine wesentlichen negativen Auswirkungen auf den Werterhalt der Firma und die geplanten Verkäufe von Unternehmensteilen erwartet. Massgebend seien vielmehr «verlässliche Informationen von RUAG International zum Zustand und zu den Risiken ihrer Informatiksysteme». Für den Bund sei ausserdem wesentlich, dass bei den Verkäufen keine sicherheitsrelevanten Daten der Armee bzw. der RUAG MRO an den Käufer übergehen. Dafür würden «die im Rahmen von Unternehmensverkäufen übliche Abtrennung der Informatiksysteme und Prüfung der übertragenen Daten auf Schadsoftware» sorgen.

3.2 Bewertung der GPK-N

Für die GPK-N stellte sich insbesondere die Frage, ob das EFD und das VBS nach dem Bericht der Rundschau angemessen reagiert haben und dafür gesorgt haben, dass die Interessen des Bundes als Eigner gewahrt werden. Diesbezüglich kann festgehalten werden, dass die Vorwürfe von den beiden Departementen umgehend aufgenommen und im Verwaltungsrat der BGRB Holding behandelt wurden. Da das EFD und das VBS – wie von der GPK-N schon früher gefordert[18] – seit dem Frühling 2021 Einsitz in dieses Gremium haben, dürfte zumindest der Informationsfluss besser als früher gewährleistet gewesen sein. Vor diesem Hintergrund und da RUAG International selber die nötigen Massnahmen einleitete, um die Vorwürfe gründlich zu klären (insbesondere durch die Beauftragung externer Experten), ist es für die Kommission nachvollziehbar, dass die zuständigen Bundesstellen in diesem Fall darauf verzichte-

15 Stellungnahme des VBS vom 15. Mai 2021 (veröffentlicht).
16 Bewältigung des Cyber-Angriffs auf die RUAG, Berichte der GPK-N vom 8. Mai 2018 (BBl **2018** 4575) und vom 19. Nov. 2019 (BBl **2020** 2549).
17 Bund nimmt Einsitz in den Verwaltungsrat von RUAG, Medienmitteilung des Bundesrates vom 12. März 2020.
18 Vgl. Fussnote 16

ten, zusätzliche eigene Abklärungen einzuleiten. Dennoch kann die Frage aufgeworfen werden, ob die von der RUAG International veranlasste Prüfung nicht durch Spezialisten des Bundes hätte auf ihre Angemessenheit überprüft werden sollen.

Viel bedeutender als die Klärung der erwähnten Frage scheint der GPK-N aber, dass sowohl das EFD als auch das VBS der Tatsache, dass sich auf den Systemen von RUAG International zum damaligen Zeitpunkt immer noch militärische oder sensitive Daten befanden (und mit einem nicht vollständig auszuschliessenden Restrisiko möglicherweise auch heute noch befinden) zu wenig Beachtung schenken. Dies zeigen die Ausführungen zur Entflechtung weiter oben bzw. die Prüfungen der EFK. Es ist daher aus Sicht der GPK-N schwierig nachzuvollziehen, dass die Vorsteherin des VBS betont, dass die sicherheitsrelevanten Daten der Armee nur noch von RUAG MRO «bearbeitet» würden. Ebenso reicht es nicht, wie vom Vorsteher des EFD geschildert, bei Unternehmensverkäufen die Informatiksysteme zu trennen und die Daten auf Schadsoftware zu überprüfen.

Die GPK-N erwartet vom Bund als Eigner, wie bereits oben erwähnt, dass er sicherstellt, dass die militärischen und anderen sensitiven Daten auf den Systemen der RUAG tatsächlich gelöscht werden, und dass er prüft, ob vor Verkäufen ein zusätzlicher Check nötig ist (vgl. Abs. 2.4, Empfehlung 1)

4 Information der GPK

4.1 Frühere Auskünfte zum Stand der Entflechtung gegenüber den GPK

Im Rahmen ihrer Abklärungen prüfte die GPK-N auch, ob sie vom Bundesrat und insbesondere vom VBS in den vergangenen Jahren transparent und korrekt über den Stand der Entflechtung und die Informatiksicherheit bei der RUAG informiert wurde. Denn der Bundesrat und das VBS hatten gegenüber der Kommission wie gegenüber der Öffentlichkeit immer betont, dass die Entflechtung und Weiterentwicklung zwar komplex, aber auf Kurs sei. So bestätigte der Bundesrat beispielsweise am 19. Februar 2020 in einer Stellungnahme zuhanden der GPK-N, dass die Trennung der Informatik bis Mitte 2020 abgeschlossen sein werde.[19] Im Juni 2020 gab die Vorsteherin des VBS gegenüber den zuständigen Subkommissionen der GPK an, dass die Entflechtung auf das Jahr 2020 in wichtigen Teilen operativ umgesetzt worden war und die Informatik der RUAG MRO über die Ostertage 2020 erfolgreich in den Sicherheitsperimeter der FUB migriert wurde. Im April 2021 hielt sie gegenüber denselben Subkommissionen fest, dass die Entflechtung «termingerecht vollzogen» wurde. Die organisatorischen, juristischen und IT-technischen Kernziele der Entflechtung seien bis Ende Juni 2020 umgesetzt gewesen.

Im Bericht des Bundesrates vom 19. März 2021 zuhanden den GPK zur Zielerreichung der RUAG im Jahr 2020 ist hingegen erwähnt, dass «die Abschlussarbeiten der Entflechtung in ein zweites Programm» übertragen werden. Weiter wird festgehalten,

19 Stellungnahme des Bundesrates vom 19. Febr. 2020 zum Bericht der GPK-N vom 19. Nov. 2020 zur Bewältigung des Cyberangriffs auf die RUAG; Medienmitteilung des Bundesrates vom 24. Febr. 2020.

dass es dabei vor allem um die Datenbereinigung sowie die Informatik-Entflechtung der TWI sowie der RUAG Real Estate gehe. Das VBS ist daher der Ansicht, dass die GPK transparent informiert wurden.

Die Vertreter der RUAG MRO gaben gegenüber der GPK-N an, dieser zweite Schritt sei geplant gewesen, es sei bei Grossprojekten üblich, «Restarbeiten» in einem zweiten Schritt zu erledigen.

4.2 Bewertung der GPK-N

Die Kommission nimmt zur Kenntnis, dass der Bundesrat den zweiten Schritt der Entflechtung in seinem Bericht vom 19. März 2021 erwähnt und genauer beschreibt. Sie stellt aber auch fest, dass diese noch ausstehenden Arbeiten vom VBS in den verschiedenen Anhörungen nie thematisiert wurden. Vielmehr wies dieses immer darauf hin, dass die Entflechtung in wesentlichen Teilen und termingerecht umgesetzt sei.[20] Die GPK-N ist daher der klaren Auffassung, dass die Kommunikation des VBS – auch vor dem Hintergrund der früheren Abklärungen der GPK – präziser und transparenter hätte sein müssen. Sie fordert das VBS und den Bundesrat auf, künftig offener zu kommunizieren.

Empfehlung 2: Transparentere Kommunikation

Die GPK-N lädt den Bundesrat ein, geeignete Massnahmen zu ergreifen, damit der Bundesrat sowie das EFD und das VBS mit ihren Eignerstellen die Oberaufsichtskommissionen künftig transparenter und zeitnah über allfällige Herausforderungen bei der Entflechtung der RUAG informieren, insbesondere auch im Zusammenhang mit der Weiterentwicklung von RUAG International.

5 Fazit

Auf der Basis der hier geschilderten Abklärungen und Schlussfolgerungen beschloss die GPK-N, ihre Abklärungen zum mutmasslichen Hackerangriff von 2021 abzuschliessen. Sie wird die erwähnten kritischen Punkte bzw. Themen weiterverfolgen und diese, zusammen mit der Geschäftsprüfungskommission des Ständerates, insbesondere im Rahmen ihrer jährlichen Befassung mit dem Bericht des Bundesrates zur

20 Das VBS hielt im Rahmen der Verwaltungskonsultation fest, dass der Bundesrat der BGRB Holding im Rahmen der strategischen Ziele vorgegeben habe, dass die verbleibenden Arbeiten bis spätestens Ende 2021 abzuschliessen seien. Seiner Ansicht nach sind diese die noch ausstehenden Arbeiten, welche im September 2020 in einem «zweiten Entflechtungsschritt» zusammengefasst wurden, «verglichen mit dem Ziel, dass die Arbeiten zu Gunsten der Armee in einer sicheren IKT-Umgebung ausgeführt werden können, von untergeordneter Bedeutung». Das VBS hält deshalb an seiner Einschätzung fest, dass die Entflechtung seit Mitte 2020 in wesentlichen Teilen vollzogen wurde und somit gemäss Frist erfolgte. Weiter hält es fest, dass die Entflechtung der RUAG als Projekt erfolgreich durchgeführt wurde. Dies sei auch von der EFK bestätigt worden, welche in ihrem Prüfbericht folgendes festgehalten habe: «Die Projektziele wurden qualitativ und quantitativ erreicht.»

Zielerreichung der RUAG aufnehmen. In diesem Zusammenhang werden sie soweit nötig und in Abstimmung mit den anderen zuständigen Kommissionen auch die Weiterentwicklung der RUAG International sowie deren Risiken verfolgen. Der Fokus der GPK liegt dabei auf der Frage, ob der Bund als Eigner seine Funktion angemessen wahrnimmt.

Die GPK-N bittet den Bundesrat darum, bis am 25. März 2022 Stellung zum vorliegenden Bericht und ihren Empfehlungen zu nehmen.

18. Februar 2022

Im Namen der Geschäftsprüfungskommission des Nationalrates

Die Präsidentin: Prisca Birrer-Heimo

Die Sekretärin: Beatrice Meli Andres

Der Präsident der Subkommission EDA/VBS: Nicolo Paganini

Die Sekretärin der Subkommission EDA/VBS: Céline Andereggen

Abkürzungsverzeichnis

BGRB	Beteiligungsgesellschaft Rüstungsbetriebe
EFD	Eidgenössisches Finanzdepartement
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
FUB	Führungsunterstützungsbasis der Armee
GPK	Geschäftsprüfungskommissionen der eidgenössischen Räte
GPK-N	Geschäftsprüfungskommission des Nationalrates
GS VBS	Generalsekretariat VBS
ITAR	Regelwerk der USA über den Handel mit Waffen sowie Rüstungs- und Verteidigungsgütern (*International Traffic in Arms Regulation*)
TWI	Technisch-Wissenschaftliche Infrastrukturen (vgl. Fussnote 9)
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport