Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatiksicherheit RUAG − Situation 2021

Bericht der Geschäftsprüfungskommission des Nationalrates vom 18. Februar 2022

Stellungnahme des Bundesrates

vom 30. März 2022

Sehr geehrte Frau Kommissionspräsidentin
Sehr geehrte Damen und Herren

Zum Bericht der Geschäftsprüfungskommission des Nationalrates vom 18. Februar 2022 über die «Informatiksicherheit RUAG – Situation 2021» nehmen wir nach Artikel 158 des Parlamentsgesetzes nachfolgend Stellung.

Wir versichern Sie, sehr geehrte Frau Kommissionspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

30. März 2022

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Ignazio Cassis
Der Bundeskanzler: Walter Thurnherr

Stellungnahme

1 Ausgangslage

Die Geschäftsprüfungskommission des Nationalrates (GPK-N) hat am 22. Februar 2022[1] ihren Bericht «Informatiksicherheit RUAG − Situation 2021» veröffentlicht. Der Bericht geht insbesondere auf den Schutz von militärischen und anderen sensitiven Daten bei den Konzerneinheiten der RUAG und auf die Kommunikation des Bundesrates sowie des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) und des Eidgenössischen Finanzdepartements (EFD) als Eignervertreter ein.

Der Bericht der GPK-N geht zurück auf einen Beitrag in der Rundschau des Schweizer Fernsehens, in welchem ausgeführt wurde, dass es Hackern gelungen sei, in das Netzwerk der RUAG International Holding AG (RUAG International) einzudringen. Weil zahlreiche Verbindungen zur RUAG MRO Holding AG (RUAG MRO) bestünden, sei damit auch ein Zugriff auf sensitive Daten der Armee möglich.

Die GPK-N kommt zum Schluss, dass es entgegen der Darstellung der Rundschau keine erhärteten Belege für einen mutmasslichen Hackerangriff auf die RUAG International im Frühjahr 2021 gibt. Die RUAG International erkannte jedoch aufgrund umgehend ausgelöster Prüfungen schwerwiegende Sicherheitsmängel. Weil dagegen sofort Massnahmen ergriffen und diese auch externen Härtetests unterzogen wurden, hat die RUAG International nach Ansicht der Kommission angemessen reagiert. Die GPK-N empfiehlt dennoch zusätzliche Massnahmen, um das Risiko des Abflusses von Daten weiter zu reduzieren.

Zudem ist die GPK-N der Frage nachgegangen, ob das EFD und das VBS im Rahmen dieses Vorfalls die Interessen des Bundes gewahrt hätten und ob der Bundesrat und insbesondere das VBS sie transparent und korrekt über den Stand der Entflechtung und der Informatiksicherheit bei der RUAG informiert hätten. Die GPK-N attestiert den beiden Departementen eine angemessene Reaktion auf den Beitrag der Rundschau. Gleichzeitig bemängelt die Kommission, dass die Kommunikation hinsichtlich der Entflechtung und der Informatiksicherheit ihr gegenüber transparenter hätte erfolgen müssen.

Insgesamt formuliert die GPK-N zwei Empfehlungen und ersucht den Bundesrat um eine Stellungnahme bis spätestens am 30. März 2022.

1 BBl **2022** 491

2 Stellungnahme des Bundesrates zur Umsetzung der Empfehlungen vom 18. Februar 2022

Zu den Empfehlungen nimmt der Bundesrat wie folgt Stellung:

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.

Einleitend kann festgehalten werden, dass eines der Hauptziele der Entflechtung war, dass nur noch die RUAG MRO Zugriff auf sicherheitsrelevante Daten der Armee hat. Beim ersten Schritt der Informatik-Entflechtung, dem sogenannten «Cut-Over» im April 2020, wurde das Gros der Daten migriert. Dieser Schritt ermöglichte es der RUAG MRO dank der Migration in den Sicherheitsperimeter der Führungsunterstützungsbasis der Armee (FUB), von einem erhöhten Sicherheitsstandard zu profitieren und so weit wie möglich unabhängig vom Netz der RUAG International ihren Betrieb aufzunehmen.

Der Bundesrat betont in diesem Zusammenhang, dass die sicherheitsrelevanten Daten der Armee heute nur noch von der RUAG MRO bearbeitet werden. Restdaten, welche noch auf Alt-Systemen der RUAG International lagerten, wurden nicht mehr bearbeitet. Vielmehr wurden diese Restdaten in einem separaten Projekt, mit welchem die Systeme manuell «durchforstet» wurden, gezielt gesucht und individuell gelöscht. Die Eidgenössische Finanzkontrolle (EFK) hat 2021 in ihrem Prüfbericht zur Informatiksicherheit der RUAG MRO[2] das Vorgehen detailliert geschildert, den Umfang abgeschätzt und die Brisanz der Restdaten eingeordnet. Sie ist unter anderem zum Schluss gekommen, dass das Konzept für die Löschung der Daten auf den Systemen der RUAG International «zweckmässig aufgebaut» sei.

Dem Bundesrat ist die Sensitivität eines potenziellen Datenabflusses bewusst. Das EFD und das VBS begleiten das Entflechtungsprojekt in seiner ganzen Komplexität deshalb eng. Die Eignerstellen verlangten sowohl von der RUAG MRO als Dateninhaberin, die für die Bereinigung verantwortlich ist, als auch von der RUAG International, dass die definitive Datenbereinigung mit grösster Sorgfalt durchgeführt wird. Dabei war eine gewisse Sequenzierung unvermeidlich. So konnte beispielsweise die endgültige Datenbereinigung nicht vor dem «Cut-Over» erfolgen. Danach wurden die sicherheitsrelevanten migrierten Daten erfasst, systematisch klassifiziert und bereinigt. Dazu gehörte auch das Erfassen und Bereinigen von Daten in Back-Ups, Archiven sowie persönlichen Shares, Mailboxen und Transfer Shares.

2 EFK (2021): Prüfung der Informatiksicherheit RUAG MRO Holding AG vom 22. Februar 2021 (EFK-20431): www.efk.admin.ch > Publikationen > Sicherheit & Umwelt > Verteidigung und Armee > Informatiksicherheit – RUAG MRO Holding AG.

Die RUAG MRO hat zudem ein externes Audit in Auftrag gegeben, das zum Ziel hat, die Eigenständigkeit und Funktionalität der entflochtenen IT-Systeme zu überprüfen. Ferner hat die EFK in ihrem Jahresprogramm 2022 eine weitere Prüfung der Informatiksicherheit der RUAG MRO angekündigt.[3]

Bei der RUAG International wurde ein neuer Chief Information Security Officer eingesetzt, der den Auftrag hat, bei den einzelnen Devestitionen den sorgfältigen Umgang mit den Daten sicherzustellen. Die Eignerstellen haben in diesem Zusammenhang die RUAG International aufgefordert, vor den einzelnen Verkäufen von Unternehmensteilen durch externe Fachleute prüfen zu lassen, ob die RUAG International angemessene Vorkehrungen getroffen habe, um die ungewollte Weitergabe sensitiver Daten zu vermeiden.

Zudem kann grundsätzlich festgehalten werden, dass die Verkäufe von Unternehmensteilen der RUAG International aufgrund der damit verbundenen Komplexitätsreduktion der IT-Systeme letztlich das Risiko für Datenabflüsse laufend verkleinern.

Der Bundesrat ist der Ansicht, dass damit zielführende Massnahmen zum Schutz von militärischen und anderen sensitiven Daten getroffen wurden. Er hält die Empfehlung 1 somit für umgesetzt.

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.

Der Bundesrat ist stets bestrebt, die Transparenz im Informationsaustausch mit den Oberaufsichtskommissionen zu gewährleisten und erfüllt dieses Anliegen nach bestem Wissen und Gewissen. Er weist an dieser Stelle darauf hin, dass gerade hinsichtlich der Herausforderungen bei der Entflechtung der RUAG im Bericht des Bundesrates über die Erreichung der strategischen Ziele für die BGRB Holding AG (RUAG) 2020[4] der Arbeitsfortschritt präzise und offen dargelegt wurde. So wurde die Umsetzung des strategischen Ziels 2.1.3, gemäss welchem der Bundesrat erwartet, dass «die Beteiligungsgesellschaft: [...] die verbleibenden Arbeiten der Entflechtung zügig vorantreibt und bis spätestens Ende 2021 abschliesst», detailliert erläutert.

Der Übertrag der Informatik von RUAG MRO in den Sicherheitsperimeter der FUB im April 2020 sowie die fast gleichzeitig erfolgte «Bilanzspaltung», mit der nach der operativen und rechtlichen Trennung der RUAG MRO und RUAG International auch deren Aktiven und Passiven aufgeteilt wurden, bildeten die zentralen Meilensteine der

3 Jahresprogramm Eidgenössische Finanzkontrolle 2022, S. 12: www.efk.admin.ch > Publikationen > Allgemeine Kommunikation > Jahresprogramme > Jahresprogramm 2022.

4 Bundesrat (2020): Bericht des Bundesrates über die Erreichung der strategischen Ziele für die BGRB Holding AG (RUAG) im Geschäftsjahr 2020 vom 19. März 2020 (vertraulicher Bericht).

Entflechtung. Die Bereinigungsarbeiten und noch ausstehenden Schritte wie das Rebranding wurden dann im September 2020 in einem «zweiten Entflechtungsschritt» zusammengefasst. Grund dafür war, dass diese mit Blick auf das Ziel, die Arbeiten zugunsten der Armee in einer sicheren IKT-Umgebung ausführen zu können, von nachgeordneter Bedeutung waren und die Entflechtung seit Mitte 2020 in den wesentlichen Teilen vollzogen wurde.

Heute kann festgehalten werden, dass die Entflechtung der RUAG erfolgreich durchgeführt wurde. Die EFK stellt ebenfalls ein gutes Zeugnis aus, indem sie zum Beispiel Kapitel 2.1 in ihrem Prüfbericht zur Informatiksicherheit der RUAG MRO wie folgt übertitelt: «Die Projektziele wurden qualitativ und quantitativ erreicht».[5]

Der Bundesrat nimmt das Anliegen der GPK ernst, transparent und zeitnah über die Herausforderungen der RUAG zu kommunizieren. Er ist bestrebt, in seiner Berichterstattung zur Erreichung der strategischen Ziele der RUAG und in jeder weiteren Kommunikation zur RUAG präzis über die für den Bund wesentlichen Entwicklungen zu informieren.

Der Bundesrat wird somit dem Anliegen der GPK-N nach einer transparenten Kommunikation in Zukunft noch grössere Beachtung schenken. Zusammenfassend hält der Bundesrat damit beide Empfehlungen für erfüllt.

5 Vgl. Fussnote 2