Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Generalsekretariat VBS
Kommunikation VBS

Anfrage SRF Rundschau (D. Meier und N. Blaser) – Informatiksicherheit RUAG

Stellungnahme VBS

15. Mai 20021

1) Entflechtung der RUAG auch im Zusammenhang mit der Informatiksicherheit

Im Frühling 2016 wurde öffentlich bekannt, dass der bundesnahe Betrieb RUAG Holding AG von einem Cyberangriff betroffen war, der potenziell zu einer schwerwiegenden Beeinträchtigung der Informatiksicherheit führen konnte. Der Bundesrat hat nach Bekanntwerden des Sicherheitsvorfalls zum ersten Mal im Frühjahr 2016 Massnahmen beschlossen.

Im März 2018 beschloss der Bundesrat die Entflechtung der RUAG Holding AG. Das bedeutet konkret, dass diejenigen Geschäftsbereiche der RUAG, die hauptsächlich für die Schweizer Armee tätig waren, und diejenigen, die sich auf dem freien Markt bewegten, organisatorisch getrennt werden sollten. Sämtliche sicherheitsrelevanten Daten und Informationen der Schweiz sollten nur noch von der RUAG MRO Holding AG bearbeitet werden, deren Informatik in den Sicherheitsperimeter des Bereichs Verteidigung (Sicherheitsperimeter V) integriert werden sollte.

Im Zusammenhang mit dem Cyber-Vorfall gab es mehrere Untersuchungen, u.a. von der GPK. Oft zitiert wird der EFK-Bericht 18517. Die Prüfungstätigkeit der EFK für diesen Bericht fand zwischen Ende Mai und Ende Juni 2018 statt. Der Bericht stellte zu diesem Zeitpunkt fest, die Informatiksicherheit sei noch nicht gewährleistet. Der Bundesrat war wie erwähnt kurz zuvor zum gleichen Schluss gekommen und hatte im März 2018 beschlossen, dass die Sicherheit der für die Verteidigung relevanten Daten nur durch einen Transfer der IT der RUAG MRO in den Sicherheitsperimeter V gewährleistet werden konnte.

Seither wurde die Entflechtung der RUAG umgesetzt. Heute, drei Jahre später, ist der Hauptteil der Arbeiten abgeschlossen. Die direkten Verbindungen zwischen RUAG MRO und RUAG International sind gekappt.

Informationen zur Informatiksicherheit aus den Jahren 2016 oder 2018 sind damit überholt. Die Situation ist heute eine andere, drei Jahre nach Beginn der Entflechtung und nach einer Investition von zweistelligen Millionenbeträgen in eine neu aufgesetzte IT und in den sicheren Transfer der Daten in den Sicherheitsperimeter V.

2) Der Transfer der IT wurde mit höchster Sorgfalt vorgenommen

Es trifft nicht zu, dass Daten «1:1 kopiert» wurden. Die FUB hat umfangreiche Vorsichtsmassnahmen getroffen, bevor sie es zugelassen hat, dass Daten der RUAG MRO in den Sicherheitsperimeter V migriert wurden. Sämtliche Daten wurden nach ihrer Identifikation und vor der Übernahme in eine Quarantäne gebracht und dort auf Schadsoftware überprüft.

Konkret: Um die Verschleppung von Malware auszuschliessen, durften keine Daten direkt vom System von RUAG in den Sicherheitsperimeter V kopiert werden. Deshalb wurden diese über extra dafür eingerichtete Datenleitungen in einen Quarantänebereich der FUB transferiert, dort auf Malware gescannt und erst dann auf die neuen Systeme übertragen.

Es kann heute festgehalten werden, dass dank dieser sorgfältigen Vorgehensweise keine Schadsoftware migriert wurde. Die FUB prüft auch die Zugänge zu ihren Systemen sehr genau. Es gibt keine unkontrollierten Schnittstellen oder Zugriffsmöglichkeiten via die RUAG International mehr.

Die IT der RUAG Real Estate wurde nicht in den Sicherheitsperimeter V migriert. Das wäre nicht sachgerecht gewesen – es ist für den Immobilien-Teil von RUAG MRO kein so hoher Schutzbedarf gegeben. Es gibt nur vereinzelte Zugänge von der IT der RUAG Real Estate in diejenigen Systeme der RUAG MRO, so zum Beispiel für die Nutzung der HR-Daten im SAP. Diese Schnittstellen werden gleich geschützt und kontrolliert, wie die Schnittstellen zu allen anderen externen Partnern in der heutigen vernetzten Welt. Die einzelnen spezialisierten Anwendungen und Insellösungen, die unter dem Begriff Technisch-Wissenschaftliche Infrastruktur (TWI) zusammengefasst werden, verbleiben auf dem Netz der RUAG International bis sie analysiert, bereinigt und sicherheitsmässig auf einen Stand gebracht sind, der die kontrollierte Überführung in den Sicherheitsperimeter V erlaubt.

3) Für RUAG MRO und RUAG International gelten nicht mehr die gleichen Standards

RUAG International soll mittelfristig privatisiert werden. Sie bearbeitet keine Daten mehr, die für die Verteidigung der Schweiz relevant sind. Ihre IT-Sicherheit soll deshalb einem Industriestandard entsprechen.

Für ihren eigenen Schutz ist die RUAG International zuständig. Es liegt nicht mehr in der Verantwortung des Bundes, sicherzustellen, dass RUAG International ausreichend gegen Cyber-Risiken geschützt ist. Damit sind Fragen zur IT von RUAG International auch nicht durch das VBS zu beantworten; das heisst unter anderem die Fragen zur Auslagerung nach Indien oder zum Sicherheitsprogramm «Impact».

Die zuständigen Bundesratsmitglieder (Chefin VBS und Chef EFD) lassen sich aber im Rahmen der Eignergespräche über den Stand der IT-Sicherheit von RUAG International regelmässig informieren. Sie nehmen auch Kenntnis von den Ergebnissen verschiedener Audits, die von externen Firmen durchgeführt wurden.

Darauf hinzuweisen ist zudem, dass mit der Entflechtung auch die Rolle des Eigners aufgeteilt worden ist. Das VBS hat die Federführung für die Kontrolle und Steuerung der BGRB Holding AG und für die Geschäfte im Bereich der RUAG MRO, das EFD für die Geschäfte der RUAG International.

Damit sind Fragen zu Ruag International und insbesondere zu deren geplanten Privatisierung nicht durch das VBS zu beantworten

4) Die Entflechtung ist nicht vollständig abgeschlossen, aber die Sicherheitsrisiken sind gebannt

Der Begriff der Entflechtung wurde nicht immer im genau gleichen Sinne gebraucht. Wenn mit der Entflechtung der Übertrag der Informatiksysteme in den Sicherheitsperimeter V

gemeint ist, so hat diese Migration mit dem sogenannten „Cut-Over“ über Ostern 2020 stattgefunden. Damit konnten die IT-Systeme der RUAG International und der RUAG MRO getrennt werden. Wenn mit Entflechtung das Gesamtprojekt gemeint ist, gibt es noch lose Enden, die bereinigt werden müssen.

Deshalb haben VBS und Bundesrat noch im März 2021 letztmalig kommuniziert, dass die Entflechtung «weitgehend abgeschlossen» sei (Bundesrat nimmt Berichterstattung über die Zielerreichung der RUAG im 2020 zur Kenntnis (admin.ch). Ein anders Beispiel ist die Stellungnahme des Bundesrates zum zweiten Bericht der GPK-N zum Cyberangriff vom Februar 2020, in welcher der Bundesrat bestätigt, dass die Entflechtung «planmässig voranschreitet» (Entflechtung und Weiterentwicklung der RUAG nach dem Cyberangriff auf Kurs (admin.ch)).

Die Behauptung, die Entflechtung sei als abgeschlossen dargestellt worden, ist falsch.

Für den entflochtenen Teil der RUAG, welcher sich seit April 2020 auf dem Sicherheitsperimeter V befindet, sind die Sicherheitsmechanismen auf dem gleichen Schutzgrad wie für die Schweizer Armee. Ein erfolgreicher Cyber-Angriff, bei dem sich Unberechtigte Zugang zu Informationen verschaffen, kann nie vollständig ausgeschlossen werden. Auch erfolgreiche Angriffe mit Ransomware können nicht kategorisch ausgeschlossen werden, allerdings sind Teilsysteme untereinander durch Sicherheitsmechanismen getrennt, so dass eine flächendeckende Ausbreitung unterbunden werden kann.

Nun werden Projekte nachfolgen, damit die Informationssicherheit weiter erhöht werden kann. Dazu gehört die Bereinigung von Archiven, um das Entflechtungsprojekt vollumfänglich abschliessen zu können. Mit entsprechenden Nachfolgeprojekten werden diese und weitere wichtige Aspekte zur kontinuierlichen Erhöhung der Informationssicherheit erarbeitet.

5) Hinweise zu einzelnen Themen

*Über das Ruag-Netzwerk gibt es offenbar einen Zugang zu **Polycom.** Ein Angreifer könnte die Kommunikation unter den Blaulichtorganisationen lahmlegen. Können Sie das ausschliessen?*

- Die RUAG MRO hat den exklusiven Vertriebskanal für die Polycom-Funkgeräte in der Schweiz. Weiter ist die RUAG MRO Reparatur- und Servicecenter für Polycom-Funkgeräte in der Schweiz (Hersteller ist Airbus, Airbus hat die RUAG MRO ausgewählt und befähigt). Zudem wird das Alarmierungs- und Meldungsvermittlungssystem Vulpus Telematik durch die RUAG MRO weiterentwickelt und sie ist für den Betrieb gegenüber armasuisse verantwortlich.

- Für beide Systeme gibt es kontrollierte Zugänge für Wartungs- und Instandhaltungsarbeiten aus dem Sicherheitsperimeter V. Bei einem Cyber-Angriff kann die Verbreitung von Schadsoftware über die Schnittstellen zu anderen Systemen nicht kategorisch ausgeschlossen werden, allerdings sind Teilsysteme untereinander durch Sicherheitsmechanismen getrennt, so dass eine flächendeckende Ausbreitung unterbunden werden kann.

*Über das Ruag-Netzwerk gibt es offenbar einen Zugang aufs Kartenmaterial von **Swisstopo.** Angreifer könnten die Daten manipulieren, Berge kleiner machen. Können Sie das ausschliessen?*

- Die RUAG beziehungsweise die heutige RUAG MRO hat für die Entwicklung und den Betrieb zahlreicher Rüstungssysteme entsprechendes Kartenmaterial (Geodaten) von swisstopo bezogen. Bedingt durch die grosse Datenmenge wurde das Kartenmaterial in der Regel «offline» geschickt (per HDD-Disk). Nach der Lieferung liegt die Verantwortung für die Speicherung und Weiterverarbeitung der swisstopo-Geodaten beim Datenempfänger, in diesem Fall bei der RUAG MRO.

- Die Geodaten von swisstopo wurden teilweise seitens RUAG MRO auch direkt über sogenannte Geodienste aus dem Geoportal des Bundes (map.geo.admin.ch) genutzt und in gewisse Systeme integriert. Es handelt sich dabei um einen öffentlichen Zugang über das Internet welcher von über 25 Millionen Nutzern pro Jahr verwendet wird.

- Einen direkten Datenbezug aus den Produktionssystemen von swisstopo für die RUAG MRO gab es nie. Unberechtigte Zugriffe in diesem Zusammenhang sind nicht bekannt.

- Eine schwerwiegende Manipulation der Geodaten innerhalb der swisstopo-Produktionssysteme, die unbemerkt bleibt, hält swisstopo angesichts der sehr grossen Nutzeranzahl ihrer Geodaten für unwahrscheinlich.

*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?*

- Der Cyberangriff von 2016 ist aufgearbeitet worden. Wir verweisen Sie auf die Berichte der GPK und die Stellungnahmen des Bundesrates (RUAG: Bundesrat nimmt Stellung zum Bericht über den Cyber-Angriff (admin.ch) und Entflechtung und Weiterentwicklung der RUAG nach dem Cyberangriff auf Kurs (admin.ch)) und machen darüber hinaus auch aus Sicherheitsgründen keine Aussage zu weiteren möglicherweise betroffenen Organisationen.