Der Selbstverteidigungskonzern

Ein Informatiker warnt den Rüstungskonzern Ruag immer wieder vor gravierenden Sicherheitsproblemen. Er erhält kein Gehör, sondern die Kündigung. Die Waffenschmiede der Schweiz kehrte Probleme bei der Cybersicherheit jahrelang unter den Teppich – das hat Folgen bis heute.

Von Adrienne Fichter und Priscilla Imboden, 31.05.2022

Im September 2014 stösst ein IT-Systemadministrator des Schweizer Technologie- und Rüstungskonzerns Ruag auf ein Dokument, das er eigentlich nicht sehen dürfte. Der Inhalt des Dokuments: technische Daten des Radarsystems Florako, entwickelt von Thales Raytheon Systems, einem Joint Venture der US-amerikanischen Firma Raytheon Company und der französischen Thales S.A. Auf die Unterlagen dürften eigentlich nur wenige, ausgewählte Personen Zugriff haben.

Warum also lag dieses vertrauliche Dokument nicht klassifiziert auf dem Ruag-Server?

Gut acht Jahre später steht der Mann an einem sommerlichen Morgen vor dem Regionalgericht Bern-Mittelland. Der Grund für den Gerichtstermin im Mai 2022: Er hat die Ruag wegen missbräuchlicher Kündigung verklagt.

Ein öffentlicher Schlagabtausch mit seinem ehemaligen Arbeitgeber bleibt aber aus: Anwesende Medienschaffende werden schon nach vier Minuten gebeten, den Saal zu verlassen, damit die Parteien über einen Vergleich verhandeln können. Und solche Vergleichsverhandlungen sind nicht öffentlich.

Dabei geht es in diesem vermeintlichen Arbeitskonflikt durchaus um Fragen von öffentlichem Interesse. Denn die Sicherheitsprobleme bei der Ruag beschäftigen die Schweizer Politik seit Jahren. 2016 löste ein Hackerangriff auf den Konzern grosse Aufregung aus. Vernachlässigte die Ruag also über Jahre ihre Cybersicherheit? Hätte sie über gravierende Sicherheitslücken in ihrem IT-System gewarnt sein müssen?

Die Fragen bleiben an diesem Morgen vor dem Berner Gericht unbeantwortet. Nach vier Stunden einigen sich beide Parteien auf einen Vergleich, über seinen Inhalt vereinbaren sie Stillschweigen.

Und doch lässt sich die lange Vorgeschichte dieser Einigung rekonstruieren. Der Republik liegen die Klageschrift und verschiedene Dokumente vor, die der Ruag-Systemadministrator Parlamentariern und auch der Gewerkschaft Unia aushändigte, die seine arbeitsrechtliche Klage mitfinanzierte. Diese Unterlagen und Gespräche mit weiteren Quellen erlauben ei-

nen seltenen und detaillierten Einblick in den sorglosen Umgang der Ruag mit geschützten Daten. Sie zeigen den mangelnden Willen des Waffen- und Technologiekonzerns, diese Sicherheitsprobleme zu lösen.

Die Verfehlungen und Nachlässigkeiten wirken bis heute nach.

Offen wie ein Telefonbuch

Die Geschichte beginnt so: B. G. (sein Name ist der Republik bekannt) verwaltet im Jahr 2014 im Auftrag des damaligen Ruag-CEO Urs Breitmeier das Datenmanagement der Ruag Defence, der Rüstungssparte des Konzerns. Systemadministrator B. G. ist auf *Computer-aided Design* (CAD) spezialisiert. Damit lassen sich etwa 3-D-Visualisierungen von technischen Daten erstellen, in diesem Fall von geheimen Waffensystemen.

Beim Aufbau einer zentralen Datenmanagement-Plattform merkt der Systemadministrator, dass etwas nicht stimmt. Eigentlich sollte er keinen Zugang haben zum oben erwähnten vertraulichen Dokument mit den technischen Daten eines Radarsystems. Er stellt bald fest, dass es sich nicht um einen Einzelfall handelt: Die ganze Datenbank ist voll von unverschlüsselten Datenablagen und damit offen wie ein Telefonbuch für fast alle Ruag-Mitarbeitenden. Mithilfe der Suchfunktion hätte er theoretisch sämtliche technischen Daten von Rüstungsgütern einsehen können.

B. G. meldet den Fund an seinen Vorgesetzten. Es folgt eine Sitzung mit dem obersten Cybersicherheitsverantwortlichen. Dieser hält im Dezember 2014 in einer E-Mail fest, eine Analyse habe «in einigen Bereichen dringenden Handlungsbedarf aufgezeigt». In einer Aktennotiz dazu schreibt er, die «nachvollziehbare Vergabe von Berechtigungen» sei «nicht ausreichend geregelt» und «das Sicherheitsprotokoll des Geheimschutzverfahrens nicht eingehalten» worden. «Die aufgezeigten Verwundbarkeiten und Nicht-Konformitäten führen zu einem erheblichen Risiko, dass Daten (...) Unberechtigten zugänglich gemacht werden.» Dies könne zu einem «erheblichen wirtschaftlichen Schaden» führen, «wenn geistiges Eigentum der Ruag kopiert wird oder die Daten durch Unberechtigte manipuliert werden».

In der Aktennotiz findet sich ausserdem ein wichtiger Vermerk: Die entdeckten Sicherheitslücken seien nicht erst durch das Datenmanagement-Projekt entstanden, an dem B. G. arbeitete.

Im Klartext: Die Lücken existierten wohl schon lange vor 2014.

Dokumente widersprechen der Ruag

Als die Ruag davon erfährt, unternimmt sie wenig, um das Problem zu lösen. Aber einiges, um den Übermittler des Problems zu bremsen. Laut Klageschrift, die der Republik vorliegt, fordert sie den Systemadministrator «knapp, aber unmissverständlich» auf, «keine weiteren Handlungen zu unternehmen».

Das fällt dem gewissenhaften Mitarbeiter schwer. Denn ein Jahr später entdeckt er etwas, das ihn noch mehr beunruhigt: Konstruktions- und Modelldaten von Waffensystemen wie der Panzerhaubitze M109, vom Maschinengewehr des Typs Browning M2 und den F/A-18-Kampfjets aus den USA sowie Informationen über den Leopard-Kampfpanzer aus Deutschland und den Mowag-Piranha-Radschützenpanzer aus der Schweiz.

Auch auf diese militärisch klassifizierten Daten hat B. G. ohne weiteres Zugriff.

Er interveniert erneut. Nicht nur einmal, sondern immer wieder, über Jahre. Aber mit zunehmender Ernüchterung muss er feststellen, dass die Ruag das Problem vor sich herschiebt statt es zu lösen.

Sein Vorgesetzter sieht das anders. Er antwortet dem Systemadministrator auf eine seiner Mahnungen im März 2015, dass nun ein Berechtigungskonzept erstellt werde und die CAD-User – also alle, die mit 3-D-Modellen und Rüstungsdaten arbeiten – daran erinnert worden seien, wie mit militärischen Informationen umzugehen sei. Alle Personen mit Zugriff auf Datenablagen seien nochmals grundlegend überprüft worden.

Mit anderen Worten: Bis zu diesem Zeitpunkt existierte kein Berechtigungskonzept für den Zugang zu Daten über militärisch geschützte Waffensysteme.

Die Ruag streitet das auf Anfrage ab: «Zugriffsberechtigungen auf Daten oder Informationen sind seit vielen Jahren streng geregelt – auch lange vor 2015.»

Dokumente, die der Republik vorliegen, widersprechen dieser Darstellung: Sie belegen, dass die Ruag versäumte, Zugriffs- und Administratorenrechte festzulegen und Betriebsgeheimnisse zu kennzeichnen. Infolgedessen hatten alle Mitarbeitenden Zugriff auf die zentrale Datenverarbeitungsplattform der Ruag Defence.

Systemadministrator B. G. macht sich immer grössere Sorgen, auch um sich selbst. Denn Daten über US-Waffensysteme unterstehen einem international gültigen Reglement namens Itar. Es schreibt vor, dass der Zugriff auf technische Daten US-amerikanischer Verteidigungs- und Militärtechnologien auf Bürgerinnen der USA beschränkt werden muss. Für alle nicht amerikanischen Mitarbeitenden gilt: Sehen sie Pläne von US-Waffensystemen, müssen sie das den US-Behörden melden. Tun sie es nicht, drohen ihnen Geldstrafen oder bis 10 Jahre Haft.

Ausserdem stellt der offene Zugang zu diesen Daten ein Sicherheitsrisiko für die Ruag dar: Je mehr Leute Zugriff auf klassifizierte Daten haben, desto höher ist das Risiko, dass korrumpierbare Mitarbeitende geheime Rüstungsdaten entwenden und weiterverkaufen. Ein Berechtigungsmanagement mit klaren Administratorenrechten wäre daher eine der wichtigsten Sicherheitsmassnahmen. Doch der Schweizer Rüstungskonzern, der laut seinem Geschäftsbericht in vierzehn Ländern auf vier Kontinenten tätig ist, erfüllt sie nicht.

Im Gegenteil: Die Ruag sah offenbar nicht einmal ein Problem darin, auch an zweifelhaften Standorten mit heiklen Daten zu hantieren.

Der Konzern plante, Waffenteile in einem 3-D-Drucker-Zentrum in Abu Dhabi in den Vereinigten Arabischen Emiraten herzustellen. Als B. G. davon erfährt, ist er in höchstem Masse beunruhigt. Er weist seine Vorgesetzten einmal mehr auf Sicherheitslücken hin: Wenn ein Mitarbeiter klassifizierte US-Daten nach Abu Dhabi mitbringe, würden diesem nach Itar-Regeln mehrere Jahre Gefängnis blühen.

Das Projekt in Abu Dhabi kam letztlich doch nicht zustande. Warum? Dazu wollte die Ruag Defence gegenüber der Republik keine Stellung nehmen.

Ein Hackerangriff sorgt für Aufregung

In der Theorie wusste der Rüstungskonzern, wie er hätte vorgehen müssen. Er hielt das in der internen Weisung «Schutz von Information» sogar ausdrücklich fest: «Im Speziellen ist zu beachten, dass auch innerhalb der Ruag klassifizierte Informationen nur berechtigten Personen zugänglich gemacht werden dürfen. Dies gilt namentlich auch für die Erteilung von Zugriffsberechtigungen im IT-Netz.»

Systemadministrator B. G. übt weiterhin intern Kritik und macht auf diese Weisung aufmerksam. Deshalb kommt es in der Folge zu weiteren Treffen, im Frühling 2016 mit Kadermitgliedern der Ruag Defence. Aus internen Dokumenten geht hervor, dass das Management dabei einräumte, dass durch «die Internationalisierung breitere Zugriffe auf Daten möglich sind, obwohl der Datenbestand nicht geprüft wurde». Ausserdem wurde bei dem Treffen schriftlich festgehalten, dass die Ruag keinen guten Überblick über die Datenbestände habe.

Bald darauf sollten die Sicherheitsprobleme bei der Ruag auch der breiten Öffentlichkeit bekannt werden.

Im Mai 2016 ist es so weit: Der Bundesrat informiert die Öffentlichkeit, dass Hacker mit einer Spionagesoftware in Ruag-Systeme eingedrungen sind. Gemäss dem Nachrichtendienst begann der Cyberspionage-Angriff bereits im Dezember 2014. Die Bundesanwaltschaft leitet eine Strafuntersuchung gegen unbekannt ein. Es ist bis heute nicht nachgewiesen, wer die Eindringlinge waren und was für Daten sie stahlen. Eine Vermutung lautet, es sei die russische staatliche Hackergruppe APT28 alias Turla gewesen: Sie habe Zugang zu Informationen über westliche Waffensysteme erhalten wollen.

Haben dieselben Datenschutzprobleme, die der interne Whistleblower B. G. kritisierte, den Hackern das Eindringen in die Ruag-Systeme erleichtert?

Diese Frage lässt sich nicht abschliessend beantworten. Denn die Hacker waren gemäss heutigem Wissensstand tief in die Systeme eingedrungen. Ob eine saubere Klassifizierung der militärisch geschützten Dokumente und die klare Zuteilung der Administratorenrechte einen solchen Datenabfluss verhindert oder zumindest verringert hätten, bleibt also Spekulation. Insider bei der Ruag, die B. G. den Rücken stärkten und die Sicherheitslücken ebenfalls als gravierend einschätzten, verneinen allerdings einen klaren Zusammenhang.

B. G. wird nach dem Bekanntwerden des Ruag-Hacks noch mulmiger zumute. Er wendet sich an den Rechtsdienst, wie in der Klageschrift zu lesen ist: «B. G. führte aus, dass durch das Einbinden von sensitiven, insbesondere auch militärisch klassifizierten Informationen in das SAP-System Geheimhaltungsvorschriften verletzt werden, die auch für ihn persönlich militärstrafrechtliche Konsequenzen haben könnten.»

Er verlangt eine Haftpflichtentlastung, damit er nicht verantwortlich gemacht werden kann, falls es zu Klagen aus den USA käme wegen nicht vorschriftsgemäss geschützter US-Rüstungstechnologie. Sein Arbeitgeber vertröstet ihn.

«Ja und??»

B. G. gibt nicht auf. Er weist hartnäckig weiter auf die Sicherheitsprobleme hin, die nach seiner Erkenntnis damals nach wie vor ungelöst sind, wie ehemalige Mitarbeitende bestätigen.

Am 16. September 2016 fand laut Dokumenten, die der Republik vorliegen, eine weitere Besprechung statt. Wieder hiessen die Traktanden: Datensicherheit und unverschlüsselte vertrauliche Daten in der CAx Domaine, also der von B. G. betreuten Datenmanagementplattform der Ruag Defence. «Im Anschluss daran wurde beschlossen, dass die Fachstelle IOS (Informations- und Objektschutz GS-VBS) des Bundes nicht sofort informiert, aber eine Task Force eingesetzt würde.»

Das heisst: Man kehrte das Problem unter den Teppich. Der Bund, der Haupteigner des Ruag-Konzerns, sollte nichts vom internen Datenchaos erfahren.

Mehr noch: Weitere interne Dokumente der Ruag offenbaren eine erstaunliche Sorglosigkeit rund um die Datensicherheit.

In einer E-Mail vom 20. September 2016 bemüht sich B. G. um eine Lösung, um den Datenzugriff korrekt zu regeln. Insbesondere soll der Zugriff aus anderen Ländern, namentlich Deutschland und Frankreich, auf die Daten in der Schweiz gemäss den Vorgaben des Staatssekretariats für Wirtschaft Seco zum Kriegsmaterialgesetz eingeschränkt und sichergestellt werden. Ziel müsse es sein, so B. G., dass die Daten, die einer Geheimhaltungsverpflichtung unterstehen, nicht von Unberechtigten eingesehen und ins Ausland übermittelt werden könnten.

Dem Systemadministrator wird daraufhin mitgeteilt, dass die Daten nicht gesperrt werden könnten. Erstaunt fragt er nach, «ob somit etwa Ruag-Mitarbeiter in Deutschland und Frankreich ohne weiteres alle (geheimen) Daten in der Schweiz einsehen könnten». Laut der Klageschrift fragt er weiter, wie das unterbunden werden könne, wenn doch vom Staatssekretariat für Wirtschaft keine Freigabe für einen Know-how-Transfer gemäss Kriegsmaterialgesetz erfolgt sei.

Die Antwort, die B. G. darauf erhält, lautet lapidar: «Ja und??»

Mit anderen Worten: Die Ruag sah das Problem nicht und war folglich auch nicht bereit, es zu lösen.

Im Juli 2017 erkundigt sich B. G. erneut nach der Regelung der Zugriffsberechtigungen. Man antwortet ihm, «dass das Problem erkannt und (unverändert) in Arbeit ist; dies notabene seit 2014», wie es in der Klageschrift heisst.

Nun geht B. G. einen Schritt weiter und wendet sich im Oktober 2017 an den damaligen Ruag-CEO Urs Breitmeier. Dieser empfängt ihn in seinem Büro und hört ihm zu. Später schreibt er dem neuen Präsidenten der Ruag Holding, Remo Lütolf, und weist ihn darauf hin, dass Unklarheiten herrschten bei der Klassifizierung von militärisch geschützten Daten innerhalb der Ruag.

Dann folgt ein Paukenschlag: Der Bundesrat kündigt an, den bundeseigenen Waffen- und Technologiekonzern aufzuteilen: in die Ruag International und die Ruag MRO – unter anderem mit dem Ziel, die Cybersicherheit zu verbessern. Der internationale Teil soll verkauft werden (was inzwischen

teilweise geschehen ist), der nationale Teil unter dem Namen Ruag MRO in Bundesbesitz bleiben und weiterhin Dienstleistungen für die Schweizer Armee erbringen.

Das bringt grosse Herausforderungen für die Informatik mit sich: Die Datennetze der beiden Teile müssen entflechtet und getrennt werden. Eine knifflige Sache, vor allem da die Ruag nicht weiss, wo sich welche Daten befinden.

In diesem Zusammenhang erhält B. G. die Aufgabe, Netzwerkübergänge der Ruag in andere Netze wie jene des Verteidigungsdepartements oder des Bundesamts für Informatik zu prüfen. Wieder weist er auf die bekannten Schwachstellen hin.

Es ist das letzte Mal.

Alarmierender Geheimbericht der Aufsichtsbehörde

Im Herbst 2019 erhält B. G. die Kündigung. Die offizielle Begründung lautet, seine Stelle werde wegen Restrukturierungen weggespart. In Wahrheit wird die Stelle neu ausgeschrieben. Der ehemalige Systemadministrator verschickt seine Unterlagen verzweifelt an verschiedene Bundesparlamentarierinnen – und wird damit zum Whistleblower.

Wurde der unbequeme interne Warner mit der Kündigung abgestraft und abserviert?

B. G. war sich dessen sicher. Deshalb verklagte er die Ruag wegen missbräuchlicher Kündigung. Darüber reden darf der ehemalige Mitarbeiter nach dem Vergleich aber nicht.

Auch die Ruag spricht nicht über den Fall. Ein Sprecher der Firma teilt mit: «Wir haben uns mit B. G. geeinigt und eine Vereinbarung getroffen. Dazu äussern wir uns öffentlich nicht, dies haben wir mit B. G. so vereinbart.» Es sei der Firma ein wichtiges Anliegen, dass sich Mitarbeitende äussern, «wenn sie den Verdacht haben, dass gegen den Verhaltenskodex oder gegen anwendbares Recht verstossen wurde».

Im Nachgang lässt sich sagen: Es wäre besser gewesen, hätte die Ruag auf ihren Systemadministrator gehört. Denn die Probleme, die er über Jahre ansprach, wurden 2018 in einem alarmierenden Bericht der Eidgenössischen Finanzkontrolle (EFK) bestätigt.

Die Republik hatte Einsicht in den vertraulichen Bericht der Finanzkontrolle. Darin hält die EFK fest, dass die Ruag nicht wusste, wo sich militärisch geschützte Daten befanden und wer darauf Zugriff hatte: «Heute kann niemand eine verlässliche Auskunft geben, ob alle heiklen Daten bekannt und deren Dataowner bestimmt sind. Daher lebt die Ruag weiterhin mit einem erhöhten Risiko, dass heikle Daten durch unberechtigte Dritte behändigt werden könnten.»

Bei Ruag Defence habe die EFK Daten mit dem Klassifizierungsvermerk «Ruag vertraulich» unverschlüsselt in elektronischen Ablagen gesehen. Ob und wie weitgehend Mitarbeitende von ausserhalb der Schweiz auf solche Daten zugreifen könnten, habe nicht geklärt werden können.

Ausserdem weist die EFK in ihrem Bericht darauf hin, dass bei der Ruag die Zahl der mit Cybersecurity betrauten Mitarbeitenden eher knapp bemessen war. So seien bei voller Besetzung 11 Angestellte für die Cybersecurity zuständig. «Das erachtet die EFK für ein Unternehmen von über

9000 Angestellten als unzureichend.» Dies notabene zwei Jahre *nachdem* der Ruag-Hack bekannt wurde. Heute sagt die Ruag auf Anfrage: «Zur Anzahl unserer Cyber-Experten geben wir öffentlich keine Auskunft.»

Sind die Probleme jetzt gelöst? Nein

Der Frust von B. G. über die IT-Nachlässigkeiten bei der Ruag war kein Einzelfall, wie die EFK im vertraulichen Bericht feststellt: viele Spezialisten für Cybersicherheit hätten die Ruag in den letzten Jahren verlassen, wertvolles Wissen sei verloren gegangen. Ein ehemaliger Mitarbeiter sagt zur Republik: «Wenn etwas schiefläuft in der Ruag, wird es sofort als geheim deklariert. Dann wird im Hintergrund gebastelt und geschwitzt.» Anschliessend bestelle die Ruag Gefälligkeitsgutachten, und alles verschwinde unter dem Teppich mit dem Vermerk: «erfolgreich abgeschlossen».

Der Fall von B. G. liefert eine mögliche Erklärung, weshalb die Ruag bis heute mit Cybersicherheitsproblemen kämpft: Der Rüstungskonzern stellt interne Warner kalt und schaut weg, wenn Probleme auftauchen.

Zahlreiche Vorfälle jüngeren Datums lassen erahnen, dass solche Probleme weiterhin bestehen. Letztes Jahr berichtete die «Rundschau» von SRF über einen weiteren mutmasslichen Hack. Untersuchungen vermochten dies nicht zu bestätigen, brachten aber erneut «ernst zu nehmende Sicherheitslücken» zutage. Und Probleme mit dem Thema Administratorenrechte gab es auch bei anderen Ruag-Projekten: So fand das IT-Portal «Inside-IT» im März 2021 heraus, dass das E-Learning-System der Armee wegen einer falschen Konfiguration des Rollen- und Rechtemanagements dazu führte, dass ganze Datensätze offen einsehbar waren, darunter auch die AHV-Nummern von Rekruten.

Und wer betreibt dieses E-Learning-System? Die Ruag.

Die Republik berichtete im Februar dieses Jahres über eine weitere Sicherheitslücke: Ein Unbekannter verschickte im Namen des CEO von Ruag International eine E-Mail an Parlamentsmitglieder und die Redaktion der Republik. Das war dank unsicheren Voreinstellungen des Mail-Dienstes möglich, ohne überhaupt hacken zu müssen.

Kurz: Acht Jahre nach den ersten Warnungen von B. G. und sechs Jahre nach dem Auffliegen des Hackerangriffs hat die Ruag die Situation immer noch nicht im Griff.

Die Sache beschäftigt das Parlament nun schon seit Jahren. Die Finanzdelegation (FinDel) hat die Eidgenössische Finanzkontrolle immer wieder beauftragt, die Informatiksicherheit der Ruag zu untersuchen. Seit 2017 hat die EFK zehn Untersuchungen durchgeführt, nur eine davon ist öffentlich zugänglich, mit geschwärzten Stellen.

Für eine Entwarnung sei es noch etwas zu früh, sagt FDP-Ständerat Thomas Hefti, Präsident der Finanzdelegation, der Republik: «Das Thema ist bei uns noch pendent.» Seine Sorge sei, dass die Entflechtung möglicherweise nicht ganz vollständig verlaufen sei: «Die Daten dürfen nicht am falschen Ort sein oder an den falschen Ort hinkommen.» Deshalb warte die Finanzdelegation noch einen weiteren Bericht von der EFK ab.

Gemäss Ständerat Hefti ist es auch ein Anliegen der FinDel, sicherzustellen, dass Ruag International nach der geplanten Löschung der Daten über keine militärischen oder anderen sensitiven Daten mehr verfügt.

Und genau hier liegt das Problem: Wenn das nicht sichergestellt ist, dann können militärisch geschützte Daten bei einem allfälligen Verkauf der Ruag International ins Ausland gelangen. Damit hätte der Bundesrat bei der Aufteilung der Ruag das Problem nur ausgelagert statt gelöst. Und falls die Ruag MRO, die in die Informatiksysteme der Schweizer Armee integriert wird, weiterhin ein Einfallstor für Hacker bleibt, sind diese Daten auch in der Schweiz nicht geschützt.

Die Ruag und ihre Cyberlöcher – die leidige Geschichte ist noch lange nicht zu Ende.