Auch Bund verschlief Kampf gegen Cyber-Crime

15. Mai 2016

Von Henry Habegger, Schweiz am Sonntag

Die Hacker-Affäre um die Ruag könnte weit dramatischere Ausmasse haben als bisher bekannt.

Für Spott ist gesorgt. Am Freitag findet in Lausanne die «Swiss Cyber Risk Research Conference 2016» statt. «Gold-Sponsor» des Sicherheitsgipfels ist der bundeseigene Rüstungsbetrieb Ruag.

Hacker, die angeblich für den russischen Militärgeheimdienst arbeiten, saugten über ein Jahr lang unbemerkt Daten aus dem bundeseigenen Rüstungsbetrieb ab. Daten der Ruag und ihrer Kunden, unter ihnen das Verteidigungsdepartement VBS mitsamt Nachrichtendienst des Bundes (NDB).

Auch Monate nach Entdeckung des Lecks scheint völlig unklar, welcher Schaden wirklich entstanden ist. Zwar haben VBS und Ruag diese Woche versucht, die Affäre tiefer zu hängen. Das VBS beruhigte seine Mitarbeiter in einem internen E-Mail, dass «die potenziell gefährdeten Daten keine privaten persönlichen Angaben» enthielten.

Die Ruag, Spezialistin in Sachen IT-Sicherheit, setzte nach Tagen des Schweigens eine Mitteilung ab, die wohl vorab an Kunden wie die USA gerichtet war: «Die Ruag hat keine Hinweise darauf, dass andere Kunden, ausser dem VBS, betroffen waren.» Und weiter: «Geheime Daten sind vom Angriff auf die Ruag nicht betroffen.» Zudem seien «weniger als 0,1 Promille der Datenmenge» abgeflossen, die die Ruag verwalte.

Entwarnung? SVP-Ständerat Alex Kuprecht, Präsident der Geheimdienstkontrollbehörde GPDel, hält nach diesen Verlautbarungen ungerührt fest: «Die GPDel hat keine Veranlassung, ihre Einschätzung zu ändern.» Diese Einschätzung ist: Der Fall ist «gravierend».

Während VBS-Chef Guy Parmelin seine Leute beruhigen liess, hüllen sich andere Departemente in Schweigen. Man hält die VBS-Entwarnung für «mutig». Beim Finanzdepartements (EFD) etwa heisst es: «Sobald ein geeigneter Zwischenstand der technischen Abklärungen vorliegt, werden wir intern informieren», so Sprecher Daniel Saameli.

Betroffen vom Cyber-Angriff auf die Ruag sind nach Angaben von Insidern auch Auslandmitarbeiter des Nachrichtendienstes (NDB), also Spione. Es gehe um «mehrere hundert Personen», wie Eingeweihte wissen. Laut Renato Kalbermatten, Sprecher des VBS, sind aber «NDB-Mitarbeitende zurzeit nicht gefährdet». Denn die Sicherheitsmassnahmen seien «überprüft» und «die nötigen Massnahmen bereits vor längerer Zeit getroffen» worden. Wann und welche Massnahmen, will das VBS nicht sagen.

Die Ruag, die zum guten Teil von VBS-Aufträgen lebt, führt für die Armee empfindlichste Aufträge aus. So ist sie Integrations- und Kompetenzzentrum für C4ISTAR. Dies ist, wie es die

«Allgemeine Militärzeitschrift» vor einigen Jahren formulierte, die «vernetzte Operationsführung in der Schweizer Armee». Sollte die nun bei den Russen oder sonst einem Geheimdienst sein? Zudem kursiert das Gerücht, dass nicht nur der Ruag Daten fehlen. Auch im Finanzdepartement seien Daten abgesaugt worden. Von einem Bundesaccount aus, einem Zugang innerhalb der Verwaltung also.

Sonja Uhlmann vom Bundesamt für Informatik und Telekommunikation (BIT) im Finanzdepartement sagt nur: «Aufgrund der laufenden Ermittlungen der Bundesanwaltschaft können wir dazu keine Antwort geben.» Auch GPDel-Chef Alex Kuprecht will sich zu einem Leck im EFD «nicht äussern».

Der Bund ist für solche Angriffe jedenfalls schlecht gewappnet: Er hat zwar Notfall-Teams, verfügt aber über keine Einrichtung, die Auffälligkeiten im Netzbetrieb entdeckt. Ein Security Operation Center (SOC) gab es bisher nicht. Vorab aus Kostengründen, so Insider, habe man darauf verzichtet.

Fehlendes Sicherheitsgesetz

Daten-Klau und Daten-Chaos beim Bund. Selbst verschuldet? Fakt ist: Nachdem 2009 das Aussendepartement Ziel eines ähnlichen Hacker-Angriffs wurde, bestellte der Bundesrat beim damaligen Verteidigungsminister Ueli Maurer ein Informationssicherheitsgesetz (ISG). Das gibt es bis heute nicht. Jetzt muss Nachfolger Guy Parmelin auch da ran. Laut VBS soll das ISG «im 2. Quartal» in den Bundesrat.

Auch die Bundesanwaltschaft (BA), die jetzt im Ruag-Angriff ermittelt, verschlief den Kampf gegen Cybercrime. Vor Jahren schon genehmigte Stellen zur Bekämpfung von Phishing liess Bundesanwalt Michael Lauber bis heute unbesetzt. Hunderte von Phishing-Fällen werden bloss «verwaltet». Die Aufsichtsbehörde über die BA konnte in ihrem letzten Jahresbericht einzig die Einberufung einer Arbeitsgruppe vermelden: «Diese hat im vergangenen Jahr zweimal getagt. Konkrete Resultate liegen noch nicht vor.»

Ein zusätzliches Problem beim Daten-Chaos und seiner Bewältigung ist: Kaum einer hat den Überblick über Datenzugänge und Schnittstellen nach aussen. Hans Stöckli, SP-Ständerat und Präsident der Geschäftsprüfungskommission (GPK), plädiert jetzt für eine Untersuchung: «Wir müssen die generelle Problematik des Datenaustausches zwischen dem Bund und bundesnahen Unternehmungen hinterfragen», sagt er. Er will wissen: «Wie hat man bei der Auslagerung unserer Bundesbetriebe die Frage des Datentransfers gehandhabt? Wer erhielt welche Daten, wer welche Zugänge?» Seine Befürchtung: Solche Zugänge könnten bei Ausschreibungen zu ungerechtfertigten Vorteilen gegenüber Mitbewerbern führen.

Offen ist, ob der Datenklau bei der Ruag Konsequenzen hat. Personell, finanziell. Die Ruag-Konzernleitung erhielt für das Datenklau-Jahr 2015 Gehälter von rund 7 Millionen Franken, inklusive Boni von gut 2 Millionen. Allein CEO Urs Breitmeier erhielt total rund 1,1 Millionen. Ruag-Präsident Hans-Peter Schwald sagt: «VR und Konzernleitung sind sich ihrer Verantwortung für das Unternehmen voll bewusst, und wir haben zusammen mit unseren Spezialisten zielgerichtet die notwendigen Schritte und Massnahmen eingeleitet, um weiteren Schaden abzuwenden.»

Und der Bund, verlangt er Schadenersatz, zieht er Aufträge zurück? Das VBS schweigt dazu. Es gibt aber offenbar auch Positives. Auf die Frage, warum der Ruag-Angriff erst nach einem Jahr entdeckt wurde, sagt Gisela Kipfer, Sprecherin beim Informatiksteuerungsorgan des Bundes (ISB): «Gezielte Angriffe, wie dies der Vorfall auf die Ruag ist, werden häufig spät oder

sogar nie entdeckt.» Der Fall Ruag bestätige, «dass die mit der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) beschlossenen Massnahmen zu greifen beginnen und weiter umzusetzen sind».