Mit Sicherheit ein Problem

Um die Cybersicherheit beim bundeseigenen Rüstungskonzern Ruag stehts nicht sehr gut. Nun zeigt sich eine weitere Lücke im System: Noch vor Tagen konnten beliebige Personen im Namen von Ruag-Mitarbeitenden Dateien verschicken.

Eine Recherche von Elia Blülle, Adrienne Fichter und Priscilla Imboden, 26.02.2022

Die Bundesräte Ueli Maurer und Viola Amherd erhielten in der Nacht auf den 23. Februar um 1.56 Uhr eine ungewöhnliche E-Mail. Der Absender: André Wall. Im Betreff: die Einladung, eine Datei herunterzuladen mit dem externen Filesharing-Dienst der Ruag «SDE Secure File Transfer».

Wall ist seit 2020 Geschäftsführer der Ruag International. Der Inhalt der E-Mail lässt aber schnell darauf schliessen, dass es nicht Wall war, der die Nachricht verschickt hat. Denn der Verfasser oder die Verfasserin nimmt Bezug auf die Cybersicherheit der Ruag und schreibt, dass weder die Ruag International noch das Nationale Zentrum für Cybersicherheit NCSC über ausreichende Expertise verfügen würden, um die IT-Herausforderungen bei der Ruag International zu meistern. Aufgrund dieser «fehlenden Fachkompetenz» sei es 2021 wie auch 2016 nicht gelungen, die erfolgten Cyberangriffe kompetent zu analysieren und die Auswirkungen zu deuten.

Der Schreiber fordert «im Namen aller Bürgerinnen und Bürger» die Politik auf, die Probleme ernst zu nehmen und die Cybersicherheit professionell zu organisieren. Die Nachricht wurde nicht nur an die Bundesräte verschickt, sondern auch an verschiedene Parlamentsmitglieder.

Die Republik erhielt ein Dokument, das zeigt, wie der anonyme Absender im Namen von André Wall E-Mails verschicken konnte, und rekonstruierte die Anleitung. Dazu war nicht einmal ein Hack nötig. Bis vor einigen Tagen konnten alle Personen mit einem Internetanschluss über die URL eines externen Filesharing-Dienstes E-Mails im Namen von Ruag-Mitarbeiterinnen verschicken – wohin sie wünschten.

Gefährliche E-Mails

Dies lief über einen Dienst namens Dasdex Mail, welcher der Firma Codebase AG in Luzern gehört. Gemäss der Website der Firma nutzt Ruag Dasdex Mail seit 2013. Der Dienst sei bei der Ruag International für den Transfer von grossen, nicht klassifizierten Datenmengen im Einsatz, schreibt der Konzern. Die Ruag bestätigt auf Anfrage, dass die fragliche Nachricht an die Bundesräte über Dasdex Mail verschickt wurde.

Viele kennen ein ähnliches Angebot vom bekannteren Dienst We Transfer. Dabei lädt man grosse Daten auf eine Website und gibt eine Absender- und eine Empfängeradresse an. Mit wenigen Klicks ist das File dann als Link in einer E-Mail beim anvisierten Empfänger.

Doch was ist nun beim Codebase-Dienst schiefgelaufen? Wieso konnten damit Nachrichten im Namen von André Wall verschickt werden? Und wie gravierend war der neuerliche Vorfall?

Für Security-Expertinnen ist klar, dass die externe Ruag-Webanwendung nicht dem Stand der Technik und dem Schutzbedarf eines Waffenkonzerns entspricht. Dass ein solcher Dienst öffentlich über das Internet erreichbar ist, gehört zum Normalfall. Doch unklar ist, weshalb die entsprechende Adresse – die nun deaktiviert worden ist – in der Eingabemaske des Benutzerkontos eine bereits vorausgefüllte E-Mail-Adresse «anonymous_user@ruag.com» samt Passwort enthielt, den sich die anonyme Person zunutze machen konnte. «Das scheint für mich ein klassischer Designfehler zu sein», sagt Informationssicherheitsberater Sven Fassbender.

Die Voreinstellungen ermöglichten es, dass man den Dienst ungehindert benutzen konnte, auch wenn man nicht der Ruag angehörte. So gelang es der unbekannten Absenderin, die E-Mail an die Bundesräte zu verschicken.

Über Zertifikatssuchverzeichnisse wie Crt.sh lässt sich ableiten, mit welchen Drittanbietern die Ruag zusammenarbeitet. Entsprechend wichtig wäre es, dass jede Ruag-Mitarbeiterin bei allen genutzten Webdiensten ein eigenes Benutzerkonto hat. Beim Dienst der Firma Codebase war das nicht der Fall.

Ferner mangelte es dem Dienst an weiteren Sicherheitsgrundlagen wie etwa einem Verifikationsmechanismus. «Es braucht für einen solchen Dienst unbedingt eine 2-Faktor-Authentifizierung», sagt Experte Fassbender. «Ausserdem sollte ein Versand nur durch Benutzer möglich sein, welche von einem Ruag-Administrator freigegeben wurden.» 2-Faktor-Authentifizierung bedeutet, dass ein Sicherheitselement allein nicht ausreicht – sondern dass zum Beispiel zusätzlich zum Passwort noch ein SMS-Code eingegeben werden muss, der an die persönliche Telefonnummer verschickt wird.

In den technischen Daten der fraglichen E-Mail an die Bundesrätinnen wird klar, dass für den Versand Dasdex-Mail-Server genutzt werden. Somit mag wohl der eine oder andere Empfänger erraten haben, dass es sich um Spam handelt – und nicht die offizielle E-Mail-Adresse des Ruag-Chefs hinter der Nachricht steckt.

Dennoch: Für Ruag-Mitarbeiterinnen, die seit 2013 womöglich mit dem Ruag Secure Data Exchange arbeiten und täglich sensible Daten verschicken müssen, könnten solche E-Mails gefährlich werden. Denn natürlich vertraut man den Kollegen und ist schneller geneigt, einen mitgelieferten Link anzuklicken. Bemerkt eine Mitarbeiterin nicht, dass es sich um Spam handelt, schnappt die Falle zu. «Das sind ernsthafte Bedrohungen, die schwerwiegende Folgen haben können», sagt Sven Fassbender.

Allgemein ist der fehlende Nachweis der Absenderadresse – also die Authentisierung – ein Problem vieler Firmen und nicht nur der Ruag. Kurz: Jeder kann ein Tool wie Dasdex nachbauen und E-Mails in fremdem Namen verschicken. Die fehlende E-Mail-Authentisierung sei das grössere und entscheidende Problem in diesem Fall, sagt Informatiker Kaspar Etter, der ein Grundlagenwerk über die technischen Standards von E-Mail schrieb. «Obwohl es technische Standards zur Verhinderung gefälschter Absenderadressen gibt, setzen viele Firmen diese leider noch nicht um.»

Die Firma Codebase aus Luzern, die den externen Ruag-Dienst Dasdex Mail anbietet, reagierte nicht auf die Anfragen der Republik.

Gravierende Mängel bei der Informatiksicherheit

Die E-Mail-Panne ist peinlich für die Ruag International und kommt zu einem denkbar schlechten Moment. Der Bundesrat entschied im Jahr 2018-, die bundeseigene Waffenschmiede, die zu einem internationalen Rüstungs- und Technologiekonzern mit 9000 Mitarbeitenden angewachsen war, aufzuteilen: in die Ruag MRO, die weiterhin Dienstleistungen für die Armee erbringt, und in den Luft- und Raumfahrtkonzern Ruag International, der verkauft werden soll.

Der Verwaltungsrat sucht jetzt Interessentinnen für den Kauf. Demnächst soll etwa die Munitionssparte, Ruag Ammotec, ins Ausland veräussert werden. Falls es aber weiterhin Cybersicherheitsprobleme gibt, ist die Ruag International wenig attraktiv für einen potenziellen Käufer.

Seit Jahren schon kämpft die Ruag mit gravierenden Lücken in der Informatiksicherheit. Zwischen 2014 und 2016 drangen Hackerinnen, mutmasslich russischer Herkunft, in die Ruag-Systeme ein. Sie erhielten so auch Zugriff auf sensible Informationen. Das ist vor allem auch deswegen problematisch, weil die Ruag über geheime Daten zu Waffensystemen wie etwa dem US-Kampfjet F/A-18 verfügt. Sie ist über internationale Abkommen verpflichtet, diese zu schützen. Welche Daten die Hacker gestohlen haben, ist bis heute nicht bekannt.

Der Hackerangriff zwang die Ruag dazu, ihre Systeme zu überarbeiten. Laut eigenen Angaben hat die Ruag aber seither ihre Cybersicherheit verbessert und sollte nun gegen Angriffe gewappnet sein.

Doch hat sie die gravierenden Sicherheitsmängel behoben?

Recherchen der «Rundschau» von 2021 lassen Zweifel aufkommen, ob die Ruag ihre Cybersicherheit im Griff hat. Die SRF-Sendung dokumentierte mit Videos, wie Hacker in die firmeneigenen E-Mail-Postfächer eindrangen. Sie konnten unter anderem Nachrichten von Ruag-CEO André Wall lesen, die er an seine Mitarbeitenden verschickt hatte. SP-Sicherheitspolitikerin Priska Seiler Graf zeigte sich daraufhin bestürzt. Die Ruag habe versichert, sie habe alle Sicherheitsdefizite behoben und sei auf Kurs, sagte sie damals gegenüber dem Schweizer Fernsehen. «Man hat uns schlicht und einfach angelogen.»

Die Ruag leitete schliesslich eine Untersuchung ein, dementierte den Hackerangriff, fand aber andere ernst zu nehmende Sicherheitsmängel vor. Sie habe deshalb zusätzliche Sicherheitsmassnahmen ergriffen, versicherte André Wall später.

Bereits im Februar 2021 stellte auch die Eidgenössische Finanzkontrolle erhebliche Sicherheitsmängel bei der Ruag International fest. In ihrem Prüfbericht fordert sie eine «umfangreiche» Nachbearbeitung. Die Geschäftsprüfungskommission des Nationalrats untersuchte später auch den Vorfall, der von SRF dokumentiert wurde. Sie kam zum Schluss, dass es keine erhärteten Belege für den von der «Rundschau» dokumentierten «mutmasslichen Hackerangriff» auf Ruag International im Mai 2021 gebe.

Entwarnung gibt die Kommission aber nicht. Sie hält fest, dass im Laufe der Untersuchungen schwerwiegende Mängel an der Informatiksicherheit der Ruag International aufgetreten seien. Es sei unverständlich, dass diese nicht vorher entdeckt worden seien. Sie verweist auf eine Einschätzung der Eidgenössischen Finanzkontrolle, gemäss der die Ruag noch nicht wisse, wo überall sich die sensitiven Daten befänden. Damit be-

stehe ein «schwer einschätzbares Risiko, dass bei einem Verkauf von Unternehmensteilen unerkannte sensitive Daten in falsche Hände gelangen». Die Geschäftsprüfungskommission fordert den Bundesrat deshalb auf, zusätzliche Massnahmen zu treffen, um sicherzustellen, dass auf den Systemen keine solchen Daten verbleiben.

Die anonyme Absenderin, die sich an den Bundesrat gewandt hat, will mit ihrer E-Mail aufzeigen, dass weiterhin gravierende Lücken im Sicherheitsdispositiv der Ruag existieren. Denn solche – unter falschem Namen – verschickten Nachrichten würden «Tür und Tor öffnen für ▯▯Social Engineering und Phishing-Attacken» – also bekannte Methoden, mit denen Hacker versuchen, in IT-Systeme einzudringen, um Daten und Informationen zu stehlen.

«Ohne die Ruag wäre die Schweizer Armee nicht einsatzfähig», sagte Verteidigungsministerin Viola Amherd 2019 an einer Medienkonferenz. Umso verheerender ist es für die militärische Sicherheit, wenn die Ruag noch immer nicht alle ihre Systeme einwandfrei gesichert hat.