Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

24. September 2020 [redacted]

Prüfbericht «Einhaltung Grundschutz Bund bei externen IKT-Partnern»

IKT-Prüfung I 2020-04 – FABIS und SAFFSA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 24. September 2020

Prüfbericht «Einhaltung Grundschutz Bund bei externen IKT-Partnern»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Einhaltung Grundschutz Bund bei externen IKT-Partnern» zukommen. Unsere Prüfarbeiten bezüglich den Systemen FABIS und SAFFSA fanden zwischen Mai und Juni 2020 bei der Firma BWO Systems AG in Schenkon statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern in der armasuisse sowie mit der BWO Systems AG besprochen. Die Stellungnahmen zu diesem Bericht sind in Kapitel 8 ersichtlich.

Diese Prüfung wurde in Übereinstimmung mit den internationalen Standards für die berufliche Praxis der internen Revision durchgeführt.

Sollten Sie Fragen zu unserem Bericht haben, stehen wir Ihnen jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
- Generalsekretär VBS
- Chef der Armee
- Rüstungschef
- BWO Systems AG

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Der Grundschutz Bund im Überblick

Informatiksicherheit ist für alle Verwaltungseinheiten (VE) der Bundesverwaltung (BV) unverzichtbar. Durch den laufenden Ausbau der digitalen Vernetzung und die Anwendung von neuen virtuellen Konzepten (z.B. das Cloud-Computing) nehmen die Risiken und Bedrohungen aus der Cyberwelt immer mehr zu. Daher kommt dem Schutz der Informatikinfrastruktur eine besondere Bedeutung zu.

Um diesen Sicherheitsanforderungen nachzukommen, hat das Informatiksteuerungsorgan des Bundes das Dokument «IKT-Grundschutz in der Bundesverwaltung» (kurz: Grundschutz Bund) geschaffen. Dieses legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich der Informatiksicherheit fest. Zudem wird darin auf die ISO/IEC 27001 Bezug genommen und diese international anerkannte Vorgabe teilweise erweitert.

Da verschiedene VE im VBS Informatiksysteme mit Unterstützung von externen Dienstleistern betreiben, kommen die Sicherheitsvorgaben des Grundschutzes Bund auch bei diesen Partnern zur Anwendung.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS beauftragte am 24. Februar 2020 die Interne Revision VBS, bei ausgewählten externen Dienstleistern zu prüfen, ob die einschlägigen Sicherheitsbestimmungen der BV eingehalten werden. Für diese Prüfung wählten wir ein risikoorientiertes Vorgehen und fokussierten auf relevante Informatiksysteme, welche von externen Partnern entwickelt oder betrieben werden. Das Auswahlverfahren stimmten wir mit unseren Ansprechpersonen in den Departementsbereichen ab. Ebenfalls wurde die Abteilung Informations- und Objektsicherheit in unsere Planungsarbeiten mit einbezogen. Dabei führten wir auch eine umfassende Dokumentenanalyse (z.B. Verträge und Auditberichte) durch.

Im Rahmen dieses Prüfauftrags beurteilten wir die Einhaltung des Grundschutzes Bund bei folgenden Systemen:

Externer Dienstleister	Prüfbericht	Prüfende Systeme
BWO Systems AG	I 2020-04	FABIS: Führung ab Bern Informationssystem SAFFSA: Swiss Air Force Flight Support Application System

In einem ersten Schritt liessen wir die Firma BWO Systems AG die Umsetzung des Grundschutzes Bund im Rahmen eines Self-Assessments beurteilen. Im Anschluss führten wir mit Schlüsselpersonen in der Unternehmung strukturierte Befragungen durch und nahmen zudem begleitete Begehungen vor. Unsere Ergebnisse spiegelten wir im Anschluss mit der armasuisse in der Rolle als Beschaffungsstelle.

Wie erwähnt hat diese Prüfung ausschliesslich die Einhaltung der Vorgaben des Grundschutzes Bund bei den Systemen FABIS und SAFFSA zum Gegenstand. Daher war zum Beispiel das Vergabeverfahren, welches zum Vertragsverhältnis führte, nicht Teil unserer Prüfung.

3 Würdigung

Unsere Prüfung ergab ein gutes Gesamtbild bezüglich der Einhaltung Grundschutz Bund. Während unserer Prüfung trafen wir bei der armasuisse sowie der BWO Systems AG ausnahmslos auf engagierte Interviewpartner[1], die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Einhaltung des Grundschutzes Bund ein wichtiges Anliegen ist. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit.

4 Systeme FABIS und SAFFSA in Kürze

Das «Führung ab Bern Informationssystem (FABIS)» ist eines von drei Managementtools der Armee (nebst FIS Heer und FIS LW). Es ist ein militärisches, sicheres Informationssystem und besteht aus verteilten Arbeitsstationen, die über ein Netzwerk mit eigenen Servern verbunden sind, um Daten zu bearbeiten und ablegen zu können. FABIS unterstützt die Kernaufgaben des Kommandos Operationen. Insbesondere werden damit die Bereitschaft der Armee sowie die mehrstufige Planung und Führung von Einsätzen vereinfacht. Das System FABIS wird durch die Führungsunterstützungsbasis betrieben und unterhalten. Einige Lizenzen und Supportleistungen werden von der BWO Systems AG bezogen.

Beim Swiss Air Force Flight Support Application System (SAFFSA) handelt es sich um eine Flugplanungsplattform der Luftwaffe. Diese dient den Piloten als Basis für die Routenplanung und Koordination mit der Luftverkehrskontrolle. Die BWO Systems AG übernimmt dabei das Hosting, die Wartung und den Support dieser Plattform.

5 BWO Systems AG

Die BWO Systems AG ist ein Schweizer IT-Beratungsunternehmen mit Standorten in Schenkon (LU) und Bern. Das Unternehmen beschäftigt rund 50 Mitarbeitende und ist auf sogenannte UltraSecure-Solutions spezialisiert. Die Kernkompetenzen der BWO Systems AG liegen im Bereich der Planung, der Realisation und dem Betrieb von IT-Infrastrukturen. Die BWO Systems AG verfügt über eine Betriebssicherheitserklärung des VBS, um Aufträge mit militärisch klassifiziertem Inhalt nach den geltenden Vorschriften zu bearbeiten.

[1] Aus Gründen der Lesbarkeit wird bei Personenbezeichnungen die männliche Form gewählt, es ist jedoch immer die weibliche Form mitgemeint.

6 Feststellungen und Beurteilung

Feststellungen: Die BWO Systems AG bedient zahlreiche Kunden aus der Privatwirtschaft wie und aus der öffentlichen Verwaltung mit hohen Sicherheitsanforderungen.

Das *System FABIS* wird durch die Gruppe Verteidigung betrieben. Daher arbeiten alle Mitarbeitenden der BWO, welche in das System FABIS eingebunden sind, ausschliesslich auf der Büroautomationsumgebung des VBS. Dank dieser Lösung bearbeitet die BWO Systems AG keine VBS-sensitiven Informationen auf der firmeneigenen Infrastruktur.

Das *System SAFFSA* wird durch die BWO Systems AG betrieben und weiterentwickelt. Als Endnutzer von SAFFSA ist die Luftwaffe dafür verantwortlich, die Sicherheitsanforderungen des Systems zu definieren und BWO damit zu beauftragen, diese umzusetzen. Während unserer Prüfungen konnte die BWO aufzeigen, dass SAFFSA als sicheres System und mit einer hohen Verfügbarkeit betrieben wird. Die BWO hält die aktuellen Sicherheitsanforderungen beim System SAFFSA ein.

Sämtliche für das VBS eingesetzten Mitarbeitenden der BWO verfügen über gültige Personensicherheitsüberprüfungen und werden im Umgang mit klassifizierten Informationen regelmässig geschult.

Beurteilung: Insgesamt gewannen wir ein positives Gesamtbild bezüglich des Informationsschutzes bei der BWO Systems AG. Die Firma hält die Vorgaben des Grundschutzes Bund im Rahmen der Systeme FABIS und SAFFSA ein. In den folgenden zwei Themenkreisen sehen wir noch Verfeinerungsbedarf. Wir haben festgestellt, dass

– keine systematische Prüfung der Anwendungen und IKT-Systeme auf Schwachstellen stattfindet. Beim System SAFFSA wurde noch nie ein solcher Test durchgeführt. Diese periodischen Prüfungen (Penetration Testing) erachten wir jedoch nur dann als sinnvoll, wenn sie in einem adäquaten Kosten-Nutzen-Verhältnis stehen.

– das Business Continuity Management (BCM) der BWO Systems AG ist derzeit noch im Aufbau. Der Sachverhalt wurde durch die BWO bereits erkannt und Massnahmen sind eingeleitet, um das BCM zu komplementieren.

7 Empfehlungen

Gestützt auf unsere Feststellungen und Beurteilung empfehlen wir der Gruppe Verteidigung:

– zu prüfen, ob periodische Schwachstellen-Prüfungen (Penetration Testing) der Systeme durchgeführt werden sollte, um die IKT Sicherheit zu erhöhen.
– zu prüfen, ob seitens VBS konkrete BCM-Anforderungen an die BWO Systems AG gestellt werden sollten.

8 Stellungnahmen

armasuisse
armasuisse bedankt sich für die Prüfung und hat zum vorliegenden Bericht keine Bemerkungen.

Gruppe Verteidigung
Die Gruppe V bedankt sich bei der Internen Revision VBS für die Überprüfung und für diesen Prüfbericht. Wir unterstützen beim System SAFFSA die Empfehlungen bezüglich der periodischen Überprüfung auf Schwachstellen sowie die konkrete Definition von BCM-Anforderungen. Bei der Plattform FABIS bzw. neu OMP unterstützen wir die Empfehlung, sie periodisch auf Schwachstellen zu überprüfen.

BWO Systems AG
Der Bericht entspricht ebenfalls unserer Wahrnehmung des Assessments. Besten Dank für die angenehme Zusammenarbeit.