Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

24. Februar 2020 [redacted]

Prüfbericht «Erledigte Massnahmen Projekt PAIS»

IKT-Prüfung I 2019-07

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. Februar 2020

IKT-Prüfung «Erledigte Massnahmen Projekt PAIS»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Erledigte Massnahmen Projekt PAIS» zukommen. Unsere Prüfarbeiten fanden zwischen November und Dezember 2019 statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern im Departement abgestimmt. Die Stellungnahme der Departementsbereiche sind im Kapitel 6 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
– DU VBS

Interne Revision VBS
Schauplatzgasse 11, 3003 Bern
Tel. +41 58 464 28 35

1 Informationssicherheit – Projekt «PAIS»

Im Jahr 2014 verfügte das VBS über rund 940 aktiv genutzte IKT-Schutzobjekte. Davon lagen für mehr als die Hälfte keine genehmigten Sicherheitsdokumente vor. Die damalige Departementsführung erkannte den Handlungsbedarf und startete das Projekt «Prüfung Altlasten IKT-Schutzobjekte» (PAIS). Mit dem Projekt wurden diese Sicherheitsdokumente systematisch nachgearbeitet und genehmigt. Die Zielsetzung war, dass alle eingestuften Schutzobjekte bis Mitte 2018 über ein genehmigtes Sicherheitsdokument verfügen.

2 Auftrag, Methodik und Abgrenzung

Im Jahr 2017 führte die IR VBS auf Antrag des damaligen Chefs VBS eine Prüfung des Projekts «PAIS» durch. Es ging dabei um die Beurteilung der systematischen Nacharbeitung der Sicherheitsdokumente. Der Prüfbericht zeigte auf, dass der damalige IKT-Sicherheitsprozess weder effektiv noch effizient ausgestaltet war. Es resultierten insgesamt drei Empfehlungen.

In unserem Bericht empfahlen wir, die Projektarbeiten per Mitte 2018 abzuschliessen und allfällige Restarbeiten im neuen Sicherheitsprozess abzuarbeiten. Weiter wurde vorgeschlagen, dass der bestehende IKT-Sicherheitsprozess weiterentwickelt und im Einklang mit dem Informations-Sicherheits-Management-System (ISMS) gebracht werden sollte. Die dritte Empfehlung richtete sich an alle Führungsebenen, welche der «Informationssicherheit» eine angemessene Bedeutung zuschreiben sollte.

Gestützt auf den angeordneten Massnahmen aus dem Jahr 2017 erteilte die Chefin VBS der IR VBS am 23. August 2019 den Auftrag zu prüfen, ob die damaligen Empfehlungen in angemessener Form umgesetzt worden sind. Wir wählten dazu ein risikoorientiertes Vorgehen mittels einer Dokumentenanalyse und Stichprobenprüfung. Zudem führten wir Befragungen mit den zuständigen Ansprechpersonen im Bereich Informations- und Objektsicherheit (IOS) sowie bei ausgewählten CISO[1] der Departementsbereiche durch.

Im Rahmen der Prüfung führten wir keine Überprüfung des ISMS.VBS durch. Diesbezüglich verweisen wir auf eine separate Prüfung[2] der IR VBS.

3 Würdigung

Während unseren Arbeiten trafen wir ausnahmslos engagierte Mitarbeitende an, die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Informationssicherheit im VBS ein wichtiges Anliegen ist. Wir danken allen Beteiligten für die zielgerichtete Zusammenarbeit.

[1] Chief Information Security Officer

[2] I 2019-06 ISMS.VBS - Konformitätsaudit vom 12. November 2019

4 Zusammenfassende Erkenntnisse

Unsere Prüfung zeigte ein deutlich verbessertes Bild im Bereich der Informationssicherheit im Vergleich zu unserer Prüfung im 2017. Die Anzahl der betriebenen IKT-Systeme ohne genehmigte Sicherheitsdokumentationen konnte seit Mitte 2017 von 301 auf 99 reduziert werden (für Details siehe Anhang 1: Entwicklung der IKT-Schutzobjekte im VBS). Bei den Verwaltungseinheiten swisstopo, NDB[3] sowie BASPO[4] verfügen sämtliche relevanten Informatik-anwendungen über gültige Sicherheitskonzepte.

Hauptgrund der noch 99 pendenten IKT-Schutzobjekte (per 30.09.2019) sind Altlasten der armasuisse. Ein Grossteil dieser Pendenzen bestehen aufgrund nicht mehr genutzter Schutzobjekte. In Zukunft wird die armasuisse ihre IKT-Schutzobjekte noch vermehrt konsolidieren, was zu einer weiteren Reduktion der nicht genehmigten Schutzobjekte führen wird. Ohne die armasuisse kommt das gesamte VBS auf einen Erfüllungsgrad von über 90%, was aus unserer Sicht einem guten Wert entspricht.

Insgesamt kommen wir zum Schluss, dass das VBS auf dem richtigen Weg ist und in den letzten beiden Jahren wesentliche Fortschritte bei der Bewirtschaftung der IKT-Schutzobjekte erzielt werden konnten. Dieser positive Trend sollte fortgesetzt werden, damit ein hoher Erfüllungsgrad nachhaltig gehalten und die laufend neu entstehenden Pendenzen zeitgerecht bereinigt werden. Es ist uns bewusst, dass aufgrund der laufenden In- und Ausserbetriebnahme von IKT-Schutzobjekten sowie der jeweils stichtagsbezogenen Auswertung ein Erfüllungsgrad von 100% schwer zu erreichen ist.

Alle anderen Empfehlungen aus unserem Prüfbericht aus dem Jahr 2017 wurden zielführend umgesetzt. Der Sicherheitsprozess wurde in Zusammenarbeit mit den Sicherheitsverantwortlichen bei der Einführung des ISMS.VBS überarbeitet. Dabei wurde den Verwaltungseinheiten eine deutlich höhere Eigenverantwortung übertragen. Diese Strategie wird nun konsequent weitergeführt (siehe Massnahmen, welche aus unserer Prüfung «ISMS.VBS – Konformitätsaudit 2019» resultieren).

5 Empfehlung

Aufgrund unserer Prüffeststellungen empfehlen wir der armasuisse, unter Einbezug der Informations- und Objektsicherheit (IOS), die noch offenen Pendenzen bei den IKT-Schutzobjekten zeitnah zu bereinigen.

[3] Nachrichtendienst des Bundes

[4] Bundesamt für Sport

6 Stellungnahmen

Generalsekretariat VBS
Das GS-VBS dankt der Internen Revision VBS für die sorgfältige Prüfung und für die Gelegenheit zur Stellungnahme. Die Informationssicherheit ist für das ganze Departement von Bedeutung. Die Prüfung zeigt ein verbessertes Bild im Bereich der Informationssicherheit und Handlungsbedarf bei IKT-Schutzobjekten auf. Wir erachten es als zielführend, dass den Verwaltungseinheiten eine deutlich höhere Eigenverantwortung übertragen wird. Das GS-VBS unterstützt die Empfehlung der Internen Revision VBS.

Nachrichtendienst des Bundes
Der NDB hat keine Bemerkungen zum Bericht.

Gruppe Verteidigung
Wir danken für die Gelegenheit zur Stellungnahme zum Prüfbericht «Erledigte Massnahmen PAIS» der Internen Revision VBS. Im Rahmen des ISMS V werden wir die Einhaltung der Vorgaben konsequent einfordern und kontrollieren. Die Gedankenanstösse im Anhang des Prüfberichtes «PAIS» wird die Gruppe Verteidigung weiterhin berücksichtigen.

armasuisse
Die armasuisse unterstützt den Bericht und dessen Erkenntnisse, zum Zeitpunkt der Erhebung, vollumfänglich. Es war so, dass das IKT-Portfolio der armasuisse keinen aktualisierten Inhalt hatte. Allerdings hat armasuisse am 24.01.2020 mit dem IOS zusammen noch einige Justierungen gemacht und die Bereinigung des IKT-Schutzobjekte-Portfolios im Q4/19 und zu Beginn des 2020 vorangetrieben. Das aktuelle Portfolio für die IKT-Objekte weist nun einen Erfüllungsgrad 88.9% auf. Somit ist dieser nun im Bereich des gesamten Erfüllungsgrad des VBS.

swisstopo
swisstopo hat den Bericht zur Kenntnis genommen und ist mit dem Inhalt einverstanden.

Bundesamt für Bevölkerungsschutz
Das BABS hat zum Bericht keine Bemerkungen. Bei dieser Gelegenheit bestätigen wir, dass das BABS alle seinerzeit im Projekt PAIS vereinbarten Pendenzen abgearbeitet hat.

Bundesamt für Sport
Das BASPO nimmt den Prüfbericht zur Kenntnis.

Anhang 1 Entwicklung der IKT-Schutzobjekte im VBS

Nachfolgende Darstellung basiert auf dem offiziellen Schutzobjekte-Portfolio der IOS. Sie zeigt auf, wie sich die Anzahl der aktiven Schutzobjekte und der nicht genehmigten Sicherheitsdokumente seit 2014 entwickelt hat: