Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

25. Juni 2024

Prüfbericht «Sicherheitsdokumentation»

IT-Prüfung I 2024-02

The Institute of Internal Auditors
IIA Switzerland

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundespräsidentin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 25. Juni 2024

Prüfbericht «Sicherheitsdokumentation»

Sehr geehrte Frau Bundespräsidentin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Sicherheitsdokumentation» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpersonen besprochen. Die Stellungnahmen der Verwaltungseinheiten zu unserem Bericht sind in Kapitel 7 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 gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
- Generalsekretär VBS
- Staatssekretär SEPOS
- Chef der Armee
- Rüstungschef

Leiter Interne Revision VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Die Interne Revision VBS (IR VBS) prüfte, ob in der Gruppe Verteidigung (Gruppe V) einheitliche und gelebte Prozesse und Strukturen bestehen, damit das Schutzobjektportfolio möglichst früh und präzise geführt wird, Grundlagendokumente (u. a. ISDS-Konzept) rechtzeitig vorliegen und notwendige Risikoupdates im Betrieb stattfinden.

Per 1. Januar 2024 sind das Informationssicherheitsgesetz (ISG)[1] und die dazugehörigen Ausführungsverordnungen in Kraft getreten. Die neue Informationssicherheitsverordnung (ISV)[2] ersetzt die beiden bisherigen Verordnungen, die Cyberrisikenverordnung (CyRV)[3] und die Informationsschutzverordnung (ISchV)[4].

Obwohl nicht alle Weisungen auf dem aktuellsten Stand sind, existieren Vorlagen für die Sicherheitsdokumente (u. a. Schutzbedarfsanalyse, IT-Grundschutz der Bundesverwaltung, Informationssicherheits- und Datenschutzkonzept), etablierte Prozesse und Kontrollen im Umgang mit der Inventarisierung, Dokumentation und Aktualisierung von Schutzobjekten in der Projektphase sowie im ordentlichen Betrieb. *Die IR VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit dem Generalsekretariat (GS-VBS), dem Staatssekretariat für Sicherheitspolitik (SEPOS) und dem Bundesamt für Rüstung (armasuisse), aufgrund der neuen rechtlichen Grundlagen, die aktuellen Weisungen und Dokumentvorlagen zu analysieren sowie zeitnah zu überarbeiten und durch die entsprechende Geschäftsleitung freizugeben.*

Die Unterschriftsberechtigungen und Kompetenzen im Sicherheitsprozess sind klar zu definieren, z. B. Geschäftsordnung, Weisung etc. Diese Dokumente sind aufeinander abzustimmen, um möglichen Widersprüchen vorzubeugen. Ohne klare Regelung kann dies bei der Unterzeichnung der Sicherheitsdokumente zu einer unzulässigen Delegation führen. *Die IR VBS empfiehlt der Gruppe Verteidigung, die Unterschriftsberechtigungen und Kompetenzen im Bereich der Sicherheit im Hinblick auf die neue Informationssicherheitsverordnung in den jeweiligen Geschäftsordnungen, Weisungen etc. zu regeln.*

Das VBS erlaubt den Einsatz von verschiedenen Public-Cloud-Anwendungen zu Geschäftszwecken. Für die Beschaffung von Public-Cloud-Anwendungen sind Regelungen und Prozesse auf Stufe Departement etabliert worden. Gegenwärtig werden die Public-Cloud-Anwendungen jedoch noch nicht umfassend als Schutzobjekte geführt. Es besteht die Gefahr von ungewolltem Informationsabfluss und der Nichteinhaltung der Vorschriften aus den Bereichen Informationssicherheit und Datenschutz. *Die IR VBS empfiehlt der Gruppe Verteidi-*

[1] SR **128** - Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) | Fedlex (admin.ch)

[2] SR **128.1** - Verordnung vom 8. November 2023 über die Informationssicherheit in der Bundesverwaltung und der Armee (Informationssicherheitsverordnung, ISV) | Fedlex (admin.ch)

[3] SR **120.73** - Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) | Fedlex (admin.ch)

[4] SR **510.411** - Verordnung vom 4. Juli 2007 über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) | Fedlex (admin.ch)

gung sicherzustellen, dass für alle Public-Cloud-Anwendungen vor deren operativen Nutzung durch die Verwaltungseinheiten eine Schutzbedarfs- und Risikoanalyse durchgeführt wird.

Bei den Sicherheitsorganisationen in allen Verwaltungseinheiten (VE) der Gruppe V wird grosser Wert darauf gelegt, dass die Sicherheitsdokumente aktuell gehalten werden und gültig sind. Die Stichprobenprüfung der IR VBS hat allerdings ergeben, dass in Ausnahmefällen Sicherheitsdokumente der Schutzobjekte von Personen unterzeichnet wurden, welche die Restrisiken nicht als Leiterin bzw. Leiter der VE resp. deren Stellvertretung oder als Mitglied der Geschäftsleitung tragen. Es sind jedoch keine Fachanwendungen ohne vorzeitigen Einbezug von Entscheidungstragenden in den ordentlichen Betrieb überführt worden.

Gemäss verbindlichem Sicherheitsverfahren ist bei jedem Informatikvorhaben vorab eine Schutzbedarfsanalyse durchzuführen. Die Informationssicherheitsbeauftragten der VE werden grossmehrheitlich frühzeitig über neue und laufende Informatikvorhaben informiert und bereits während der Projektinitialisierungsphase eingebunden. Dies erfolgt jedoch nicht durchgehend für Folge- oder Nachbeschaffungen sowie kleinere Anschaffungen von Fachanwendungen. Aus diesem Grund *empfiehlt die IR VBS der Gruppe Verteidigung, die Informationssicherheitsbeauftragten bzw. zuständige Fachstelle der Verwaltungseinheiten frühzeitig zu Vorhaben mit Fachanwendungen einzubeziehen.*

Die Schutzobjekte des VBS werden gegenwärtig in einem zentralen Register als Übergangslösung geführt, welche viele Einschränkungen hat (u. a. dezentrale Ablage verschlüsselter Dokumente, fehlende Abhängigkeiten zu externen IT-Lieferanten/Dienstleister, Abbildung der Restrisiken und Massnahmen). Auch die Datenqualität entspricht noch nicht den Anforderungen an ein effizientes und benutzerfreundliches Schutzobjektregister. Die Stichprobenüberprüfung hat gezeigt, dass grösstenteils einheitliche und gelebte Prozesse und Strukturen bestehen, damit das Schutzobjektportfolio gemäss den Vorgaben aktualisiert wird.

Für die Informationssicherheitsverantwortlichen sowie die -beauftragten gibt es gegenwärtig keine adäquate Schulung und Sensibilisierung. Eine spezifische Schulung zum Thema der Schutzobjekte und der dazu gehörenden Prozesse und Verantwortlichkeiten gibt es aktuell nicht. *Die IR VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit dem Generalsekretariat (GS-VBS), die Schulung und Sensibilisierung der im Sicherheitsprozess beteiligten Personen stufengerecht zu gewährleisten.*

Bis Ende 2023 erbrachten das Bundesamt für Informatik und Telekommunikation (BIT) sowie die Führungsunterstützungsbasis der Armee (FUB) gleichartige Informatikleistungen. Die offenen Fragen bezüglich Umsetzung der Governance im Zusammenhang mit den Schutzobjekten als Folge der Transition ins BIT bzw. Kommando Cyber stellen aktuell, v. a. beim Kdo Cy sowie dem Armeestab, eine Herausforderung dar. *Die IR VBS empfiehlt der Gruppe Verteidigung, die Governance im Zusammenhang mit ihren Schutzobjekten, v. a. beim Armeestab sowie dem Kommando Cyber, schnellstmöglich zu finalisieren und umzusetzen.*

1 Ausgangslage

Im Zusammenhang mit der Informationssicherheit sind im Rahmen eines Projektes sowie im anschliessenden ordentlichen Betrieb für jedes Schutzobjekt[5], als Teil des Sicherheitsverfahrens, Minimalanforderungen bezüglich Sicherheitsdokumente zwingend einzuhalten. Diese sind bei veränderten Risiken anzupassen und haben gegenwärtig eine Gültigkeit von maximal 5 Jahren.

Per 1. Januar 2024 sind das Informationssicherheitsgesetz (ISG) und die dazugehörigen Ausführungsverordnungen in Kraft getreten. Die neue Informationssicherheitsverordnung (ISV) ersetzt die beiden bisherige Verordnungen, die Cyberrisikenverordnung (CyRV) und die Informationsschutzverordnung (ISchV). Das ISG schafft im Staatssekretariat für Sicherheitspolitik (SEPOS) zudem eine Fachstelle des Bundes für Informationssicherheit. Vorgaben zum Sicherheitsverfahren und zu den Minimalanforderungen an Schutzobjekte und Informatiksicherheitsprozesse werden in einer Übergangszeit weiterhin vom Bundesamt für Cybersicherheit (BACS) erlassen. Bestehende Vorgaben, die das Nationale Zentrum für Cybersicherheit (NCSC) bis zum 31. Dezember 2023 erlassen hat, bleiben bis 31. Dezember 2026 in Kraft.

Bei jedem Informatikvorhaben ist vorab eine Schutzbedarfsanalyse (Schuban) durchzuführen. Das Resultat der Schuban ist eine Einstufungsbeurteilung der Anwendung oder des Projektes.

Der IT-Grundschutz der Bundesverwaltung (Grundschutz) legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Für jedes Informatikmittel ist als Minimum der Grundschutz umzusetzen.

Ergibt die Schuban einen Schutzbedarf auf der Sicherheitsstufe «hoher Schutz» oder «sehr hoher Schutz», so ist zusätzlich zur Dokumentation der Umsetzung des Grundschutzes ein Informationssicherheits- und Datenschutzkonzept (ISDS) mit Risikoanalyse zu erstellen. Das ISDS-Konzept gilt als Hauptdokument der Informationssicherheit und des Datenschutzes im Projekt und während des Betriebes.

Bei einer automatisierten Datenbearbeitung muss das verantwortliche Bundesorgan und sein Auftragsbearbeiter zudem ein Bearbeitungsreglement erstellen, wenn sie u. a. besonders schützenswerte Personendaten bearbeiten (Art. 6 Abs. 1 Bst. a DSV).

[5] Als Schutzobjekte gelten gemäss Informationssicherheitsverordnung (ISV) Artikel 7 Absatz 2 einzelne oder mehrere gleichartige oder zusammenhängende:
a. Sammlungen von Informationen, die zur Abwicklung eines Geschäftsprozesses des Bundes bearbeitet werden;
b. Informatikmittel: Mittel der Informations- und Kommunikationstechnik, namentlich Anwendungen, Informationssysteme und Datensammlungen sowie Einrichtungen, Produkte und Dienste, die zur elektronischen Verarbeitung von Informationen dienen.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision (IR VBS) am 16. Dezember 2023 den Auftrag zu prüfen, ob in der Gruppe Verteidigung (Gruppe V) einheitliche und gelebte Prozesse und Strukturen bestehen, damit das Schutzobjektportfolio möglichst früh und präzise geführt wird, Grundlagendokumente (u. a. ISDS-Konzept) rechtzeitig vorliegen und notwendige Risikoupdates im Betrieb stattfinden.

Im Rahmen dieses Prüfauftrages führte die IR VBS strukturierte Befragungen mit Schlüsselpersonen in den VE[6] der Gruppe V durch. Ergänzend analysierte die IR VBS zur Verfügung gestellte Dokumente und zog externe, öffentlich zugängliche Unterlagen bei.

Die Stichprobenprüfung von ausgewählten Schutzobjekten, verteilt über alle VE der Gruppe V, basiert auf dem zentralen Register des VBS sowie Informationen aus dem PM-Tool[7]. Eine inhaltliche Beurteilung der Sicherheitsdokumente hat nicht stattgefunden. Auch wurde aufgrund des Prüfungszeitpunktes im ersten Quartal 2024 nicht beurteilt, ob die Vorgaben des neuen Rechtes (ISG/ISV sowie DSG/DSV) bereits umgesetzt worden sind.

Die Prüfungshandlungen haben im März 2024 begonnen und wurden per Ende April 2024 abgeschlossen. Darauf basieren auch die Beurteilungen und Empfehlungen. Der vorliegende Bericht berücksichtigt nicht die weitere Entwicklung nach Abschluss der Prüfungsdurchführung.

3 Unterlagen und Auskunftserteilung

Die Interviewpartnerinnen und Interviewpartner der Gruppe V haben der IR VBS die notwendigen Auskünfte umfassend und zuvorkommend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung. Die IR VBS dankt für die gewährte Unterstützung.

---

6 SR **172.214.1** - Organisationsverordnung für das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (OV-VBS) vom 7. März 2003 | Fedlex (admin.ch), Artikel 11

7 PM-Tool: Applikation für das Projektportfolio-Management der Gruppe Verteidigung und armasuisse

4 Rechtliche Grundlagen

An der Sitzung vom 8. November 2023 hat der Bundesrat entschieden, das Informationssicherheitsgesetz (ISG) und die dazugehörige Informationssicherheitsverordnung (ISV) per 1. Januar 2024 in Kraft zu setzen. Damit verstärkt der Bundesrat den Schutz der Informationen und die Cybersicherheit des Bundes. Die ISV ersetzt die Cyberrisiken- (CyRV) und die Informationsschutzverordnung (ISchV). Mit der ISV ist die Gruppe V verpflichtet, ein Inventar ihrer Schutzobjekte zu führen und dieses aktuell zu halten (Art. 7 Abs. 1 ISV).

Des Weiteren wird der Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen bei den Personendaten im Bundesgesetz über den Datenschutz (DSG)[8] vom 25. September 2020 sowie der dazugehörigen Ausführungsverordnung (DSV)[9] vom 31. August 2022 geregelt. Zur Gewährleistung einer angemessenen Datensicherheit müssen der Verantwortliche und der Auftragsbearbeiter den Schutzbedarf der Personendaten bestimmen und die im Hinblick auf das Risiko geeigneten technischen und organisatorischen Massnahmen festlegen (Art. 1 Abs. 1 DSV). Zudem regeln das Bundesgesetz über militärische und andere Informationssysteme im VBS (MIG)[10] vom 3. Oktober 2008 sowie deren Verordnung (MIV)[11] vom 16. Dezember 2009 die Bearbeitung von Personendaten natürlicher und juristischer Personen (Daten), einschliesslich besonders schützenswerter Personendaten, in Informationssystemen und beim Einsatz von Überwachungsmitteln der Armee und des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) u. a. durch Kommandantinnen, Kommandanten und Kommandostellen der Armee (militärische Kommandos) sowie Kommandantinnen und Kommandanten des Zivilschutzes.

Auf der nächsten Ebene regeln die Weisungen über die Informationssicherheit im VBS (WIns VBS) vom 16. Dezember 2016 die Prozesse, Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Bereich der Informationssicherheit VBS, die mit Hilfe eines ISMS[12] etabliert, gesteuert und kontinuierlich verbessert werden. Damit wird definiert, wie die Anforderungen des Standards ISO/IEC 27001:2015[13] im VBS und in dessen Gruppen sowie den VE umgesetzt werden. In Ziffer 19 wird festgehalten, dass die im Rahmen eines Projektes entstehenden oder sich verändernden Schutzobjekte im Hinblick auf neue oder geänderte Informationssicherheitsrisiken zu beurteilen und die Risiken entsprechend zu behandeln sind. Zudem ist die Datenschutzberaterin bzw. der Datenschutzberater bereits in der Phase der Projektini-

8 SR **235.1** - Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG) | Fedlex (admin.ch)

9 SR **235.11** - Verordnung vom 31.August 2022 über den Datenschutz (Datenschutzverordnung, DSV) | Fedlex (admin.ch)

10 SR **510.91** - Bundesgesetz vom 3. Oktober 2008 über militärische und andere Informationssysteme im VBS (MIG) | Fedlex (admin.ch)

11 SR **510.911** - Verordnung vom 16. Dezember 2009 über militärische und andere Informationssysteme im VBS (MIV) | Fedlex (admin.ch)

12 ISMS: Informationssicherheits-Managementsystem

13 ISO: International Organization for Standardization

tialisierung beizuziehen, wenn in einem geplanten Schutzobjekt die Bearbeitung von Personendaten vorgesehen ist.

Die Beschaffung von Systemen / Material, IT (IKT[14]-Systeme, Daten / Informationen) inkl. Immobilienvorhaben wird in der Regel als Projekt mittels der dafür vorgesehenen Projektmanagementmethode HERMES[15] abgewickelt. Dabei kommen die Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA)[16] zur Anwendung, welche die gemeinsamen Sachgeschäfte über den gesamten Lebensweg von Systemen, Material und IT regeln.

Obwohl nicht alle Weisungen auf dem aktuellsten Stand sind, existieren Vorlagen für die Sicherheitsdokumente (u. a. Schuban, Grundschutz, ISDS-Konzept), etablierte Prozesse und Kontrollen im Umgang mit der Inventarisierung, Dokumentation und Aktualisierung von Schutzobjekten in der Projektphase sowie im ordentlichen Betrieb.

Beurteilung

Da mit dem ISG und der ISV per 1. Januar 2024 sowie dem DSG und der DSV per 1. September 2023 neue rechtliche Grundlagen in Kraft gesetzt wurden, sind u. a. die vorerwähnten Weisungen und Dokumentvorlagen bezüglich angepasster Regelungen zu analysieren und zeitnah zu überarbeiten. Anschliessend sollen diese Unterlagen mindestens jährlich überprüft und aktualisiert werden.

Empfehlung 1: Weisungen und Dokumentvorlagen überarbeiten

Die IR VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit dem Generalsekretariat (GS-VBS), dem Staatssekretariat für Sicherheitspolitik (SEPOS) und dem Bundesamt für Rüstung (armasuisse), aufgrund der neuen rechtlichen Grundlagen, die aktuellen Weisungen und Dokumentvorlagen zu analysieren sowie zeitnah zu überarbeiten und durch die entsprechende Geschäftsleitung freizugeben.

[14] IKT: Informations- und Kommunikationstechnologie

[15] HERMES ist die Projektmanagementmethode für Projekte im Bereich der Informatik, der Entwicklung von Dienstleistungen und Produkten sowie der Anpassung der Geschäftsorganisation. HERMES unterstützt die Steuerung, Führung und Ausführung von Projekten verschiedener Charakteristiken und Komplexität.

[16] Weisungen über die Zusammenarbeit der Departementsbereiche Verteidigung und armasuisse (ZUVA) vom 1. Dezember 2022

5 Prozesse und Strukturen

5.1 Unterschriftsberechtigungen und Kompetenzen im Sicherheitsprozess

In Artikel 36 Absatz 1 und 2 der ISV wird die Verantwortung und Delegation für die Informationssicherheit geregelt. Direktorinnen und Direktoren der VE nach Artikel 2 Absatz 1 Buchstabe c ISV tragen in ihrem Zuständigkeitsbereich die Verantwortung für die Informationssicherheit. Weiter wird in Artikel 27 Absatz 4 der ISV zum Sicherheitsverfahren festgehalten, dass die Informationssicherheitsverantwortlichen entscheiden können, ob Restrisiken getragen werden. Sie können diesen Entscheid einem Mitglied der Geschäftsleitung (GL) delegieren.

In der CyRV, welche bis Ende Dezember 2023 in Kraft war, wird in Artikel 14*d* im Rahmen des Sicherheitsverfahrens bezüglich Restrisiken festgehalten, dass die Leitung der VE diese zur Kenntnis nehmen und schriftlich bestätigen muss. Der Entscheid darüber, ob bekannte Restrisiken in Kauf genommen werden, obliegt der Leiterin oder dem Leiter der zuständigen VE. Eine Delegation an ein GL-Mitglied ist nicht explizit vorgesehen. Gemäss der aktuell immer noch gültigen Dokumentvorlagen des Grundschutzes[17] sowie des ISDS-Konzeptes[18] hingegen kann das Sicherheitsdokument von einem verantwortlichen GL-Mitglied unterzeichnet werden.

Auch das Handbuch zum Risikomanagement Bund vom 15. September 2022 hält fest, dass die Risiken aus IT-Projekten und aus dem IT-Betrieb zu identifizieren, bewerten und durch angemessene Massnahmen im Rahmen des Sicherheitsverfahrens zu reduzieren bzw. eliminieren sind. Restrisiken müssen der Leitung der VE bekannt sein und von ihr bewusst in Kauf genommen werden.[19]

Die Unterschriftsberechtigungen und Kompetenzen in der Gruppe V gemäss Artikel 49 des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG)[20] sind in den jeweiligen Geschäftsordnungen für die Bereiche wie z. B. Grundsätzliches, Finanzen, Personelles etc. umfassend definiert und festgehalten.

Die Unterschriftsberechtigungen und Kompetenzen im Bereich der Sicherheit hingegen sind in den heutigen Geschäftsordnungen noch nicht definiert. Zudem sind die Unterschriftsberechtigungen und Kompetenzen im Sicherheitsprozess aktuell in verschiedenen übergeord-

17 Grundschutz (admin.ch) (Stand 24.04.2024)

18 Erhöhter Schutz (admin.ch) (Stand 24.04.2024)

19 Risiko- und Versicherungspolitik (admin.ch) (Stand 31.05.2024)

20 SR **172.010** - Regierungs- und Verwaltungsorganisationsgesetz (RVOG) vom 21. März 1997 | Fedlex (admin.ch)

neten Dokumenten wie z. B. WIns VBS, WeFOS[21], ZUVA etc. und Dokumentvorlagen (Schuban, Grundschutz, ISDS-Konzept) festgehalten.

Beurteilung

Die Unterschriftsberechtigungen und Kompetenzen im Sicherheitsprozess sind klar zu definieren, z. B. Geschäftsordnung, Weisung etc. Diese Dokumente sind aufeinander abzustimmen, um möglichen Widersprüchen vorzubeugen. Ohne klare Regelung kann dies bei der Unterzeichnung der Sicherheitsdokumente zu einer unzulässigen Delegation führen (siehe Abschnitt 5.3).

Empfehlung 2: Unterschriftsberechtigungen und Kompetenzen im Sicherheitsprozess

Die IR VBS empfiehlt der Gruppe Verteidigung, die Unterschriftsberechtigungen und Kompetenzen im Bereich der Sicherheit im Hinblick auf die neue Informationssicherheitsverordnung in den jeweiligen Geschäftsordnungen, Weisungen etc. zu regeln.

5.2 Herausforderung mit Public-Cloud-Anwendungen

Das VBS erlaubt den Einsatz von verschiedenen Public-Cloud-Anwendungen zu Geschäftszwecken. Nicht erlaubt hingegen sind die Bearbeitung und Speicherung klassifizierter Informationen der Stufe INTERN oder höher, besonders schützenswerte Personendaten oder Persönlichkeitsprofile sowie Informationen die dem Amtsgeheimnis unterliegen. Die Anwendungsverantwortlichen sind definiert und vom GS-VBS wird ein Verzeichnis der freigeschalteten Public-Cloud-Anwendungen geführt.

Für die Beschaffung von Public-Cloud-Anwendungen sind Regelungen und Prozesse auf Stufe Departement etabliert worden. Dadurch kann auch die Gruppe V solche Public-Cloud-Anwendungen einsetzen. Die Verantwortung für die Einhaltung des Daten- und Informationsschutzes obliegt der jeweiligen VE. Die Nachfrage zur Nutzung von Kollaborationsplattformen oder Werkzeugen mit generativer künstlicher Intelligenz (KI)[22] wie z. B. ChatGPT, welche in der Public-Cloud angesiedelt sind, steigt auch in der Gruppe V stetig an.

Gegenwärtig werden die Public-Cloud-Anwendungen bei der Gruppe V noch nicht umfassend als Schutzobjekte geführt.

---

[21] Weisungen über die Führung und Organisation der Sicherheit im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (WeFOS) vom 18. Dezember 2019

[22] Zur allgemeinen Terminologie siehe Terminologie - CNAI - Kompetenznetzwerk für künstliche Intelligenz (Kapitel 3): «Generative KI» ist ein weit gefasster Begriff, der sich auf KI-Systeme bezieht, die auf grosse Mengen von Daten aus der realen und virtuellen Welt trainiert werden, um selbst Daten zu generieren (z.B. Texte, Bilder, Tonaufnahmen, Videos, Simulationen, Codes). Sie sind oft multimodal, z. B. mit Eingaben und/oder Ausgaben in einer oder mehreren Modalitäten (z. B. Text, Bild, Video).

Beurteilung

Es besteht die Gefahr von ungewolltem Informationsabfluss und der Nichteinhaltung der Vorschriften aus den Bereichen Informationssicherheit und Datenschutz. Die IR VBS ist der Ansicht, dass eine Risikobeurteilung aus Sicht der VE notwendig und die Freigabe durch die jeweiligen Sicherheitsverantwortlichen und Informationssicherheitsbeauftragten der VE (ISBO) erforderlich ist. Risikominimierende Massnahmen wie z. B. Sensibilisierungen, Schulungen und technische Absicherungen sind nicht oder nur ungenügend vorhanden.

Empfehlung 3: Sicherheitsprozess für Public-Cloud-Anwendungen

Die IR VBS empfiehlt der Gruppe Verteidigung sicherzustellen, dass für alle Public-Cloud-Anwendungen vor deren operativen Nutzung durch die Verwaltungseinheiten eine Schutzbedarfs- und Risikoanalyse durchgeführt wird.

5.3 Gültigkeit der Sicherheitsdokumente

Im Rahmen des Berichtes Informatiksicherheit Bund 2023 des VBS an das damalige Nationale Zentrum für Cybersicherheit (NCSC; seit 1. Januar 2024 BACS) wurde seitens Gruppe V bestätigt, dass alle Schutzobjekte im Betrieb über die erforderlichen Sicherheitsdokumente verfügen. Zudem wurde bestätigt, dass das Inventar der Schutzobjekte in der Projektphase sowie der Schutzobjekte im Betrieb (Art. 14 Abs. 3 Bst. a CyRV) vorhanden und aktuell ist. Der Inhalt des Berichtes basiert auf den Informationen im zentralen Register der Schutzobjekte des VBS. Diese werden vom CISO V sowie allen ISBO bei der Berichterstattung jeweils verifiziert.

Anlässlich der Stichprobenprüfung hat die IR VBS beurteilt, ob die Sicherheitsdokumente (u. a. Schuban, Grundschutz, ISDS-Konzept, Bearbeitungsreglement) einerseits vorliegen sowie gültig sind und andererseits von den Verantwortungstragenden vor der Überführung vom Projektbetrieb in den ordentlichen Betrieb freigegeben wurden. Bei allen Stichproben wurde festgestellt, dass die Sicherheitsdokumente vorliegen respektive in Erarbeitung sind. Alle Fachanwendungen im ordentlichen Betrieb verfügen über einen unterzeichneten und gültigen Grundschutz sowie bei erhöhtem Schutzbedarf über ein ISDS-Konzept. Diese Sicherheitsdokumente werden von den Schlüsselpersonen (u. a. ISBO, Auftraggeberin/Auftraggeber bzw. Projektleiterin/Projektleiter, Geschäftsprozessverantwortliche/Geschäftsprozessverantwortlicher) sowie gemäss gängiger Praxis grossmehrheitlich entweder von der Leiterin bzw. dem Leiter der VE resp. deren Stellvertretung oder einem GL-Mitglied unterzeichnet.

Die IR VBS hat jedoch festgestellt, dass der Grundschutz resp. das ISDS-Konzept in Ausnahmefällen von einer Person unterzeichnet wurde, welche die bekannten Restrisiken in Kauf genommen hat, ohne dass eine formell dokumentierte Delegation seitens Leiterin oder Leiter der zuständigen VE vorliegt (siehe Abschnitt 5.1).

Beurteilung

Bei den Sicherheitsorganisationen in allen VE der Gruppe V wird grosser Wert darauf gelegt, dass die Sicherheitsdokumente aktuell gehalten werden und gültig sind. Die ISBO wie auch die Auftraggeberin oder der Auftraggeber und der oder die Geschäftsprozessverantwortliche werden in den Prozess einbezogen. Auch die jährliche Berichterstattung ans BACS erfolgt unter Einbindung aller ISBO.

Obwohl die Stichprobenprüfung gezeigt hat, dass in Ausnahmefällen Sicherheitsdokumente der Schutzobjekte von Personen unterzeichnet wurden, welche die Restrisiken nicht als Leiterin bzw. Leiter der VE resp. deren Stellvertretung oder als Mitglied der GL tragen, kann festgehalten werden, dass keine Fachanwendungen ohne vorzeitigen Einbezug von Entscheidungstragenden in den ordentlichen Betrieb überführt worden sind.

Im Rahmen der kontinuierlichen Überprüfung sind die Genehmigungen der Sicherheitsdokumente kritisch zu hinterfragen und bei Bedarf gemäss neuem Recht zu ergänzen (siehe Abschnitt 5.1). Die entsprechenden Sicherheitsdokumente sind zeitnah zu genehmigen und freizugeben.

5.4 Sicherheitsdokumente während der Projektphase

Gemäss verbindlichem Sicherheitsverfahren ist bei jedem Informatikvorhaben vorab eine Schuban durchzuführen. Der Zeitpunkt der Analyse richtet sich nach dem Projektvorgehensmodell HERMES und soll während der Initialisierungsphase erstellt werden.

Die komplexen Erst- und Initialbeschaffungen (Kategorien A und B) werden im PM-Tool umfassend geführt und in der Regel als Projekte mit der dafür vorgesehenen Projektmanagementmethode HERMES abgewickelt. Nur in reduziertem Umfang hingegen werden die Folgebeschaffungen (Kategorie C) geführt, u. a. Grunddaten, Projektrollen und Personalressourcen. Die Nachbeschaffungen (Kategorie D) finden keinen Eingang im PM-Tool.

Die ISBO werden grundsätzlich über neue und laufende Informatikvorhaben durch Teilnahmen an Projekt- und Fachausschüssen informiert. Bei Rüstungsprojekten und Beschaffungen mit entsprechenden Fachanwendungen hingegen sind die ISBO nicht durchgängig von Beginn weg involviert. Die ISBO haben u. a. die Möglichkeit, Informationen über den Umsetzungsstand der Projekte bzw. Beschaffungen aus dem PM-Tool zu beziehen. Gegenwärtig findet im Rahmen der einzelnen Projektphasen bzw. Beschaffungen keine automatische Benachrichtigung zu Vorhaben mit Fachanwendungen statt. Dadurch ist nicht umfassend sichergestellt, dass die ISBO frühzeitig in die Projekte und Beschaffungen einbezogen werden und die Informatiksicherheit von Anfang an berücksichtigt wird. Die ISBO sind daher auf die Kontaktaufnahme durch die Projekt- bzw. die Beschaffungsleitung angewiesen. Auch werden die ISBO aussagegemäss nicht immer oder erst verspätet über Beschaffungen von Fachanwendungen informiert, welche ausschliesslich im kleinen Rahmen (z. B. innerhalb einer Abteilung) eingesetzt werden, aber dennoch ein Sicherheitsverfahren durchlaufen müssen.

Beurteilung

Dass die ISBO grossmehrheitlich frühzeitig über neue und laufende Informatikvorhaben informiert und bereits während der Projektinitialisierungsphase eingebunden werden, wertet die IR VBS als positives Signal, dass der Prozess grundsätzlich etabliert ist. Allerdings haben die Gespräche mit den ISBO ergeben, dass sie auf eine proaktive Kommunikation zum Stand der Beschaffungen der Kategorien C und D angewiesen sind, d. h. Folge- oder Nachbeschaffungen sowie kleinere Anschaffungen von Fachanwendungen.

Damit das zentrale Register der Schutzobjekte des VBS frühzeitig aktualisiert und der Informatiksicherheit von Anfang an Rechnung getragen werden kann, ist die IR VBS der Ansicht, dass bei allen Vorhaben mit Fachanwendungen eine automatisch generierte Benachrichtigung an die ISBO Abhilfe schaffen würde. Allenfalls könnte das bestehende PM-Tool mit einer entsprechenden Funktionalität erweitert werden, um die ISBO zumindest bei Projekten der Kategorien A und B sowie Folgebeschaffungen (Kategorie C) frühzeitig zu informieren und in den Prozess einzubeziehen.

Empfehlung 4: Benachrichtigungen zu Fachanwendungen bei Vorhaben (Beschaffung / Projekt)

Die IR VBS empfiehlt der Gruppe Verteidigung, die Informationssicherheitsbeauftragten bzw. zuständige Fachstelle der Verwaltungseinheiten frühzeitig zu Vorhaben mit Fachanwendungen einzubeziehen.

5.5 Sicherheitsdokumente im ordentlichen Betrieb

Die Schutzobjekte des VBS werden gegenwärtig in einem zentralen Register als Übergangslösung geführt, welche viele Einschränkungen hat (u. a. dezentrale Ablage verschlüsselter Dokumente, fehlende Abhängigkeiten zu externen IT-Lieferanten/Dienstleister, Abbildung der Restrisiken und Massnahmen). Auch die Datenqualität entspricht noch nicht den Anforderungen an ein effizientes und benutzerfreundliches Schutzobjektregister. Die Verantwortung für die regelmässige Datenpflege im zentralen Register obliegt den VE.

Unter der Gesamtprojektleitung des VBS wurde in den letzten Monaten eine Marktleistung durch das Bundesamt für Informatik und Telekommunikation (BIT) zur Digitalisierung der Sicherheitsprozesse evaluiert. Eine WTO-Ausschreibung[23] wurde Ende September 2023 gestartet. Der Zuschlag erfolgte Mitte März 2024. Bis im Jahr 2025 soll die Beschaffung und Einführung mit ersten Pilotprojekten im VBS stattfinden.

Die ISBO beaufsichtigen gemäss Ziffer 6 der WIns VBS das Inventar der Schutzobjekte und das Verzeichnis der Ausnahmen. Zudem informieren sie die Anwendungsverantwortlichen proaktiv über anstehende Wiederholungen des Sicherheitsverfahrens, damit diese vor Ablauf der Fünfjahresfrist erfolgen. Die Anwendungsverantwortlichen, welche die IR VBS im Rah-

[23] Simap.ch: ISMS-Tool, 20.03.2024, Projekt-ID 265558, Meldungsnummer 1405503

men der Stichprobenprüfung befragt hat, sind sich ihrer Verantwortung bewusst und sind mit den Prozessen vertraut. Zudem hat die Stichprobenprüfung gezeigt, dass die Sicherheitsdokumente auch unterjährig angepasst werden, sofern sich die Anforderungen an die Informationssicherheit und den Datenschutz infolge von Anpassungen der IT-Umgebung seit der letzten Dokumentenfreigabe geändert haben.

Mit dem Inkrafttreten des ISG per 1. Januar 2024 sehen das Gesetz sowie deren Ausführungsverordnung entsprechende Übergangsfristen vor. Ein Jahr, um in einem Klassifizierungskatalog festzuhalten, wie Informationen in ihrem Zuständigkeitsbereich gemäss neuem Recht zu klassifizieren sind (vgl. Art. 51 Abs. 5 ISV) sowie zwei Jahre, um eine Schutzbedarfsanalyse durchzuführen und ihre Informatikmittel gemäss neuem Recht einzustufen (vgl. Art. 90 Abs. 2 ISG). Diese Arbeiten werden in den VE bereits heute eingeplant und befinden sich teilweise schon in der Umsetzungsphase.

Beurteilung

Die Anwendungsverantwortlichen werden von den ISBO unterstützt, um die Sicherheitsdokumente im ordentlichen Betrieb auf dem aktuellsten Stand zu halten. Insgesamt wird die Zusammenarbeit von den Beteiligten als positiv wahrgenommen. Die Stichprobenüberprüfung hat gezeigt, dass grösstenteils einheitliche und gelebte Prozesse und Strukturen bestehen, damit das Schutzobjektportfolio gemäss den Vorgaben aktualisiert wird.

Aktuell sind für eine gesamtheitliche Analyse der Sicherheitsdokumente und einer daraus folgenden Berichterstattung, z. B. bei einem Sicherheitsvorfall, zeitintensive manuelle Arbeitsschritte erforderlich. Die Einführung einer neuen Anwendung, welche die aktuellen Einschränkungen adressieren soll, ist frühestens per 2025 möglich. Die Informationen zu den Schutzobjekten sind heutzutage in einzelnen Sicherheitsdokumenten abgelegt. Inskünftig sollen die Informationen direkt in der neuen Anwendung erfasst, verarbeitet und ausgewertet werden können.

5.6 Schulung und Sensibilisierung

Alle Mitarbeitenden sind beim Eintritt ins Departement VBS verpflichtet, eine Grundschulung zur Informationssicherheit in der Bundesverwaltung abzuschliessen.

Für die Informationssicherheitsverantwortlichen und -beauftragten gibt es gegenwärtig keine adäquate Schulung und Sensibilisierung. Eine spezifische Schulung zum Thema der Schutzobjekte und der dazu gehörenden Prozesse und Verantwortlichkeiten gibt es aktuell nicht. Zudem hat die IR VBS im Rahmen ihrer Prüfung festgestellt, dass aktuelle Schulungen bzw. Hilfsmittel und Vorlagen für die Anwendungsverantwortlichen, Projektleitenden sowie ISBO, infolge rechtlicher Anpassungen wie z. B. ISG/ISV und DSG/DSV, fehlen.

Beurteilung

Aufgrund der umfangreichen Vorgaben an die Schutzobjekte würde die IR VBS erwarten, dass ein verstärktes Augenmerk auf die stufengerechte Schulung und Sensibilisierung gelegt wird. Regelmässige Auseinandersetzungen mit möglichen Risiken und deren Auswirkungen sowie dem Prozess von der initialen Erfassung von Schutzobjekten bis zu deren Ausserbetriebssetzung können den bewussten Umgang damit fördern.

Empfehlung 5: Stufengerechte Schulung und Sensibilisierung

Die IR VBS empfiehlt der Gruppe Verteidigung, in Zusammenarbeit mit dem Generalsekretariat (GS-VBS), die Schulung und Sensibilisierung der im Sicherheitsprozess beteiligten Personen stufengerecht zu gewährleisten.

6 Governance im Zusammenhang mit Schutzobjekten

Bis Ende 2023 erbrachten das Bundesamt für Informatik und Telekommunikation (BIT) sowie die Führungsunterstützungsbasis der Armee (FUB) gleichartige Informatikleistungen. Der Unterschied bestand hauptsächlich darin, dass die FUB ausschliesslich Leistungen für die Armee erbrachte. Die am 3. April 2020 durch den Bundesrat festgelegte IKT-Strategie des Bundes 2020-2023[24] sieht vor, dass die internen IKT-Leistungserbringer entsprechend ihren Kernkompetenzen zueinander komplementäre Leistungsangebote führen. In der Transitionsphase im vergangenen Jahr wurden die vereinbarten IKT-Services und Anwendungen der Gruppe V als «Blockmove» ins BIT oder als Offboarding Vorhaben ins Kommando Cyber (Kdo Cy) überführt. In der Transformationsphase ab 2024 wird einerseits begonnen, soweit technisch und betriebswirtschaftlich sinnvoll, nicht einsatzkritische Anwendungen und Services in die Regelbetriebsstrukturen des BIT zu überführen. Andererseits werden einsatzkritische Anwendungen entweder ausser Dienst gestellt, in den BIT Regelbetrieb integriert oder ins Kdo Cy rückgeführt.

In der Folgevereinbarung über die Zusammenarbeit im Bereich des Betriebes, Unterhalt und Weiterentwicklung von zivilen und militärischen Systemen, Anwendungen und Services der Armee zwischen dem VBS (vertreten durch den Armeestab) und dem Eidgenössischen Finanzdepartement (vertreten durch das BIT) vom 21. Dezember 2022 wird festgehalten, dass die Gruppe V auch bei der Übergabe des Betriebs an das BIT der Inhaber und damit der Verantwortliche für die betreffenden Anwendungen bleibt. Der Armeestab als Verantwortlicher für die zu übertragenden Schutzobjekte ist zuständig für die entsprechende und aktualisierte Dokumentation und stellt sicher, dass die entsprechenden Sicherheitsverfahren gemäss der dannzumal geltenden CyRV durchlaufen werden.

Die Überführung der Schutzobjekte ins BIT bzw. das Offboarding Vorhaben ins Kdo Cy haben dazu geführt, dass Fragen zur Governance zwischen den involvierten Parteien (Armee-

[24] IKT-Strategie des Bundes 2020–2023 (admin.ch) (Stand 16.04.2024)

stab, Kdo Cy, DU CdA) u. a. im IKT-Zielbild 2028 vom 1. Februar 2024 definiert wurden, deren Umsetzung zum Prüfungszeitpunkt aber noch nicht abschliessend geregelt bzw. etabliert wurde. Das IKT-Zielbild 2028 besagt u. a., dass das Kdo Cy die IKT- und Cybersicherheit der Armee sowie der Militärverwaltung verantwortet. Der Informationssicherheitsverantwortliche des Kdo Cy und der Chef Informationssicherheit Verteidigung (CISO V) sind zurzeit an der Finalisierung der Governance.

Die offenen Fragen bezüglich Umsetzung der Governance im Zusammenhang mit den Schutzobjekten stellen aktuell, v. a. beim Kdo Cy sowie dem Armeestab, eine Herausforderung dar, da ohne klare Regelung bei der Umsetzung u. a. nicht sichergestellt ist, dass die Sicherheitsdokumente zeitnah erstellt bzw. aktualisiert und Sicherheitsmassnahmen aus Schutzobjekten umgesetzt werden.

Beurteilung

Die IR VBS ist der Ansicht, dass die Governance im Zusammenhang mit den Schutzobjekten schnellstmöglich geklärt und umgesetzt werden muss, damit einerseits die Sicherheitsdokumente weiterhin den Vorgaben aus dem Sicherheitsverfahren entsprechen und andererseits die daraus abzuleitenden Sicherheitsmassnahmen nahtlos implementiert werden, unabhängig vom Leistungserbringer.

Empfehlung 6: Governance im Zusammenhang mit den Schutzobjekten finalisieren und umsetzen

Die IR VBS empfiehlt der Gruppe Verteidigung, die Governance im Zusammenhang mit ihren Schutzobjekten, v. a. beim Armeestab sowie dem Kommando Cyber, schnellstmöglich zu finalisieren und umzusetzen.

7 Stellungnahmen

Generalsekretariat (GS-VBS)
Wir danken für die Möglichkeit, Stellung zu nehmen. Wir sind mit den Empfehlungen einverstanden.

Staatssekretariat für Sicherheitspolitik (SEPOS)
Besten Dank für die Möglichkeit zur Stellungnahme. Das SEPOS hat keine Anmerkungen.

Gruppe Verteidigung
Die Gruppe Verteidigung dankt für die Gelegenheit zur Stellungnahme und ist mit dem Prüfbericht einverstanden.

Bundesamt für Rüstung (armasuisse)
armasuisse begrüsst die Empfehlungen und hat keine weiteren Bemerkungen.