Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

5. Februar 2024

Prüfbericht «ISMS VBS Audit 2023 – Vorfallmanagement»

IT-Prüfung I 2023-05

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, 5. Februar 2024

Prüfbericht «ISMS VBS Audit 2023 – Vorfallmanagement»

Sehr geehrte Frau Bundespräsidentin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «ISMS VBS Audit 2023 – Vorfallmanagement» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern 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
– DU Chefin VBS

Leiter Interne Revision VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Die Interne Revision VBS (IR VBS) hat geprüft, ob der Teilprozess «TP SiKP1.13 (WeMBS) Vorfallmanagement» auf Ebene Departement sowie in den jeweiligen Verwaltungseinheiten (VE) den Vorgaben der Weisungen über die Meldung und die Bewältigung von Sicherheitsvorfällen im VBS (WeMBS VBS)[1] und den ISO[2]-Anforderungen entspricht.

Mit der Verordnung über den Schutz von Informationen des Bundes (ISchV)[3] vom 4. Juli 2007 sowie der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV)[4] vom 27. Mai 2020 bestanden zum Prüfungszeitpunkt die notwendigen rechtlichen Grundlagen zum Schutz von Informationen des Bundes und der Armee. Per 1. Januar 2024 wurden mit dem Informationssicherheitsgesetz (ISG)[5] und der Informationssicherheitsverordnung (ISV)[6] jedoch neue rechtliche Grundlagen in Kraft gesetzt. Dadurch sind auch die aktuell gültigen Weisungen bezüglich angepasster Regelungen zu analysieren und bei Bedarf zeitnah zu überarbeiten. Des Weiteren sind neue Erkenntnisse und Resultate aus Informationssicherheitsvorfällen zeitnah in die Grundlagendokumente einzuarbeiten. *Die IR VBS empfiehlt der Sicherheit VBS und allen Verwaltungseinheiten des VBS, aufgrund der neuen rechtlichen Grundlagen per 1. Januar 2024, die aktuellen Weisungen zu analysieren sowie die Grundlagendokumente zum Vorfallmanagement zeitnah zu erarbeiten respektive zu überarbeiten und durch die entsprechende Geschäftsleitung freizugeben.*

Der Teilprozess Vorfallmanagement des Informationssicherheits-Managementsystems (ISMS) auf Stufe Departement ist in der Sicherheitsorganisation VBS eingebunden. *Die IR VBS empfiehlt der Sicherheit VBS, die Sicherheitsgovernance VBS zu erarbeiten sowie das Vorfallmanagement darin einzubetten, um eine effektive Steuerung und Überwachung der Informationssicherheit im Departement zu gewährleisten.*

Der Prozess zur Meldung von Informationssicherheitsvorfällen ist definiert und den VE stehen entsprechende Kommunikationskanäle zur Verfügung. Die grösseren Informationssicherheitsvorfälle in der jüngsten Vergangenheit – bei welchen das VBS bzw. einzelne VE betroffen waren – haben gezeigt, dass sich die Prozesse im Bereich Vorfallmanagement jedoch noch einspielen müssen. Unabhängig vom Vorfall obliegt die Verantwortung für die Bewältigung von Sicherheitsvorfällen den VE. Die gegenwärtig eingesetzten Übergangslösungen für die Erfassung von Informationssicherheitsmeldungen bis hin zur Bewältigung des Vorfalles

---

1 Weisungen über die Meldung und Bewältigung von Sicherheitsvorfällen im Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (WeMBS VBS) vom 30. März 2022

2 ISO: International Organization for Standardization

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

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

5 SR **128** - Bundesgesetz vom 18. Dezember 2020 über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) (admin.ch)

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

haben viele Einschränkungen und die Datenqualität entspricht noch nicht den Anforderungen an ein vernetztes, dezentrales ISMS. Für eine gesamtheitliche Berichterstattung sind zeitintensive manuelle Arbeitsschritte erforderlich. Die Verantwortung für die vollständige und akkurate Datenerfassung von Informationssicherheitsvorfällen und die regelmässige Datenpflege im zentralen Register obliegt den VE. Eine unverzügliche Erfassung aller relevanten Informationssicherheitsvorfälle im zentralen Register gemäss den WeMBS VBS ist unabdingbar, damit rasch auf Informationssicherheitsvorfälle reagiert werden kann. Zum aktuellen Zeitpunkt hat die Sicherheit VBS kein Weisungsrecht gegenüber den VE. *Die IR VBS empfiehlt der Sicherheit VBS, in Zusammenarbeit mit den Verwaltungseinheiten des VBS, Massnahmen zu ergreifen, um die Melde- und Datenqualität in der aktuellen Anwendungsumgebung durch die verantwortlichen Verwaltungseinheiten zu verbessern, damit zeitnah gesamtheitliche Berichte zu Informationssicherheitsvorfällen für die Entscheidungstragenden erstellt werden können.*

Der Prozess des Vorfallmanagements in den VE folgt dem ISO/IEC 27001-Standard. Die Vorgaben gemäss den WeMBS VBS werden grundsätzlich eingehalten. Jedoch ist die IR VBS der Ansicht, dass die Mitarbeitenden der VE stufengerecht zu schulen und zu sensibilisieren sind, um einerseits eine unverzügliche Erfassung von Informationssicherheitsmeldungen sicherzustellen und andererseits deren Qualität zu verbessern. Obwohl alle Mitarbeitenden beim Eintritt ins Departement VBS verpflichtet sind, eine Grundschulung zur Informationssicherheit in der Bundesverwaltung abzuschliessen, fehlt eine spezifische und stufengerechte Schulung und Sensibilisierung des Personals zum Thema Informationssicherheitsvorfälle. *Aus diesem Grund empfiehlt die IR VBS der Sicherheit VBS, in Zusammenarbeit mit den Verwaltungseinheiten des VBS, zu prüfen, inwiefern die Schulung und Sensibilisierung aller Mitarbeitenden im VBS sowie der IT-Dienstleistungserbringer zum Thema der Informationssicherheitsvorfälle stufengerecht durchgeführt werden kann.*

Seit Ende 2017 betreiben alle VE des VBS ein eigenes ISMS. Die VE armasuisse, swisstopo und Bundesamt für Sport (BASPO) lassen sich freiwillig nach dem ISO/IEC 27001-Standard zertifizieren. Die Zertifizierungen bestätigen dabei, dass die jeweiligen VE proaktiv Informationssicherheitsrisiken verwalten, gesetzliche und regulatorische Anforderungen erfüllen und sich auf die kontinuierliche Verbesserung ihrer Informationssicherheitspraktiken konzentrieren. Beim GS-VBS, dem Nachrichtendienst des Bundes (NDB) und dem Bundesamt für Bevölkerungsschutz (BABS) haben in regelmässigen Abständen (rund alle 2-4 Jahre) Konformitäts- bzw. Aufrechterhaltungsaudits durch die Sicherheit VBS stattgefunden. Bei der Gruppe Verteidigung (Gruppe V) wurde letztmals Ende 2018 ein ISMS-Audit durch die Sicherheit VBS durchgeführt. *Die IR VBS empfiehlt deshalb den Verwaltungseinheiten des VBS sicherzustellen, dass die gemäss ISV bei ihnen geforderten ISMS-Audits durch die Sicherheit VBS oder von einer unabhängigen Stelle regelmässig durchgeführt werden.*

1 Ausgangslage

1.1 Das Informationssicherheits-Managementsystem (ISMS)

Informationen stellen wesentliche Werte in der öffentlichen Verwaltung sowie in Unternehmen der Privatwirtschaft dar und müssen daher angemessen geschützt werden. Die meisten Informationen werden heutzutage mit Informations- und Kommunikationstechnik (IKT) erstellt, gespeichert, transportiert oder verarbeitet. Unzureichend geschützte Informationen stellen einen häufig unterschätzten Risikofaktor dar, der für eine Institution bedrohend sein kann. Deshalb sollte jede Organisation einen angemessenen Informationsschutz sicherstellen.

Der internationale Standard ISO/IEC 27001 setzt die allgemein anerkannten Rahmenbedingungen für die Implementierung eines ISMS. In Verbindung mit dem Risikomanagementprozess stellt ein ISMS die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicher und signalisiert nach innen und aussen, welche Sicherheitsanforderungen eine Organisation leben will.

ISO/IEC 27001 beschreibt ein ISMS als systematisches Modell für die Einführung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Pflege und die kontinuierliche Verbesserung der Informationssicherheit einer Organisation, um Geschäftsziele zu erreichen. Dabei wird der Ansatz einer kontinuierlichen Verbesserung der Informationssicherheit in den Vordergrund gestellt.

1.2 Das ISMS im VBS

Gemäss Artikel 36 Ziffer 1 der ISV tragen die Generalsekretärinnen und Generalsekretäre sowie die Direktorinnen und Direktoren der VE in ihrem Zuständigkeitsbereich die Verantwortung für die Informationssicherheit. Des Weiteren sind die VE für den Schutz der Informationen, die sie bearbeiten oder deren Bearbeitung sie in Auftrag geben sowie die Sicherheit der Informatikmittel, die sie selber betreiben oder durch Dritte betreiben lassen, verantwortlich (Art. 4 Abs. 1 ISV). Zudem erstellen die VE je ein ISMS (Art. 5 Abs. 1 ISV).

Seit Ende 2017 betreiben alle VE des VBS ein eigenes ISMS. Einige der ISMS auf Stufe VE sind nach dem Standard ISO/IEC 27001 zertifiziert worden. Auch das ISMS auf Stufe Departement hat in der Vergangenheit eine Zertifizierung erlangt.

1.3 Das Vorfallmanagement innerhalb des ISMS

Gemäss dem ISO/IEC 27001-Standard bezieht sich das Vorfallmanagement auf den systematischen Prozess zur Identifizierung, Reaktion, Untersuchung und Bewältigung von Informationssicherheitsvorfällen sowie der Behebung von Schwachstellen in einer Organisation.

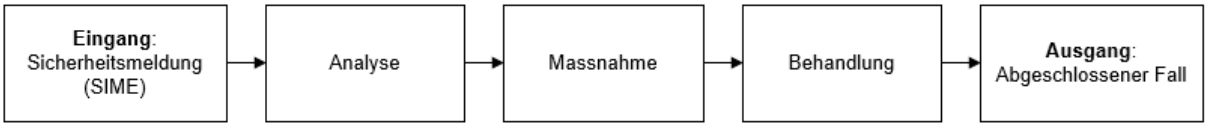

Abbildung 1: Prozess Vorfallerfassung und -bewältigung in Anlehnung an das zentrale Register «ISMS VBS»

Im Departement VBS wird der Umgang mit Sicherheitsvorfällen, Beinahe-Sicherheitsvorfällen sowie Schwachstellen in den WeMBS VBS geregelt.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der IR VBS am 23. August 2023 den Auftrag zu prüfen, ob der Teilprozess «TP SiKP1.13 (WeMBS) Vorfallmanagement» auf Ebene Departement sowie in den jeweiligen VE den Vorgaben der WeMBS VBS und den ISO-Anforderungen entspricht.

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

Die Aufgabe der IR VBS war es nicht, ISMS-Konformitätsaudits in den einzelnen VE des VBS (d. h. auf dezentraler Ebene) durchzuführen. Zudem stellt dieser Audit keine Zertifizierungsprüfung dar.

Die Prüfungshandlungen haben Mitte Oktober 2023 begonnen und wurden per Anfang Dezember 2023 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 VE 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.

4 Rechtliche Grundlagen

An der Sitzung vom 8. November 2023 hat der Bundesrat entschieden, das Informationssicherheitsgesetz (ISG) und seine vier Ausführungsverordnungen (Informationssicherheitsverordnung, ISV; Personensicherheitsprüfung, VPSP; Betriebssicherheitsverfahren, VBSV; Identitätsverwaltungs-Systeme und Verzeichnisdienste des Bundes, IAMV) 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 müssen u. a. die Generalsekretariate, die Gruppen und die Bundesämter nun ein ISMS erstellen und dieses mindestens alle drei Jahre von einer unabhängigen Stelle oder vom Departement überprüfen lassen. Details zum Vorfallmanagement sind in Artikel 12 der ISV festgehalten.

Die WIns VBS regeln die Prozesse, Aufgaben, Kompetenzen und Verantwortlichkeiten (AKV) im Bereich der Informationssicherheit VBS, die mit Hilfe eines ISMS etabliert, gesteuert und kontinuierlich verbessert werden. Damit wird definiert, wie die Anforderungen des Standards ISO/IEC 27001:2015 im VBS und in dessen Gruppen sowie den VE umgesetzt werden.

Im Bereich des Vorfallmanagements kommen die WeMBS VBS zur Anwendung. Diese regeln die Meldung von Sicherheitsvorfällen und Schwachstellen u. a. in den Bereichen Cyber- und Informationssicherheit und sollen die frühzeitige Erkennung von Sicherheitsverletzungen und -lücken fördern sowie der Erhaltung, Wiederherstellung und kontinuierlichen Verbesserung der Sicherheit nach Sicherheitsvorfällen dienen.

Obwohl nicht alle Grundlagendokumente auf dem aktuellsten Stand sind, existieren etablierte Prozesse und Kontrollen im Umgang mit Informationssicherheitsvorfällen. Sicherheitsvorfälle, welche innerhalb der entsprechenden VE bewältigt werden können, folgen einem strukturierten Prozess und werden entsprechend dokumentiert.

Beurteilung

Mit der ISchV sowie der CyRV bestanden zum Prüfungszeitpunkt die notwendigen rechtlichen Grundlagen zum Schutz von Informationen des Bundes und der Armee. Da mit dem ISG und der ISV per 1. Januar 2024 neue rechtliche Grundlagen in Kraft gesetzt wurden, sind u. a. die vorerwähnten Weisungen bezüglich angepasster Regelungen zu analysieren und bei Bedarf zeitnah zu überarbeiten.

Die Sicherheitsvorfälle während den letzten Monaten haben die Bedeutung und Wichtigkeit eines ausgereiften und gut funktionierenden Vorfallmanagementprozesses hervorgehoben. Die Grundlagendokumente müssen erarbeitet, respektive überarbeitet und durch die Geschäftsleitung freigegeben werden. Neue Erkenntnisse und Resultate aus Ereignissen sowie neue rechtliche Grundlagen wie z. B. ISG/ISV sind zeitnah in die entsprechenden Dokumente einzuarbeiten, um eine kontinuierliche Weiterentwicklung und Verbesserung sicherzu-

stellen. Anschliessend sollen diese Unterlagen mindestens jährlich überprüft und aktualisiert werden.

Empfehlung 1: Weisungen und Grundlagendokumente zum Vorfallmanagement erarbeiten resp. überarbeiten

Die IR VBS empfiehlt der Sicherheit VBS und allen Verwaltungseinheiten des VBS, aufgrund der neuen rechtlichen Grundlagen per 1. Januar 2024, die aktuellen Weisungen zu analysieren sowie die Grundlagendokumente zum Vorfallmanagement zeitnah zu erarbeiten respektive zu überarbeiten und durch die entsprechende Geschäftsleitung freizugeben.

5 Vorfallmanagement auf Stufe Departement

5.1 Governance beim Vorfallmanagement

Der Teilprozess Vorfallmanagement des ISMS auf Stufe Departement ist in der Sicherheitsorganisation VBS eingebunden. Die Erarbeitung einer Governance für die Sicherheitsorganisation VBS wurde aufgrund von Ressourcenengpässen von Oktober 2023 auf das Frühjahr 2024 verschoben.

Als Grundlagen für die Bewältigung eines Informationssicherheitsvorfalles dienen die WeMBS VBS, internationale Standards sowie die Erfahrungswerte aus den letzten grösseren Vorfällen. Der Teilprozess Vorfallmanagement wird aktuell weiterentwickelt. Für den Informationsaustausch sind auf verschiedenen Ebenen Gremien vorhanden, u. a. über das Fachorgan Informationssicherheit (FINS), den Cyber- und Sicherheitsrat VBS und die Sicherheitszellengespräche.

Beurteilung

Die geplante Ausarbeitung der Sicherheitsgovernance im Departement (unter Einbezug des Vorfallmanagements), welche die Aufgabenteilung zwischen Departement und VE berücksichtigt und die Rollen, Gremien, Aufgaben und Arbeitsprozesse definiert und konkretisiert, ist nach Ansicht der IR VBS wichtig. Sie würde den Rahmen für eine effektive Steuerung und Überwachung der Informationssicherheit im Departement bieten.

Empfehlung 2: Integration des Vorfallmanagements in die zu erarbeitende Sicherheitsgovernance VBS

Die IR VBS empfiehlt der Sicherheit VBS, die Sicherheitsgovernance VBS zu erarbeiten sowie das Vorfallmanagement darin einzubetten, um eine effektive Steuerung und Überwachung der Informationssicherheit im Departement zu gewährleisten.

5.2 Darstellung der Informationssicherheitslage

Aktuell sind in den VE verschiedene Anwendungen im Einsatz, um Informationssicherheitsmeldungen bis hin zur Bewältigung des Vorfalles zu bearbeiten. Parallel wird durch die Sicherheit VBS ein zentrales Register für Informationssicherheitsmeldungen gemäss Ziffer 6 der WeMBS geführt, welches von diversen VE als primäre Anwendung eingesetzt wird. Die Datenkonsolidierung, die Koordination und das Reporting erfolgen primär manuell. Zudem werden Sicherheitsmeldungen infolge der Klassifikation dezentral bearbeitet.

Des Weiteren haben die Prüfhandlungen ergeben, dass die Datenqualität (u. a. Umsetzungsstand der SIME, Vollständigkeit, Genauigkeit, Abhängigkeiten zwischen Anwendungen sowie zu externen IT-Lieferanten/Dienstleister) im Zusammenhang mit der Erfassung von Informationssicherheitsmeldungen durch die VE nicht durchgängig sichergestellt ist. Die Verantwortung für die vollständige und akkurate Datenerfassung von Informationssicherheitsvorfällen und die regelmässige Datenpflege im zentralen Register obliegt den VE. Zum aktuellen Zeitpunkt hat die Sicherheit VBS kein Weisungsrecht gegenüber den VE.

Unter der Gesamtprojektleitung des VBS wird zurzeit eine Marktleistung durch das Bundesamt für Informatik und Telekommunikation (BIT) zur Digitalisierung der Sicherheitsprozesse evaluiert. Eine WTO-Ausschreibung wurde Ende September 2023 gestartet.[7] Anfang Januar 2024 wird über eine Anbieterpräsentation ein künftiger Partner evaluiert. Bis im Jahr 2025 soll die Beschaffung und Einführung mit ersten Pilotprojekten im VBS stattfinden.

Beurteilung

Die gegenwärtig eingesetzten Übergangslösungen für die Erfassung von Informationssicherheitsmeldungen bis hin zur Bewältigung des Vorfalles haben viele Einschränkungen und die Datenqualität entspricht noch nicht den Anforderungen an ein vernetztes, dezentrales ISMS. Aktuell sind für eine gesamtheitliche Berichterstattung zeitintensive manuelle Arbeitsschritte erforderlich.

Die Einführung einer neuen Anwendung, welche die aktuellen Einschränkungen adressieren soll, ist frühestens per 2025 möglich. Dabei sind Informationen (z. B. Schutzobjekte, Verträge mit IT-Lieferanten/Dienstleister, Informationssicherheits- und Datenschutzkonzepte), wenn möglich mittels automatisierter Schnittstellen in die neue Anwendung zu integrieren.

Empfehlung 3: Gesamtheitliche Darstellung der Informationssicherheitslage

Die IR VBS empfiehlt der Sicherheit VBS, in Zusammenarbeit mit den Verwaltungseinheiten des VBS, Massnahmen zu ergreifen, um die Melde- und Datenqualität in der aktuellen Anwendungsumgebung durch die verantwortlichen Verwaltungseinheiten zu verbessern, damit zeitnah gesamtheitliche Berichte zu Informationssicherheitsvorfällen für die Entscheidungstragenden erstellt werden können.

[7] Simap.ch: ISMS-Tool, 29.09.2023, Projekt-ID 265558, Meldungsnummer 1365255

5.3 Bewältigung von Informationssicherheitsvorfällen

Der Prozess zur Meldung von Informationssicherheitsvorfällen ist definiert und den VE stehen entsprechende Kommunikationskanäle zur Verfügung. Informationssicherheitsmeldungen sind gemäss Artikel 5 in den WeMBS unverzüglich an die für die Bewältigung des Sicherheitsvorfalles zuständige Stelle in der VE weiterzuleiten und gleichzeitig ist Sicherheit VBS zu informieren. Diese prüft in angemessener Weise, ob die VE die gemeldeten Informationssicherheitsvorfälle und Schwachstellen zweckmässig und wirksam bewältigen beziehungsweise beheben. Der Austausch mit den Informationssicherheitsbeauftragten in den VE erfolgt periodisch über die zur Verfügung stehenden Gremien wie die FINS oder Sicherheitszellengespräche. Ergänzend finden bei grösseren Informationssicherheitsvorfällen ad hoc Gespräche mit Schlüsselpersonen der betroffenen VE statt.

Die Prüfung der IR VBS hat ergeben, dass Meldungen von Informationssicherheitsvorfällen nicht unmittelbar nach Kenntnisnahme durch die VE an die Sicherheit VBS erfolgten. Diese Informationen sind zum Teil erst mit mehreren Tagen respektive Wochen Verzögerung an die Sicherheit VBS kommuniziert und im zentralen Register für Sicherheitsvorfälle erfasst worden. Dies führte dazu, dass die Sicherheitsmeldungen nur mit Verzögerung auf Stufe Departement analysiert und bewertet werden konnten.

Wenn die Cybersicherheit der Bundesverwaltung oder ein Informatiklieferant oder -dienstleister des Bundes betroffen ist, wird dem Nationalen Zentrum für Cybersicherheit (NCSC, seit 1.1.2024 BACS) umgehend Meldung erstattet. Zudem ist der Informationssicherheitsbeauftragte des Departements VBS in überdepartementalen Gremien vertreten.

Die IR VBS hat festgestellt, dass sich die Anzahl an Informationssicherheitsvorfällen in den vergangenen zwei Jahren beinahe verdoppelt hat (davon vier grössere Vorfälle im 2023) und für die Bearbeitung der Vorfälle bei der Sicherheit VBS mehr Ressourcen gebunden wurden.

Beurteilung

Die grösseren Informationssicherheitsvorfälle in der jüngsten Vergangenheit – bei welchen das VBS bzw. einzelne VE betroffen waren – haben gezeigt, dass sich die Prozesse im Bereich Vorfallmanagement noch einspielen müssen. Die Kommunikation zum NCSC hat grundsätzlich funktioniert und die Entscheidungsträgerinnen und Entscheidungsträger im VBS wurden durch die Sicherheit VBS situationsgerecht über den aktuellen Stand informiert.

Unabhängig vom Vorfall obliegt die Verantwortung für die Bewältigung von Sicherheitsvorfällen den VE. Eine unverzügliche Erfassung aller relevanten Informationssicherheitsvorfälle im zentralen Register gemäss den WeMBS VBS ist unabdingbar, damit rasch auf Informationssicherheitsvorfälle reagiert werden kann. Diese Verantwortung der unverzüglichen Kommunikation an die Sicherheit VBS durch die VE wurde nicht durchgängig wahrgenommen. Aus diesem Grund ist das Bewusstsein über meldepflichtige Informationssicherheitsvorfälle zu schärfen und die Mitarbeitenden sind für dieses Thema verstärkt zu sensibilisieren (siehe Abschnitt 5.4).

Die IR VBS erachtet es als wichtig, dass die Informationssicherheitsbeauftragten in den VE proaktiv von der Sicherheit VBS zu aktuellen Vorfällen und Erkenntnissen im VBS – auch ausserhalb der zur Verfügung stehenden Gremien – informiert werden. Demgegenüber ist die Sicherheit VBS regelmässig über den Umsetzungsstand der laufenden Informationssicherheitsmeldungen aus den VE in Kenntnis zu setzen.

5.4 Schulung und Sensibilisierung von Mitarbeitenden

Alle Mitarbeitenden sind beim Eintritt ins Departement VBS verpflichtet, eine Grundschulung zur Informationssicherheit in der Bundesverwaltung abzuschliessen. Eine spezifische Schulung zum Thema Informationssicherheitsvorfälle gibt es aktuell nicht. Bei einigen VE werden die Mitarbeitenden zusätzlich mittels periodischen Newslettern und Eintrittsschulungen sensibilisiert. Zudem hat die IR VBS im Rahmen ihrer Prüfung festgestellt, dass spezifische Schulungen bzw. Hilfsmittel für die Informationssicherheitsbeauftragten, gestützt auf Erkenntnissen aus aktuellen Informationssicherheitsvorfällen oder infolge rechtlicher Anpassungen wie z. B. ISG/ISV, fehlen.

Beurteilung

Aufgrund der umfangreichen Anforderungen an die Informationssicherheit würde die IR VBS erwarten, dass ein verstärktes Augenmerk auf die stufengerechte Schulung und Sensibilisierung des Personals gelegt wird. Regelmässige Auseinandersetzungen mit möglichen Risiken und deren Auswirkungen sowie dem Prozess von der Erfassung von Informationssicherheitsmeldungen bis hin zur Bewältigung der Vorfälle können den bewussten Umgang damit fördern.

Empfehlung 4: Stufengerechte Schulung und Sensibilisierung aller Mitarbeitenden im VBS sowie der IT-Dienstleistungserbringer

Die IR VBS empfiehlt der Sicherheit VBS, in Zusammenarbeit mit den Verwaltungseinheiten des VBS, zu prüfen, inwiefern die Schulung und Sensibilisierung aller Mitarbeitenden im VBS sowie der IT-Dienstleistungserbringer zum Thema der Informationssicherheitsvorfälle stufengerecht durchgeführt werden kann.

6 Vorfallmanagement in den Verwaltungseinheiten

6.1 Extern zertifizierte Verwaltungseinheiten (armasuisse, swisstopo, BASPO)

Seit Ende 2017 betreiben alle VE des VBS ein eigenes ISMS und sind verpflichtet, ein ISMS nach der massgebenden ISO/IEC-Norm umzusetzen. Dabei wurde auch die Verpflichtung einer ISMS-Zertifizierung bereits mehrfach kritisch beurteilt, so auch im Rahmen des Berichtes «Standortbestimmung und Zielbild Sicherheitsmanagement VBS». Gemäss dieser Auslegeordnung wird zurzeit auf eine Zertifizierungspflicht verzichtet.[8]

Unabhängig von den Vorgaben im Departement liessen sich einzelne VE freiwillig nach dem ISO/IEC 27001-Standard zertifizieren. Während die Zertifizierung bei armasuisse und swisstopo noch bis im Jahr 2025 gültig ist, wurde beim BASPO im Oktober 2023 eine ordentliche Zertifizierung durchgeführt und bestätigt, dass das Zertifikat für drei weitere Jahre gilt.

Beurteilung

Die IR VBS stützt sich auf diese Zertifizierungen ab, welche bestätigen, dass die jeweiligen VE ein ISMS gemäss ISO/IEC 27001-Standard implementiert haben. Die Zertifizierungen bestätigen dabei, dass die jeweiligen VE proaktiv Informationssicherheitsrisiken verwalten, gesetzliche und regulatorische Anforderungen erfüllen und sich auf die kontinuierliche Verbesserung ihrer Informationssicherheitspraktiken konzentrieren. Die Vorgaben gemäss den WeMBS VBS werden grundsätzlich eingehalten. Jedoch ist die IR VBS der Ansicht, dass die Mitarbeitenden der VE stufengerecht zu schulen und zu sensibilisieren sind, um einerseits eine unverzügliche Erfassung von Informationssicherheitsmeldungen sicherzustellen und andererseits die Qualität bei den Informationssicherheitsmeldungen zu verbessern (siehe Abschnitte 5.2 - 5.4).

6.2 Verwaltungseinheiten ohne externe Zertifizierung (GS-VBS, NDB, Gruppe V, BABS)

Beim GS-VBS, dem NDB und dem BABS haben in regelmässigen Abständen (rund alle 2-4 Jahre) Konformitäts- bzw. Aufrechterhaltungsaudits durch die Sicherheit VBS stattgefunden, welche auch den Teilprozess Vorfallmanagement abdecken. In diesem Teilprozess wurden keine Abweichungen zum ISO/IEC 27001-Standard festgestellt.

Im Rahmen der Prüfhandlungen zum Vorfallmanagement in der Gruppe V hat die IR VBS festgestellt, dass auf Ebene Armeestab ein integriertes ISMS implementiert wurde, welches alle Sicherheitsvorfälle innerhalb der Gruppe V gesamtheitlich betrachtet. Zudem existieren bei der Führungsunterstützungsbasis (FUB) resp. beim Kommando Cyber (Kdo Cy) eta-

[8] Sicherheitsmanagement im VBS - Standortbestimmung und Zielbild vom 27. März 2023, Seite 6

blierte Prozesse und Kontrollen gemäss internationalen Standards. Das letzte ISMS-Audit bei der Gruppe V durch die Sicherheit VBS wurde Ende 2018 durchgeführt.

Beurteilung

In der ab 1. Januar 2024 geltenden ISV wird festgehalten, dass die VE ihr ISMS mindestens alle drei Jahre von einer unabhängigen Stelle oder ihrem Departement überprüfen lassen (Art. 5 Abs. 3 ISV). Falls interne Ressourcen nicht zur Verfügung stehen, könnten solche Audits auch mit externen Partnern durchgeführt werden.

In Anbetracht des überdurchschnittlichen Risikos von Informationssicherheitsvorfällen bei der Gruppe V – aufgrund von deren Grösse und der betriebenen Applikationen – ist die IR VBS der Ansicht, dass ein ISMS-Audit nach ISO/IEC 27001 (unter Berücksichtigung des Teilprozesses Vorfallmanagement) bei der Gruppe V in kürzeren Zeitabständen durchgeführt werden sollte, als die regelmässig vorgenommenen Konformitäts- bzw. Aufrechterhaltungsaudits beim GS-VBS, dem NDB und dem BABS.

Zudem muss sichergestellt werden, dass die ISMS-Audits auch auf das SEPOS und BACS ausgeweitet werden.

Der Prozess des Vorfallmanagements in den VE folgt dem ISO/IEC 27001-Standard. Die Vorgaben gemäss den WeMBS VBS werden grundsätzlich eingehalten. Jedoch ist die IR VBS der Ansicht, dass die Mitarbeitenden der VE stufengerecht zu schulen und zu sensibilisieren sind, um einerseits eine unverzügliche Erfassung von Informationssicherheitsmeldungen sicherzustellen und andererseits deren Qualität zu verbessern (siehe Abschnitte 5.2 - 5.4).

Empfehlung 5: Regelmässige ISMS-Audits gemäss Informationssicherheitsverordnung (ISV)

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS sicherzustellen, dass die gemäss ISV bei ihnen geforderten ISMS-Audits durch die Sicherheit VBS oder von einer unabhängigen Stelle regelmässig durchgeführt werden.

7 Stellungnahmen

Generalsekretariat VBS
Das GS-VBS dankt für die Möglichkeit zur Stellungnahme. Das GS-VBS ist mit der Beurteilung und den Empfehlungen einverstanden.

Nachrichtendienst des Bundes
Keine Bemerkungen seitens NDB; wir sind mit dem Bericht einverstanden.

Gruppe Verteidigung
Wir danken für die Möglichkeit zum vorliegenden Bericht Stellung nehmen zu können und sind mit den im Bericht formulierten Empfehlungen einverstanden.

armasuisse
armasuisse dankt der internen Revision VBS für die sorgfältige Prüfung des Sachverhaltes. armasuisse hat keine weiteren Bemerkungen.

swisstopo
swisstopo ist mit den Aussagen im Bericht einverstanden und hat keine Ergänzungen oder Änderungsanträge. Falls sich die Steuerung und Überwachung der Informationssicherheit auf Stufe Departement (vgl. Empfehlung 2) ändert, ist eine entsprechende Schulung der Sicherheitsverantwortlichen in den Ämtern notwendig, damit das Zusammenspiel verbessert werden kann.

Bundesamt für Bevölkerungsschutz
Zu den Empfehlungen der IR VBS hat das BABS keine Bemerkungen oder Ergänzungen.

Bundesamt für Sport
Wir sind mit den vorgeschlagenen Empfehlungen einverstanden. Ein Fokus sollte auf die Reduktion der zeitintensiven manuellen Arbeitsschritte gelegt werden. Zudem erachten wir es als notwendig, den gegenseitigen Erfahrungsaustausch zu intensivieren. Damit könnte vermehrt aus Fehlern gelernt, diese zukünftig vermieden und die Sicherheit gesamtheitlich gestärkt werden.

Anhang 1 Schlüsselkontrollen nach ISO/IEC 27002:2022 für den Teilprozess Vorfallmanagement

- **5.24**: Die Organisation sollte das Management von Informationssicherheitsvorfällen planen und vorbereiten, indem sie Prozesse, Rollen und Verantwortlichkeiten für das Management von Informationssicherheitsvorfällen definiert, einführt und kommuniziert.
- **5.25**: Die Organisation sollte Ereignisse im Bereich der Informationssicherheit bewerten und entscheiden, ob sie als Vorfälle im Bereich der Informationssicherheit eingestuft werden sollen.
- **5.26**: Auf Vorfälle im Bereich der Informationssicherheit sollte gemäss den dokumentierten Verfahren reagiert werden.
- **5.27**: Die aus Vorfällen im Bereich der Informationssicherheit gewonnenen Erkenntnisse sollten zur Verstärkung und Verbesserung der Informationssicherheitskontrollen genutzt werden.
- **5.28**: Die Organisation sollte Verfahren für die Identifizierung, Sammlung, Beschaffung und Aufbewahrung von Beweismitteln im Zusammenhang mit Informationssicherheitsvorfällen einführen und umsetzen.
- **6.8**: Die Organisation sollte einen Mechanismus vorsehen, mit dem das Personal beobachtete oder vermutete Ereignisse im Bereich der Informationssicherheit über die geeigneten Kanäle rechtzeitig zu melden.