Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

4. Februar 2025

Prüfbericht «Schutz der sensitiven Daten bei externen IT-Partnern des VBS in deren Entwicklungs- und Testumgebungen»

IT-Prüfung I 2024-03

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
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 4. Februar 2025

Prüfbericht «Schutz der sensitiven Daten bei externen IT-Partnern des VBS in deren Entwicklungs- und Testumgebungen»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Schutz der sensitiven Daten bei externen IT-Partnern des VBS in deren Entwicklungs- und Testumgebungen» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpersonen besprochen. Die Stellungnahmen der Verwaltungseinheiten zu unserem Bericht sind in 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 gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– DU C VBS

Leiter Interne Revision VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Das VBS arbeitet mit einer Vielzahl von externen IT-Lieferanten zusammen, welche möglicherweise sensitive Daten in deren Entwicklungs- und Testumgebungen halten bzw. bearbeiten. Der Ransomware-Angriff auf die Firma Xplain im Mai 2023 hat deutlich gemacht, welche gravierenden Folgen ein Datenabfluss für dessen Kunden haben kann.

Die Interne Revision VBS (IR VBS) prüfte, ob im VBS wirksame Prozesse und Kontrollen etabliert sind, um sicherzustellen, dass bei externen IT-Lieferanten des VBS sensitive Daten in deren Entwicklungs- und Testumgebungen nur mit den erforderlichen Schutzmassnahmen verwendet werden.

Per 1. Januar 2024 sind das Informationssicherheitsgesetz (ISG) und die dazugehörigen Ausführungsverordnungen in Kraft getreten. Die neue Informationssicherheitsverordnung (ISV) ersetzt die beiden bisherigen Verordnungen, die Cyberrisikenverordnung (CyRV) und die Informationsschutzverordnung (ISchV). Obwohl die Weisungen nicht auf dem aktuellen Stand sind, existieren Grundlagendokumente im Umgang mit der Herausgabe und dem Zugänglichmachen von Informationen in elektronischer Form. *Die IR VBS empfiehlt dem Generalsekretariat (GS-VBS), aufgrund der neuen rechtlichen Grundlagen, die aktuellen Weisungen über die Herausgabe und das Zugänglichmachen von Informationen in elektronischer Form durch IKT-Leistungserbringer zu analysieren sowie zeitnah zu überarbeiten und von der Geschäftsleitung zu verabschieden.*

Die Schutzobjekte des VBS werden derzeit in einem zentralen Register verwaltet, das als Übergangslösung dient und noch zahlreiche Einschränkungen aufweist. Insbesondere fehlen wichtige Angaben zu externen IT-Lieferanten und Dienstleistern (u. a. dezentrale Ablage verschlüsselter Dokumente und Verträge, fehlende Abhängigkeiten zu externen IT-Lieferanten). Zudem entspricht die Datenqualität noch nicht den Anforderungen an ein effizientes und benutzerfreundliches Schutzobjektregister. Die Stichprobenüberprüfung hat gezeigt, dass nur mit zeitintensiven und manuellen Arbeitsschritten eine Übersicht erstellt werden kann, wo gegebenenfalls sensitive Daten an externe IT-Lieferanten herausgegeben werden.

Die Stichprobenprüfung hat zudem gezeigt, dass grundsätzlich keine sensitiven Daten an externe IT-Lieferanten für die Weiterentwicklung, Tests oder Wartung von Anwendungen herausgegeben werden. Daten für die Weiterentwicklung, Tests oder Wartung werden mehrheitlich synthetisch erzeugt. Alternativ werden Produktivdaten anonymisiert.

Gegenwärtig werden im Zusammenhang mit der Herausgabe von Daten an externe IT-Lieferanten unterschiedliche Prozesse angewendet. Diese Prozesse sind heute nicht formal dokumentiert. Im VBS liegt keine verbindliche Prozessdokumentation vor, welche den Prozess gesamtheitlich (d. h. vom Antragseingang bis zur Herausgabe der Informationen) abbildet. *Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, einen einheitlichen Prozess zu de-*

finieren. Im Prozess sind auch relevante Schlüsselkontrollen einzubauen. Der formal dokumentierte Prozess soll anschliessend durch die Sicherheitsverantwortlichen der entsprechenden Verwaltungseinheit freigegeben und geschult werden.

Des Weiteren hat die Stichprobenprüfung ergeben, dass grossmehrheitlich auf die Ausgabe der allgemeinen Geschäftsbedingungen des Bundes aus dem Jahr 2010 abgestützt wird, welche die heutigen Anforderungen an die Informationssicherheit nicht mehr vollumfänglich abdecken. Zudem war die Vereinbarung betreffend Umgang mit schutzwürdigen Informationen bei den stichprobengeprüften Schutzobjekten nicht durchgängig ein fester Bestandteil des Vertragsinhaltes, d. h. die Bearbeitungsvorschriften fehlen teilweise. *Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit dem Bundesamt für Rüstung (armasuisse) sowie dem Bundesamt für Bauten und Logistik (BBL), sicherzustellen, dass die Verträge mit externen IT-Lieferanten einer kritischen Prüfung unterzogen und bei Bedarf durch Nachträge ergänzt werden. Dabei sollten insbesondere Aspekte wie Datenschutz und Datensicherheit, Klauseln zum Schutz der Informatikmittel vor Cyberangriffen, Meldepflichten sowie das Auditrecht zur Überprüfung der Einhaltung von Informationssicherheits- und Datenschutzanforderungen bei externen IT-Lieferanten berücksichtigt werden.*

Dem Betriebssicherheitsverfahren kommt dabei eine tragende Rolle zu, denn die externen IT-Lieferanten sollen von Beginn an wissen, was im Informationssicherheitsbereich von ihnen verlangt wird. Dies bedingt, dass alle seitens VBS involvierten Personen mit den entsprechenden Prozessabläufen vertraut sind. *Die IR VBS empfiehlt den Verwaltungseinheiten des VBS sicherzustellen, dass primär die Projektleitenden, die Anwendungsverantwortlichen und die Beschaffungsverantwortlichen im Bereich der Informationssicherheit regelmässig geschult und sensibilisiert werden.*

Weiter hat die IR VBS anlässlich der Stichprobenprüfung beurteilt, ob für die Zusammenarbeit mit den externen IT-Lieferanten einerseits eine Betriebssicherheitserklärung (BSE) gemäss Artikel 61 ISG ausgestellt wurde und andererseits, ob von Audits bei Dritten gemäss Artikel 13 Absatz 2 ISV Gebrauch gemacht wurde. Das Betriebssicherheitsverfahren wurde nicht für alle stichprobengeprüften Schutzobjekte respektive den entsprechenden externen IT-Lieferanten mit Sitz in der Schweiz durchgeführt, obwohl dies gemäss rechtlicher Grundlage erforderlich wäre. *Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit der Fachstelle für Betriebssicherheit, bei Bedarf ein Betriebssicherheitsverfahren unverzüglich einzuleiten.*

Das Auditrecht ist nur bei einem Bruchteil der Verträge explizit festgehalten. In den vergangenen Jahren wurde nur bei einem der externen IT-Lieferanten aus der Stichprobe ein Informationssicherheitsaudit durch das VBS beauftragt und durchgeführt. *Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Koordination mit der Fachstelle des Bundes für Betriebssicherheit, sicherzustellen, dass die Informationssicherheit bei Dritten im Rahmen von regelmässigen Audits risikobasiert überprüft wird.*

1 Ausgangslage

Das VBS arbeitet mit einer Vielzahl von externen IT-Lieferanten zusammen, welche möglicherweise sensitive und/oder personenbezogene Daten in deren Entwicklungs- und Testumgebungen halten bzw. bearbeiten. Diese Umgebungen werden oft nicht mit der gleichen Sorgfalt gesichert wie die produktiven Systeme. Es ist für das VBS entscheidend, dass auch Testdaten den gleichen Sicherheitsanforderungen entsprechen wie Produktionsdaten. Besonders kritisch ist dies bei sensitiven oder personenbezogenen Daten. Werden solche Daten in ihrer ursprünglichen Form an externe IT-Lieferanten weitergegeben, besteht das Risiko von Missbrauch oder einer unbefugten Weitergabe. Der Ransomware-Angriff auf die Firma Xplain im Mai 2023 hat deutlich gemacht, welche gravierenden Folgen ein Datenabfluss bei einem externen IT-Lieferanten für dessen Kunden haben kann. Solche Vorfälle führen oft zu erheblichen Reputationsschäden sowie hohen finanziellen Ausgaben und personellen Belastungen. Daher muss das VBS sicherstellen, dass Prozesse und Kontrollen implementiert sind, um die Informationssicherheit während des gesamten Lebenszykluses einer Anwendung, von der Entwicklung über den laufenden Betrieb bis hin zur Ausserbetriebnahme, zu gewährleisten.

Je nach Art des Informationssicherheitsvorfalles können sensitive und/oder personenbezogene Daten betroffen sein. Möglicherweise beabsichtigen die Angreifer, die Daten im Darknet zu publizieren, womit diese Daten auch öffentlich einsehbar werden.

Nach Bekanntwerden eines Informationssicherheitsvorfalles müssen umgehend Sofortmassen ergriffen werden, um unmittelbare Risiken einzudämmen und Betroffene zu informieren. Dabei ist zu prüfen, ob Systeme und Datenbanken des VBS kompromittiert wurden. Zudem müssen Schritte eingeleitet werden, um den Betrieb der Systeme wiederherzustellen. In einigen Fällen kann es notwendig sein, wichtige Systeme vorübergehend ausser Betrieb zu nehmen. Diese Arbeiten sind zeitintensiv und kostspielig. Zusätzlich zu den direkten Auswirkungen kann dem VBS ein langfristiger Schaden entstehen, da das Vertrauen in die Datensicherheit des VBS beeinträchtigt wird. Solche Informationssicherheitsvorfälle und ihre Folgen lassen sich nicht vollständig verhindern. Durch gezielte Massnahmen kann das VBS jedoch das Risiko erheblich reduzieren.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision (IR VBS) am 23. April 2024 den Auftrag zu prüfen, ob im VBS wirksame Prozesse und Kontrollen etabliert sind, um sicherzustellen, dass bei externen IT-Lieferanten des VBS sensitive Daten in deren Entwicklungs- und Testumgebungen nur mit den erforderlichen Schutzmassnahmen verwendet werden.

Im Rahmen dieses Prüfauftrages führte die IR VBS strukturierte Befragungen mit Schlüsselpersonen in den Verwaltungseinheiten (VE) durch. Zudem wurden weitere Vertreterinnen und Vertreter innerhalb des Departements, des Bundesamtes für Bauten und Logistik (BBL)

sowie der Privatwirtschaft befragt, welche in ihrer Funktion mit dem VBS zusammenarbeiten. Ergänzend analysierte die IR VBS Dokumente, welche ihr zur Verfügung gestellt wurden. Des Weiteren zog die IR VBS externe, öffentlich zugängliche Unterlagen bei.

Die Stichprobenprüfung von ausgewählten Schutzobjekten[1], für die Verträge mit externen IT-Lieferanten für Entwicklungen, Weiterentwicklungen und/oder Wartungen bestehen, stützt sich auf Informationen aus dem zentralen Schutzobjektregister des VBS sowie auf Umfragen bei den VE. Eine umfassende inhaltliche Beurteilung der vorgelegten Verträge wurde nicht durchgeführt. Ebenso wurde aufgrund des Prüfungszeitpunktes in der zweiten Jahreshälfte 2024 nicht beurteilt, ob die Vorgaben des neuen Rechtes (ISG/ISV sowie DSG/DSV) bereits umgesetzt worden sind.

Die Feststellungen beziehen sich auf den Zustand bis zum Abschluss der Prüfungshandlungen per Ende November 2024. Auf dieser Basis wurden auch die Beurteilungen und Empfehlungen formuliert. Entwicklungen nach Abschluss der Prüfungshandlungen sind in diesem Bericht nicht berücksichtigt.

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.

[1] 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.

4 Rechtliche Grundlagen

An der Sitzung vom 8. November 2023 hat der Bundesrat entschieden, das Informationssicherheitsgesetz (ISG)[2] und die dazugehörige Informationssicherheitsverordnung (ISV)[3] 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)[4] und die Informationsschutzverordnung (ISchV)[5]. In Artikel 9 des ISG wird festgehalten, dass die verpflichteten Behörden und Organisationen bei der Zusammenarbeit mit Dritten dafür sorgen, dass die Anforderungen und Massnahmen nach diesem Gesetz in den entsprechenden Vereinbarungen und Verträgen festgehalten werden. Zudem sorgen sie für eine angemessene Überprüfung der Umsetzung der Massnahmen.

Des Weiteren wird der Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen bei den Personendaten im Bundesgesetz über den Datenschutz (DSG)[6] vom 25. September 2020 sowie der dazugehörigen Ausführungsverordnung (DSV)[7] 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)[8] vom 3. Oktober 2008 sowie deren Verordnung (MIV)[9] 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).

Darüber hinaus regelt die Verordnung über das öffentliche Beschaffungswesen (VöB)[10] vom 12. Februar 2020 die Grundsätze und Verfahren für die Vergabe von Aufträgen an externe Leistungserbringer. Sie gewährleistet Transparenz, Gleichbehandlung und den wirtschaftli-

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

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

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

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

6 SR **235.1** - Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG)

7 SR **235.11** - Verordnung vom 31. August 2022 über den Datenschutz (Datenschutzverordnung, DSV)

8 SR **510.91** - Bundesgesetz vom 3. Oktober 2008 über militärische und andere Informationssysteme im VBS (MIG)

9 SR **510.911** - Verordnung vom 16. Dezember 2009 über militärische und andere Informationssysteme im VBS (MIV)

10 SR **172.056.11** - Verordnung vom 12. Februar 2020 über das öffentliche Beschaffungswesen (VöB)

chen Einsatz von Ressourcen. Im Kontext von Informationssicherheit und Datenschutz ist sicherzustellen, dass die Vorgaben des ISG, DSG und deren Ausführungsverordnungen in öffentlichen Ausschreibungen berücksichtigt werden.

Auf der nächsten Ebene sind die Weisungen über die Herausgabe und das Zugänglichmachen von Informationen in elektronischer Form durch IKT[11]-Leistungserbringer vom 27. September 2018 zu berücksichtigen. Sie sollen verhindern, dass das Amtsgeheimnis nach Artikel 320 des Schweizerischen Strafgesetzbuches (StGB)[12] vom 21. Dezember 1937, im Rahmen der Herausgabe von Informationen in elektronischer Form durch IKT-Leistungserbringer an Personen ausserhalb der Bundesverwaltung sowie an externe Personen, verletzt wird. Bundesinterne Leistungserbringer (z. B. Bundesamt für Informatik und Telekommunikation, Kommando Cyber) sind aus Kosten- und Effizienzgründen auf die Zusammenarbeit mit externen IT-Lieferanten angewiesen. Dies kann mit sich bringen, dass diesen in Einzelfällen sensitive und/oder personenbezogene Daten nach ISG/ISV bzw. DSG/DSV, die nicht allgemein zugänglich sind, offengelegt werden müssen, damit der Betrieb der Informationssysteme gewährleistet werden kann (z. B. zu Entwicklungs-, Test- oder Wartungszwecken).

Obwohl die VBS-Weisungen nicht auf dem aktuellen Stand sind, existieren Grundlagendokumente im Umgang mit der Herausgabe und dem Zugänglichmachen von Informationen in elektronischer Form.

Beurteilung

Die bestehenden Weisungen sind aufgrund der neuen rechtlichen Vorgaben im ISG und der ISV per 1. Januar 2024 sowie dem DSG und der DSV per 1. September 2023 nicht mehr aktuell. Eine zeitnahe Überarbeitung ist erforderlich, um die Konformität mit den geltenden Bestimmungen sicherzustellen. Darüber hinaus sind eine regelmässige, mindestens jährliche Überprüfung und Aktualisierung der Dokumente notwendig, um ihre Relevanz und Wirksamkeit langfristig zu gewährleisten.

Empfehlung 1: Weisungen überarbeiten

Die IR VBS empfiehlt dem Generalsekretariat (GS-VBS), aufgrund der neuen rechtlichen Grundlagen, die aktuellen Weisungen über die Herausgabe und das Zugänglichmachen von Informationen in elektronischer Form durch IKT-Leistungserbringer zu analysieren sowie zeitnah zu überarbeiten und von der Geschäftsleitung zu verabschieden.

[11] IKT: Informations- und Kommunikationstechnologie

[12] SR **311.0** - Schweizerisches Strafgesetzbuch vom 21. Dezember 1937

5 Prozesse und Kontrollen

5.1 Sicherheitsprozess Schutzobjektregister

Die Schutzobjekte des VBS werden derzeit in einem zentralen Register verwaltet, das als Übergangslösung dient und noch zahlreiche Einschränkungen aufweist. Insbesondere fehlen wichtige Angaben zu externen IT-Lieferanten und Dienstleistern (u. a. dezentrale Ablage verschlüsselter Dokumente und Verträge, fehlende Abhängigkeiten zu externen IT-Lieferanten). Zudem entspricht die Datenqualität noch nicht den Anforderungen an ein effizientes und benutzerfreundliches Schutzobjektregister. Die Verantwortung für die regelmässige Pflege der Daten im zentralen Register liegt bei den VE.

Zur Digitalisierung der Sicherheitsprozesse wurde unter der Leitung des VBS eine Standardlösung evaluiert und wird voraussichtlich per Mai 2025 mittels Pilotinstallationen eingeführt.

Beurteilung

Die Stichprobenüberprüfung hat gezeigt, dass nur mit zeitintensiven und manuellen Arbeitsschritten eine Übersicht erstellt werden kann, wo gegebenenfalls sensitive Daten an externe IT-Lieferanten herausgegeben werden. Die Einführung einer neuen Anwendung, welche die aktuellen Einschränkungen beheben soll, ist geplant. Derzeit werden diese Informationen zu den Schutzobjekten in einzelnen, dezentralen Sicherheitsdokumenten und Verträgen verwaltet. Inskünftig sollen diese Daten direkt in der neuen Anwendung erfasst, verarbeitet und ausgewertet werden können, um die Effizienz und Verfügbarkeit der Informationen zu verbessern. Die IR VBS hat im Rahmen von früheren Prüfungen[13,14] bereits mehrfach darauf hingewiesen, dass die Situation mit der Erfassung und dem Unterhalt der Schutzobjekte und deren Informationen im zentralen Register (als Übergangslösung) unbefriedigend ist. Aufgrund dessen, dass sich die Anwendung gegenwärtig in der Pilotphase befindet, verzichtet die IR VBS auf die Abgabe einer erneuten Empfehlung.

5.2 Prozessdokumentation und Schlüsselkontrollen

Die Stichprobenprüfung hat gezeigt, dass grundsätzlich keine sensitive und/oder personenbezogene Daten an externe IT-Lieferanten für die Weiterentwicklung, Tests oder Wartung von Anwendungen herausgegeben werden. Daten für die Weiterentwicklung, Tests oder Wartung werden mehrheitlich synthetisch erzeugt. Alternativ werden Produktivdaten anonymisiert. Bei Logdaten wird der Inhalt aufs Minimum reduziert. In allen Fällen wird grosser Wert daraufgelegt, dass die Aktivitäten nachvollziehbar dokumentiert werden.

---

[13] Interne Revision VBS, Prüfbericht vom 5. Februar 2024 «ISMS VBS Audit 2023 - Vorfallmanagement» (I 2023-05), Seite 9

[14] Interne Revision VBS, Prüfbericht vom 25. Juni 2024 «Sicherheitsdokumentation» (I 2024-02), Seiten 13 & 14

Die Gespräche mit den Informationssicherheitsbeauftragten der VE (ISBO) sowie den Projektleitenden und/oder Anwendungsverantwortlichen der stichprobengeprüften Schutzobjekte haben ergeben, dass im Zusammenhang mit der Herausgabe von Daten an externe IT-Lieferanten unterschiedliche Prozesse angewendet werden. Diese Prozesse sind heute nicht formal dokumentiert. Im VBS liegt keine verbindliche Prozessdokumentation vor, welche den Prozess gesamtheitlich (d. h. vom Antragseingang bis zur Herausgabe der Informationen) abbildet.

Das VBS verfügt zwar über Weisungen zur Herausgabe und das Zugänglichmachen von Informationen in elektronischer Form durch IKT-Leistungserbringer und das BIT hat eine Anleitung für die Datenweitergabe an externe Dritte publiziert. Es fehlt jedoch eine umfassende Prozessbeschreibung, die zentrale Schlüsselkontrollen wie die Überprüfung der Daten vor der Herausgabe oder die Quittierung der Aushändigung klar definiert.

Beurteilung

Eine formal dokumentierte Prozessbeschreibung sorgt für eine klare Kommunikation und ein besseres Verständnis innerhalb des Teams. Sie stellt sicher, dass Prozesse wiederholbar und konsistent durchgeführt werden. Fehlt eine solche Dokumentation, steigt das Risiko von Missverständnissen, Fehlinterpretationen und Abweichungen vom vorgesehenen Ablauf. Angesichts der zahlreichen rechtlichen Anforderungen, wie dem ISG, DSG und den dazugehörigen Ausführungsverordnungen, erleichtert eine vollständige Prozessbeschreibung die Nachvollziehbarkeit der Prozessschritte. Darüber hinaus schafft sie die Grundlage für Prozessverbesserungen, da Schwachstellen schneller erkannt und gezielt behoben werden können.

Empfehlung 2: Prozessdokumentation und Schlüsselkontrollen

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, einen einheitlichen Prozess zu definieren. Im Prozess sind auch relevante Schlüsselkontrollen einzubauen. Der formal dokumentierte Prozess soll anschliessend durch die Sicherheitsverantwortlichen der entsprechenden Verwaltungseinheit freigegeben und geschult werden.

5.3 Lieferantenverträge

Die Auftraggebenden des Bundes sind verpflichtet, grundsätzlich die allgemeinen Geschäftsbedingungen (AGB) gemäss Artikel 11 Absatz 2 VöB anzuwenden. Die AGB des Bundes stützen sich in wesentlichen Fragen auf das Obligationenrecht. Die Aushandlung besonderer und abweichender vertraglicher Regelungen ist zulässig, wenn sie sachlich gerechtfertigt sind. Damit können Beschaffungsverträge für das jeweilige Beschaffungsgeschäft bedürfnisgerecht und ausgewogen formuliert werden.

Im Rahmen der Stichprobenprüfung hat die IR VBS beurteilt, ob in den Verträgen bzw. den integrierten Bestandteilen (AGB) u. a. dem Datenschutz und der Datensicherheit, dem

Schutz der Informatikmittel vor Cyberangriffen und der Meldepflicht sowie dem Auditrecht zur Überprüfung von Informationssicherheits- und Datenschutzanforderungen bei externen IT-Lieferanten genügend Rechnung getragen worden ist.

Grossmehrheitlich wird auf die Ausgabe der allgemeinen Geschäftsbedingungen des Bundes aus dem Jahr 2010 abgestützt, welche die heutigen Anforderungen an die Informationssicherheit nicht mehr vollumfänglich abdecken. Ein Bezug zur ISchV, welche bis Ende 2023 in Kraft war, fehlte in den AGB gänzlich. In den neuen AGB hingegen, welche ab dem 1. Januar 2024 gelten, wird auf das ISG und DSG sowie deren Ausführungsverordnungen verwiesen. Artikel 9 ISG besagt, dass die verpflichteten Behörden und Organisationen bei der Zusammenarbeit mit Dritten dafür zu sorgen haben, dass die Anforderungen und Massnahmen nach dem ISG in den entsprechenden Vereinbarungen und Verträgen festgehalten werden.

Im DSG sowie ISG wird verbindlich vorgegeben, wie mit schutzwürdigen Informationen umzugehen ist. Darunter fallen u. a. die Bearbeitung von Informationen unter dem Amts- (Art. 320 StGB), Berufs- (Art. 321 StGB) und/oder Geschäftsgeheimnis (Art. 162 StGB) oder Personendaten (Art. 1 und Art. 2 DSG), der Erhalt von Informationen mit einem Klassifizierungsvermerk (VERTRAULICH oder GEHEIM) (Art. 5 Bst. b Ziff. 1 ISG), der Zugang zu Informatikmitteln des Bundes (Art. 5 Bst. b Ziff. 2 ISG) oder der Zugang zu Sicherheits- oder Schutzzonen 2 oder 3 einer militärischen Anlage (Art. 5 Bst. b Ziff. 3 ISG sowie Art. 2 und Art. 3 Anlageschutzverordnung[15]). Bei den stichprobengeprüften Schutzobjekten, welche der vorigen Definition unterliegen, war die Vereinbarung betreffend Umgang mit schutzwürdigen Informationen nicht durchgängig ein fester Bestandteil des Vertragsinhaltes, d. h. die Bearbeitungsvorschriften fehlen teilweise.

Exkurs: Massnahmenpaket zur Vermeidung künftiger Datenabflüsse
Der Bundesrat hat an seiner Sitzung vom 1. Mai 2024 Massnahmen beschlossen, mit denen Datenabflüsse bei IT-Lieferanten zukünftig verhindert werden sollen. Im Dokument «Massnahmenpaket zur Vermeidung künftiger Datenabflüsse» wird u. a. festgehalten, dass die AGB des Bundes und die Standardklauseln zu Cybersicherheitsbedrohungen[16] in der Praxis oft zu unspezifisch sind, um mit den Lieferanten die konkreten, auftragsbezogenen Sicherheitsbedürfnisse zu stipulieren. Die Gestaltung von standardisierten Vertragsklauseln hat sich als schwierig erwiesen, weil gewisse dafür nötige technische Sicherheitsvorgaben heute entweder fehlen oder für Externe teilweise schwierig umzusetzen sind (z. B. IKT-Grundschutz des Bundes[17]). Das Staatssekretariat für Sicherheitspolitik (SEPOS) wurde einerseits damit beauftragt, standardisierte Vertragsklauseln zur Informationssicherheit nach Artikel 10 Absatz 3 ISV sowie Sicherheitsvorgaben zur Zusammenarbeit mit Lieferanten bis Ende 2024 zu erarbeiten. Andererseits ist der IKT-Grundschutz des

[15] SR **510.518.1** - Verordnung vom 2. Mai 1990 über den Schutz militärischer Anlagen (Anlageschutzverordnung)

[16] Beschaffungskonferenz des Bundes BKB, Mustervertragsklausel der BKB betreffend Cyberangriffen (admin.ch) (Stand 22.11.2024)

[17] Bundesamt für Cybersicherheit BACS, Grundschutz (admin.ch) (Stand 22.11.2024)

Bundes zu überprüfen und der Bundesrat über allfällige Anpassungen zu informieren. Die neuen Vorgaben des Bundes sind so zu gestalten, dass sie grundsätzlich sowohl für die internen Leistungserbringer des Bundes als auch für externe Dienstleister praktisch umsetzbar und in den Verträgen vereinbar sind.[18]

Beurteilung

Die IR VBS ist der Ansicht, dass die Vertragsklauseln und die Sicherheitsvorgaben zur Zusammenarbeit mit externen IT-Lieferanten überarbeitet bzw. weiterentwickelt werden sollten, um den heutigen Anforderungen an die Informationssicherheit gerecht zu werden. Aufgrund dessen, dass der Bundesrat das SEPOS bereits damit beauftragt hat, Massnahmen hinsichtlich standardisierter Vertragsklauseln und Sicherheitsvorgaben zur Zusammenarbeit mit externen Lieferanten zu entwickeln sowie den IKT-Grundschutz des Bundes bis Ende 2024 zu überprüfen, verzichtet die IR VBS auf die Abgabe einer Empfehlung.

Die IR VBS erachtet es als wichtig, dass alle Verträge mit externen IT-Lieferanten kritisch beurteilt und bei Bedarf mittels Nachträge ergänzt werden. Dabei sollte sorgfältig bewertet werden, ob die Anforderungen aus den neuen Gesetzen (ISG/DSG) und deren Ausführungsverordnungen im Hinblick auf Informations- und Datenschutz bereits abgedeckt werden. Da Verhandlungen über Nachträge mehrere Monate dauern und möglicherweise Mehrkosten verursachen können, ist eine gründliche Analyse der Notwendigkeit solcher Ergänzungen vorab essenziell.

Empfehlung 3: Vertragsnachträge

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit dem Bundesamt für Rüstung (armasuisse) sowie dem Bundesamt für Bauten und Logistik (BBL), sicherzustellen, dass die Verträge mit externen IT-Lieferanten einer kritischen Prüfung unterzogen und bei Bedarf durch Nachträge ergänzt werden. Dabei sollten insbesondere Aspekte wie Datenschutz und Datensicherheit, Klauseln zum Schutz der Informatikmittel vor Cyberangriffen, Meldepflichten sowie das Auditrecht zur Überprüfung der Einhaltung von Informationssicherheits- und Datenschutzanforderungen bei externen IT-Lieferanten berücksichtigt werden.

5.4 Betriebssicherheitsverfahren und Audits bei Dritten

Anlässlich der Stichprobenprüfung hat die IR VBS beurteilt, ob für die Zusammenarbeit mit den externen IT-Lieferanten einerseits eine Betriebssicherheitserklärung (BSE) gemäss Artikel 61 ISG ausgestellt wurde und andererseits, ob von Audits bei Dritten gemäss Artikel 13 Absatz 2 ISV Gebrauch gemacht wurde.

[18] Der Bundesrat, Abschluss der Administrativuntersuchung zum Hackerangriff auf die Xplain AG: Bundesrat beschliesst Massnahmen, Abschnitt 1.1 (Stand: 11.10.2024)

Das Betriebssicherheitsverfahren kommt grundsätzlich dann zur Anwendung, wenn der Auftrag des Dritten eine sicherheitsempfindliche Tätigkeit nach Artikel 5 Buchstabe b ISG beinhaltet. In Artikel 26 der Verordnung über das Betriebssicherheitsverfahren (VBSV)[19] vom 8. November 2023 wird festgehalten, dass für Aufträge, die vor Inkrafttreten der Verordnung erteilt wurden, sowie für Geheimschutzverfahren gemäss Geheimschutzverordnung[20], die im Zeitpunkt des Inkrafttretens dieser Verordnung hängig sind, das bisherige Recht gilt. Für Vertragsabschlüsse und Abrufe ab dem 1. Januar 2024 hingegen, muss das Betriebssicherheitsverfahren mindestens dann durchgeführt werden, wenn der sicherheitsempfindliche Auftrag die Bearbeitung als «geheim» klassifizierter Informationen oder die Verwaltung, den Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «sehr hoher Schutz» umfasst. Bei einem sicherheitsempfindlichen Auftrag, der die Verwaltung, den Betrieb, die Wartung oder die Überprüfung von Informatikmitteln der Sicherheitsstufe «hoher Schutz» umfasst, die für die Erfüllung behörden- oder departementsübergreifender Aufgaben eingesetzt werden, wird auf Artikel 5 Absatz 2 Buchstabe c VBSV abgestützt.

Bei der Mehrheit der Stichproben konnte der Nachweis einer BSE erbracht werden. Die IR VBS hat allerdings festgestellt, dass das Betriebssicherheitsverfahren nicht für alle stichprobengeprüften Schutzobjekte respektive den entsprechenden externen IT-Lieferanten mit Sitz in der Schweiz durchgeführt wurde, obwohl dies gemäss rechtlicher Grundlage erforderlich wäre.

Weiter hat die Stichprobenprüfung ergeben, dass das Auditrecht nur bei einem Bruchteil der Verträge explizit festgehalten wurde (siehe auch Abschnitt 5.3) und in den vergangenen Jahren nur bei einem der externen IT-Lieferanten aus der Stichprobe ein Informationssicherheitsaudit durch das VBS beauftragt und durchgeführt worden ist. Ob dies darauf zu schliessen ist, dass die Vertragspartner des VBS möglicherweise ein solches Audit abgelehnt haben, seitens VBS keine Anfrage gestellt wurde oder aufgrund von Ressourcenengpässen nicht durchgeführt werden konnte, kann nicht abschliessend beurteilt werden.

Beurteilung

Das VBS setzt für seine Aufgabenerfüllung zunehmend auf die enge Zusammenarbeit mit externen IT-Lieferanten. Damit die Informationssicherheit bei der Zusammenarbeit mit der Privatwirtschaft sichergestellt werden kann, ist es aus Sicht der IR VBS unerlässlich, dass die Prozesse im Sicherheitsbereich allen Beteiligten klar und verständlich vermittelt werden. Dem Betriebssicherheitsverfahren kommt dabei eine tragende Rolle zu, denn die externen IT-Lieferanten sollen von Beginn an wissen, was im Informationssicherheitsbereich von ihnen verlangt wird. Aus diesem Grund sollen die Bedarfsstellen bei der Fachstelle Betriebssicherheit die Einleitung des Betriebssicherheitsverfahrens beantragen, bevor ein öffentli-

[19] SR **128.41** - Verordnung vom 8. November 2023 über das Betriebssicherheitsverfahren (VBSV)

[20] SR **510.413** - Verordnung vom 29. August 1990 über das Geheimschutzverfahren bei Aufträgen mit militärisch klassifiziertem Inhalt (Geheimschutzverordnung)

ches Vergabeverfahren in die Wege geleitet wird. Dies gewährleistet, dass die Informationssicherheit bereits zu Beginn berücksichtigt und kontinuierlich mit dem Fortschreiten der Vergabe und des Projekts weiterentwickelt wird. Zudem müssen die ISBO von den Projektleitenden (PL) und den Anwendungsverantwortlichen (AV) proaktiv über anstehende Wiederholungen des Betriebssicherheitsverfahrens informiert werden, um sicherzustellen, dass diese vor Ablauf der Fünfjahresfrist erfolgen. Dies bedingt jedoch, dass nicht nur die ISBO, sondern auch die PL und AV mit den entsprechenden Prozessen vertraut sind und im Bereich der Informationssicherheit regelmässig geschult und sensibilisiert werden.

Empfehlung 4: Schulung und Sensibilisierung

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, sicherzustellen, dass primär die Projektleitenden, die Anwendungsverantwortlichen und die Beschaffungsverantwortlichen im Bereich der Informationssicherheit regelmässig geschult und sensibilisiert werden.

Obwohl der Nachweis einer BSE im Rahmen der Stichprobenprüfung nicht durchgängig erbracht werden konnte, kann die IR VBS festhalten, dass grossmehrheitlich auf das Verwaltungsverfahren im Inland durch die Fachstelle Betriebssicherheit abgestützt wird und die BSE vorliegen. Aufgrund der geänderten rechtlichen Grundlagen besteht die grösste Gefahr von fehlenden BSE bei der Zusammenarbeit mit externen IT-Lieferanten dort, wo der Umgang mit schutzwürdigen Informationen in der Vergangenheit nicht unter das Geheimschutzverfahren gefallen ist.

Empfehlung 5: Betriebssicherheitsverfahren

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Zusammenarbeit mit der Fachstelle für Betriebssicherheit, bei Bedarf ein Betriebssicherheitsverfahren unverzüglich einzuleiten.

Zusätzlich sollten risikoorientiert Audits durchgeführt werden, um die Einhaltung der erforderlichen Sicherheitsstandards durch externe IT-Lieferanten zu überprüfen. Gemäss Artikel 13 Absatz 4 ISV kann die Fachstelle des Bundes für Informationssicherheit im Einvernehmen mit der Bundeskanzlei (BK) oder dem zuständigen Departement Audits durchführen oder die Durchführung der Eidgenössischen Finanzkontrolle (EFK) beantragen.

Empfehlung 6: Risikoorientierte Durchführung von Audits bei Dritten

Die IR VBS empfiehlt den Verwaltungseinheiten des VBS, in Koordination mit der Fachstelle des Bundes für Betriebssicherheit, sicherzustellen, dass die Informationssicherheit bei Dritten im Rahmen von regelmässigen Audits risikobasiert überprüft wird.

6 Stellungnahmen

Generalsekretariat (GS-VBS)

Wir danken für den Bericht und die Möglichkeit, Stellung zu nehmen. Wir sind mit den Empfehlungen einverstanden.

Staatssekretariat für Sicherheitspolitik (SEPOS)

Das SEPOS ist mit dem Bericht einverstanden. Es erachtet die Erkenntnisse und Empfehlungen als zutreffend und realistisch.

Nachrichtendienst des Bundes (NDB)

Der NDB ist mit den Feststellungen und Empfehlungen einverstanden und begrüsst insbesondere das Auditrecht bei Externen und die regelmässige Schulung und Sensibilisierung von Projektteilnehmenden.

Gruppe Verteidigung

Die Gruppe Verteidigung dankt für den Einbezug und ist mit dem Bericht und den Empfehlungen einverstanden. Der A Stab hat beides mit dem Kdo Operationen, dem Kdo Cyber, dem Kdo Ausbildung sowie der LBA abgesprochen.

Bundesamt für Rüstung (armasuisse)

Die Verantwortlichen der Informationssicherheit armasuisse unterstützen den Bericht und dessen Erkenntnisse vollumfänglich.
Wir erachten es als sehr wichtig, dass die Empfehlungen zeitnah umgesetzt werden, damit die Lücken, vor allem im Bereich Lieferantenbeziehungen aufgearbeitet werden. Die armasuisse arbeitet bereits heute mit Vertragsannexen bezüglich Cybersicherheit.
Das ISMS armasuisse ist seit 2019 ISO 27001 zertifiziert. Wir verbessern uns in diversen Themen der Informationssicherheit stetig.

Bundesamt für Landestopografie (swisstopo)

swisstopo ist mit den Empfehlungen grundsätzlich einverstanden.
Ein einheitlicher Prozess ist zu begrüssen (Empfehlung 2), idealerweise unter dem Lead des GS VBS.
Die Sensibilisierung und Schulung bezüglich Informationssicherheit (Empfehlung 4) war ein Jahresziel 2024 und ist erfolgt. Selbstverständlich ist dieses Ziel auch weiterhin aktiv zu verfolgen.
Auch wenn swisstopo keine sensitiven Daten gegenüber Dritten weitergibt, ist die Stossrichtung risikoorientierter Audits bei Lieferanten und Geschäftspartnern aufgrund der Erfahrung in letzter Zeit zu begrüssen (Empfehlung 6).

Bundesamt für Bevölkerungsschutz (BABS)
Das BABS ist mit den Empfehlungen einverstanden und hat die Empfehlungen 2-6 bereits initialisiert.

Bundesamt für Sport (BASPO)
Besten Dank für die Möglichkeit zur Stellungnahme. Das BASPO ist mit den Empfehlungen einverstanden. Diverse Empfehlungen werden beim BASPO bereits umgesetzt, wie zum Beispiel die Informationssicherheitsklauseln und die Anwendbarkeit der aktuellen AGB des Bundes in den Verträgen.

Bundesamt für Cybersicherheit (BACS)
Das BACS dankt für die Möglichkeit, Stellung zu nehmen. Wir zeigen uns mit dem Bericht und den Einschätzungen einverstanden.