Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

26. Juni 2024

Prüfbericht «Einhaltung Grundschutz Bund bei der Firma Eviden AG»

IT-Prüfung I 2024-01

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, 26. Juni 2024

Prüfbericht «Einhaltung Grundschutz Bund bei der Firma Eviden AG»

Sehr geehrte Frau Bundespräsidentin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Einhaltung Grundschutz Bund bei der Firma Eviden AG» zukommen. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern besprochen. Die Stellungnahmen der Verwaltungseinheit und der Firma Eviden AG 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]
Leiter Interne Revision VBS

[redacted]
Prüfexperte

Verteiler
– Generalsekretär VBS
– Direktorin BABS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

Management Summary

Es ist wichtig, die potenziellen Cyberrisiken bei der Auslagerung von Informatikdienstleistungen zu berücksichtigen. Die Vergangenheit hat gezeigt, dass Sicherheitslücken bei Dienstleistern zu erfolgreichen Cyberangriffen geführt haben. Daher ist es unabdingbar, angemessene Sicherheitsmassnahmen zu ergreifen, um unbefugtes Eindringen durch Dritte zu verhindern. Die Sicherheit der Daten der Bundesverwaltung (BV) sollte oberste Priorität haben.

Die Interne Revision VBS (IR VBS) hat bei der Firma Eviden AG (EVIDEN) geprüft, ob die Sicherheitsanforderungen des Grundschutzes Bund bei der Erbringung von Informatikdienstleistungen zugunsten des Bundesamtes für Bevölkerungsschutz (BABS) eingehalten wurden.

Die Firma EVIDEN betreibt für das BABS die BIAS (Betrieb Informations- und Alarmierungssysteme) Plattform ATLAS für Polyalert. Diese Plattform ist die Basis für wichtige Anwendungen des BABS wie beispielsweise Polyalert für die zentrale Auslösung der Sirenen.

Die IR VBS beurteilte die externe Leistungserbringung der Firma EVIDEN im Rahmen der entsprechenden Sicherheitsbestimmungen und stellte fest, dass die relevanten Sicherheitsvorgaben des Grundschutzes Bund im operativen Betrieb eingehalten wurden.

1 Ausgangslage

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

Die Auslagerung von Informatikdienstleistungen bergen jedoch nicht unerhebliche Cyberrisiken in sich. In der Vergangenheit waren die Cyber-Angriffe auf die Daten der BV teilweise durch Sicherheitslücken bei den Informatikdienstleistern erfolgreich. Deshalb ist ein solches unbefugtes Eindringen durch Dritte mit adäquaten Sicherheitsmassnahmen zu verhindern.

Um diesen Sicherheitsanforderungen nachzukommen, hat das Nationale Zentrum für Cybersicherheit[1] (NCSC) die minimalen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich festgelegt[2]. Diese Vorgaben sind im Dokument «IKT-Grundschutz in der Bundesverwaltung» (kurz: Grundschutz Bund) festgehalten. Dieser Grundschutz Bund lehnt sich an den Standard ISO/IEC 27002 und ist auf die Bedürfnisse und Anforderungen der Bundesverwaltungsmassnahmen angepasst und wo notwendig entsprechend ergänzt worden. Insgesamt bietet der Grundschutz Bund eine Methode, um eine angemessene und effektive Informationssicherheit in Behörden und Organisationen des öffentlichen Sektors zu gewährleisten. Für die Sicherheitsvorgaben wurden Grundlagen im Bundesgesetz über die Informatiksicherheit beim Bund überarbeitet und diese wurden per 1.1.2024 in Kraft gesetzt. Der Grundschutz Bund basiert noch in einer Übergangsphase bis Ende 2025 auf den Vorgaben des NCSC, welches seit dem 1.1.2024 in das neue Bundesamt für Cybersicherheit (BACS) übertragen wurde.

Der Grundschutz Bund legt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich fest. Für jedes Informatikschutzobjekt ist als Minimum der IKT-Grundschutz umzusetzen.

Die Umsetzung der Sicherheitsvorgaben[3] und -massnahmen sind durch die verantwortlichen VE zu überprüfen und zu dokumentieren.

EVIDEN betreibt für das BABS den Business Services AEI Polyalert auf der BIAS Plattform ATLAS, weitere Business Services (Erweiterungen von Services und Applikationen) können zu einem späteren Zeitpunkt auf der gleichen Plattform betrieben werden. Unser Prüfauftrag konzentriert sich auf die BIAS Plattform und die Anwendung Polyalert Service. Ergänzend wurde der Service- & Operations- Desk (BIAS SOD) beurteilt. Dank der modularen Architek-

---

1 SR **120.73** - Verordnung über den Schutz von Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) vom 27. Mai 2020 (Stand am 1. April 2021)

2 SR **172.010.1** - Regierungs- und Verwaltungsorganisationsverordnung vom 25. November 1998 (RVOV) (admin.ch) (1.2.2024)

3 Version 5.0: Si001 – IT-Grundschutz in der Bundesverwaltung vom 1. März 2022.

tur besteht die Möglichkeit, einzelne Teilleistungen auch für weitere BABS Business Services von anderen Dienstleistern auf der gleichen Basis zu unterstützen.

Die Firma übernimmt im BIAS SOD die Koordination zwischen dem Auftraggeber BABS, den BIAS Service Kunden (Behörden und Dritt-Partnern) und den zur Leistungserbringung benötigten Partnern des BABS.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS beauftragte am 9. Dezember 2023 die IR VBS bei der Firma EVIDEN, einem externen Dienstleister des BABS, zu prüfen, ob die einschlägigen Sicherheitsbestimmungen beim Erbringen von Leistungen im Informations- und Alarmierungsbereich eingehalten werden. Für die Prüfung beim externen Dienstleister wählte die IR VBS ein risikoorientiertes Vorgehen und fokussierten uns auf die relevanten Informatikkomponenten, welche vom externen Lieferanten entwickelt und betrieben werden. Die Auswahl für diesen Lieferanten leitete die IR VBS aus den bedeutenden Informatikdiensten zugunsten des BABS ab.

Im Rahmen dieses Prüfauftrags beurteilten die IR VBS die Einhaltung des Grundschutzes Bund bezüglich der von der Firma EVIDEN betriebenen Plattform BIAS, welche zugunsten des BABS zentrale Informatikdienstleistungen erbringt.

Die Prüfungshandlungen wurden zwischen März und April 2024 durchgeführt. Die Beurteilungen im Bericht basieren demnach auf den Erkenntnissen und Ergebnissen der Prüfungshandlungen in diesem Zeitraum.

3 Unterlagen und Auskunftserteilung

Die Interviewpartnerinnen und Interviewpartner des BABS sowie der Firma EVIDEN haben der IR VBS die notwendigen Auskünfte umfassend erteilt. Die gewünschten Unterlagen standen dem Prüfteam vollumfänglich zur Verfügung. Während unserer Prüfung traf die IR VBS auf engagierte Ansprechpersonen, die uns unterstützt und die notwendigen Informationen transparent zur Verfügung gestellt haben. Zudem hatten die IR VBS den Eindruck, dass der Firma EVIDEN der Grundschutz Bund ein wichtiges Anliegen ist und der IT-Sicherheit die notwendige Beachtung beigemessen wird. Die IR VBS dankt für die zielführende Unterstützung.

4 Firma Eviden AG

Die Firma EVIDEN ist ein Unternehmen innerhalb der Atos-Gruppe und spielt eine bedeutende Rolle in der digitalen Transformation, insbesondere im Bereich datengesteuerter Lö-

sungen. Mit einem Jahresumsatz von etwa 5 Milliarden Euro gehört die Firma EVIDEN zu den wichtigen Umsatzbringern innerhalb der Atos-Gruppe.

Als weltweit führend in datengesteuerter digitaler Transformation konzentriert sich die Firma EVIDEN darauf, vertrauenswürdige und nachhaltige Lösungen anzubieten, die Organisationen dabei unterstützen, ihre Geschäftsprozesse und -modelle mithilfe von Daten zu optimieren und zu transformieren.

5 Dienstleistung gegenüber BABS

Der BIAS SOD stellt einen 1st-Level-Plus Support (inkl. Vor-Analyse, Triage und Benutzer Unterstützung) für definierte Business Services sicher und koordiniert die Betriebsleistungen der einzelnen Business Service mit den BIAS Core Services sowie mit extern involvierten Stellen. Die Erfüllung der Partnerleistungen muss die Firma EVIDEN überwachen und sicherstellen. Mit eigenen oder BIAS dedizierten Service Management Tools (Unterstützungsmittel) unterstützt die Firma EVIDEN die Leistungserbringung der betroffenen BABS Business Services. Standardanfragen von Kunden (Behörden und Dritt-Partnern) werden direkt vom SOD bearbeitet. Die Firma EVIDEN verfügt beim BIAS SOD über zwei voll ausgestattete Standorte (Thema Business Continuity).

5.1 Dokumentation Plattform BIAS

Die Leistungserbringung der Plattform und Anwendung Polyalert wird in einem umfangreichen Vertragswerk mit Rahmenvertrag, Servicevertrag, Service-Level-Vereinbarungen etc. geregelt. In den Verträgen sind u. a. die Vorgaben zur Informatiksicherheit und zum Datenschutz festgehalten. Die Firma EVIDEN dokumentiert im Betriebshandbuch sämtliche Betriebsthemen der Business- und Core-Services inkl. Unterstützungsmittel und Umsysteme gemäss den Vorgaben des Bundes[4]. Die Prüfung ergab ein positives Gesamtbild bezüglich der Dokumentation und Nachvollziehbarkeit des Grundschutzes Bund.

Beurteilung
Die IR VBS erachtet es als wichtig, dass die Beschreibungen zur Umsetzung der Anforderungen aus dem Grundschutz Bund vollständig und nachvollziehbar dokumentiert werden. Dieser Nachweis konnte durch die Firma EVIDEN geliefert werden. Die IR VBS beurteilt die Kontrollen bezüglich den Sicherheitsanforderungen wie der Authentifizierung, Zugriffskontrolle auf Systeme und Anwendungen, Betriebssicherheit und Kommunikationssicherheit als angemessen.

[4] Grundschutz Bund

5.2 Betrieb Plattform BIAS

Solide Sicherheitsmassnahmen und -prozesse sind entscheidend, um Risiken zu minimieren und vertrauliche Daten sowie kritische Systeme vor Bedrohungen zu schützen. Die vorhandenen Massnahmen und Prozesse im Sicherheitsbereich zeigen, dass die Firma EVIDEN die Bedeutung von Informationssicherheit ernst nimmt und die erforderlichen Schritte unternimmt, um sicherzustellen, dass die Vorgaben des Grundschutzes Bund erfüllt werden. Die Zusammenarbeit zwischen BABS und der Auftragnehmerin wird als zielführend wahrgenommen.

Damit wird sichergestellt, dass die Plattform und Polyalert als hochsicheres System und mit einer hohen Verfügbarkeit betrieben und laufend weiterentwickelt wird.
Die folgenden für den Betrieb notwendigen Prozesse sind geregelt und mit den entsprechenden Kontrollen versehen:

– Incident / Problem - Management
– Change / Release - Management
– Wartung
– Support
– Logistik und Instandhaltung
– Standardaufträge gemäss Dienstleistungsvereinbarung

Die IR VBS überprüfte neben der Einhaltung der Vorgaben anhand der zur Verfügung gestellten Unterlagen und Serviceberichten die Überwachung des operativen Betriebs durch die Firma EVIDEN. Weiter beurteilte die IR VBS die unabhängig durchgeführten und dokumentierten Sicherheitsberichte durch einen externen Auditor. Die festgestellten Abweichungen zu den Vorgaben werden zeitnah mit dem BABS besprochen und wo nötig mit den entsprechenden Massnahmen behoben oder es werden zusätzliche Verbesserungen implementiert, damit die festgestellten Sicherheitsrisiken minimiert werden können.

Beurteilung
Die aktuellen Beschreibungen und Darstellungen (inkl. Grafiken und Diagrammen) entsprechen den erwarteten Standard Service-Prozessen zwischen der Firma EVIDEN, dem BABS und den Partnerorganisationen. Aus Sicht der IR VBS wird den betrieblichen Anforderungen gemäss Grundschutz Bund genügend Beachtung geschenkt. Die Prüfung ergab ein positives Gesamtbild und die IR VBS gewann den Eindruck, dass die Firma EVIDEN der Umsetzung des Grundschutzes Bund beim Betrieb der Plattform zugunsten des BABS die notwendige Beachtung zukommen lässt.

6 Stellungnahmen

Bundesamt für Bevölkerungsschutz (BABS)
Besten Dank für den Bericht, welchen wir gerne so zur Kenntnis genommen haben. Das BABS ist mit dem Bericht einverstanden.

Firma Eviden AG
Wir bedanken uns für die offene und konstruktive Art der Durchführung der Prüfung und der Interviews. Zum Inhalt des Prüfberichts haben wir keine weiteren Anmerkungen.