Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

25. Oktober 2021 [redacted]

Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern»: Kommunikations-plattform CMS und Alertswiss

IT-Prüfung I 2021-07

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 25. Oktober 2021

Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern»: Kommunikationsplattform CMS und Alertswiss

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Einhaltung Grundschutz Bund bei externen IT-Partnern» zukommen. Unsere Prüfarbeiten im Zusammenhang mit der Kommunikationsplattform CMS und Alertswiss fanden zwischen August und September 2021 bei der Firma Merkle Switzerland AG in Zürich statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern im GS-VBS, BABS sowie bei der armasuisse besprochen. Ebenfalls haben wir das Dokument mit den Verantwortlichen der Merkle Switzerland AG abgestimmt. Die Stellungnahmen zu diesem Bericht sind in Kapitel 8 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] [redacted]

Verteiler
- Generalsekretär VBS
- Direktorin BABS
- Rüstungschef
- Merkle Switzerland AG

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Einleitung / Kurzüberblick

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

Um diesen Sicherheitsanforderungen nachzukommen, hat das Nationale Zentrum für Cybersicherheit (NCSC) die minimalen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich festgelegt[1]. Diese Vorgaben sind im Dokument «IKT[2]-Grundschutz in der Bundesverwaltung» (kurz: Grundschutz Bund) festgehalten[3]. Dieser Grundschutz Bund ist ein Tailoring des Standards ISO/IEC 27002:2013, erweitert mit spezifischen Bundesverwaltungsmassnahmen. Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichtete VE zu dokumentieren und zu überprüfen[4].

Da verschiedene VE im VBS Informatiksysteme mit Unterstützung von externen Dienstleistern aufbauen und betreiben, kommen die Sicherheitsvorgaben des Grundschutzes Bund auch bei diesen Partnern zur Anwendung.

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS beauftragte am 25. Januar 2021 die Interne Revision VBS bei ausgewählten externen Dienstleistern zu prüfen, ob die einschlägigen Sicherheitsbestimmungen der BV eingehalten werden. Für die Auswahl dieser Prüfungen wählten wir ein risikoorientiertes Vorgehen und fokussierten uns auf relevante Informatiksysteme, welche von externen Partnern entwickelt oder betrieben werden. Das Auswahlverfahren stimmten wir mit unseren Ansprechpersonen in den Departementsbereichen ab. Ebenfalls wurde die Abteilung Digitalisierung und Cybersicherheit VBS in unsere Planungsarbeiten miteinbezogen. Dabei führten wir auch eine umfassende Dokumentenanalyse (z. B. Verträge und Auditberichte) durch.

Im Rahmen dieses Prüfauftrags beurteilten wir die Einhaltung des Grundschutzes Bund bei der Kommunikationsplattform CMS und Elementen von Alertswiss. Die Prüfung umfasste die Merkle Switzerland AG (nachfolgend Merkle) als Leistungserbringerin, das Generalsekretariat VBS (GS-VBS) sowie Bundesamt für Bevölkerungsschutz (BABS) als Leistungsbezüger

[1] SR **120.73 -** Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) (admin.ch) (25.10.2021)

[2] IKT = Informations- und Kommunikationstechnologie

[3] Nationale Zentrum für Cybersicherheit (NCSC) - IKT-Grundschutz in der Bundesverwaltung, Grundschutz (admin.ch) (25.10.2021)

[4] BBl **2019 1303 -** Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung (admin.ch), Ziff. 2.2 Abs. 2, Ziff. 2.3 Abs. 2 und Ziff. 3.2 Abs. 3 (25.10.2021)

und armasuisse als Beschaffungsstelle, wobei nur die Umsetzung des Grundschutzes Bund im Verantwortungsbereich von Merkle geprüft wurde.

In einem ersten Schritt liessen wir Merkle die Umsetzung des Grundschutzes Bund im Rahmen einer Selbsteinschätzung beurteilen.

Anschliessend erfolgte eine Beurteilung durch Dokumentenanalyse sowie durch strukturierte Befragungen der Schlüsselpersonen, stichprobenweise Einsicht in die Systeme und durch eine Begehung des Rechenzentrums. Unsere Ergebnisse spiegelten wir im Anschluss mit Merkle als Leistungserbringerin, dem GS-VBS und dem BABS als Leistungsbezüger, sowie der armasuisse in der Rolle als Beschaffungsstelle.

Das Vergabeverfahren, welches zum Vertragsverhältnis führte, war nicht Teil unserer Prüfung.

3 Würdigung

Während unserer Prüfung trafen wir bei Merkle, dem GS-VBS, dem BABS und der armasuisse, ausnahmslos auf engagierte Ansprechpersonen, die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen die Umsetzung der Anforderungen aus dem Grundschutz Bund ein wichtiges Anliegen ist und der IKT-Sicherheit die notwendige Beachtung beigemessen wird. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit während der Prüfung.

4 Kommunikationsplattform CMS und Alertswiss

Content Management Systems (CMS) dienen der Erfassung, Bearbeitung und Verbreitung von Internet- und Intranet-Inhalten. Die Bundesverwaltung setzt für ihre Webauftritte CMS ein. CMS stellen sicher, dass Webinhalte durch die Redaktoren einfach und schnell angepasst werden können. Zudem sorgen sie dafür, dass die Auftritte in einem einheitlichen Erscheinungsbild publiziert werden. Für die Bundesverwaltung gibt die Bundeskanzlei dieses Erscheinungsbild (Corporate Design Bund)[5] vor.

Das GS-VBS lässt ihre Kommunikationsplattform CMS mit Elementen von Alertswiss sowie der dazugehörenden IKT-Infrastruktur von einer externen Leistungserbringerin betreiben und bezieht die Leistung als Service. Am 24. Februar 2014 erhielt die Firma Namics AG (heute Merkle Switzerland AG) den Zuschlag, welcher auf simap.ch publiziert wurde. Der Grundauftrag belief sich auf 7.3 Millionen Franken (Aufbau des Service und fünf Jahre Betrieb). Dieser

[5] Bundeskanzlei BK: CD-Manual (admin.ch) (25.10.2021)

Grundauftrag wurde mit dem Nachtrag vom 17. November 2017 bis am 2. Dezember 2024 verlängert.

Auf Alertswiss fliessen die relevanten Informationen rund um die Vorsorge und das Verhalten bei Katastrophen und Notlagen in der Schweiz zusammen: eine Informationsdrehscheibe, die Leben schützen und retten kann. Die Anwendung Alertswiss teilt sich in die zwei Bereiche Webseite im CMS und Alarmierung via Polyalert[6] auf. Die Prüfung beschränkte sich ausschliesslich auf die Webseite im CMS.

Als Vertragspartner von Merkle tritt ausschliesslich die armasuisse auf. Das GS-VBS trägt die Verantwortung für die Überwachung der vertragsgemässen Auftragserfüllung der Merkle. Die inhaltliche Verantwortung für Alertswiss liegt beim BABS.

5 Merkle Switzerland AG in Kürze

Namics wurde im Jahre 1995 gegründet und war bis zum Verkauf an Merkle (Ende 2018) inhabergeführt. Seit dem Verkauf ist Namics Teil des dentsu[7] Netzwerkes.

Merkle Switzerland AG[8] ist eine datengetriebene Full-Service-Agentur mit Fokus auf Customer Experience Transformation[9] mit Hauptsitz in Zürich. Sie berät die Kunden bei der Digitalisierung ihres Unternehmens und liefert ihnen umfassende Leistungen in der Beratung zur digitalen Transformation sowie im Bereich Customer Experience Management.

6 Feststellung und Beurteilung

6.1 Vertragliche Vereinbarungen und ISDS-Konzept

Feststellung: Die Leistungserbringung für die Kommunikationsplattform CMS und Alertswiss durch Merkle ist in einem umfangreichen Vertragswerk mit Rahmenvertrag, Nachtrag, Servicevertrag, Service-Level Agreements, etc. geregelt. In den Verträgen sind u. a. die Vorgaben zur Informationssicherheit und zum Datenschutz festgehalten. Die Alertswiss Webseite ist Bestandteil der Kommunikationsplattform CMS und unterstehen dessen vertraglichen Vereinbarungen. Das heute gültige Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) bildet die neuesten Entwicklungen und Anforderungen, d. h. die Leistungserbringung durch Merkle sowie die Alertswiss Webseite, noch nicht ab. Daher wird dieses momentan überarbeitet. Die dazugehörenden Dokumente wie die Schutzbedarfsanalyse, die Risikoanalyse und die Massnahmenumsetzung wurden bereits nachgeführt.

---

6 BABS - Polyalert: das System für die Alarmierung der Bevölkerung: Polyalert (admin.ch) (25.10.2021)

7 Dentsu Schweiz - Homepage: dentsu (25.10.2021)

8 Merkle - Homepage: Merkle – Ihr Customer Experience Management Partner (merkleinc.ch) (25.10.2021)

9 Deutsche Übersetzung: Optimierung des Kundenerlebnisses

Beurteilung: Unsere Prüfung ergab ein positives Gesamtbild bezüglich dem Vertragswerk. Das bestehende ISDS-Konzept ist gültig, sollte aber aufgrund der veränderten vertraglichen Gegebenheiten sowie fehlender Abbildung von Alertswiss zeitnah aktualisiert werden.

6.2 Vertragspartner der Merkle Switzerland AG

Feststellung: Zur Auftragserfüllung hat Merkle einen Subakkordanten, Aspectra AG als Hostingpartner für Daten und Services, beigezogen. Die vertragliche Vereinbarung mit Merkle sieht zudem vor, dass weitere Sub-Subakkordanten beigezogen werden können. Die Verantwortung für das Erbringen der Leistungen verbleibt stets bei Merkle.

1) Die Firma Aspectra AG als Subakkordant betreibt die Infrastruktur des CMS und ist für deren Betrieb und Verfügbarkeit verantwortlich. Die IKT-Systeme werden in der Schweiz gehostet. Das Kontrollumfeld und die IKT-Sicherheit der Aspectra AG werden jährlich überprüft. Im Januar 2021 wurde durch Ernst & Young AG eine ISAE 3000 Type II und im März 2021 durch KPMG AG eine ISO/IEC 27001:2013 Zertifizierung ohne Einschränkungen erteilt.

2) Ein zentraler Sub-Subakkordant ist Akamai Technologies, Inc. (nachfolgend Akamai), ein global tätiger Dienstleister für CDN-Dienste (Content Delivery Network[10]). Im Hintergrund gewährleistet Akamai, dass die Alertswiss Webseite auch bei grossen Lastspitzen immer aufgerufen werden kann. Für diese Dienstleistung wurde ein Vertrag mit Akamai in Deutschland abgeschlossen.

Beurteilung: Aspectra AG hält die Vorgaben des Grundschutzes Bund für die Infrastruktur der Kommunikationsplattform CMS und der Alertswiss Webseite ein.

In einer Krisensituation können sich die Bedürfnisse und Interessen im Ausland rasch verändern. Falls in einer solchen ausserordentlichen Lage die vom CMS benötigten Serveranbindungen im Ausland unterbrochen würden, könnte dies dazu führen, dass die Alertswiss Webseite vorübergehend nicht mehr aufrufbar ist. Auf einen ausländischen Vertragspartner kann in einer solchen ausserordentlichen Lage nur eingeschränkt Einfluss genommen werden. Dieses Risiko könnte durch einen inländischen Dienstleister minimiert werden. Allenfalls müssten auch die Anforderungen an die Spitzenlast, d. h. Anzahl der Nutzerinnen und Nutzer mit gleichzeitigem Zugriff auf die Alertswiss Webseite, durch das BABS überdenkt werden.

6.3 Sicherheitsvorgaben des Grundschutzes Bund

Feststellung: Der Firma Merkle sowie deren Subakkordanten ist die Umsetzung der Anforderungen aus dem Grundschutz Bund ein wichtiges Anliegen. Der IKT-Sicherheit wird die notwendige Beachtung beigemessen.

[10] TechTarget: What is a CDN? How Do Content Delivery Networks Work? (techtarget.com) (25.10.2021)

Beurteilung: Unsere Prüfung ergab ein positives Gesamtbild bezüglich der Einhaltung des Grundschutzes Bund. Die Firma Merkle hält die Vorgaben des Grundschutzes Bund in Bezug auf die Kommunikationsplattform CMS sowie Alertswiss ein.

7 Empfehlung

Aufgrund unserer Feststellung empfehlen wir dem GS-VBS

zu 6.1 die Überarbeitung des ISDS-Konzeptes zeitnah abzuschliessen und zu genehmigen sowie

zu 6.2 zu überprüfen, inwiefern das Verfügbarkeitsrisiko mit einem inländischen Dienstleister für CDN-Dienste minimiert werden könnte.

8 Stellungnahmen

Generalsekretariat VBS
Das Generalsekretariat VBS dankt der internen Revision VBS für die Gelegenheit zur Stellungnahme. Das ISDS-Konzept wird zurzeit finalisiert und bis Ende 2021 werden die Arbeiten daran abgeschlossen sein. Die Laufzeit des aktuellen CMS-Service ist bis 2024 beschränkt. Spätestens zu diesem Zeitpunkt muss der Standarddienst Web alle CMS-Funktionen übernehmen können. Aufgrund der kurzen Restlaufzeit lohnt sich der Aufwand nicht, die gut funktionierenden Systeme vorzeitig abzulösen. Die Thematik wird im Rahmen der Integration in den Standarddienst Web aufgenommen und adressiert.

Bundesamt für Bevölkerungsschutz
Das BABS begrüsst den Prüfbericht und die beiden dargelegten Empfehlungen. Das GS VBS ist zwar der Vertragspartner für die CMS Web Plattform aber die Empfehlungen sind natürlich auch für das BABS ausserordentlich wichtig. Insbesondere die Prüfung der Reduzierung des Verfügbarkeitsrisikos mit einem inländischen Dienstleister für CDN-Dienste erachten wir als sehr wertvoll. Diese Herausforderung sollte jedoch im Rahmen des DTI-Projektes «Standartdienste -Web» geprüft und weiterverfolgt werden, da eine Gesamtablösung ansteht.

armasuisse
armasuisse bedankt sich für den Bericht. armasuisse ist mit dem Bericht und den Schlussfolgerungen einverstanden und hat keine weiteren Bemerkungen.

Merkle Switzerland AG
Auf die Einhaltung des Grundschutzes Bund legen wir grossen Wert und haben diese Anforderungen in unseren Prozessen entsprechend eingebunden bzw. berücksichtigt. Mit dem Audit durch die Interne Revision VBS konnten diese Massnahmen zur Einhaltung des Grundschutzes Bund gemeinsam detailliert überprüft und von der Internen Revision VBS anschliessend beurteilt werden. Sowohl die gemeinsame Überprüfung wie auch die neutrale Beurteilung ist für uns als Dienstleister für das VBS sehr wichtig und hilfreich. Die Empfehlungen aus diesem Audit können wir sehr gut nachvollziehen und stehen unterstützend bei deren Umsetzungen gerne zur Verfügung.