



1. Juni 2022

Prüfbericht «Einhaltung Grundsatz Bund bei externen IT-Partnern des VBS: Alertswiss-App 2.0»

IT-Prüfung I 2022-02



Frau
Bundesrätin Viola Amherd
Chefin VBS
Bundeshaus Ost
3003 Bern

Bern, 1. Juni 2022

**Prüfbericht «Einhaltung Grundsatz Bund bei externen IT-Partnern des VBS:
Alertswiss-App 2.0»**

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Einhaltung Grundsatz Bund bei externen IT-Partnern des VBS: Alertswiss-App 2.0» zukommen. Unsere Prüfarbeiten fanden zwischen Februar und März 2022 bei der Firma Ubique Innovation AG in Zürich statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern im BABS besprochen. Ebenfalls haben wir das Dokument mit den Verantwortlichen der Ubique Innovation AG abgestimmt. Die Stellungnahmen zu unserem 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

Verteiler

- Generalsekretär VBS
- Direktorin BABS
- Ubique Innovation AG

1 Informatiksicherheit in der Bundesverwaltung

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 (National Cyber Security Centre - NCSC) die minimalen Sicherheitsvorgaben im Bereich Informatiksicherheit in einer Verordnung¹ verbindlich festgelegt. Diese Vorgaben sind im Dokument «Si001 – IT-Grundschatz in der Bundesverwaltung» (kurz: Grundschatz Bund) festgehalten². Der Grundschatz Bund beschreibt die minimalen organisatorischen, personellen und technischen Sicherheitsvorgaben. Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichtete VE zu dokumentieren und zu überprüfen³.

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

2 Auftrag, Methodik und Abgrenzung

Die Chefin VBS beauftragte am 28. Januar 2022 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. Dabei führten wir auch eine umfassende Dokumentenanalyse (z. B. Verträge und Auditberichte) durch.

Basierend auf dem bestehenden Vertragsverhältnis prüfte die Interne Revision VBS, ob die einschlägigen IT-Sicherheitsbestimmungen der Bundesverwaltung im Zusammenhang mit der Alertswiss-App 2.0, welche von der Firma Ubique Innovation AG (nachfolgend Ubique) entwickelt und betrieben wird, eingehalten werden.

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

² IKT-Grundschatz in der Bundesverwaltung, [Grundschatz \(admin.ch\)](#) (01.06.2022)

³ BBI 2019 1303 [Weisungen des Bundesrates über die IKT-Sicherheit in der Bundesverwaltung vom 16. Januar 2019 \(admin.ch\)](#), Ziff. 2.2 Abs. 2, Ziff. 2.3 Abs. 2 und Ziff. 3.2 Abs. 3

Die Prüfung umfasste Ubique als Leistungserbringerin, das Bundesamt für Bevölkerungsschutz (BABS) als Leistungsbezügerin und Beschaffungsstelle, wobei nur die Umsetzung des Grundschatzes Bund im Verantwortungsbereich von Ubique geprüft wurde.

Die Beurteilung erfolgte durch Dokumentenanalysen sowie durch strukturierte Befragungen der Schlüsselpersonen und eine stichprobenweise Einsicht in die Systeme. Unsere Ergebnisse spiegeln wir im Anschluss mit Ubique als Leistungserbringerin und dem BABS als Leistungsbezügerin sowie Beschaffungsstelle.

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

3 Würdigung

Während unserer Prüfung trafen wir bei Ubique und dem BABS 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 Grundschatz Bund ein wichtiges Anliegen ist und der IT-Sicherheit die notwendige Beachtung beigemessen wird. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit während der Prüfung.

4 Alertswiss-App 2.0

Im Ernstfall ist es besonders wichtig, die betroffene Bevölkerung schnell und möglichst direkt zu erreichen. Auf Alertswiss fliessen die relevanten Informationen bei Ereignissen in der Schweiz auf einer Informationsdrehseibe zusammen, die Leben schützen und retten kann.⁴

Alertswiss nutzt für die Alarmierung der Bevölkerung auch eine nationale Alarm-App. Via Polyalert⁵ werden die Alarme, Warnungen und Informationen für unterschiedliche Gefahren direkt auf das Smartphone der betroffenen Bevölkerung übertragen. Parallel zu den Meldungen in der App werden die Ereignisinformationen auch auf der Alertswiss-Webseite publiziert (vgl. letztjährigen Prüfbericht zur Kommunikationsplattform CMS und Alertswiss⁶). Diese Prüfung beschränkt sich ausschliesslich auf die Alertswiss-App 2.0.

⁴ BABS - Alertswiss: Alarmierung und Information, [Alertswiss \(admin.ch\)](#) (01.06.2022)

⁵ BABS - Polyalert: das System für die Alarmierung der Bevölkerung: [Polyalert \(admin.ch\)](#) (01.06.2022)

⁶ [Prüfbericht «Einhaltung Grundschatz Bund bei externen IT-Partnern»: Kommunikationsplattform CMS und Alertswiss \(admin.ch\)](#) vom 25.10.2021 (01.06.2022)

Am 20.12.2016 erhielt Ubique den Zuschlag für die Entwicklung und den Betrieb der Alertswiss-App 2.0, welcher auf simap.ch publiziert wurde. Der Grundauftrag belief sich auf 1,5 Millionen Franken.

Als Vertragspartner von Ubique tritt ausschliesslich das BABS auf. Es trägt auch die Verantwortung für die Überwachung der Auftragserfüllung der Ubique. Die inhaltliche Verantwortung für die Alertswiss-App 2.0 liegt ebenfalls beim BABS.

5 Kurzportrait der Ubique Innovation AG

Ubique ist ein 2010 gegründetes Digitalunternehmen mit Sitz in Zürich. Heute besteht die Firma aus einem interdisziplinären Team mit fünfzig Mitarbeitenden.

Ubique realisiert digitale Produkte für Endnutzende mit Fokus auf ganzheitliche technische Entwicklungen und hochwertige User Experience. Hierbei entstehen technisch anspruchsvolle Lösungen in den Bereichen Datenvisualisierung, IT-Security und hochverfügbare skalierbare Systeme zu einer umfassenden Mobile Experience.

Ferner entwickelt Ubique zukunftsorientierte Lösungen in den Feldern Digital Health, New Work und Mobilität.

6 Feststellungen und Beurteilungen

6.1 Vertragswerk und Sicherheitsprozess

Feststellung: In einem umfassenden Vertragswerk sind die Entwicklung und der Betrieb der Alertswiss-App 2.0 geregelt. Dieses Vertragswerk beinhaltet auch ein umfangreiches Pflichtenheft. Darin sind u. a. die Vorgaben zur Informationssicherheit und dem Datenschutz detailliert festgehalten. Für die Alertswiss-App 2.0 wurde auch ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt. Die Umsetzung dieser Vorgaben wird vom BABS mit regelmässigen Sicherheitsaudits überprüft. Die heute gültige Version dieses ISDS-Konzepts bildet jedoch noch nicht die neusten Entwicklungen und Erkenntnisse ab.

Beurteilung: Unsere Prüfung ergab ein positives Gesamtbild bezüglich dem Vertragswerk und dem Sicherheitsprozess beim BABS. Das bestehende ISDS-Konzept ist gültig, sollte aber aufgrund der veränderten Gegebenheiten zeitnah aktualisiert werden.

6.2 Vertragspartner der Ubique Innovation AG

Feststellung: Für die Auftragserfüllung hat Ubique die folgenden zwei Subakkordanten beigezogen. Die Verantwortung für das Erbringen der Leistungen gegenüber dem BABS verbleibt aber stets bei Ubique.

1) Die Firma Swisscom (Schweiz) AG (nachfolgend Swisscom) betreibt die Infrastruktur für die Meldungsaufbereitung der Alertswiss-App 2.0. Diese IT-Systeme werden in der Schweiz gehostet. Das Kontrollumfeld und die IT-Sicherheit werden regelmässig überprüft. Seit dem 1. Januar 2008 besitzt die Swisscom eine ISO/IEC 27001:2013 Zertifizierung ohne Einschränkungen.

2) Die Firma Amazon Web Services, Inc. (nachfolgend AWS) in Frankfurt ermöglicht mit ihren CDN-Diensten (Content Delivery Network⁷) die Meldungsverbreitung. Im Hintergrund gewährleistet AWS damit, dass auch bei grossen Lastspitzen die Meldungen rasch verbreitet werden können. Diese IT-Systeme werden in Deutschland gehostet. Das Kontrollumfeld und die IT-Sicherheit werden regelmässig überprüft. Seit dem 18. November 2010 besitzt AWS eine ISO/IEC 27001:2013 Zertifizierung ohne Einschränkungen.

Beurteilung: Die beiden Vertragspartner Swisscom und AWS halten die Vorgaben des Grundschatzes Bund für die Infrastruktur der Alertswiss-App 2.0 ein.

6.3 Verfügbarkeit in Krisensituationen

Feststellung: In einer Krisensituation können sich die Bedürfnisse und Interessen im Ausland rasch verändern. Falls in einer ausserordentlichen Lage die von der Alertswiss-App 2.0 benötigten Systeme im Ausland unterbrochen würden, könnte dies dazu führen, dass auf den Smartphones vorübergehend keine Meldungen mehr empfangen werden könnten.

Da in einer ausserordentlichen Lage auf einen ausländischen Vertragspartner nur eingeschränkt Einfluss genommen werden kann, birgt dies ein gewisses Risiko. Im Fall der Alertswiss-App 2.0 betrifft dies primär die Firmen AWS in Deutschland mit ihren CDN-Diensten sowie Apple Inc. und Google LLC in den USA für die Push-Notification-Services⁸.

Beurteilung: Mit inländischen CDN-Dienstleistern könnte das Verfügbarkeitsrisiko teilweise minimiert werden.

6.4 Sicherheitsvorgaben des Grundschatzes Bund

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

⁷ TechTarget: [What is a CDN? How Do Content Delivery Networks Work? \(techtarget.com\)](https://www.techtarget.com/what-is-a-cdn/) (01.06.2022)

⁸ Push-Notification-Services: [Introduction to Push Notifications | Web | Google Developers](https://developers.google.com/firebase/docs/cloud-messaging/) - [Local and Remote Notification Programming Guide: APNs Overview \(apple.com\)](https://developer.apple.com/documentation/usernotifications/) (01.06.2022)

Beurteilung: Unsere Prüfung ergab ein positives Gesamtbild bezüglich der Einhaltung des Grundschatzes Bund. Die Firma Ubique hält die Vorgaben des Grundschatzes Bund in Bezug auf die Systeme der Alertswiss-App 2.0 ein.

7 Empfehlungen

Aufgrund unserer Feststellungen empfehlen wir dem BABS,

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

- zu 6.3 zu überprüfen, inwiefern das Verfügbarkeitsrisiko mit einem inländischen Dienstleister für CDN-Dienste teilweise minimiert werden könnte.

8 **Stellungnahmen**

Bundesamt für Bevölkerungsschutz

Das BABS dankt der Internen Revision VBS für die Gelegenheit zur Stellungnahme und ist mit dem vorliegenden Bericht einverstanden. Die beiden Empfehlungen beabsichtigt das BABS im Rahmen des Life Cycle Managements aufzunehmen.

Ubique Innovation AG

Ubique nimmt die Sicherheit ihrer Lösungen ernst, was durch das Audit über den Grundschatz Bund bestätigt wurde. Wir nehmen die Empfehlungen zur Kenntnis und stehen dem VBS / BABS zur Verfügung, sobald eine Entscheidung in dieser Hinsicht getroffen wird.