Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Interne Revision VBS

22. Dezember 2021 [redacted]

Prüfbericht «Videokonferenzen im VBS»

IT-Prüfung I 2021-04

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, 22. Dezember 2021

Prüfbericht «Videokonferenzen im VBS»

Sehr geehrte Frau Bundesrätin Amherd

Gerne lassen wir Ihnen unseren Prüfbericht «Videokonferenzen im VBS» zukommen. Unsere Prüfarbeiten fanden zwischen Juli und September 2021 statt. Den vorliegenden Bericht haben wir mit unseren Ansprechpartnern besprochen. Die Stellungnahmen der Departementsbereiche 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 jederzeit gerne zur Verfügung.

Freundliche Grüsse

Interne Revision VBS

[redacted]

Verteiler
– Generalsekretär VBS
– DU Chefin VBS

Interne Revision VBS
Schauplatzgasse 11
3003 Bern

1 Management Summary

Im Zeitalter der Digitalisierung hat sich die Art und Weise wie miteinander kommuniziert wird, stark gewandelt. Die Nachfrage und Nutzung von Videokonferenzanwendung hat sich im dezentral ausgerichteten VBS aufgrund der Pandemie-Situation stark erhöht. Im Auftrag der Departementschefin vom 28. Juni 2021 prüften wir, welche Arten von Videokonferenzen im VBS eingesetzt werden und ob die relevanten Standards sowie Cybersicherheits- und Datenschutzbestimmungen eingehalten werden. Der Fokus lag auf den wesentlichen und breit eingesetzten Lösungen im VBS. Spezifische Insellösungen mit kleinen Benutzerkreisen, wie sie z. B. in der Armee und im Nachrichtendienst des Bundes (NDB) eingesetzt werden, wurden in dieser Prüfung ausgeschlossen.

Die vorliegende Prüfung ergab, dass heute im VBS verschiedene Videokonferenzlösungen im Einsatz sind, welche die Stufe VERTRAULICH nach der Informationsschutzverordnung (ISchV[1]) momentan nicht abdecken können. Diese Lücke sollte geschlossen werden.

Weiter stellt sich die Frage, ob die angedachte Ablösung von «Skype for Business» mit einer ausländischen Cloud-Architektur zielführend ist. Der im März 2018 verabschiedete «Clarifying Lawful Overseas Use of Data Act» (CLOUD Act)[2] hat für die US-Strafverfolgungsbehörden und Cloud Service Provider (CSP) extraterritoriale Wirkungen. Es erlaubt den US-Strafverfolgungsbehörden, Zugang zu den Daten zu erhalten, die von CSP mit Sitz in den USA aufbewahrt werden. Und dies unabhängig davon, wo auf der Welt die Daten gespeichert sind. Dieses US-Bundesgesetz hat weitreichende Auswirkungen auf die in der Bundesverwaltung (BV) geplante Lösung.

Die Herausforderungen im Bereich der sicheren Videokonferenzlösung sowie des Nachfolgeprodukts für «Skype for Business» können aufgrund der Verordnung über die Koordination der digitalen Transformation und die IKT-Lenkung in der BV nicht alleine vom VBS angegangen und gelöst werden, sondern bedingen eine Zusammenarbeit mit der Bundeskanzlei und den anderen Departementen in der BV.

Des Weiteren hat die Prüfung ergeben, dass die möglichen Anwendungs- und Einsatzbereiche der Videokonferenzlösungen zum Zeitpunkt der Prüfung nicht umfassend festgehalten waren. Auch gibt es aktuell weder auf Stufe Bund noch im VBS eine spezifische und verpflichtende Schulung zum sicheren Einsatz und Umgang mit Videokonferenzlösungen. Die vorhandenen Möglichkeiten und Risiken der Videokonferenzsysteme müssen den Benutzern proaktiv bekannt gemacht werden, damit diese die geeigneten Anwendungen korrekt einsetzen können.

---

1 SR **510.411** Verordnung vom 4. Juli 2007 (Stand 1. Januar 2021) über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) (9.12.2021)

2 Congress.Gov: H.R.1625 - 115th Congress (2017-2018): Consolidated Appropriations Act, 2018 | Congress.gov | Library of Congress, Division V - CLOUD ACT (9.12.2021)

2 Nutzen und Risiken von Videokonferenzen

Videokonferenzanwendungen wurden sehr benutzerfreundlich und der Funktionsumfang ist so umfassend gewachsen, dass sie nicht mehr aus dem Arbeitsalltag wegzudenken sind. Auf einfache Art und Weise können damit über grosse Distanzen Gespräche, Sitzungen, Konferenzen, Rapporte und Ausbildungsveranstaltungen durchgeführt werden. Dies nicht nur innerhalb der BV, sondern auch mit externen Stellen und der Miliz. Auch Homeoffice und Teamarbeit werden durch diese modernen Anwendungen unterstützt. Sei es durch den Austausch von Informationen am Bildschirm, dem Einsatz der Chatfunktion oder durch die gemeinsame Bearbeitung von Dokumenten. Aufgrund der Pandemie-Situation hat sich seit Anfang 2020 die Nachfrage und Nutzung solcher Videokonferenzanwendungen stark erhöht.

Bereits seit einigen Jahren sind im VBS auf den Laptops, Tablets und Smartphones Videokonferenzanwendungen installiert. Wie wertvoll diese Anwendungen sein können, hat sich während der Homeoffice-Pflicht gezeigt. Insbesondere im Hinblick auf die Zusammenarbeit in Teams, aber auch bezogen auf die Steigerung der Effizienz und der Produktivität sowie der Reduktion von Reisekosten und Minderung von Umweltbelastungen.

Aus Sicht der Cybersicherheit bergen die Videokonferenzanwendungen jedoch auch viele, komplexe Herausforderungen. Diverse Akteure versuchen permanent mögliche Schwachstellen solcher Anwendungen auszunutzen, um an Zugangsdaten, persönliche Daten oder Geschäftsinformationen zu gelangen. Nach dem Motto «digital, aber sicher» sind folglich auch bei Videokonferenzanwendungen eine Vielzahl von Sicherheitsmassnahmen und rechtlichen Vorgaben (u. a. ISchV, DSG[3], CyRV[4]) zu beachten.

3 Auftrag, Methodik und Abgrenzung

Die Chefin VBS erteilte der Internen Revision VBS am 28. Juni 2021 den Auftrag zu prüfen, welche Arten von Videokonferenzen im Departement eingesetzt werden. Zudem beurteilten wir, ob die relevanten Standards sowie Sicherheits- und Datenschutzbestimmungen eingehalten werden und zeigen allfälligen Handlungs- und Optimierungsbedarf auf.

Im Rahmen dieses Prüfauftrags führten wir strukturierte Befragungen durch und analysierten Dokumente. Wir interviewten die Chief Information Security Officers (CISO) und Informationssicherheitsbeauftragten (ISBO) des VBS sowie weitere Fachexperten in der BV (u. a. Bundeskanzlei und fedpol). Zudem führten wir Gespräche mit den Leistungserbringern bei der Führungsunterstützungsbasis (FUB) sowie dem Bundesamt für Informatik (BIT). Dabei wählten wir ein risikoorientiertes Vorgehen.

[3] SR **235.1** Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG)

[4] SR **120.73** SR 120.73 - Verordnung vom 27. Mai 2020 über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) (admin.ch) (9.12.2021)

Der Fokus dieser Prüfung lag auf den wesentlichen und breit eingesetzten Lösungen im VBS. Spezifische Insellösungen mit kleinen Benutzerkreisen, wie sie z. B. in der Armee, im Nachrichtendienst des Bundes (NDB), von der Departementsleitung oder dem Generalsekretariat eingesetzt werden, wurden in dieser Prüfung explizit ausgeschlossen.

4 Würdigung

Während unserer Prüfung trafen wir ausnahmslos auf engagierte Ansprechpersonen, die uns unterstützt und Informationen transparent zur Verfügung gestellt haben. Zudem gewannen wir den Eindruck, dass all unseren Ansprechpersonen das Thema Videokonferenzen ein wichtiges Anliegen ist und der Einhaltung von Standards und Vorgaben sowie der Cybersicherheit die notwendige Beachtung beigemessen wird. Wir bedanken uns bei allen Beteiligten für die zielführende Zusammenarbeit. Besonders bedanken wir uns bei den Fachexperten in der Bundeskanzlei, dem BIT und fedpol für die Unterstützung sowie die Dialogbereitschaft.

5 Videokonferenzanwendungen im VBS

Im VBS werden primär «Skype for Business» und «Webex Meetings» eingesetzt. Zusätzlich steht einem eingeschränkten Benutzerkreis das Produkt «Microsoft Teams» – im Rahmen einer Projektphase – zur Verfügung. All diese Produkte erlauben eine zielführende Videokonferenz ohne Anspruch auf erweiterte Kollaborationsmöglichkeiten und gestatten eine Zusammenarbeit mit externen Partnern. Diese Kommunikationsmittel dürfen für die Übermittlung von bis INTERN klassifizierten Informationen und «Nicht besonders schützenswerte Personendaten» nach dem DSG benutzt werden.

Beim Einsatz von Videokonferenzanwendungen stützt sich das VBS auf die Verordnungen sowie Einsatzrichtlinien des Schweizerischen Bundesrates, respektive der Bundeskanzlei. Diese regeln den Einsatz der breit eingesetzten IKT[5]-Anwendungen in der Bundesverwaltung und haben auch für das VBS Gültigkeit. Für den Einsatz von Videokonferenzanwendungen sind insbesondere die Einsatzrichtlinien UCC[6] sowie die Umgebung CEBA Agil[7,8] massgebend. Die Verantwortung zur Einhaltung dieser Richtlinien obliegt den Vorgesetzten in den jeweiligen Verwaltungseinheiten (VE).

Damit das Personal der Bundesverwaltung bei Bedarf auf bundesexterne Kollaborations-

5 IKT = Informations- und Kommunikationstechnologie

6 E017 – Einsatzrichtlinie UCC Weisung zur Bundesinformatik

7 CEBA Agil = Cloud Enabling Büroautomation Agil

8 E031 – Einsatzrichtlinie Umgebung CEBA Agil

und Kommunikationslösungen zugreifen kann, die im internen Bundnetzwerk gesperrt sind (z. B. Zoom, Jitsi, BigBlueButton, Miro, usw.), kann seit Mitte September 2021 «Internet Desktop VDI[9]» eingesetzt werden. Dieses Produkt bietet allerdings keinen Schutz der Vertraulichkeit und die Kommunikation klassifizierter Inhalte ist nicht gestattet.

Um den Sicherheitsanforderungen nachzukommen, hat das Nationale Zentrum für Cybersicherheit (NCSC) die minimalen Sicherheitsvorgaben im Bereich Informatiksicherheit verbindlich festgelegt. Diese Vorgaben sind im Dokument «IKT-Grundschutz in der Bundesverwaltung» (kurz: Grundschutz Bund) festgehalten.[10] Dieser Grundschutz Bund ist ein Tailoring des Standards ISO/IEC 27002:2013, erweitert mit spezifischen Massnahmen der Bundesverwaltung. Die Umsetzung der Sicherheitsvorgaben und -massnahmen sind durch die verpflichtete VE zu dokumentieren und zu überprüfen (Art. 14b–14e CyRV).

Nachfolgend beleuchten wir die Herausforderungen mit den primär eingesetzten Videokonferenzanwendungen kritisch.

5.1 Videokonferenzanwendungen während der Corona-Pandemie

Feststellung: Vor allem zu Beginn der Corona-Pandemie kamen vereinzelt auch Kollaborations- sowie Kommunikationslösungen zum Einsatz, die nicht über die Einsatzrichtlinien abgebildet und im internen Bundesnetzwerk standardmässig gesperrt sind (z. B. Zoom, Slack, Jitsi, Miro, usw.). Dies einerseits aufgrund dessen, dass auch mit der Homeoffice-Pflicht das tägliche Geschäft effizient fortgeführt werden konnte, andererseits wurden mit den Standardprodukten die neuen Geschäftsbedürfnisse nicht vollumfänglich abgedeckt. Z. B. fehlten erweiterte Kollaborationsmöglichkeiten und die maximal erlaubte Anzahl von Konferenzteilnehmern war oft zu gering. Mit «Internet Desktop VDI» wird seit Mitte September 2021 eine Marktleistung offeriert, welche die Teilnahme an bundesexternen Web-Konferenzen erlaubt. Allerdings nur für den Austausch von nicht klassifizierten Informationen. Es gibt keine gesamtheitliche Übersicht mit einer Auflistung der möglichen Videokonferenzanwendungen und deren Einsatzmöglichkeiten unter Berücksichtigung der Klassifizierungsstufen.

Beurteilung: Die zur Verfügung gestellten Videokonferenzanwendungen müssen die geschäftlichen Bedürfnisse (Funktionalität und Sicherheit) erfüllen und praktikabel einsetzbar sein. Ansonsten besteht die Gefahr, dass die Anwenderinnen und Anwender auf bundesexterne Kommunikationsgeräte ausweichen und gegen Richtlinien verstossen. Aufgrund dessen, dass kein aktives und durchgehendes Monitoring der eingesetzten Videokonferenzanwendungen bzw. kein «whitelisting[11]» stattfindet, kann nicht rekonstruiert werden, welche Anwendungen eingesetzt werden, resp. eingesetzt worden sind. Bestimmungen zur Cybersi-

9 VDI = Virtuelle Desktop Infrastruktur

10 Nationale Zentrum für Cybersicherheit (NCSC) - IKT-Grundschutz in der Bundesverwaltung, Grundschutz (admin.ch) (9.12.2021)

11 ComputerWeekly.de: Was ist Application Whitelisting? - Definition von WhatIs.com (computerweekly.com) (9.12.2021)

cherheit, dem Informations- und dem Datenschutz wurden womöglich nicht umfassend angewendet. Aus unserer Sicht wäre es hilfreich, wenn für die gängigsten Videokonferenzlösungen eine gesamtheitliche Übersicht mit klaren und einfach verständlichen Anweisungen aufbereitet und proaktiv kommuniziert würde, damit sich das Bundespersonal daran orientieren kann.

5.2 Cloudbasierte Nachfolgelösung

Feststellung: «Skype for Business» deckt die heutigen Bedürfnisse nicht mehr vollumfänglich ab und erreicht am 1. September 2024 das Ende seines Lebenszyklus. Aufgrund einer Laufzeitverlängerung wird dieses Microsoft Produkt noch bis Mitte Oktober 2025 unterstützt. «Microsoft Teams» könnte das Nachfolgeprodukt von «Skype for Business» werden. Im Rahmen des CEBA-Projekts steht «Microsoft Teams» heute einem eingeschränkten Benutzerkreis zur Verfügung. Diese temporär bereitgestellte Anwendung wird durch Microsoft in einer Public Cloud, grösstenteils innerhalb der Schweiz, betrieben. Mit «Microsoft Teams» können Informationen bis zur Klassifizierungsstufe INTERN bearbeitet und/oder gespeichert werden, nicht aber besonders schützenswerte Personendaten oder Persönlichkeitsprofile sowie Informationen, die dem Amtsgeheimnis unterliegen.[12]

Beurteilung: Unter welchen rechtlichen Bedingungen und Sicherheitsmassnahmen eine Nachfolgelösung von «Skype for Business» eingesetzt werden kann, ist noch nicht abschliessend geklärt. Wir erachten die Evaluation einer cloudbasierten Nachfolgelösung als kritisch, falls die Kommunikation der Bundesverwaltung über eine ausländische Cloud-Infrastruktur laufen sollte. Aus unserer Sicht gibt es gewisse Bedenken zur Durchsetzung des Schweizer Rechts bezüglich dem Datenschutz und den klassifizierten Informationen. Problematisch ist dies vor allem wegen dem CLOUD Act von 2018, welcher der US-Strafverfolgungsbehörde erlaubt, Zugang zu den Daten zu erhalten, die von CSP (z. B. Microsoft) mit Sitz in den USA aufbewahrt werden. Und dies unabhängig davon, wo auf der Welt die Daten gespeichert sind. Da die bedeutsamsten CSP ihren Sitz in den USA haben, sollte sich auch die BV Gedanken zur Zusammenarbeit mit den USA bezüglich der elektronischen Beweismittel machen. Dabei gilt es die Vereinbarkeit des CLOUD Act mit dem Schweizer Recht, insbesondere hinsichtlich des Datenschutzrechts sowie der Prinzipien des Rechts der zwischenstaatlichen Zusammenarbeit in Strafsachen genau zu prüfen.[13] Diese Thematik kann nicht alleine vom VBS angegangen und gelöst werden, sondern bedingt eine gemeinsame Herangehensweise unter Einbezug der Bundeskanzlei und den anderen Departementen in der BV.

5.3 Austausch von VERTRAULICH klassifizierten Informationen

Feststellung: Die heute in der Bundesverwaltung verwendeten Produkte «Skype for Business», «Microsoft Teams» und «Webex Meetings» lassen sich nur für den Austausch von

[12] E031 – Einsatzrichtlinie Umgebung CEBA Agil

[13] Bundesamt für Justiz: Bericht zum US CLOUD Act (admin.ch), Seite 46 (9.12.2021)

Informationen bis zur Klassifizierungsstufe INTERN und für nicht besonders schützenswerte Personendaten einsetzen. Nebst diesen Anwendungen steht den Mitarbeitenden auf dem Smartphone die Softwarelösung «Threema» zur Verfügung, mit deren Hilfe die verschlüsselte Sprachkommunikation (VSK[14]) unter Auflagen bis Klassifizierungsstufe VERTRAULICH betrieben werden kann. Diese Anwendung offeriert allerdings ausschliesslich eine Punkt-zu-Punkt Kommunikation. Somit fehlt heute eine Videokonferenzanwendung, welche sich für den Austausch von VERTRAULICH klassifizierten Informationen eignet (z. B. auch für den Austausch mit nationalen und internationalen Behörden und externen Partnern).

Beurteilung: Wir sind der Auffassung, dass insbesondere der geschäftliche und militärische Bedarf mit den aktuellen Anwendungen noch nicht zielführend abgedeckt wird. Damit die Kommunikation klassifizierter Inhalte bis Klassifizierungsstufe INTERN und mittelfristig bis VERTRAULICH sichergestellt werden kann, muss ein Nachfolgeprodukt evaluiert und implementiert werden, das im Sinne der CyRV über den geforderten Schutzbedarf verfügt und mit einer tauglichen Verschlüsselungs- und Sicherheitslösung ausgestattet ist. Das letztes Jahr beschlossene Informationssicherheitsgesetz (ISG)[15] wird dazu beitragen, einheitliche Standards für Behörden der Schweiz zu schaffen, was eine Voraussetzung für einen angemessenen Schutz bildet. Ohne Nachfolgeprodukt besteht die Gefahr, dass die täglichen Geschäfte nicht mehr unter Einhaltung der angemessenen Sicherheit abgewickelt werden können. Die Evaluation einer sicheren Videokonferenzlösung sollte weiter vorangetrieben werden. Dabei ist anzumerken, dass nicht nur die Sicherheit der Videokonferenzlösung per se, sondern auch die für den Einsatz der Lösung verwendeten Endgeräte und Plattformen dieselben Sicherheitsniveaus erfüllen müssen.

5.4 Schulung der Nutzer von Videokonferenzanwendungen

Feststellung: Eine spezifische und verpflichtende Schulung zum sicheren Einsatz und Umgang mit Videokonferenzlösungen auf Stufe Bund sowie im VBS gibt es aktuell nicht. Bei einigen Verwaltungseinheiten werden die Mitarbeiterinnen und Mitarbeiter zum Thema Cybersicherheit und Datenschutz mittels periodischen Newslettern und Eintrittsschulungen sensibilisiert. Im Rahmen unserer Prüfung haben wir festgestellt, dass einige wenige Kurse (d. h. kurze E-Learning Sequenzen) zum Thema Videokonferenzen auf der Lernplattform LMS Bund aufgeschaltet sind, diese den interviewten Fachpersonen jedoch nicht oder nur teilweise bekannt sind.

Beurteilung: Aufgrund der umfangreichen Anforderungen an die Cybersicherheit und den Datenschutz beim Einsatz von Videokonferenzlösungen würden wir erwarten, dass ein verstärktes Augenmerk auf die Schulung und Sensibilisierung des Bundespersonals gelegt wird. Regelmässige Auseinandersetzungen mit möglichen Risiken und deren Auswirkungen können den bewussten Umgang damit fördern.

---

[14] E027 – Einsatzrichtlinie Verschlüsselte Sprachkommunikation (VSK)

[15] Die Bundesversammlung - Das Schweizer Parlament: 17.028 - Informationssicherheitsgesetz | Geschäft | Das Schweizer Parlament (9.12.2021)

6 Empfehlungen

Aufgrund unserer Feststellungen empfehlen wir dem Generalsekretariat VBS

Zu 5.1:
– zusammen mit der Bundeskanzlei und den anderen Departementen zu prüfen, ob ein aktives und durchgehendes Monitoring bzw. ein «whitelisting» der eingesetzten Kollaborations- und Kommunikationslösungen angestrebt werden soll.
– zusammen mit der Bundeskanzlei und den anderen Departementen, klare und einfach verständliche Anweisungen zum Einsatz von Videokonferenzlösungen auszuarbeiten und proaktiv zu kommunizieren.

Zu 5.2:
– zusammen mit der Bundeskanzlei und den anderen Departementen zu prüfen, ob eine ausländische Cloud-Architektur als mögliche Nachfolgelösung von «Skype for Business» im Hinblick auf Informations- und Datenschutzüberlegungen zielführend ist.

Zu 5.3:
– zusammen mit der Bundeskanzlei und den anderen Departementen die Evaluation einer sicheren Videokonferenzlösung bis Klassifizierungsstufe VERTRAULICH voranzutreiben, damit die geschäftlichen wie auch die sicherheitsmässigen Anforderungen umgesetzt resp. sichergestellt werden können.

Zu 5.4:
– zu prüfen, inwiefern die Schulung und Sensibilisierung der Mitarbeitenden ausgebaut und die regelmässige Auseinandersetzung mit möglichen Risiken und deren Auswirkungen gefördert werden kann.

7 Stellungnahmen

Generalsekretariat VBS

Das GS-VBS dankt der Internen Revision VBS für die Gelegenheit zur Stellungnahme und ist mit den Empfehlungen einverstanden.

Gruppe Verteidigung

Die Gruppe Verteidigung bedankt sich für die Gelegenheit zur Stellungnahme und ist mit den vorgeschlagenen Empfehlungen einverstanden; das GS-VBS wird bei deren Umsetzung unterstützt.

Zur Empfehlung 5.3 schlägt die Gruppe Verteidigung vor, die Evaluation einer sicheren Videokonferenzlösung in den Gesamtkontext von Kollaborations- und Kommunikationslösungen mit erhöhten Anforderungen (bezüglich Sicherheit, Verfügbarkeit und Interoperabilität) zu stellen. Diese Evaluation ist mit den militärischen Anforderungen abzustimmen, um einen gemeinsamen Lösungsansatz für Bundesverwaltung SVS, und Armee zu finden.

armasuisse

Die armasuisse dankt für die Einsicht und die Möglichkeit zur Stellungnahme zum Bericht und unterstützt die Empfehlungen vollumfänglich. Grundsätzlich sind cloudbasierte Lösungen auch in der ganzen BV nicht mehr wegzudenken. Daher ist es sehr dringlich, dass für die Mitarbeitenden der BV rasch verständliche Anweisungen im Umgang mit Cloudanwendungen ausgearbeitet werden.

Bundesamt für Bevölkerungsschutz

Das BABS begrüsst die vorgeschlagenen Empfehlungen und die Koordination in der gesamten Bundesverwaltung. Das BABS erachtet es als wichtig, möglichst zeitnah über moderne UCC-Kommunikationskanäle zu verfügen. Es ist den externen Gesprächspartnern teilweise schwer erklärbar, dass wir zwar zu Remote-Sitzungen eingeladen werden können, selber aber mit dem gleichen Tool nicht einladen können resp. dürfen. Dabei muss ein Weg gefunden werden, welcher die Übertragung von vertraulich klassifizierten Informationen ermöglicht. Der Aspekt Sicherheit ist wichtig, allerdings muss gelten "so viel wie nötig" und nicht "so viel wie möglich".

Bundesamt für Sport

Das BASPO ist mit den empfohlenen Prüfaufträgen einverstanden, insbesondere die Sensibilisierung der Mitarbeitenden wird als wichtig erachtet. Es ist zu berücksichtigen, dass Dienststellen unterschiedliche Anforderungen an solche Kollaborations- und Kommunikationslösungen haben. Es sollte deshalb eine Mehrproduktestrategie verfolgt werden. Im

Falle des BASPO müssen die Lösungen auch für den Studienbetrieb an der EHSM, virtuelle und/oder hybride Fachveranstaltungen mit Teilnehmenden ausserhalb der Bundesverwaltung und dergleichen geeignet sein. Die Bundesverwaltung sollte über die meist verbreiteten Lösungen erreichbar sein. Allenfalls macht für den Austausch klassifizierter Informationen eine einzige Lösung Sinn.

Nachrichtendienst des Bundes

Der NDB ist mit den Empfehlungen einverstanden. Die beiden letzten Jahre zeigen deutlich den Bedarf an Videokonferenzen und deren Nutzen auf. In Hinsicht auf die im Vergleich zur übrigen Bundesverwaltung höheren Sicherheitsanforderungen steht für den NDB die Empfehlung zu 5.3 (Evaluation einer sicheren Videokonferenzlösung bis Klassifizierungsstufe VERTRAULICH) im Vordergrund.

swisstopo

swisstopo begrüsst die Stossrichtung der Empfehlungen, insbesondere bezüglich Ausbau der Sensibilisierung und Schulung bezüglich der Konferenz-Anwendungen. Mit den Aussagen im Bericht sind wir einverstanden und haben keine ergänzenden Bemerkungen.