Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI für Videokonferenzdienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 07.10.2021

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	07.10.2021	Erstveröffentlichung

Tabelle 1: Versionsgeschichte des Mindeststandards für Videokonferenzdienste.

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de/mindeststandards

Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Absatz 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 (UP Bund) legt fest, dass die Mindeststandards des BSI auf Basis § 8 Absatz 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. UP Bund, S. 4 (Bundesministerium des Innern, für Bau und Heimat (BMI), 2017)
[2] Analog „Informationssicherheitsbeauftragte (ISB)“
[3] Vgl. FAQ zu den Mindeststandards (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

Inhalt

1 Beschreibung

1.1 Einleitung und Abgrenzung

Videokonferenzdienste[5] haben heute eine zentrale Bedeutung für die Zusammenarbeit auf Distanz. Sie ermöglichen nicht nur ortsunabhängige Kommunikation durch die Übertragung von Sprach- und Videodaten, sondern bieten häufig zahlreiche erweiterte Funktionalitäten zur Kollaboration, wie z. B. das gemeinsame Erstellen und Bearbeiten von Dokumenten. Zwangsläufig können bei der Nutzung solcher Dienste aber auch Risiken für die Vertraulichkeit, Verfügbarkeit und Integrität der Daten entstehen.

Das BSI hat 2020 das Kompendium Videokonferenzsysteme (KoViKo)[6] veröffentlicht, das detaillierte Informationen zu dem Thema bereitstellt. Es beschreibt unterschiedliche Arten von Videokonferenzsystemen, ihre Funktionsweise und stellt die Gefährdungslage dar. Außerdem stellt es umfassende Sicherheitsanforderungen vor, die einen sicheren Betrieb von Videokonferenzdiensten ermöglichen.

Der vorliegende Mindeststandard basiert auf dem KoViKo. Er hebt wesentliche Aspekte hervor, die aus Sicht des BSI beachtet werden müssen, um ein definiertes Mindestsicherheitsniveau beim Einsatz von Videokonferenzdiensten in der Bundesverwaltung zu erreichen. Des Weiteren wurde die systemorientierte Sichtweise des KoViKo im Mindeststandard zu einer dienstorientierten verändert. Dies trägt dem Umstand Rechnung, dass die Verbreitung und Entwicklungen von Videokonferenzlösungen durch die Corona-Pandemie stark beschleunigt wurden. So konnten insbesondere in dieser entstandene ad hoc verfügbare Videokonferenzdienste im KoViKo noch keine Berücksichtigung finden. Der Mindeststandard beschreibt daher Sicherheitsanforderungen, die auf ein breites Spektrum an Lösungen zutreffen. Hierzu thematisiert er die Konzeption und Beschaffung eines Videokonferenzdienstes sowie funktionale Anforderungen an den Dienst und Anforderungen an den Betrieb und die Benutzer.

Neben reinen Videokonferenzdiensten haben auch andere Anwendungen wie Messenger-Dienste häufig Videofunktionen, diese sind jedoch nicht Betrachtungsgegenstand dieses Mindeststandards. Auch stehen spezielle Anwendungsformate wie (öffentliche) virtuelle Großveranstaltungen nicht im Fokus, da hier besondere Rahmenbedingungen wie öffentliche Zugänglichkeit und große Teilnahmezahlen einige Anforderungen nicht anwendbar oder impraktikabel machen. Die Abgrenzung zwischen Großveranstaltungen und „klassischen“ Videokonferenzen kann jedoch nicht pauschal getroffen werden und muss von der Einrichtung jeweils unter Berücksichtigung der eigenen Anforderungen erfolgen.

Neben den Videokonferenzdiensten sind auch die Endpunkte[7], auf denen sie genutzt werden, von entscheidender Bedeutung für die IT-Sicherheit. Daher wird gemäß Umsetzungsplan Bund 2017[8] ein Managementsystem für Informationssicherheit (ISMS) auf Basis der IT-Grundschutz-Vorgehensweise vorausgesetzt.[9] Es wird davon ausgegangen, dass die entsprechenden Endpunkte in das ISMS der Einrichtung eingebunden werden. Sie werden im Weiteren nur explizit erwähnt, wenn sie direkten Einfluss auf die Umsetzung der Sicherheitsanforderungen an Videokonferenzdienste haben.

Sicherheitsanforderungen aus weiteren Standards und Regelwerken müssen darüber hinaus ebenfalls eingehalten werden und bleiben von diesem Mindeststandard unberührt. Dies gilt insbesondere auch für Anforderungen an den Datenschutz, die für das Thema Videokonferenzen eine zentrale Bedeutung haben. Da die Mindeststandards des BSI nur den Bereich der IT-Sicherheit betrachten, stellt dieses Dokument keine spezifischen Datenschutzanforderungen auf. Deshalb sollten bei der Planung des Einsatzes von

[5] Definition s. Glossar
[6] Vgl. KoViKo (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)
[7] Definition s. Glossar
[8] Vgl. UP Bund, S. 8 (Bundesministerium des Innern, für Bau und Heimat (BMI), 2017)
[9] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

Videokonferenzdiensten von Anfang an die Datenschutzbeauftragten der Einrichtung einbezogen werden, um sicherzustellen, dass die geltenden Regelungen zum Datenschutz berücksichtigt werden.

1.2 Betriebsmodelle

Dieser Mindeststandard regelt den eigenen Einsatz eines Videokonferenzdienstes durch die Einrichtung. Im Gegensatz dazu ist die Teilnahme an Videokonferenzen Dritter nicht Gegenstand der Betrachtung.

Das Angebot an Videokonferenzlösungen für den eigenen Einsatz ist vielfältig. Bei der Auswahl gilt es nicht nur, einen geeigneten Dienst zu finden, sondern die Einrichtung hat grundsätzlich auch verschiedene Möglichkeiten, ihn zu betreiben bzw. zu nutzen. Dieser Mindeststandard gilt für alle Betriebsmodelle (s.u.). Jedoch lassen sich viele Sicherheitsanforderungen nicht unabhängig vom Betriebsmodell betrachten. Beispielsweise muss die Umsetzung von Anforderungen an das Hosting abhängig vom Betriebsmodell an unterschiedlichen Stellen gewährleistet werden (Ist z. B. der IT-Betrieb der Einrichtung verantwortlich oder muss die Einhaltung durch Dienstleistungsunternehmen vertraglich zugesichert werden?). In Kapitel 2 wird daher an den entsprechenden Stellen darauf hingewiesen, auf welche Betriebsmodelle sich die jeweiligen Sicherheitsanforderungen beziehen oder für welches Betriebsmodell Besonderheiten gelten. Dazu werden im Groben die folgenden zwei Optionen unterschieden:

- Selbstgehostet: Die Einrichtung hostet den Videokonferenzdienst selbst. Dabei kann eingekaufte Software verwendet werden, die auf den eigenen Servern betrieben wird. Der IT-Betrieb der Einrichtung ist damit in der Regel direkt für die Umsetzung der Sicherheitsmaßnahmen verantwortlich.
- Fremdgehostet: Ein externes Dienstleistungsunternehmen betreibt den Videokonferenzdienst. Es besteht in der Regel ein Vertragsverhältnis, das die relevanten Aspekte regelt. Wird ein Videokonferenzdienst ohne direkte Beauftragung durch die Behörde genutzt (z. B. Online-Dienste, die auch kostenlos von Privatpersonen genutzt werden können), müssen verfügbare Informationen und Nutzungsbedingungen kritisch geprüft werden (s. Kapitel 2.3).

1.3 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert werden und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

[10] Vgl. BSI-Standard 200-2, S. 18 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)
[11] Vgl. Key words for use in RFCs (Internet Engineering Task Force (IETF), 1997)
[12] Vgl. DIN 820-2: Gestaltung von Dokumenten (Deutsches Institut für Normung e.V. (DIN), 2018)

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Die Begründung muss dokumentiert werden und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

2 Sicherheitsanforderungen

2.1 Konzeption

Bevor ein Videokonferenzdienst eingesetzt werden kann, ist eine sorgfältige Konzeption von zentraler Bedeutung, um potenzielle Risiken zu identifizieren und entsprechende Sicherheitsmaßnahmen planen zu können. Die folgenden Anforderungen sind unabhängig vom Betriebsmodell.

VK.2.1.01 – Sicherheitsrichtlinie für Videokonferenzdienste

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie nach IT-Grundschutz für Videokonferenzdienste erstellen[13]. Diese MUSS konkrete Sicherheitsvorgaben beinhalten, mit denen sich Videokonferenzdienste innerhalb der Institution umsetzen lassen. Außerdem MÜSSEN darin spezielle Sicherheitsanforderungen an die Dienstanbietenden sowie das festgelegte Schutzniveau für Videokonferenzdienste hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit dokumentiert werden.

b) Wenn international angebotene Videokonferenzdienste genutzt werden, MÜSSEN die speziellen länderspezifischen Anforderungen und gesetzlichen Bestimmungen berücksichtigt werden.

c) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragten bei der Erstellung der Sicherheitsrichtlinie beteiligen.

VK.2.1.02 – Sicherheitskonzept für den Videokonferenzdienst

a) Auf Grundlage der identifizierten Sicherheitsanforderungen (vgl. VK.2.1.01) MUSS die Einrichtung jeweils ein Sicherheitskonzept nach IT-Grundschutz für jeden Videokonferenzdienst erstellen[14].

b) Die Einrichtung MUSS – sofern betroffen – die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragten bei der Erstellung des Sicherheitskonzeptes beteiligen.

c) Aus dem Sicherheitskonzept MUSS hervorgehen, in welchem Szenario (z. B. innerhalb der Netze des Bundes (NdB), in einem anderen bundeseigenen WAN oder über offene Netze) der Videokonferenzdienst eingesetzt wird. Für Videokonferenzdienste, die innerhalb von NdB eingesetzt werden, MÜSSEN auch die Anforderungen des Mindeststandards NdB[15] eingehalten werden.

d) Die Einrichtung MUSS festlegen, für welche Datenkategorien[16] der Videokonferenzdienst freigegeben werden soll. Die Einrichtung MUSS bei der Freigabe der Datenkategorien Geheim- und Datenschutzaspekte sowie Personen-, Geschäfts- und Dienstgeheimnisse berücksichtigen.

e) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des Videokonferenzdienstes entstehen können, umfassend ermitteln und bewerten[17]. Die Einrichtung DARF den Videokonferenzdienst NUR

[13] Vgl. IT-Grundschutz-Kompendium: Glossar (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

[14] Vgl. IT-Grundschutz-Kompendium: Glossar (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

[15] Vgl. MST NdB (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2019)

[16] Als Orientierung können beispielsweise die Datenkategorien gemäß Mindeststandard zur Nutzung externer Cloud-Dienste (NCD) genutzt werden: *(1) Privat- und Dienstgeheimnisse, (2) personenbezogene Daten, (3) Verschlusssachen, (4) sonstige Daten*, vgl. NCD.2.1.01 g) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

[17] Hinweis: Bei dieser Prüfung geht es um eine angebotsunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Nutzungsszenario mit den Sicherheitsanforderungen der Behörde vereinbar ist (z. B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?) Vgl. auch KoViKo Kapitel 5 – Gefährdungslage, S. 53ff (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)

nutzen, wenn die ermittelten Risiken wirksam vermieden oder hinreichend reduziert oder (in Übereinstimmung mit den Risikoakzeptanzkriterien) getragen werden können.

VK.2.1.03 – Rollen- und Berechtigungskonzepte

a) Für die Nutzung sowie die Administration des Videokonferenzdienstes MUSS ein Rollen- und Berechtigungskonzept erstellt werden, welches den Rollen gemäß IT-Grundschutz-Anforderung ORP.4.A2[18] nur die minimal notwendigen Berechtigungen zuweist.

b) Das Berechtigungskonzept MUSS auch den Zugriff auf Benutzendendaten sowie Administrationsdaten regeln.

VK.2.1.04 – Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[19] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint, das sowohl präventive als auch reaktive Maßnahmen in Notfällen und Krisensituationen umfasst. Es gilt im Weiteren die Begrifflichkeit des BSI-Standards 100-4.

a) Die Einrichtung MUSS bewerten, welche Bedeutung der Videokonferenzdienst in Notfällen einnehmen würde.[20]

b) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den Videokonferenzdienst zugreifen können muss. Die zuständigen Notfallbeauftragten MUSS entsprechend eingebunden werden.

VK.2.1.05 – Störungsmeldung und -behebung

a) Vor Inbetriebnahme des Videokonferenzdienstes MÜSSEN Prozesse für die Störungsmeldung und -behebung gemäß IT-Grundschutz-Baustein DER.2.1[21] definiert werden.

b) Die Benutzenden MÜSSEN in geeigneter Weise über Kontaktmöglichkeiten zur Störungsmeldung informiert werden.

c) Die Benutzenden SOLLTEN über die voraussichtliche Dauer bis zur vollständigen Wiederherstellung der Verfügbarkeit informiert werden.

VK.2.1.06 – Cloud-Nutzung

Wenn es sich bei einem Videokonferenzdienst oder einer seiner Komponenten um einen externen Cloud-Dienst handelt, MUSS zusätzlich zu dem vorliegenden Mindeststandard der Mindeststandard des BSI zur Nutzung externer Cloud-Dienste[22] eingehalten werden.

2.2 Funktionale Anforderungen

Videokonferenzdienste sind komplex und bieten viele Funktionen. Daher muss die Einrichtung vor der Beschaffung eines Dienstes prüfen, welcher Bedarf (Funktionen, technische Anforderungen) besteht und inwieweit ein Dienst diesen Bedarf erfüllen kann. Die folgenden Anforderungen müssen mindestens erfüllt

[18] Vgl. IT-Grundschutz-Kompendium – Baustein ORP.4: Identitäts- und Berechtigungsmanagement (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

[19] Vgl. BSI-Standard 100-4 – Notfallmanagement, S. 1ff. (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008)

[20] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Videokonferenzdienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Videokonferenzdienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Videokonferenzdienst für die Bewältigung eines Notfalls relevant?

[21] Vgl. IT-Grundschutz-Kompendium – Baustein DER.2.1: Behandlung von Sicherheitsvorfällen (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

[22] Vgl. MST NCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

sein, um später einen sicheren Betrieb zu ermöglichen. Sie gelten für alle Betriebsmodelle und führen zum Ausschluss eines Dienstes, wenn er die Anforderungen nicht erfüllt.

VK.2.2.01 – Verschlüsselung

a) Bei der Übertragung von Daten über nicht vertrauenswürdige Strecken MUSS der Videokonferenzdienst eine Verschlüsselung der Medien- und Signalisierungsdaten gewährleisten[23]. Die Verschlüsselung SOLLTE entsprechend den Empfehlungen der Technischen Richtlinien TR-02102[24] umgesetzt sein. Wenn die Verschlüsselung abweichend von den Empfehlungen der Technischen Richtlinien umgesetzt ist, MUSS die Einrichtung dies bewerten, dokumentieren und im Rahmen des eigenen Risikomanagements behandeln.

b) Wenn für den Verbindungsaufbau bzw. die Anmeldung oder administrative Arbeiten eine Web-Schnittstelle verwendet wird, MUSS das HTTPS-Protokoll gemäß den Empfehlungen der Technischen Richtlinie TR-02102 eingesetzt werden.

VK.2.2.02 – Signalisierung der Kamera- und Mikrofonaktivität

a) Der Endpunkt des Videokonferenzdienstes MUSS optisch darstellen können, ob Kamera und/oder Mikrofon aktiviert sind, damit das Ausspähen von Personen und Räumlichkeiten erkannt werden kann.

b) Die optische Darstellung KANN sowohl auf Hardwareebene erfolgen (z. B. LEDs neben Webcams), als auch auf Softwareebene (z. B. Kamera- und Mikrofonsymbole).

c) Um eine barrierefreie Signalisierung zu ermöglichen, SOLLTE zusätzlich zur optischen Darstellung ein akustisches Signal für die Kamera- und Mikrofonaktivität konfiguriert werden können.

d) Der Videokonferenzdienst SOLLTE die Möglichkeit bereitstellen, dass Teilnehmende ihre Sprach- und Videoübertragung vor dem Beitritt initial deaktivieren können.

VK.2.2.03 – Anzeige der Teilnehmenden

a) Alle Teilnehmenden MÜSSEN jederzeit die Möglichkeit haben, sich eine Liste der in der Videokonferenz befindlichen Teilnehmenden anzeigen zu lassen.

b) Treten einer Videokonferenz neue Teilnehmende bei, so MUSS dieser Vorgang bei allen in der Videokonferenz befindlichen Teilnehmenden signalisiert werden können (z. B. über einen Aufmerksamkeitston oder ein optisches Pop-up).

c) Verlassen Teilnehmende eine Videokonferenz, SOLLTE dieser Vorgang ebenfalls signalisiert werden können.

VK.2.2.04 – Aufzeichnung von Videokonferenzen

Wenn die Aufzeichnungsfunktion aktiv ist oder ein Screenshot der Videokonferenz angefertigt wird, MUSS dies allen Teilnehmenden zu jeder Zeit signalisiert werden.[25]

VK.2.2.05 – Teilen von Bildschirminhalten

Funktionen zum Teilen von Bildschirminhalten MÜSSEN eine zuverlässige Auswahl der zu teilenden Inhalte (z. B. gesamter Desktop oder nur bestimmte Fenster, Programme oder Dateien) ermöglichen.

[23] Dabei ist zu beachten, dass viele Lösungen, die über Server der jeweiligen Dienstanbietenden laufen, als sogenannte Ende-zu-Ende-Verschlüsselung beschrieben werden. Diese Aussagen sind kritisch zu hinterfragen, da die Dienstanbietenden möglicherweise dennoch auf die Daten zugreifen können (z. B. können die Daten zwar verschlüsselt sein, aber der Schlüssel ist den Dienstanbietenden bekannt).

[24] Vgl. TR-02102 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

[25] Diese Anforderung bezieht sich auf integrierte Funktionen des Videokonferenzdienstes, falls diese vorhanden sind. Unabhängig davon können Aufzeichnungen und Screenshots auch unbemerkt (z. B. über separate Programme) von anderen Teilnehmenden angefertigt werden. Für dieses Risiko müssen Benutzende entsprechend sensibilisiert werden (vgl. VK.2.5.01 b).

VK.2.2.06 – Chat-Funktion

a) Wenn der Videokonferenzdienst eine Chat-Funktion bietet, SOLLTE diese durch die Moderierenden einer Konferenz deaktiviert werden können.

b) Gesendete Chat-Nachrichten SOLLTEN spätestens beim Beenden einer Konferenz automatisch gelöscht werden.

c) Wenn der Chat-Verlauf archiviert werden soll, MÜSSEN alle Teilnehmenden darauf hingewiesen werden (entweder automatisch durch den Videokonferenzdienst oder durch die Veranstaltenden der Videokonferenz).

VK.2.2.07 – Absicherung von Dateiablagen

a) Videokonferenzdienste KÖNNEN für Benutzendendaten sowie Administrationsdaten sowohl interne Dateiablagen des Dienstes als auch externe Dateiablagen (z. B. Cloud-Dienste) nutzen.

b) Die verwendeten Dateiablagen MÜSSEN die in der Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen der Einrichtung erfüllen (vgl. VK.2.1.01).

c) Werden Videokonferenzaufzeichnungen gespeichert, MÜSSEN sie passwortgeschützt gespeichert sein. Der Zugriff auf Aufzeichnungen DARF NUR durch Benutzende erfolgen, die gemäß Berechtigungskonzept (vgl. VK.2.1.03) dazu autorisiert sind.

VK.2.2.08 – Deaktivierung sicherheitskritischer Leistungsmerkmale

Die Einrichtung MUSS im Vorfeld entscheiden, welche Leistungsmerkmale benötigt werden und einen Videokonferenzdienst auswählen, bei dem nicht benötigte sicherheitskritische Leistungsmerkmale[26] deaktiviert oder sicher konfiguriert werden können.

2.3 Beschaffung

Für den Beschaffungsprozess sind die Vorgaben des Vergaberechts einschlägig. Die Einrichtung muss darüber hinaus dafür Sorge tragen, dass die folgenden Sicherheitsanforderungen beachtet werden. Durch wen dies geschieht, hängt hierbei vom jeweiligen Betriebsmodell ab.

Entscheidet sich die Einrichtung für eine selbstgehostete Lösung, ist der IT-Betrieb für die Umsetzung der Anforderungen an das Hosting zuständig. Entsprechend gelten dann Sicherheitsanforderungen an die eingesetzte Software (an den jeweiligen Stellen wird daher auf „Dienst bzw. Software“ verwiesen).

Bei fremdgehosteten Diensten kann die Einhaltung der Sicherheitsanforderungen vertraglich zugesichert werden. Sie müssen dann entsprechend schon in der Leistungsbeschreibung berücksichtigt werden. Besteht jedoch kein Einfluss bei der Vertragsgestaltung (z. B. wenn lediglich Nutzungsbedingungen akzeptiert werden), können diese Regelungen nicht in jedem Fall zugesichert werden. In diesem Fall sollte die Einrichtung die für ihr Einsatzszenario relevanten Informationen sichten (z. B. zur Verfügbarkeit oder Datenlokation) und auf dieser Basis prüfen, ob die Sicherheitsanforderungen erfüllt werden.

VK.2.3.01 – Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS die Erfüllung der in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (vgl. VK.2.1.01) bereits in der Leistungsbeschreibung als Ausschlusskriterium fordern.

b) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob diese Sicherheitsanforderungen erfüllt werden können.

[26] Als *sicherheitskritisch* sind insbesondere automatisierte Funktionen anzusehen, die beispielsweise Inhaltsdaten verarbeiten (z. B. Spracherkennung) und somit die Gefahr eines ungewollten Datenabflusses vergrößern (vgl. VK.2.4.03).

c) Die Einrichtung MUSS für sich festlegen, wie häufig sie Sicherheitsnachweise über den Dienst bzw. die Software prüft (z.B. initial sowie anlassbezogen bei Aktualisierungen). Die Vorlage der Sicherheitsnachweise SOLLTE durch die Anbietenden vertraglich zugesichert werden, sie KÖNNEN aber auch öffentlich bereitgestellt werden.[27]

d) Diese Sicherheitsnachweise MÜSSEN

- die aktuelle Dokumentation der Systembeschreibung sowie
- die Aktualität von vertraglich zugesicherten Unterlagen (z. B. Zertifizierungen, Testierungen, Prüfberichte)

umfassen.

e) Die Einrichtung MUSS die Sicherheitsnachweise über den Dienst bzw. die Software auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum keine zeitlichen Lücken enthalten.

f) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Nutzung von Videokonferenzdiensten relevant sind. Diese Anforderungen werden durch diesen Mindeststandard nicht berührt.

VK.2.3.02 – Datenlokation

a) Für fremdgehostete Dienste MÜSSEN die Dienstanbietenden darlegen, an welchen Lokationen[28] Daten gespeichert und verarbeitet werden.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Risikoanalyse (vgl. VK.2.1.02 e) sowie die mögliche Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

VK.2.3.03 – Dienstverfügbarkeit

Die Einrichtung MUSS festlegen, wie hoch die Verfügbarkeit des Videokonferenzdienstes sein muss. Der Grad der Verfügbarkeit SOLLTE vom Betrieb zugesichert werden.

VK.2.3.04 – Aktualisierung

a) Die Dienstanbietenden bzw. Softwareherstellenden MÜSSEN Sicherheitsupdates für den Videokonferenzdienst bedarfsgerecht und schnell bereitstellen.

b) Bei öffentlich bekannten, kritischen Schwachstellen[29] SOLLTEN die Dienstanbietenden bzw. Softwareherstellenden innerhalb von 21 Tagen, nachdem ihm die Schwachstelle bekannt wurde, ein Update bereitstellen.

c) Die Dienstanbietenden bzw. Softwareherstellenden SOLLTEN Benutzende umgehend über bekanntgewordene Schwachstellen und (falls verfügbar) mögliche Workarounds informieren.

VK.2.3.05 – Kontaktmöglichkeit

Um potenzielle Schwachstellen melden zu können, MÜSSEN Kontaktmöglichkeiten zu Sicherheitsteams der Dienst- bzw. Softwareherstellenden bereitgestellt werden.

---

[27] Wenn bspw. kein direktes Vertragsverhältnis zwischen der Einrichtung und den Dienstanbietenden besteht, müssen geeignete Nachweise öffentlich zugänglich sein, damit die Einrichtung dennoch die relevanten Informationen sichten und prüfen kann.

[28] Hier ist insbesondere das anwendbare Recht in der Verarbeitungs-Lokation relevant, da es z. B. Zugriffsrechte durch Ermittlungsbehörden regeln kann. Lokationen könnten bspw. aufgeteilt sein in *innerhalb Deutschlands, innerhalb der EU* und *außerhalb der EU.*

[29] Definition kritischer Schwachstelle s. Glossar

2.4 Anforderungen an den Betrieb

Unabhängig davon, ob Videokonferenzdienste fremd- oder selbstgehostet eingesetzt werden, muss die Einrichtung einen sicheren Betrieb gewährleisten. Dazu gehört ein ganzheitliches Managementsystem für Informationssicherheit sowie eine geeignete Administration.

VK.2.4.01 – Managementsystem für Informationssicherheit

Die Einrichtung MUSS den Videokonferenzdienst in ihr eigenes ISMS einbinden.

VK.2.4.02 – Deaktivierung nicht benötigter Leistungsmerkmale

a) Von der Einrichtung als sicherheitskritisch identifizierte Leistungsmerkmale, die nicht benötigt werden, MÜSSEN deaktiviert oder sicher konfiguriert werden (vgl. VK.2.2.08).

b) Automatische Verbindungsannahmen MÜSSEN deaktiviert werden.[30]

c) Die Einrichtung MUSS im Vorfeld kritisch prüfen, welche Methoden zur automatischen Auswertung (KI-Verfahren, z. B. Gesichtserkennung oder automatische Untertitel) von Videokonferenzinhalten der Videokonferenzdienst bietet. Nicht benötigte KI-Funktionen MÜSSEN deaktiviert werden.

VK.2.4.03 – Deaktivierung nicht benötigter Netzdienste und Protokolle

a) Bei selbstgehosteten Diensten MÜSSEN alle nicht benötigten Netzdienste und Protokolle gemäß IT-Grundschutz-Anforderung SYS.1.1.A6[31] deaktiviert werden.

b) Bei selbstgehosteten Diensten MÜSSEN alle benötigten unsicheren Netzdienste und Protokolle im Rahmen der Risikoanalyse behandelt werden (vgl. VK.2.1.02 e). Im Zuge der Risikoanalyse identifizierte risikomindernde Maßnahmen MÜSSEN auf dem Server umgesetzt werden.

VK.2.4.04 – Konfiguration

Gemäß Kapitel 2.2 MUSS ein Dienst ausgewählt werden, der die dort beschriebenen funktionalen Anforderungen erfüllt. Je nach eingesetztem Produkt können diese Funktionen jedoch ggf. einzeln konfiguriert werden. In diesem Fall MÜSSEN folgende Konfigurationen vorgenommen werden:

a) Die Signalisierung der Kamera- und Mikrofonaktivität MUSS aktiviert sein (vgl. VK.2.2.02 a-b). Wenn sie benötigt wird, MUSS die akustische Signalisierung ebenfalls aktiviert sein (vgl. VK.2.2.02 c).

b) Die Anzeige der Teilnehmenden MUSS aktiviert sein (vgl. VK.2.2.03 a).

c) Die Signalisierung beim Beitritt neuer Teilnehmender zur Videokonferenz MUSS aktiviert sein (vgl. VK.2.2.03 b).

d) Die Signalisierung beim Verlassen Teilnehmender SOLLTE aktiviert sein (vgl. VK.2.2.03 b).

VK.2.4.05 – Aktualisierung

a) Der Betrieb MUSS Aktualisierungen nach VK.2.3.04 unverzüglich einspielen.

b) Unabhängig von der Verfügbarkeit eines Updates, MUSS der Betrieb spätestens sieben Tage nach Bekanntwerden einer kritischen Schwachstelle[32] Maßnahmen zur Mitigation ergreifen.

[30] Ansonsten kann ein Anruf auf eine bekannte Adresse eines Videoendpunktes initiiert werden, was zu einer unbemerkten Überwachung und Ausspähung von Räumen und Benutzenden führt.
[31] Vgl. IT-Grundschutz-Kompendium – Baustein SYS.1.1: Allgemeiner Server (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)
[32] Definition kritischer Schwachstelle s. Glossar

VK.2.4.06 – Sicherheitsanforderungen an den Betrieb im Rechenzentrum

Rechenzentren, in denen Videokonferenzdienstleistungen oder Teile davon betrieben werden, MÜSSEN den Mindeststandard des BSI für die Anwendung des HV-Benchmark kompakt 4.0[33] einhalten. Für fremdgehostete Dienste MUSS dies im Rahmen der Beschaffung sichergestellt werden (z. B. durch vertragliche Zusicherung oder Sichtung veröffentlichter Informationen).

2.5 Regelungen für Benutzende

Um eine sichere Nutzung des Videokonferenzdienstes zu gewährleisten, müssen alle Benutzenden für den sicheren Umgang sensibilisiert werden. Die folgenden Sicherheitsanforderungen sind unabhängig vom Betriebsmodell umzusetzen.

VK.2.5.01 – Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzdiensten

a) Die Einrichtung MUSS eine Einweisung für Benutzende in geeigneter Form durchführen, die insbesondere Anweisungen bezüglich Informationssicherheit sowie die zu beachtenden Regularien umfasst.

b) Die Einweisung MUSS unter anderem vermitteln

- welche Bedeutungen die angezeigten Symbole auf dem Display haben;
- wie der Status der Kamera und des Mikrofons angezeigt werden kann;
- welche Bedeutung Hinweistöne und Hinweismeldungen haben;
- welche Verbindungen zu welchen Gegenstellen sicher verschlüsselt[34] sind (Ende-zu-Ende oder abschnittsweise);
- für welche Datenkategorien der Videokonferenzdienst freigegeben ist (vgl. VK.2.1.02 d);
- dass andere Teilnehmende unbemerkt Screenshots, Sprach- und Videoaufzeichnungen anfertigen können (z. B. über separate Programme), auch bei deaktivierter Aufzeichnungsfunktion (vgl. VK.2.2.04);
- dass beim Einsatz von Kamera und Mikrofon trotz Deaktivierung auf Softwareebene grundsätzlich das Risiko einer ungewollten Übertragung besteht (z. B. durch Bedienfehler, Sicherheitslücken oder Angriffe).

c) Benutzende SOLLTEN Testsitzungen durchführen, damit sie sich den sicheren Umgang mit dem Dienst erarbeiten können.

VK.2.5.02 – Sicherer Umgang mit Videokonferenzdaten

a) Die Einrichtung MUSS Benutzende verpflichten, Zugangsdaten und andere kritische Benutzenden- und Administrationsdaten (wie z. B. Konferenz- bzw. Benutzendenprofile, Videokonferenzaufzeichnungen, PINs und Passwörter zur Freischaltung des Zugangs zu Konferenzräumen) so aufzubewahren, zu speichern und zu teilen, dass Dritte keine Kenntnis von ihnen erlangen.

b) Vor der Anfertigung von Videokonferenzaufzeichnungen MUSS die Einwilligung aller Teilnehmenden eingeholt werden. Der rechtskonforme Umgang mit Videokonferenzaufzeichnungen MUSS geregelt sein.

VK.2.5.03 – Geeignete Standortwahl für Videoendpunkte

a) Die Einrichtung MUSS Benutzende verpflichten, bei jeder Benutzung auf eine geeignete Standortwahl seines Videoendpunktes zu achten, um die Gefährdung durch einen versehentlichen Informationsabfluss in

[33] Vgl. MST HVB-k (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2018)

[34] Dabei ist zu berücksichtigen, dass viele Videokonferenzanlagen ein Schlosssymbol für Verschlüsselung anzeigen, dieses aber nicht zwingend etwas über die Qualität der Verschlüsselung aussagt. Außerdem wird bei Verwendung eines Konferenzservers bzw. einer Multipoint Control Unit (MCU) die Verschlüsselung dort aufgebrochen. Daher müssen alle Teilnehmenden einer Konferenz verschlüsselt eingewählt sein, um ein Mindestmaß an Sicherheit zu gewährleisten.

Bild und Ton zu minimieren[35]. Zusätzlich KÖNNEN Funktionen des Videokonferenzdienstes zur Hintergrundauswahl (virtueller oder verwischter Hintergrund) genutzt werden.

b) Bei Bedarf MÜSSEN Benutzende geeignet ausgestattet werden (z. B. mit Headsets und Sichtschutzfolien), um auch bei mobilem Arbeiten eine sichere Teilnahme an Videokonferenzen zu ermöglichen.

c) Für fest installierte Videokonferenzsysteme (z. B. Raumsysteme) MUSS die Einrichtung den Standort entsprechend sicher auswählen und einrichten.

VK.2.5.04 – Prüfung der Teilnehmenden

Die unberechtigte Teilnahme an Videokonferenzen MUSS verhindert werden. Dazu MUSS mindestens eine der folgenden Möglichkeiten umgesetzt werden:

- Vertrauliche Zugangsdaten werden vorab nur mit berechtigten Personen geteilt.
- Die Moderierenden schließen unberechtigte Teilnehmende aus der Videokonferenz aus.
- Der Videokonferenzdienst stellt Warteräume für Videokonferenzsitzungen bereit, so dass neue Teilnehmende erst nach erfolgreicher Identifizierung an der Sitzung teilnehmen können.

VK.2.5.05 – Sicheres Beenden einer Videokonferenzsitzung

Nach dem Ende einer Videokonferenz MÜSSEN die Benutzenden die Sitzung auf ihren Endgeräten beenden, damit es im Nachgang der Sitzung nicht zu einem ungewollten Informationsabfluss kommt. Bei gemeinsam genutzten Geräten mit personalisierten Accounts, z. B. Raumsystemen, MUSS auch zusätzlich ein Abmelden der Benutzenden am Gerät erfolgen.

[35] Das können einerseits zum Beispiel Informationen auf Whiteboards im Sichtbereich der Kamera sein oder Gespräche im Umfeld, die von Mikrofonen aufgenommen werden. Andererseits gilt dies auch für den Abfluss der Inhalte aus der Videokonferenz nach außen (s. dazu auch Unterpunkt b).

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. [Online] 2021. [Zitat vom: 01. September 2021.] https://www.bsi.bund.de/dok/433400.

—. 2008. BSI-Standard 100-4 – Notfallmanagement. [Online] 2008. [Zitat vom: 02. August 2021.] https://www.bsi.bund.de/dok/128600.

—. 2017. BSI-Standard 200-2 – IT-Grundschutz-Methodik. [Online] 2017. [Zitat vom: 22. Juli 2021.] https://www.bsi.bund.de/dok/128640.

—. 2017. BSI-Standard 200-3 – Risikoanalyse auf der Basis von IT-Grundschutz. [Online] 2017. [Zitat vom: 22. Juli 2021.] https://www.bsi.bund.de/dok/407502.

—. 2021. IT-Grundschutz-Kompendium. [Online] 2021. [Zitat vom: 22. Juli 2021.] https://www.bsi.bund.de/dok/128568.

—. 2020. Kompendium Videokonferenzsysteme. [Online] 2020. [Zitat vom: 01. September 2021.] https://www.bsi.bund.de/dok/523216.

—. 2018. Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0. [Online] 2018. [Zitat vom: 01. September 2021.]

—. 2019. Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes („Nutzerpflichten NdB“). [Online] 2019. [Zitat vom: 01. September 2021.]

—. 2017. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste. [Online] 2017. [Zitat vom: 01. September 2021.]

—. 2021. Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards. [Online] 2021. [Zitat vom: 01. September 2021.] https://www.bsi.bund.de/dok/11916758.

Bundesministerium des Innern, für Bau und Heimat (BMI). 2017. *Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung.* Berlin : s.n., 2017.

Deutsches Institut für Normung e.V. (DIN). 2018. *DIN 820-2:2018-09: Normungsarbeit – Teil 2: Gestaltung von Dokumenten.* Berlin : Beuth Verlag GmbH, 2018.

FIRST. 2019. *Common Vulnerability Scoring System (CVSS).* Version 3.1. 2019.

Internet Engineering Task Force (IETF). 1997. RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. [Online] 1997. [Zitat vom: 23. 07 2020.] https://tools.ietf.org/html/rfc2119.

Abkürzungsverzeichnis

BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DIN	Deutsches Institut für Normung e.V.
EU	Europäische Union
FAQ	Frequently Asked Questions
HTTPS	Hypertext Transfer Protocol Secure
HV	Hochverfügbarkeit
HVB-k	Hochverfügbarkeitsbenchmark kompakt
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte (analog zu IT-SiBe, s. Vorwort)
ISMS	Managementsystem für Informationssicherheit
IT	Informationstechnologie
IT-SiBe	IT-Sicherheitsbeauftragte (wird hier analog zu ISB verwendet, vgl. Vorwort)
KI	Künstliche Intelligenz
KoViKo	Kompendium Videokonferenzsysteme
LED	Light-Emitting Diode
MCU	Multipoint Control Unit
MST	Mindeststandard
NCD	Nutzung externer Cloud-Dienste
NdB	Netze des Bundes
RFC	Request for Comments
TR	Technische Richtlinie
UP Bund	Umsetzungsplan Bund 2017
VK	Videokonferenz
WAN	Wide Area Network

Glossar

Benutzende

Benutzende sind Mitarbeitende der Einrichtung, die informationstechnische Systeme im Rahmen der Erledigung ihrer Aufgaben benutzen. *IT-Benutzende* und *Benutzende* sind hierbei als Synonyme zu betrachten, da heutzutage nahezu alle Mitarbeitenden eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung ihrer Aufgaben benutzen.[36]

(Videokonferenz-) Dienst

Ein *Videokonferenzdienst* ist ein Kommunikationsdienst für zwei oder mehr Teilnehmende, der die Übertragung und Vermittlung von Audio- und Videodaten in Echtzeit anbietet. Moderne Dienste bieten meist zusätzliche Leitungsmerkmale wie Chat, das Teilen von Bildschirminhalten, eine Kalenderintegration, das gemeinsame Bearbeiten von Dokumenten oder den Dateiaustausch an. Schnittstelle für Benutzende ist der Videoendpunkt (Definition s.u.), in den auch die zusätzlichen Leistungsmerkmale integriert sind.

Einrichtung

Die Mindeststandards des BSI verwenden den Begriff *Einrichtung* zur besseren Lesbarkeit synonym zu *Stellen des Bundes* gemäß § 8 Abs. 1 BSIG.

(Video-) Endpunkt

Als *Videoendpunkte*, auch *Videoterminals* genannt, werden die Endgeräte bezeichnet, mit denen Benutzende an einer Videokonferenz teilnehmen können. Sie existieren als dedizierte proprietäre Hardware (klassische Raum- oder Desktopsysteme), als Anwendung auf Standard-IT-Ausstattung wie Desktopcomputern und Laptops oder als Applikation auf mobilen Endgeräten wie Smartphones und Tablets. Videoendpunkte stellen die Anfangs- und Endpunkte der Bild- und Tonübertragung dar.[37]

Kritische Schwachstelle

Eine Schwachstelle wird als *kritisch* bezeichnet, wenn sie nach dem Industriestandard Common Vulnerability Scoring System (CVSS) v3.1 mit High (7.0-8.9) oder Critical (9.0-10.0) bewertet wird (vgl. CVSS (FIRST, 2019)).

Moderierende

Als *Moderierende* (auch engl. *Hosts*) werden Teilnehmende einer Videokonferenz bezeichnet, die gegenüber anderen Teilnehmenden erweiterte Berechtigungen besitzen, insbesondere Rechte zur Zugangskontrolle (z. B. die Möglichkeit, andere Teilnehmende auszuschließen) sowie i.d.R. das Starten und Beenden der Videokonferenz.

Teilnehmende

Als *Teilnehmende* einer Videokonferenzsitzung im Sinne dieses Mindeststandards gelten jegliche bestehenden Verbindungen von einem Endpunkten zur jeweiligen Sitzung. Dabei müssen *Teilnehmende* nicht immer einer natürlichen Person entsprechen, da mehrere Personen über denselben Endpunkt an einer Videokonferenzsitzung teilnehmen können oder auch eine Person mehrere Verbindungen aufbauen kann (z. B. zur Nutzung mehrerer Endpunkte für Präsentationszwecke).

[36] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)
[37] Vgl. KoViKo, S. 30f (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)