Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI für Videokonferenzdienste

nach § 8 Absatz 1 Satz 1 BSIG – Version 0.4 vom 09.02.2021

COMMUNITY DRAFT

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 für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 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 „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)
[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 haben heute eine zentrale Bedeutung für die Zusammenarbeit über 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 übertragenen Daten entstehen.

Das BSI hat 2020 das Kompendium Videokonferenzsysteme (KoViKo)[5] 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 in wesentlichen Teilen auf dem KoViKo. Er richtet sich speziell an Stellen des Bundes und hebt die Aspekte hervor, die aus Sicht des BSI beachtet werden müssen, um beim Einsatz von Videokonferenzdiensten innerhalb der Bundesverwaltung ein definiertes Mindestsicherheitsniveau zu erreichen. Gleichzeitig kann er auch allen anderen Interessierten einen kompakten Einstieg in die Thematik bieten.

Dieser Mindeststandard beschreibt vorwiegend Sicherheitsanforderungen an Videokonferenzdienste selbst. Neben den Diensten sind aber auch die Endpunkte[6], auf denen sie genutzt werden, von entscheidender Bedeutung für die IT-Sicherheit. Sicherheitsanforderungen aus weiteren Standards und Regelwerken müssen für diese IT-Systeme eingehalten werden und bleiben von diesem Mindeststandard unberührt. Insbesondere setzt der Mindeststandard ein Managementsystem für Informationssicherheit (ISMS) auf Basis der IT-Grundschutz-Vorgehensweise voraus.[7] Es wird davon ausgegangen, dass die entsprechenden Endpunkte bereits in das ISMS der Einrichtung eingebunden sind. Sie werden hier nur beispielhaft erwähnt, wenn sie direkten Einfluss auf die Umsetzung der Sicherheitsanforderungen haben.

1.2 Nutzungsmodelle

Das Angebot an Videokonferenzlösungen 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. Wie oben beschrieben, gilt dieser Mindeststandard für alle Nutzungsmodelle. Jedoch lassen sich viele Sicherheitsanforderungen nicht unabhängig vom Einsatzszenario 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 Dienstleister vertraglich zugesichert werden?). In Kapitel 2 wird daher an den entsprechenden Stellen darauf hingewiesen, auf welche Nutzungsmodelle sich die jeweiligen Sicherheitsanforderungen beziehen oder für welches Nutzungsmodell 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 technischen Maßnahmen verantwortlich.

[5] Vgl. KoViKo (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)
[6] Definition s. Glossar
[7] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

- Fremdgehostet: Ein externer Dienstleister 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), müssen verfügbare Informationen und Nutzungsbedingungen kritisch geprüft werden.

1.3 Modalverben

In Anlehnung an den IT-Grundschutz[8] 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[9] und DIN 820-2: 2018[10].

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. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

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

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

2 Sicherheitsanforderungen

2.1 Konzeption

Bevor eine Videokonferenzlösung 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 Nutzungsmodell.

VK.2.1.01 IT-Sicherheitsrichtlinie für den Videokonferenzdienst

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie nach IT-Grundschutz für Videokonferenzdienste erstellen.

b) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragten bei der Erstellung der Sicherheitsrichtlinie beteiligen.

VK.2.1.02 IT-Sicherheitskonzept für den Videokonferenzdienst

a) Die Einrichtung MUSS ein IT-Sicherheitskonzept nach IT-Grundschutz für Videokonferenzdienste erstellen.

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

Aus dem IT-Sicherheitskonzept MUSS hervorgehen, in welchem Szenario (z. B. innerhalb der Netze des Bundes (NdB) oder über offene Netze) welcher Videokonferenzdienst eingesetzt wird. Für Videokonferenzdienste, die innerhalb von NdB eingesetzt werden, MÜSSEN die Anforderungen des Mindeststandards NdB[11] eingehalten werden.

c) Die Einrichtung MUSS festlegen, für welche Datenkategorien[12] der Videokonferenzdienst freigegeben werden soll. Die Einrichtung MUSS bei der Freigabe der Datenkategorien Geheim- und Datenschutzaspekte sowie Personen- und Dienstgeheimnisse berücksichtigen.

d) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des Videokonferenzdienstes entstehen können, umfassend ermitteln[13]. Die ermittelten Risiken MÜSSEN dem Risikomanagement der Einrichtung nach BSI-Standard 200-3[14] unterzogen werden. Die Einrichtung DARF den Videokonferenzdienst NUR nutzen, wenn die ermittelten Risiken wirksam vermieden oder hinreichend reduziert oder getragen werden können.

VK.2.1.03 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[15] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im Weiteren die Begrifflichkeit des BSI-Standards 100-4.

---

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

[12] Die Datenkategorien können durch den IT-SiBe festgelegt werden. Als Orientierung können beispielsweise die Datenkategorien gemäß Mindeststandard zur Nutzung externer Cloud-Dienste (NCD) genutzt werden: *Privat- und Dienstgeheimnisse, personenbezogene Daten, Verschlusssachen, sonstige Daten*, vgl. NCD.2.1.01 g) (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

[13] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige 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?)

[14] Vgl. BSI-Standard 200-3 – Risikoanalyse (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017)

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

a) Die Einrichtung MUSS bewerten, welche Bedeutung der Videokonferenzdienst in Notfällen einnehmen würde.[16]

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

VK.2.1.04 – Störungsmeldung und -behebung

Vor Inbetriebnahme des Videokonferenzdienstes MÜSSEN Prozesse für die Störungsmeldung und -behebung definiert werden. Die Benutzer MÜSSEN in geeigneter Weise über Kontaktmöglichkeiten sowie die voraussichtliche Dauer bis zur vollständigen Wiederherstellung der Verfügbarkeit informiert werden.

VK.2.1.05 – 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[17] eingehalten werden.

2.2 Funktionale Anforderungen

Videokonferenzdienste sind komplex und bieten viele Funktionen. Daher muss die Einrichtung vor der Beschaffung des Dienstes festlegen, welche Funktionen er bieten muss und welche technischen Anforderungen er erfüllen muss. Die folgenden Anforderungen müssen mindestens erfüllt sein, um später einen sicheren Betrieb zu ermöglichen. Sie gelten für alle Nutzungsmodelle 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[18]. Die Verschlüsselung MUSS entsprechend den Empfehlungen der Technischen Richtlinie TR-02102[19] umgesetzt sein.

b) Für webbasierte Schnittstellen des Videokonferenzdienstes 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 die Kamera- und Mikrofonaktivität optisch darstellen[20], damit das Ausspähen von Personen und Räumlichkeiten erkannt werden kann.

b) Der Videokonferenzdienst SOLLTE die Möglichkeit bereitstellen, dass Teilnehmer ihre Sprach- und Videoübertragung beim Beitritt initial deaktivieren können.

VK.2.2.03 – Anzeige der Teilnehmer

[16] 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?

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

[18] Dabei ist zu beachten, dass viele Lösungen, die über Server des jeweiligen Anbieters laufen, als „Ende-zu-Ende“-Verschlüsselung beschrieben werden. Diese Aussagen sind kritisch zu hinterfragen, da der Anbieter möglicherweise dennoch auf die Daten zugreifen kann (z. B. können sie zwar verschlüsselt sein, aber der Schlüssel ist dem Anbieter bekannt).

[19] Vgl. TR-02102 (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020)

[20] Die Darstellung kann sowohl auf Hardware-Ebene stattfinden (z. B. LEDs neben Webcams), als auch auf Software-Ebene (z. B. Kamera- und Mikrofon-Symbole).

a) Die Anzeige des Video-Endpunkts MUSS die Teilnehmer der Videokonferenz anzeigen können.

b) Treten einer Videokonferenz neue Teilnehmer bei oder treten Teilnehmer aus, so MUSS dieser Vorgang bei allen in der Videokonferenz befindlichen Teilnehmern signalisiert werden (z. B. über einen Aufmerksamkeitston).

VK.2.2.04 – Aufzeichnung von Videokonferenzen

Wenn die Aufzeichnungsfunktion aktiv ist, MUSS dies allen Teilnehmern zu jeder Zeit signalisiert werden.

VK.2.2.05 – Absicherung von Dateiablagen

Videokonferenzdienste KÖNNEN sowohl interne Dateiablagen des Dienstes als auch externe Dateiablagen (z. B. Cloud-Dienste)[21] nutzen. Die verwendeten Dateiablagen MÜSSEN den Sicherheitsvorgaben des IT-SiBe folgen.

VK.2.2.06 – Deaktivierung sicherheitsrelevanter Leistungsmerkmale

Die Einrichtung MUSS im Vorfeld entscheiden, welche Leistungsmerkmale benötigt werden und einen Videokonferenzdienst auswählen, bei dem nicht benötigte sicherheitskritische Leistungsmerkmale deaktiviert 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 Nutzungsmodell ab.

Entscheidet die Einrichtung für eine selbstgehostete Lösung, ist der IT-Betrieb für die Umsetzung der Anforderungen an das Hosting zuständig.

Bei fremdgehosteten Diensten können die 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 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 vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe VK.2.1.01) vom Dienstanbieter erfüllt werden können.

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung einfordern.

c) Die Einrichtung MUSS für sich festlegen, wie häufig sie Sicherheitsnachweise des Dienstanbieters prüft (z.B. initial sowie anlassbezogen bei Aktualisierungen). Die Vorlage der Sicherheitsnachweise SOLLTE durch den Dienstanbieter vertraglich zugesichert werden, sie können aber auch öffentlich bereitgestellt werden.[22] Bei selbstgehosteten Diensten gilt dies entsprechend für verwendete Software.

d) Diese Sicherheitsnachweise MÜSSEN

- die aktuelle Dokumentation der Systembeschreibung,

[21] Bei der Nutzung von Cloud-Diensten sind zusätzlich die Regelungen des Mindeststandards zur Nutzung externer Cloud-Dienste zu beachten, vgl. MST NCD (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2017).

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

- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- bei fremdgehosteten Diensten: einen Beleg der ordnungsgemäßen Durchführung von Datensicherungen und erprobten Rücksicherungen (Datensicherungskonzept)[23]

umfassen.

e) Die Einrichtung MUSS die Sicherheitsnachweise des Dienstanbieters bzw. Softwareherstellers 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. Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

VK.2.3.02 – Datenlokation

a) Für fremdgehostete Dienste MUSS der Dienstanbieter darlegen, an welchen Lokationen[24] Videokonferenzdaten 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 (siehe VK.2.1.02e)) sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

VK.2.3.03 – Dienst-Verfügbarkeit

Die Einrichtung MUSS festlegen, wie hoch die Verfügbarkeit des Dienstes sein muss. Der Grad der Verfügbarkeit SOLLTE vom Dienstanbieter (ggf. vertraglich) festgelegt werden.

VK.2.3.04 – Aktualisierung

a) Der Dienstanbieter bzw. Softwarehersteller MUSS Sicherheitsupdates für den Videokonferenzdienst bereitstellen.

b) Bei öffentlich bekannten, kritischen Schwachstellen[25] SOLLTE der Dienstanbieter bzw. Softwarehersteller innerhalb von 21 Tagen, nachdem ihm die Schwachstelle bekannt wurde, ein Update bereitstellen.

c) Der Dienstanbieter bzw. Softwarehersteller SOLLTE Benutzer 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 des Anbieters bzw. Herstellers bereitgestellt werden.

VK.2.3.06 – Sicherheitsanforderungen an den Betrieb im Rechenzentrum

Für die Rechenzentren, aus denen Videokonferenz-Dienstleistungen oder Teile davon erbracht werden, MUSS zusätzlich zu dem vorliegenden Mindeststandard der Mindeststandard des BSI für die Anwendung

[23] Dies ist nicht nur relevant, wenn Inhalte (wie Textdateien) über den Dienst verarbeitet werden, sondern auch bspw. für Benutzerprofile oder Rechnungsdaten.

[24] 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.*

[25] 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).

des HV-Benchmark kompakt 4.0[26] eingehalten werden. Das gilt für eigene Rechenzentren der Einrichtung ebenso wie für Rechenzentren von Dritten. Die Ergebnisse des HV-Benchmark können auch durch die Einrichtung aus den vom Dienstanbieter veröffentlichten Informationen ermittelt werden.

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 – Rollen- und Berechtigungskonzepte

a) Für die Nutzung des Videokonferenzdienstes MUSS ein Rollen- und Berechtigungskonzept erstellt werden, welches den Rollen nur die minimal notwendigen Berechtigungen zuweist.

b) Das Berechtigungskonzept MUSS auch den Zugriff auf Videokonferenzdaten (z. B. Aufzeichnungen) regeln.

VK.2.4.03 – Deaktivierung nicht benötigter Leistungsmerkmale

a) Sicherheitskritische Leistungsmerkmale, die nicht benötigt werden, MÜSSEN deaktiviert werden.

b) Folgende Leistungsmerkmale der Endpunkte MÜSSEN in jedem Fall deaktiviert werden:

- Sprachsteuerung
- Automatische Verbindungsannahme ohne Benutzerinteraktion[27]

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

VK.2.4.04 – Deaktivierung nicht benötigter Netzdienste und Protokolle

a) Bei selbstgehosteten Diensten MÜSSEN auf dem genutzten Server alle unsicheren Netzdienste und Protokolle (z. B. Telnet, FTP, http, SNMP, syslog) deaktiviert werden.

b) Bei selbstgehosteten Diensten MÜSSEN alle nicht benötigten Netzdienste und Protokolle gemäß IT-Grundschutz-Anforderung SYS.1.1.A6[28] deaktiviert werden.

2.5 Regelungen für Benutzer

Um eine sichere Nutzung des Videokonferenzdienstes zu gewährleisten, muss jeder einzelne Benutzer für den sicheren Umgang sensibilisiert werden. Die folgenden Sicherheitsanforderungen sind unabhängig vom Nutzungsmodell umsetzen.

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

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

b) Die Einweisung MUSS unter anderem vermitteln

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

[27] Ansonsten kann ein Anruf auf eine bekannte Adresse eines Video-Endpunktes initiiert werden, was zu einer unbemerkten Überwachung und Ausspähung von Räumen und Benutzern führt.

[28] Vgl. IT-GS-Baustein SYS.1.1: Allgemeiner Server (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021)

- 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[29] sind (Ende-zu-Ende oder abschnittsweise);
- für welche Daten der Videokonferenzdienst freigegeben ist (vgl. VK.2.1.02 d));
- dass andere Teilnehmer auch bei deaktivierter Aufzeichnungsfunktion (vgl. VK.2.2.04) Sprach- und Videoaufzeichnungen anfertigen können (z. B. über separate Programme); und
- dass beim Einsatz von Kamera und Mikrofon trotz Deaktivierung auf Software-Ebene grundsätzlich das Risiko einer ungewollten Übertragung besteht (z. B. durch Bedienfehler, Sicherheitslücken oder Angriffe);

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

VK.2.5.02 – Sicherer Umgang mit Videokonferenzdaten

Die Einrichtung MUSS Benutzer verpflichten, Benutzerdaten, Zugangsdaten und andere kritische Videokonferenzdaten, wie z. B. Konferenz- bzw. Benutzerprofile, Videokonferenzaufzeichnungen, PINs und Passwörter zur Freischaltung des Zugangs zu Konferenzräumen, sicher zu speichern und bei der Weitergabe an andere Benutzer sicher zu teilen.

VK.2.5.03 – Geeignete Standortwahl für Video-Endpunkte

a) Die Einrichtung MUSS Benutzer verpflichten, bei jeder Benutzung auf eine geeignete Standortwahl seines Video-Endpunktes zu achten, um die Gefährdung durch einen versehentlichen Informationsabfluss in Bild und Ton zu minimieren[30].

b) Bei Bedarf MÜSSEN Benutzer 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 Teilnehmer

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

- Vertrauliche Zugangsdaten werden vorab nur mit berechtigten Personen geteilt.

ODER

- Der Host (oder auch Gastgeber bzw. Moderator) schließt unberechtigte Teilnehmer aus der Videokonferenz aus.

ODER

[29] Dabei ist zu berücksichtigen, dass viele Videokonferenzanlagen ein Schloss-Symbol 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 Teilnehmer einer Konferenz verschlüsselt eingewählt sein, um ein Mindestmaß an Sicherheit zu gewährleisten.

[30] Das können zum Beispiel Informationen auf Whiteboards im Sichtbereich der Kamera sein oder Gespräche im Umfeld, die von Mikrofonen aufgenommen werden.

- Der Videokonferenzdienst stellt Warteräume für Videokonferenzsitzungen bereit, so dass neue Teilnehmer erst nach erfolgreicher Identifizierung an der Sitzung teilnehmen können.

VK.2.5.05 – Sicheres Beenden einer Videokonferenzsitzung

Nach dem Ende einer Videokonferenz MUSS die Sitzung beendet werden, damit es im Nachgang der Sitzung nicht zu einem ungewollten Informationsabfluss kommt. Bei gemeinsam genutzten Geräten, z. B. Raumsystemen, MUSS auch zusätzlich ein Abmelden des Benutzers am Gerät erfolgen. Das Videokonferenzsystem SOLLTE vom Strom getrennt werden, wenn es nicht genutzt wird.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2020. *BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen.* 2020-01. Bonn : s.n., 2020.

—. 2008. *BSI-Standard 100-4 - Notfallmanagement.* Version 1.0. Bonn : s.n., 2008.

—. 2017. *BSI-Standard 200-2 - IT-Grundschutz-Methodik.* Version 1.0. Bonn : s.n., 2017.

—. 2017. *BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz.* Version 1.0. Bonn : s.n., 2017.

—. 2021. *IT-Grundschutz-Kompendium.* Bonn : s.n., 2021.

—. 2020. *Kompendium Videokonferenzsysteme.* Version 1.0.1. Bonn : s.n., 2020.

—. 2018. *Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0.* Version 1.1 vom 19.06.2018. Bonn : s.n., 2018.

—. 2019. *Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikations-netze des Bundes („Nutzerpflichten NdB“).* Version 2.0 vom 24.09.2019. Bonn : s.n., 2019.

—. 2017. *Mindeststandard des BSI zur Nutzung externer Cloud-Dienste.* Version 1.0 vom 24.04.2017. Bonn : s.n., 2017.

—. 2020. Mindeststandards - Antworten auf häufig gestellte Fragen zu den Mindeststandards. [Online] 2020. [Zitat vom: 23. 07 2020.] 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 Normierung 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 Normierung e.V.
FAQ	Frequently Asked Questions
MST	Mindeststandard
NCD	Nutzung externer Cloud-Dienste
NdB	Netze des Bundes
IETF	Internet Engineering Task Force
RFC	Request for Comments

Glossar

Benutzer

Ein *Benutzer* ist ein Mitarbeiter der Einrichtung, der informationstechnische Systeme im Rahmen der Erledigung seiner Aufgaben benutzt. *IT-Benutzer* und *Benutzer* sind hierbei als Synonyme zu betrachten, da heutzutage nahezu jeder Mitarbeiter eines Unternehmens bzw. einer Behörde informationstechnische Systeme während der Erledigung seiner Aufgaben benutzt.[31]

(Video-) Endpunkt

Als *Video-Endpunkte*, auch *Video-Terminals* genannt, werden die Endgeräte bezeichnet, mit denen Nutzer an einer Videokonferenz teilnehmen können. Sie stellen die Anfangs- und Endpunkte der Bild- und Tonübertragung dar. Die Spannweite reicht hier von klassischen Raumsystemen, über Standard-IT-Ausstattung wie PC und Laptop und Videotelefone bis hin zu mobilen Endgeräten wie Smartphones oder Tablets.[32]

Host / Moderator / Gastgeber

Als *Host, Moderator* oder *Gastgeber* wird ein Teilnehmer einer Videokonferenz bezeichnet, der gegenüber anderen Teilnehmern erweiterte Berechtigungen besitzt, insbesondere Rechte zur Zugangskontrolle (z. B. die Möglichkeit, andere Teilnehmer auszuschließen).

Teilnehmer

Als *Teilnehmer* einer Videokonferenzsitzung gilt jede bestehende Verbindung von einem Endpunkt zur jeweiligen Sitzung. Dabei muss ein Teilnehmer 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).

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