

Sicherheitsanforderungen für Videokonferenzsysteme

Videokonferenzen gehören heute zum Arbeitsalltag. Ob Microsoft Teams, Zoom, Webex oder andere Plattformen – ohne Videokonferenzsysteme wären Homeoffice und hybride Arbeitsmodelle kaum denkbar. Mit der zunehmenden Verbreitung steigt jedoch auch die Bedeutung der Informationssicherheit. Schliesslich werden über diese Systeme vertrauliche Gespräche geführt, Bildschirminhalte geteilt und oftmals auch Aufzeichnungen gespeichert.

Mit der DIN SPEC 27008 wurde Anfang 2024 ein Dokument veröffentlicht, das grundlegende IT-Sicherheitsmassnahmen für Videokonferenzsysteme beschreibt. Ziel der Spezifikation ist es, Mindestanforderungen für die Sicherheit solcher Dienste festzulegen und typische Bedrohungen sowie geeignete Gegenmassnahmen zu definieren.

Nicht verwechseln mit ISO/IEC 27008

Der Name kann leicht zu Verwirrung führen. Neben der DIN SPEC 27008 existiert auch die internationale Norm ISO/IEC 27008. Beide Dokumente haben jedoch nichts miteinander zu tun.

Die ISO/IEC 27008 unterstützt Auditoren bei der Überprüfung von Informationssicherheitsmassnahmen innerhalb eines ISMS nach ISO/IEC 27001. Sie richtet sich in erster Linie an Auditoren und Organisationen, die ein Informationssicherheitsmanagementsystem betreiben.

Die DIN SPEC 27008 verfolgt dagegen einen ganz anderen Ansatz. Sie beschäftigt sich ausschliesslich mit der Sicherheit von Videokonferenzsystemen und beschreibt die typischen Bedrohungen sowie die erforderlichen Mindestmassnahmen. Gemeinsam

haben beide Dokumente lediglich die Nummer 27008.

Wie ist die DIN SPEC 27008 aufgebaut?

Die DIN SPEC 27008 ist übersichtlich aufgebaut und umfasst fünf Kapitel sowie einen informativen Anhang.

Die Struktur gliedert sich wie folgt:

1. Geltungsbereich
2. Normative Verweise
3. Begriffe und Definitionen
4. Bedrohungen
5. Mindestsicherheitskriterien
6. Anhang A mit Prüfspezifikationen und Checklisten

Den Schwerpunkt bilden dabei die Kapitel 4 und 5. Während Kapitel 4 die verschiedenen Bedrohungsszenarien beschreibt, definiert Kapitel 5 die entsprechenden Sicherheitsmassnahmen. Zusätzlich enthält Anhang A eine Checkliste, mit deren Hilfe Anbieter ihre Umsetzung selbst

überprüfen können. Damit verfolgt die DIN SPEC einen praxisnahen Ansatz.

Worum geht es in der DIN SPEC 27008?

Videokonferenzdienste haben sich in den letzten Jahren stark verändert. Moderne Plattformen bieten längst nicht mehr nur Audio- und Videoübertragung, sondern zusätzlich Chatfunktionen, Bildschirmfreigaben, Aufzeichnungen und verschiedene Kollaborationsmöglichkeiten.

Gleichzeitig verschwimmen die Grenzen zwischen privaten und geschäftlichen Anwendungen. Viele ursprünglich für Unternehmen entwickelte Lösungen werden heute auch von Privatpersonen verwendet. Aus Sicht der Informationssicherheit bringt diese Entwicklung neue Herausforderungen mit sich.

Die DIN SPEC 27008 konzentriert sich deshalb auf Mindestanforderungen für Videokonferenzsysteme in einer Consumer-Umgebung. Im Mittelpunkt stehen dabei die klassischen Schutzziele der Informationssicherheit:

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Betrachtet werden unter anderem:

- Audio- und Videoübertragung,
- Chatfunktionen,
- Bildschirmfreigaben,
- Aufzeichnungen,
- Browser- und Client-Anwendungen,
- die zugrunde liegende Infrastruktur sowie
- die Verwaltung von Verschlüsselungsschlüsseln.

Nicht Bestandteil der Spezifikation sind Datenschutzanforderungen. Ebenso wenig werden Themen wie Whiteboards, Umfragen, Gamification-Funktionen oder externe Hardware wie Kameras und Mikrofone betrachtet.

Welche Inhalte behandelt die DIN SPEC 27008?

Im Zentrum der Spezifikation stehen verschiedene Bedrohungsszenarien und die dazugehörigen Schutzmassnahmen.

Risiken beim Softwareanbieter

Ein schlecht entwickeltes oder unzureichend gepflegtes System kann erhebliche Sicherheitsrisiken verursachen. Die DIN SPEC nennt unter anderem:

- fehlendes oder unzureichendes Patchmanagement,

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch



Videokonferenzdienste haben sich in den letzten Jahren stark verändert.

Bild: Pixabay

- veraltete Softwareversionen,
- Schwachstellen in der Softwarearchitektur,
- fehlerhafte Implementierungen,
- Manipulation von Clients,
- Cross-Site-Scripting und
- die Verbreitung manipulierten Programmcodes.

Damit wird deutlich, dass die Sicherheit bereits bei der Entwicklung der Software beginnt.

Risiken beim Dienstanbieter

Auch die Infrastruktur des Anbieters spielt eine wichtige Rolle. Hier nennt die DIN SPEC beispielsweise:

- unbefugten Zugriff auf Systeme und Server,
- Angriffe auf die Infrastruktur,
- DDoS-Angriffe,
- unbefugten physischen Zugriff auf Rechenzentren,
- ungesicherte Kommunikationswege,
- das Abfangen von Datenströmen sowie
- Advanced Persistent Threats (APT).

Gerade bei cloudbasierten Diensten sind diese Risiken besonders relevant.

Risiken bei Gastgebern und Teilnehmern

Viele Sicherheitsprobleme entstehen durch die Nutzung selbst. Deshalb betrachtet die DIN SPEC auch Bedrohungen auf Anwenderseite. Dazu gehören:

- unbefugter Zugriff auf Meetings,
- Identitätsdiebstahl,
- gemeinsam genutzte Benutzerkonten,
- unbeabsichtigte Offenlegung von Informationen,
- sogenannte Meeting-Bombings,
- unkontrollierte Aufzeichnungen,
- unzureichend geschützte gespeicherte Daten sowie
- Spear-Phishing über Besprechungseinladungen.

Gerade die unbeabsichtigte Offenlegung von Informationen

kann in der Praxis häufig beobachtet werden. Ein falsches Fenster bei der Bildschirmfreigabe oder ein sichtbarer Hintergrund können bereits dazu führen, dass vertrauliche Informationen preisgegeben werden.

Welche Mindestanforderungen definiert die Norm?

Den eigentlichen Kern der DIN SPEC 27008 bildet Kapitel 5. Dort werden den Bedrohungen konkrete Massnahmen zugeordnet.

Sichere Softwareentwicklung
Softwareanbieter sollen sichere Entwicklungsverfahren einsetzen und Prozesse zur Behandlung von Schwachstellen etablieren.

Patch- und Schwachstellenmanagement

Die Spezifikation fordert unter anderem:

- die Identifikation von Schwachstellen,
- ein geregeltes Vulnerability Management,
- regelmässige Sicherheitsupdates,
- automatische Updatefunktionen,
- Informationen über verfügbare Updates,
- Verfahren zur Überprüfung der Echtheit von Softwareversionen sowie
- eine schnelle Behandlung kritischer Schwachstellen.

Schutz der Infrastruktur

Dienstleister sollen geeignete technische und organisatorische Massnahmen umsetzen, um die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Dienste sicherzustellen. Dazu gehören insbesondere:

- Backup-Lösungen,
- Notfallwiederherstellung,
- Schutz vor Datenverlust und
- resiliente Infrastrukturen.

Zugriffsmanagement

Die DIN SPEC fordert ausserdem geeignete Verfahren zur Zugriffskontrolle. Diese Anforderungen

orientieren sich teilweise an ISO/IEC 27001 und umfassen:

- Zugriffskontrollen,
- Schutz physischer Einrichtungen,
- erweiterte Authentifizierungsverfahren,
- Möglichkeit zur Konto-löschung,
- Verwaltung von Identitäten und Berechtigungen sowie
- zusätzliche Prüfungen bei verdächtigen Anmeldungen.

Wie kann die DIN SPEC 27008 umgesetzt werden?

Die Spezifikation richtet sich in erster Linie an Anbieter von Videokonferenzdiensten. Dennoch können auch Unternehmen, die solche Systeme einsetzen, von den Anforderungen profitieren. Ein möglicher Ansatz besteht aus fünf Schritten.

1. Risiken analysieren

Die in Kapitel 4 beschriebenen Bedrohungen sollten mit der eingesetzten Lösung verglichen werden. Dadurch lassen sich relevante Risiken identifizieren.

2. Sicherheitsfunktionen prüfen

Unternehmen sollten bewerten, welche Sicherheitsfunktionen ihre Videokonferenzplattform unterstützt. Dazu gehören beispielsweise:

- Mehrfaktor-Authentisierung,
- Ende-zu-Ende-Verschlüsselung,
- Wartezimmerfunktionen,
- Teilnehmerverwaltung,
- sichere Aufzeichnungen und
- automatische Updates.

3. Anbieter bewerten

Viele Anforderungen betreffen den Betreiber der Plattform. Deshalb sollte bei der Auswahl eines Anbieters geprüft werden, ob:

- ein geregeltes Schwachstellenmanagement existiert,
- Sicherheitsupdates regelmässig bereitgestellt werden,
- Backup- und Wiederherstellungskonzepte vorhanden sind,

- etablierte Standards wie ISO/IEC 27001 oder BSI C5 berücksichtigt werden.

4. Anwender sensibilisieren

Technische Massnahmen allein reichen nicht aus. Schulungen und Sensibilisierungsmassnahmen helfen dabei, Risiken wie Phishing, Meeting-Bombing oder die unbeabsichtigte Offenlegung vertraulicher Informationen zu reduzieren.

5. Die Checkliste aus Anhang A nutzen

Anhang A enthält eine Prüfspezifikation für ein Selbstaudit. Mithilfe dieser Checkliste können Anbieter ihre Umsetzung systematisch überprüfen und Verbesserungspotenziale identifizieren.

Fazit

Die DIN SPEC 27008 schafft erstmals einen einheitlichen Rahmen für grundlegende Sicherheitsanforderungen an Videokonferenzsysteme. Sie beschreibt typische Bedrohungen und definiert konkrete Massnahmen, mit denen Anbieter ihre Dienste sicherer gestalten können.

Auch wenn sich die Spezifikation in erster Linie an Anbieter richtet, liefert sie wertvolle Kriterien für Unternehmen, die Videokonferenzplattformen auswählen oder bewerten möchten.

Die DIN SPEC 27008 ersetzt weder ein Informationssicherheitsmanagementsystem nach ISO/IEC 27001 noch eine umfassende Sicherheitsstrategie. Sie ergänzt bestehende Standards jedoch sinnvoll und bietet eine praxisnahe Orientierung für die sichere Nutzung moderner Videokonferenzsysteme.

Die DIN SPEC 27008 ist kostenlos unter https://www.dinmedia.de/de/technische-regel/din-spec-27008/37591_7409 oder mittels QR-Code zu beziehen.



Anzeige

manUplast


A SWISS-BASED ENTITY, SUPPORTED BY THE
STRENGTH OF AN INTERNATIONAL GROUP

Tool manufacturing
and precision injection molding

Technical
and complex part

Emmanuel MAREDAZ
+41 21 843 33 17
info@manuplast.ch
www.manuplast.ch