

ICS 33.160.60; 35.030

Basis IT-Sicherheitsmaßnahmen für Videokonferenz-Systeme; Text Englisch

Basic IT security measures for video conferencing systems;
Text in English

Mesures de sécurité informatique de base pour les systèmes de vidéoconférence;
Texte en anglais

Gesamtumfang 22 Seiten

Dieses Dokument wurde durch die im Vorwort genannten Verfasser erarbeitet und verabschiedet.

Contents

	Page
Foreword	3
Introduction	4
1 Scope	5
2 Normative references	5
3 Terms and definitions	5
4 Threats	7
4.1 Software provider	7
4.1.1 Lack of software management in the production environment	7
4.1.2 Poor design or architecture of the software	7
4.2 Service provider	7
4.2.1 Unauthorized access to systems, servers and applications	7
4.2.2 Attacks against infrastructures	7
4.2.3 Unauthorized access to physical facilities	7
4.2.4 Unprotected or uncontrolled communication paths	8
4.2.5 Meeting data interception/theft/spoofing	8
4.2.6 Advanced persistent threat (APT)	8
4.3 Account owner – host/co-host – participant	8
4.3.1 Insufficient identification of participants/unauthorized access to meetings	8
4.3.2 Misuse of shared profiles	8
4.3.3 Unintended disclosure of information	8
4.3.4 Meeting disruptions	8
4.3.5 Unchecked recording of video conferencing calls	9
4.3.6 Insufficiently secured data storage	9
4.3.7 Spear phishing through invites	9
5 Minimum security criteria	9
Annex A (informative) Test specification	14
A.1 General	14
A.2 Checklist	15
Bibliography	22

Tables

Table 1 — Threats and Mitigations	9
Table A.1 — Checklist	15

Foreword

This DIN SPEC has been developed according to the PAS procedure. The development of a DIN SPEC according to the PAS procedure is carried out in DIN SPEC-consortiums and does not require the participation of all stakeholders.

This document has been developed and adopted by the initiator(s) and authors named below:

— Zoom Video Communications Germany GmbH

Lena Maria Stork

— Microsoft Deutschland GmbH

Ralf Wigand

— TeamViewer Germany GmbH

Robert Haist

— alfaview gmbh

Claudia Baum

Franz C. Krüger

At present, there are no standards covering this topic in the body of German Standards.

DIN SPECs are not part of the body of German Standards.

A draft of this DIN SPEC has not been published.

Despite great efforts to ensure the accuracy, reliability and precision of technical and non-technical information, the DIN SPEC-consortium cannot give any explicit or implicit assurance or warranty in respect of the accuracy of the document. Users of this document are hereby made aware that the consortium cannot be held liable for any damage or loss. The application of this DIN SPEC does not release users from the responsibility for their own actions and is applied at their own risk.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. DIN shall not be held responsible for identifying any or all such patent rights.

Provision of this document free of charge as a PDF via the Beuth WebShop has been financed in advance.

For current information on this standard, please go to DIN's website (www.din.de) and search for the document number in question.

Introduction

Video-conferencing services (VCS) are an integral part of work-life, enabling remote and hybrid employment models through the transmission of audio and video data. VCS have developed quickly over the last years: Increased usability and functionality have made them ubiquitous in private and work life, replacing telephone conference and e-mail communication. Since its invention, additional services like chat and collaboration tools have been added to many VCS. Video-conferencing is poised to become part of Unified Communication and Collaboration (UCC) service offerings. With more functionality comes more complexity – including security issues. In order to protect the confidentiality, availability and integrity of the user data, this document has been developed.

One of the most distinctive developments in VCS is the blurring of the lines between consumer- and enterprise-grade solutions. Ease of use has propelled solutions originally intended to be enterprise software into the hands of consumers. From a security perspective, this development poses some challenges, as enterprises manage IT security differently than consumers.

This document is specifically designed to describe minimum security criteria, with the aim being to advance the security of VCS for use in personal computing. Consequently, the scope of this document is oriented toward the security needs of consumers the security needs of consumers:

- Modern VCS combine audio, video and chat capabilities. Chats can be persistent (i.e. exist independent of specific meetings) or non-persistent (are part of a meeting and erased at the end of a meeting). Video capabilities include screenshare, chat and recordings.
- VCS can either be implemented via a client installed on endpoints or accessed via browsers. This document focuses on clients provided by the VCS provider to access their VCS services via a browser or client application.
- The underlying IT infrastructure is part of VCS and therefore covered by this document. Underlying IT infrastructure is defined as the software and hardware components controlled by the VCS provider for establishing, maintaining and closing the communication channel between the peers/participants involved in the communication itself also including all software and hardware components which ensure the creation, exchange, storage and rotation of the encryption keys needed to implement the secure communication channels either for symmetric or asymmetric (public key cryptography) algorithms and either for encryption at rest and in transit. Self-hosted services are not in scope of this document.

Features like whiteboards, surveys and “gamification” functionalities are not in scope of this document. It also does not cover any adjacent hardware solutions like external cameras or microphones, speaker systems or “room” management. Furthermore, it does not include many security questions related to other components adjacent to VCS – be it the underlying operating system, browser software, connectivity devices like routers or Wireless Local Area Network (WLAN) amplifiers – all of which are important to ensure end-to-end security. Lastly, privacy-related matters are also out of scope.

The specific threat scenarios for VCS are developed in Clause 4. Clause 5 defines the minimum criteria. It does so by following the customer journey – from setting up an account to closing a meeting. Annex A describes the test specifications for the self-audit for VCS companies.

1 Scope

This document specifies minimum requirements with regard to IT security for video conferencing services in a consumer grade environment. This document does not cover data privacy requirements.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

DIN EN ISO/IEC 27001:2017-06, *Information technology — Security techniques — Information security management systems — Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015); German version EN ISO/IEC 27001:2017*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

DIN and DKE maintain terminological databases for use in standardization at the following addresses:

- DIN-TERMinologieportal: available at <https://www.din.de/go/din-term>
- DKE-IEV: available at <https://www.dke.de/DKE-IEV>

3.1 Roles

3.1.1

software provider

company which develops video conferencing software

3.1.2

service provider

company which provides the actual video conferencing service to the user, be it on premise, in a cloud environment or as a hybrid solution

Note 1 to entry: Software provider and service provider might be – but do not have to be – the same entity.

3.1.3

account owner

person who has signed a licensing agreement on the use of the software with the service provider

3.1.4

host/co-host

one or more persons who have control over key functionalities of a meeting that allows the management of participants and contribution

3.1.5

participant

person attending a meeting, including both people with the option to contribute and people who only view the meeting

3.1.6

authorized participant

participant who is authorized to participate with specific meeting links, token, or similar mechanisms

3.1.7

uninvited participant

person in a meeting who was not invited to the meeting

3.2 Features

3.2.1

waiting room

feature that allows a host or meeting owner to control when a participant joins a meeting, sometimes also called a green room

3.2.2

security-relevant meeting function

function in the application that needs to be protected from unauthorized usage, including but not limited to video, audio, in-meeting chats, file transfers, screen share, renaming, recording and remote desktop control

3.2.3

end-to-end encryption

method of secure communication that prevents third parties from accessing data while it is transferred from one endpoint device to another where the data is encrypted on the sender's device, and only the intended recipients can decrypt it

Note 1 to entry: As it travels to its destination, the content cannot be read or tampered with by any third party.

3.2.4

encryption status

function to show which type of encryption (e.g. end-to-end or hop-by-hop) is used by the video conferencing application for data in transit

3.2.5

recording

recording of a meeting that can include audio, video, chat, screenshare, and transcriptions

3.3 Other

3.3.1

IT infrastructure

software and hardware components for establishing, maintaining and closing the communication channel between the peers/participants involved in the communication itself also including all software and hardware components which ensure the creation, exchange, storage and rotation of the encryption keys needed to implement the secure communication channels either for symmetric or asymmetric (public key cryptography) algorithms and either for encryption at rest and in transit

3.3.2

software client

software application, be it "fat" or "thin" client, which can be configured by the end user

3.3.3

security vulnerability

weakness in an information system, system security procedures, internal controls, or implementation that can be exploited or triggered by a threat

3.3.4

login

authentication in order to access the administration interface or the video conferencing application on an endpoint device

3.3.5**ending a meeting**

initiated by the host or co-host, the action effectively ends the meeting for every participant and all communication as well as recording is terminated, making the meeting no longer accessible

3.3.6**leaving a meeting**

initiated by any participant, the action effectively ends the meeting for that participant and all communication from that participant is terminated

3.3.7**private**

restricted participation to a meeting only to authorized participants

3.3.8**state of the art**

developed stage of technical capability at a given time as regards products, processes and services, based on the relevant consolidated findings of science, technology and experience

[SOURCE: DIN EN 45020:2007-03, 1.4]

4 Threats**4.1 Software provider****4.1.1 Lack of software management in the production environment**

Outdated software versions create a general risk for computer systems. This risk is caused by a failure to manage software versions properly or a faulty patch management of internal systems. This may enable attackers to exploit vulnerabilities in order to access confidential information, take over control of meetings, or install malware.

4.1.2 Poor design or architecture of the software

For both web, fat clients and mobile applications, a poor architecture or implementation could lead to data leaks or stolen data, ranging from credential theft to cross site scripting (XSS) to tampering with the client software. A poor implementation may lead to a modification of the binary, leveraged to execute arbitrary pieces of code or the distribution of a malicious version of the binary.

4.2 Service provider**4.2.1 Unauthorized access to systems, servers and applications**

Risk of unauthorized logical access to the supporting IT systems, servers and infrastructure (including network devices/appliances) supporting the execution of the IT processes (clients) needed to deliver the service, e.g. by identity theft.

4.2.2 Attacks against infrastructures

A VCS, especially when offered as SaaS, is potentially susceptible to all types of attacks on their internet exposed infrastructure. A common attack being a distributed denial of service (DDoS). Such an attack may partially or fully take down the service.

4.2.3 Unauthorized access to physical facilities

A VCS is typically running as a SaaS (Software as a Service). This implies a hosting environment, which does not necessarily belong to the service provider. The facilities usually leveraged to host the service are data centers