Sichere und resiliente Open-Source-Videokonferenzlösung

Studiengang: MAS Information Technology

Die Thesis untersucht, ob sich sichere Videokonferenzlösungen auf Basis freier Open-Source-Software realisieren lassen. Sie identifiziert eine geeignete Plattform und entwickelt darauf eine referenzfähige Architektur. Das Vorgehen wird durch Proof-of-Concepts und Bedrohungsanalysen strukturiert. Iterative Ausbaustufen verfeinern darauf aufbauend das Design. Begleitend werden ethische Fragen zu digitaler Souveränität, Abhängigkeiten und Krisenfestigkeit adressiert.

Alexander Wolfeil

Problem und Ziel

Herausforderungen sind hohe Sicherheitsanforderungen und souveräne Betriebsziele für sichere Videokonferenzlösungen in Organisationen. Die Thesis liefert eine methodisch abgesicherte Auswahl einer Open-Source-Plattform und formt daraus eine referenzfähige Architektur. Das Ziel liegt darin überprüfbaren Schutzprinzipien, nachvollziehbaren Designentscheidungen und einer klaren Abgrenzung dessen, was unter den angenommenen Rahmenbedingungen technisch tragfähig ist, zu identifizieren. Zugleich adressiert die Thesis typische Angriffsrealitäten rund um Videokonferenzen, etwa Fehlkonfigurationen, missbrauchte Einladungen, unzureichende Identitätsprüfungen und Metadatenlecks.

Vorgehen und Auswahl

Das Vorgehen orientiert sich am Design-Science-Research-Ansatz mit zwei Proof-of-Concepts (PoCs) sowie einer kombinierten STRIDE- und MITRE-Betrachtung. Ein erster PoC klärt Basisintegration und Identität, ein zweiter PoC schärft Kollaboration mit Dritten, Medienebene und sichere Konfiguration. Die Lösungsauswahl stellt die Identitätsführung, die Trennung von Vertrauensdomänen, eine starke Verschlüsselung und die Betriebsreife in den Mittelpunkt. Ergänzend flossen Integrationsfähigkeit in bestehende Identitätslandschaften, Maturität und Pflegegrad des Open-Source-Projekts und Sicherheitsaspekte wie End-to-End-Verschlüsselung ein. Unter diesen Randbedingungen erweist sich Matrix mit Element als schlüssige Basis, ohne Alternativen grundsätzlich auszuschliessen.

Referenzarchitektur und Ergebnisse

Die Architektur entsteht iterativ. Zuerst wird eine interne Umgebung für sichere Konferenzen und belastbare Grundkonfiguration geschaffen. Danach wird eine separate Umgebung für die Zusammenarbeit mit Externen entwickelt, die kontrollierte Zusammenarbeit sowie ein verlässliches Onboarding sicherstellt. Abschliessend erfolgen Schritte wie Konsolidierung, Härtung und Monitoring. Redundanzen und definierte Notfallpfade sichern die Kommunikationsfähigkeit bei Störungen. Leitend sind konsequent geführte Identitäten mit starker Anmeldung und sparsamer Rechtevergabe, minimal exponierte Schnittstellen, Entkopplung der Medienkomponenten sowie klare Client-Prioritäten für den Zugang zu Videokonferenzen. Die Lösung erfüllt die wesentlichen Muss-Anforderungen und einen grossen Teil der Soll-Anforderungen. Grenzen bleiben dort, wo Qualität externer Identitätsprüfungen und Endgeräte die Sicherheit begrenzen. Die Risikoanalyse bündelt Schwerpunkte bei privilegierten Zugängen, Grenzen zwischen Kommunikationsbereichen, Schlüsselmaterial und Verfügbarkeit und verknüpft sie mit prüfbaren Massnahmen. Der Reifegrad wird über realitätsnahe Tests, geplante Penetrationstests und messbare Qualitätsziele der Medienebene weiter untermauert.

Einordnung und Ausblick

Die Arbeit verbindet technische Machbarkeit mit ethischen Fragen zu Souveränität, Abhängigkeiten und Krisenfestigkeit. Sie zeigt, dass Open Source in diesem Feld eine tragfähige Option sein kann, wenn Governance, Identität und Betrieb konsequent geführt werden. Sicherheit bleibt zugleich eine Frage der Risikoakzeptanz einer Organisation. Im aktuellen geopolitischen Umfeld mit wachsenden Spannungen und zielgerichteten Cyberangriffen steigt der Bedarf an sicheren und souveränen Videokonferenzlösungen, weil sie Handlungsfähigkeit und Vertraulichkeit auch unter Druck sichern. Für die Weiterentwicklung empfiehlt sich kryptografische Agilität mit MLS (Message Layer Security) im Protokoll und die Vorbereitung auf quantenresistente Verfahren im WebRTC-Stack, ergänzt um gehärtete und attestierbare Clients. Regelmässige Tests und eine laufende Neubewertung der Bedrohungslage halten die Lösung wirksam.