

Alles Skype oder was?

Aktuelle Trends in der Videokommunikation

Kai-Oliver Detken

Verteilte Standorte, mobile Vertriebsmitarbeiter und eine zunehmende Meeting-Kultur prägen heutige Unternehmen. Zur Unterstützung werden oftmals Videokonferenzsysteme eingesetzt, wenn auch diese immer noch nicht den Verbreitungsgrad erreicht haben, wie vorhergesagt. Aber die Technik ist in stetiger Entwicklung. Daher ist es mal wieder an der Zeit, einen kurzen Überblick über vorhandene Lösungen und Einsatzszenarien zu geben. Auch die Sicherheit findet dabei Beachtung.

Auf der Liste der meistgenutzten Videokonferenzen steht nach wie vor Skype (*Bild 1*). Dieser im Jahr 2003 eingeführte und immer noch kostenlose Instant-Messaging-Dienst unterstützt verschiedene Arten der Kommunikation:

- Instant Messaging (IM);
- IP-Telefonie;
- Videokonferenzen;
- Dateiübertragung;
- Screen Sharing.

Die Einfachheit der Benutzung und enge Verbindung zu Windows (seit 2011 ist Skype im Besitz von Microsoft) haben einen unschlagbaren Vorteil gegenüber allen Wettbewerbern.

Zudem geht der Trend beim Arbeitsplatzrechner immer mehr zum Laptop und in der Freizeit zum Tablet. Beide Varianten besitzen bereits eingebaute Mikrofone und Kameras, die ohne großen Zusatzaufwand genutzt werden können. Da

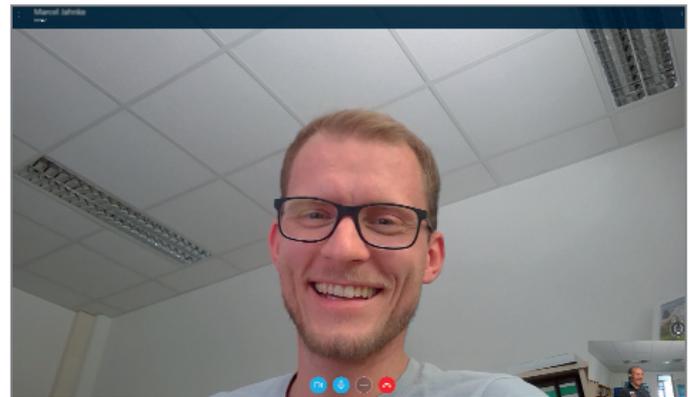


Bild 1: Skype-Kommunikation zwischen zwei Teilnehmern

Skype auf allen aktuellen Betriebssystemen (Windows 7/8/10, macOS 10.8-10.13, iOS 7-11, Android, Linux 64 Bit) funktioniert und sogar mittels Skype for Web in Browsern (Edge/IE 10+, Chrome 38+, Firefox 33+, Safari 6+) verwendet werden kann, gibt es keine technischen Einschränkungen oder Hürden bei der Nutzung.

Durch die technischen Eigenschaften des Produkts können auch absolute Neulinge die Software beherrschen und eine Kommunikation etablieren. Mussten früher noch Ports an der Firewall für Videokonferenzen freigeschaltet werden, arbeitet Skype unabhängig von diesen, indem von intern die Kommunikation zu einem exter-

nen Skype-Server aufgebaut wird. Dies kann sogar in Netzen erfolgreich durchgeführt werden, die nur http (Port 80) oder https (Port 443) zum Verbindungsaufbau zulassen.

Was für den Anwender handhabungsfreundlich ist, wird bei IT-Sicherheitsexperten eher negativ gesehen. Denn Skype trickst bei weit verbreiteten portbasierten Firewalls die Sicherheitssysteme aus. Nur Application Firewalls oder Intrusion-Detection-Systeme (IDS), die den Datenverkehr innerhalb eines Ports überprüfen können, wären in der Lage zu erkennen, dass nicht nur vordefinierte Daten übertragen werden.

IT-Sicherheit versteht der Hersteller im Grunde genommen anders: Bei der Verbindung zum Skype-Server wird laut Microsoft eine verschlüsselte Verbindung mit AES 256 verwendet. Allerdings lässt sich dies nicht überprüfen, da es sich bei Skype um eine proprietäre Anwendung handelt. Unabhängig davon wäre aber jedes Gespräch abhörbar, sobald der zentrale Skype-Server von einem Hacker übernommen wird, denn alle Gespräche müssen zwecks Weitervermittlung ent- und wieder verschlüsselt werden. Hat man den Server unter Kontrolle, ließe sich daher jedes Gespräch, ohne dass die Teilnehmer etwas bemerken würden, abhören.

Durch die Skype-out-Funktion ist eine Kommunikation auch zu Festnetz- und Mobilfunktelefonen möglich, um diese z.B. zu einer Konferenz hinzuzufügen. Daher fällt das proprietäre Kommunikationsprotokoll von Skype nicht so negativ ins Gewicht. Allerdings fallen entsprechende Kosten an, denn über das sog. Skypeln (Teilnehmer erwirbt eine Festnetznummer bei Skype) wird sogar die Annahme von Anrufen ermöglicht. Inzwischen sind auch Konferenzschaltungen mit bis zu 25 Teilnehmern möglich, die Audio und Video gleichermaßen unterstützen. Dann hängt jedoch die Sprachqualität noch stärker von der nutzbaren Bandbreite und Rechnerleistung ab, was das Ausschöpfen der maximalen Ressourcen nicht empfehlenswert macht. Um Skype einheitlich mit Microsoft-Anwendungen anbieten zu können, wurde Skype for Business etabliert. Hier werden verschiedene Kommunikationsmedien wie Echtzeitkollaboration, IP-Telefonie und Videokonferenzen in einer einheitlichen Anwendungsumgebung von Office 365 für Unternehmen zusammengefasst. Skype löste damit 2015 den Lync-Server ab, der sich nicht entsprechend durchsetzen konnte. Vorteilhaft ist für den Anwender, dass auf diese Weise Kontaktdaten und Präsenzinformationen automatisch miteinander verknüpft werden. Nachteilig könnte dies für den Datenschutz sein, da diese Informationen nicht unbedingt transparent für den Anwender im Hintergrund zusammenlaufen.

Softwarebasierte Lösungen

Skype gehört zu den softwarebasierten Videolösungen, die durch ihre Hardwareunabhängigkeit sehr flexibel sind. Obwohl Skype heute geschätzt den größten Anteil am Videokonferenzmarkt hat, gibt es Alternativen. So hat Apple mit FaceTime ein eigenes Produkt geschaffen, das aber nur Apple-Nutzern zugänglich ist. Auch hier sind Telefonie, Messaging und Kontakte vereint, wodurch diverse Möglichkeiten vorhanden sind, um einen Anruf zu starten. So kann der Teilnehmer aus einer Kontaktliste seinen Kommunikationspartner auswählen,

damit dieser einer Videositzung beiträgt. Auf Protokollebene verlässt sich FaceTime, im Gegensatz zu Skype, auf offene Standards. So wird das Session Initiation Protocol (SIP) zum Auf- und Abbau sowie zur Steuerung einer Kommunikationssitzung verwendet. Auch bei den Video- und Audiocodes geht man mit H.264 und Advanced Audio Coding (AAC) keinen proprietären Weg. Ähnlich wie Skype wird aber auch das Protokoll Session Traversal Utilities for NAT (STUN) genutzt, um Firewalls und NAT-Router zu erkennen und letztendlich ohne Schranken zu durchdringen. Eine Verschlüsselung der Kommunikation wird über das Secure Real-Time Transport Protocol (SRTP) angeboten, das im Internetstandard RFC-3711 beschrieben ist und standardmäßig zur IP-Telefonie eingesetzt wird. Hemmend für die Verbreitung ist der Einsatz auf reinen Apple-Geräten, so dass häufiger Skype genutzt wird.

Ein anderer mächtiger Konzern geht mit Google Hangouts ebenfalls andere Wege (Bild 2). Da hier ein Instant Messenger und Videokonferenzsystem integriert sind, wurden die älteren Projekte Google+ Messenger und Google Talk abgelöst. Über Webseiten von Gmail (E-Mail-Dienst), Inbox (Verwaltung von E-Mails, Terminen und Aufgaben) und Google+ (soziales Netz) kann es aufgerufen werden. Dies geht allerdings auch direkt über Apps auf Android oder iOS. Auch eine Erweiterung für den Browser Chrome ist nutzbar, um Google Hangouts direkt nutzen zu können. Während bei Chats durchaus bis zu 150 Teilnehmer unterstützt werden, sind Videokonferenzen nur bis zu zehn Teilnehmern zugelassen. Auch hier findet die zentrale Kommunikation immer über einen zentralen Server statt, der zudem in der Lage ist, die jeweiligen Endgeräte miteinander zu synchronisieren und z.B. Chat-Verläufe mitzuschneiden.

Nachteilig ist, dass Google in relativ schneller Folge neue Apps auf den Markt bringt, die entweder so weiterentwickelt werden, dass man Schwierigkeiten hat, zu folgen bzw. geliebte Funktionen vermisst, oder nach einer Eingewöhnungsphase wieder ver-

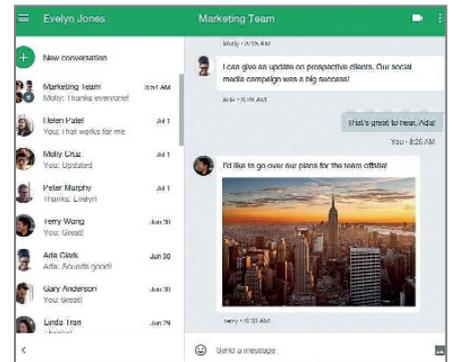


Bild 2: Konversation und Chatverläufe in Google Hangouts
(Quelle: <https://www.googlewatchblog.de>)

schwinden. Immerhin ist Google Hangouts auch unter iOS nutzbar, aber so flexibel wie Skype ist es dadurch noch lange nicht. Aber es gibt auch Alternativen zu den Big Playern. Mikogo z.B. ist eine solche, die Webkonferenzen mit Desktop Sharing für Fernwartung, Onlinepräsentationen und E-Learning anbietet (Bild 3). Sie ist gleichermaßen für

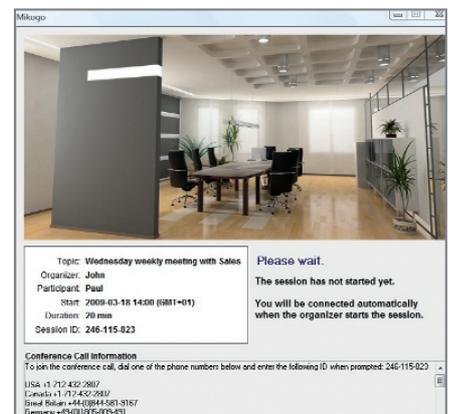


Bild 3: Virtueller Warteraum vor dem Start einer Videokonferenz bei Mikogo (Bild: Mikogo)

Windows-, MacOS- und Linux-Betriebssysteme geeignet und kann privat kostenlos verwendet werden. Sie ist eigentlich für Wartungszwecke geschrieben worden, weshalb eine Tunneltechnik über Port 80/443 verwendet wird, so dass keine Modifizierung der Firewall notwendig ist. Die Session wird kontinuierlich mittels 256-bit-AES-Verschlüsselung gesichert. Zur Übertragung seines Bildschirms, muss die Software auf dem Rechner des Teilnehmers installiert werden. Die angezeigte Sitzungsnummer nach Programmstart kann anderen Benutzern zur Verfügung gestellt werden und berechtigt dann zu einer Meeting-Teil-

nahme. Das Meeting kann aufgezeichnet werden, auch die anderen Teilnehmer können ihren Desktop freigeben. Maus und Tastatur kann man anderen Nutzern freischalten, was aber explizit erlaubt werden muss.

Einen ähnlichen Weg geht Branchenprimus Teamviewer, dessen Software ursprünglich als reine Fernwartungslösung entwickelt wurde. Inzwischen sind Leistungsmerkmale wie Screen Sharing, Videokonferenzen, Dateitransfer und VPN mit enthalten. TeamViewer arbeitet als Onlinedienst und ist damit unabhängig von Firewalls, Network Address Translation (NAT) und Proxyservern. Im Gegensatz zu Mikogo werden nicht die Standardprotokolle TCP und http verwendet, sondern ein proprietäres Protokoll. Es werden neben Windows, MacOS und Linux auch mobile Betriebssysteme wie Android und iOS unterstützt. Ab Version 5 werden Audio- und Videoübertragungen angeboten. Beim Verbindungsaufbau wird zuerst überprüft, welche Verbindungsart bei den vorhandenen Sicherheitsmaßnahmen genutzt werden kann. Die Aushandlung der Verschlüsselung wird immer über den Server vorgenommen, der im Anschluss versucht, die beiden Endgeräte miteinander zu verbinden, damit die anschließende Datenübertragung direkt erfolgen kann. Es wird auch hier eine AES-Verschlüsselung mit 256 bit auf Basis von RSA verwendet. Ein Angriff ist daher eigentlich nur möglich, wenn der Server selbst kompromittiert oder der administrative Zugriff ausgenutzt wird. Die Lösung hat sich für Fernwartungszwecke deutschlandweit als Quasistandard etabliert, kann aber auch als Videosystem verwendet werden.

Als letzte sehr verbreitete Softwarevariante lässt sich WhatsApp nennen. Als reiner IM-Dienst gestartet, können Nutzer inzwischen auch Textnachrichten, Bilder, Videos und Audiodaten austauschen. Durch den zusätzlichen Dienstemehrwert setzte sich WhatsApp gegenüber der SMS durch. Nachdem Facebook den Dienst übernommen hat, wurden weitere Neuerungen integriert. So kann ab 2015 auch IP-Telefonie darüber abgewickelt werden, was vielen Telefonie-Providern

missfällt, da hierdurch die entsprechenden Tarife untergraben werden. Seit Ende 2017 sind auch Video-Gruppen-Chats möglich. Die Ton- und Bildqualität hängt dabei aber stark von der Anzahl der Teilnehmer ab. Stark diskutiert wird, ob man WhatsApp im Unternehmensumfeld nutzen sollte. Die Verbindung zu Facebook legt nahe, dass Kontaktdaten direkt zwischen den Diensten ausgetauscht werden. Trotz inzwischen vorhandener Verschlüsselung werden immer wieder Sicherheitslücken bekannt. Durch den proprietären Charakter kann die Qualität der Verschlüsselung nicht überprüft werden. Hinzu kommt, dass es unklar ist, wie das Unternehmen mit den Kundendaten umgeht.

Hardwarebasierte Lösungen

Neben den softwarebasierten Lösungen, die sehr flexibel ohne zusätzliches Equipment einsetzbar sind, gibt es nach wie vor die klassischen Videokonferenzsysteme. Hier unterscheidet man u.a. zwischen Desktop- und Raumsystemen sowie Telepräsenzen. Ein neues System kommt z.B. von dem IP-Telefoniespezialisten Yealink, der Audiokonferenzen mit dem Mehrwert Videokommunikation aufwerten möchte. Das VC120-Videokonferenzsystem, bestehend aus VC120 Codec, VCS-Telefon, PTZ-Kamera und Fernbedienung, ist eine Full-HD-Lösung, die für Zweigstellen und kleine Außenbüros geeignet ist (Bild 4). Zur einfachen Handhabung ist Firewall-Traversal integriert, um diese automatisiert zu umgehen und einfach einen Kommunikationspfad etablieren zu können. Eine adaptive Bandbreitenanpassung und der darin enthaltene geringe Paketverlust von max. 8 % soll die Audio- und Videoqualität auf ein Höchstmaß anheben. Videositzungen können aufgezeichnet werden. Die PTZ-Kamera besitzt einen 18-fach optischen Zoom und mittels H.264 eine Auflösung von 1.080p bei 30 Frames/s. Aktuell werden acht gleichzeitige Teilnehmer bei Multipunkt-konferenzen unterstützt. Auch Smartphones können eingesetzt werden. Ähnliche Lösungen sind u.a. von Cisco, Lifesize, Avaya, Huawei, Polycom



Bild 4: Videokonferenzsystem Yealink VC120 auf Hardwarebasis (Foto: Yealink)

und Logitech verfügbar. Im Vergleich zu den softwarebasierten Lösungen ist in jedem Fall zusätzliche Hardware erforderlich, die möglichst auf beiden Kommunikationsseiten verfügbar sein sollte, um die höchstmögliche Qualität erreichen zu können. Hier wird der Schwerpunkt also auf den visuellen Aspekt gelegt, was mit höheren Kosten einhergeht.

Fazit

Videokonferenzen verbreiten sich besonders durch frei verfügbare Tools wie Skype auf bestehenden Betriebssystemplattformen. Die geschickte Integration von Skype mit anderen Microsoft-Produkten lässt beim Nutzer oft gar nicht erst die Frage aufkommen, ob eine Videokonferenz für ihn wichtig ist. Verwendet er bereits Office-Anwendungen wie Word, Excel, PowerPoint, OneNote sowie Besprechungsplanung, kann er durch die Skype-Integration z.B. die Chat-Funktion zusätzlich nutzen, Dateien mit anderen teilen und eine Besprechung einberufen. Auffällig ist, dass selbst bei Meetings mit mehreren Teilnehmern die Videofunktion bei softwarebasierten Lösungen oftmals unterdrückt wird. Dies ist bei hardwarebasierten Lösungen gänzlich anders, da diese Systeme speziell aufgrund ihrer visuellen Qualität angeschafft bzw. genutzt werden. Als Hindernis stehen oft nur die zusätzlichen Anschaffungskosten im Weg. Die Konfiguration ist heute leichter denn je und führt auch automatisiert an Firewall-Systemen vorbei. Dieses handhabungsfreundliche Merkmal kann allerdings ggf. auch Sicherheitslücken beinhalten, was im Unternehmenseinsatz immer bedacht werden sollte. (bk)