

# Sichere Videokonferenzen und „Application Sharing“

Mario Weis

**Moderne Kommunikationslösungen machen es Mitarbeitern heutzutage leicht, sich auch mit Kollegen an anderen Firmenstandorten von Angesicht zu Angesicht auszutauschen und mit ihnen gemeinsam in Anwendungen zu arbeiten. Unternehmen, die sich für die Einführung von Unified-Communications-Anwendungen entscheiden, sollten dabei aber die Netz- und Datensicherheit im Blick behalten.**

Die Zeiten, in denen Videokonferenzen ausschließlich großen Unternehmen vorbehalten waren und in eigens dafür ausgestatteten Räumen stattfanden, sind vorbei. Längst ist keine teure Spezialhardware mehr nötig, um Kollegen an anderen Standorten von Angesicht zu Angesicht gegenüberzusitzen: Erschwingliche Desktoplösungen wie z.B. PlaceCam 3 von daviko ermöglichen heute auch hochauflösende Mehrpunkt-Videokonferenzen über PC (unter Windows oder Mac OS), ohne dass die Mitarbeiter ihren Arbeitsplatz verlassen müssen. Die Informationen, die in solchen virtuellen Treffen rund um die Welt geschickt werden, sind dabei aber meist nur zum internen Gebrauch gedacht. Und wer möchte, dass die benutzten Werkzeuge reibungslos funk-

tionieren, wird die Firmenfirewall abhängig von der verwendeten Lösung konfigurieren müssen. Unified Communications im Unternehmen hat also immer auch eine sicherheitsrelevante Dimension, weswegen Betriebe bei der Auswahl einer Lösung auch ihre spezifischen Anforderungen an die Netz- und Datensicherheit im Blick behalten sollten.

## Löcher in der Firewall

Wer an einer Videokonferenz teilnimmt oder gemeinsam mit entfernten Kollegen an Präsentationen oder Dokumenten arbeitet, ist sowohl Versender als auch Empfänger von Daten. Der Transfer der Video- und Audioinformationen sowie der Anwendungsdaten zwischen den verschiedenen Konferenz-

teilnehmern kann dabei je nach genutzter Lösung verschieden organisiert werden – mit unterschiedlichen Auswirkungen auf die Netz-sicherheit: Wird die Verbindung über ein Peer-to-Peer-Netz realisiert, werden die Computer aller Konferenzteilnehmer (Peers) auf direktem Weg miteinander verbunden. Die ausgehenden Daten eines Nutzers müssen folglich auch an alle mit ihm verbundenen Peers geschickt werden. Das sorgt bei Konferenzen mit hohen Teilnehmerzahlen nicht nur für einen hohen „Upload“, sondern erschwert zudem auch die Konfiguration eines sicheren Firmennetzes.

Denn damit die Firewalls, hinter denen sich die Konferenzteilnehmer befinden, nicht vor jedem virtuellen Treffen für die jeweils teilnehmenden Peers konfiguriert werden müssen, bedienen sich Peer-to-Peer-Lösungen in der Regel eines Tricks: Die Mitarbeiter werden über eine getunnelte Verbindung zusammenschaltet, die die Firewalls zwischen ihnen „austrickst“. Dabei werden die zuvor verschlüsselten Daten so konvertiert, dass sie zur Übertragung in ein anderes Protokoll eingebettet werden können. Der Versand und Empfang der Daten kann so über gängige HTTP(S)-Ports laufen.

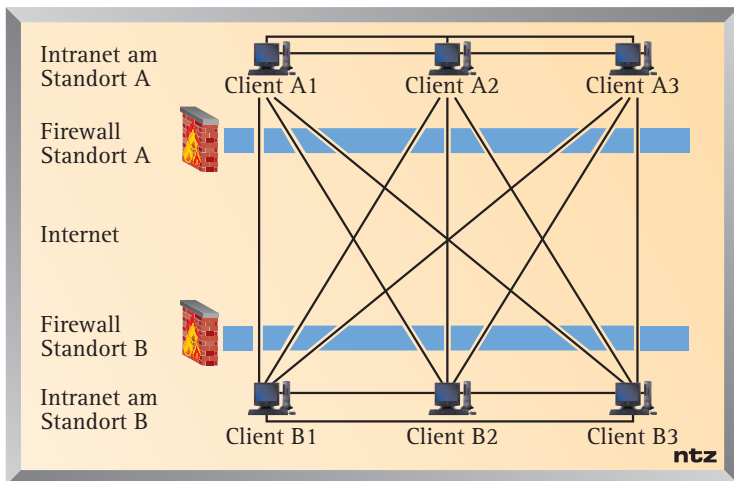
Da die Teilnehmer bei virtuellen Treffen oft wechseln und somit bei jeder Sitzung verschiedene Rechner am Datenaustausch beteiligt sind, erschweren Peer-to-Peer-Lösungen die Überwachung derjenigen Peers, die zur Nutzung dieser getunnelten Verbindungen berechtigt sind. Der Gefahr, dass sensible Daten durch die Firewall nach draußen geschmuggelt werden oder dass Unbefugte von außen Malware einschleusen, lässt sich also schwerer Herr werden.

## Verteilserver schafft Überblick

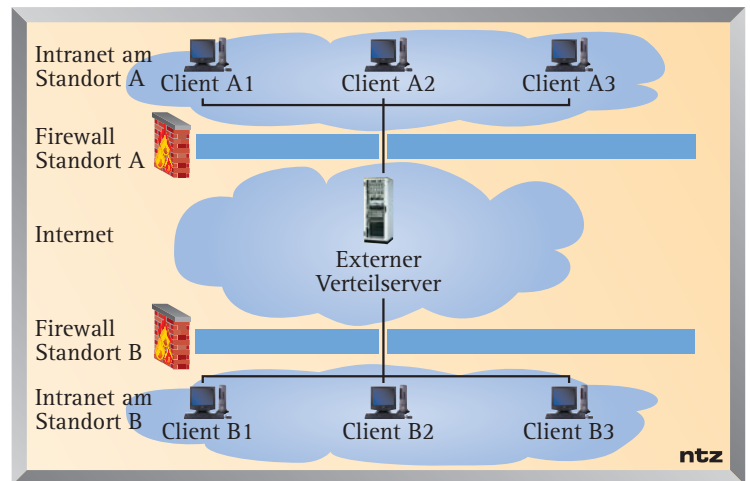
Videokonferenzlösungen für eine professionelle Nutzung setzen deshalb auf das Client-Server-Prinzip: Hierbei werden die Computer der einzelnen Mitarbeiter nicht direkt miteinander verbunden, sondern über einen zentralen Verteilserver. Das hat nicht nur den Vorteil, dass jeder Client sämtliche Audio-, Video- und Application-Sharing-Daten nur noch einmal an den Server senden muss, der dann die Weiterleitung an alle anderen Konferenzteilnehmer übernimmt, auch die Gewährleistung eines sicheren Netzes wird so erheblich erleichtert. Für die Nutzung von PlaceCam 3 kann z.B. entweder ein eigener Inhouse-Server oder der zentrale Server des Herstellers daviko zur Datenverteilung genutzt werden. Während der Konferenz nutzt die Soft-



Für die Nutzung von PlaceCam 3 kann entweder ein eigener Inhouse-Server oder der zentrale Server des Herstellers daviko zur Datenverteilung genutzt werden (Quelle: daviko)



Peer-to-Peer-Lösungen erschweren die Überwachung derjenigen Endgeräte im Firmennetz, die zur Nutzung der getunnelten Verbindungen berechtigt sind (Quelle: daviko)



Wenn die Clients die Daten nur mit dem fest definierbaren Verteilserver austauschen, lässt sich die Firewall präzise konfigurieren und der Datenverkehr besser kontrollieren (Quelle: daviko)

ware sowohl für die Übertragung von Video- und Audiodaten als auch für die Übermittlung sämtlicher Daten aus dem Application-Sharing normalerweise einen für die Echtzeitkommunikation prädestinierten UDP-Port. Gibt es hierbei Probleme, weicht sie auf HTTPS aus, um eine Verbindung zu gewährleisten.

Da die beteiligten Clients die verschiedenen Daten aber nur mit dem fest definierbaren Verteilserver und nicht mit allen potenziellen Konferenzteilnehmern direkt austauschen müssen, lässt sich die Firewall präzise konfigurieren und der Datenverkehr besser kontrollieren. Aus sicherheitstechnischen Erwägungen sollten Unternehmen also darauf achten, dass die genutzten Videokonferenz- und Kollaborationslösungen Verbindungen über einen Verteilserver realisieren, damit die Firmenfirewall auch bei der „grenzenlosen Kommunikation“ maximalen Schutz bietet.

### Daten sicher versenden

Mitarbeiter, die standortübergreifend kommunizieren und zusammenarbeiten, senden oft unternehmensbezogene Informationen hin und her, die außerhalb der Firma niemanden etwas angehen. Deswegen liegt die Frage nahe, wie das Versenden der Audio-, Video- und Anwendungsdaten vonstattengeht und wie verhindert wird, dass Dritte an die versendeten Informationen gelangen. Zu diesem Zweck werden die Daten vor dem Versand verschlüsselt. Die meisten Videokonferenzlösungen verwenden hierfür eine AES-256-bit-Verschlüsselung und schützen die Unternehmen somit optimal vor Datendiebstahl. Die Kommunikation über den zentralen Server ist so-

mit nach dem heutigen Stand der Technik vollkommen sicher.

Dennoch bietet der Berliner Softwarehersteller Unternehmen die Möglichkeit, PlaceCam 3 auch über einen eigenen „Inhouse“-Server zu nutzen. Firmen, die häufig mit sehr sensiblen Daten hantieren oder damit rechnen müssen, Opfer gezielter Cyberattacken zu werden, können Videokonferenzen und die standortübergreifende Zusammenarbeit somit auch als geschlossene Unternehmenslösung in einem virtuellen privaten Netz (VPN) realisieren. Diese Art der Nutzung hat sich bisher beispielsweise bei Banken oder Krankenhäusern bewährt.

Welches Schutzniveau gegen Datendiebstahl angemessen ist, hängt also auch von der Quantität und der Qualität der versendeten Daten ab: Unternehmen sollten sich fragen, wie oft sie die betreffende Lösung nutzen und welche Art Informationen darüber verbreitet werden sollen.

### Rechte intern regeln

Doch auch die beste Datenverschlüsselung wappnet Unternehmen nicht gegen Datendiebstahl oder -pannen, wenn es interne Risiken gibt. Eine Unified-Communications-Lösung sollte deshalb auch dazu beitragen, dem Datenklau durch eigene Mitarbeiter vorzubeugen, und berücksichtigen, dass möglicherweise auch wenig IT-affine Mitarbeiter die Lösung nutzen, die leichter Opfer von Cyberkriminellen werden. Um zu verhindern, dass Angestellte mutwillig oder aus Unwissenheit Daten über Unified-Communications-Werkzeuge an Unbefugte weitergeben, muss die jeweilige Lösung zentral zu verwalten sein. Mit PlaceCam 3 können Unternehmen beispielsweise zentral



Mario Weis ist Redakteur bei der Tema Technologie Marketing AG in Berlin. E-Mail: weis@tema.de

entscheiden, ob ihre Mitarbeiter über die Suchfunktion für alle PlaceCam-3-Nutzer zu finden sein sollen oder ob sie nur firmenintern sichtbar sind und der Informationsfluss über PlaceCam somit weitestgehend innerhalb des Unternehmens abläuft. Administratoren haben hier zudem die Möglichkeit, den einzelnen Nutzern verschiedene Rechte zuzuweisen, die neben allen Kontakten eines Nutzers in einer Datenbank auf dem genutzten Verteilserver hinterlegt sind: Sie können festlegen, ob einzelnen Teilnehmern während der Videokonferenz das Application-Sharing und der Dateiversand überhaupt zur Verfügung stehen sollen oder nicht. Vertrauenswürdigen Mitarbeitern kann der Administrator auch Moderationsrechte zuweisen und ihnen so, neben der Möglichkeit, Videokonferenzen zu leiten und zu steuern, auch das Recht einräumen, komplette Sitzungen aufzuzeichnen.

Zusätzlich zur sicher konfigurierten Firewall sollten Unternehmen also auch darauf achten, wem sie zu welchem Zeitpunkt welche Rechte im Umgang mit Unified-Communications-Lösungen einräumen. Werden diese Punkte bei der Auswahl der Lösung beachtet, steht der sorgen- und grenzenlosen Kommunikation schon bald nichts mehr im Wege. ■