Sichere Videokollaboration:

Wie Sie die Sicherheit Ihrer Cloud - Videokonferenzlösung gewährleisten

FROST & SULLIVAN

A Frost & Sullivan White Paper

Sponsored by Lifesize

contents

EINFÜHRUNG

In den letzten Jahren geht der Trend ganz klar in Richtung Cloud-Computing. Große, aber auch kleine und mittelständische Unternehmen (KMUs), profitieren von der Einführung der neuesten Technologien für Kommunikation und Zusammenarbeit, die in der „Cloud" ohne anfängliche Investitionen verfügbar sind. Tatsächlich bieten cloudbasierte Videokonferenzlösungen vielfältige Vorteile. So können Unternehmen hohe Investitionsaufwendungen einsparen und auf das IT-Management von Hardware und Software verzichten, während sie gleichzeitig die Flexibilität genießen, Services-on-Demand mit besserer Skalierbarkeit zu nutzen. Die Pay-as-you-consume-Option eröffnet allen, die auf Produktivitätssteigerungen und Kosteneinsparungen aus sind, ideale Voraussetzungen Videokonferenztechnologien zu implementieren.

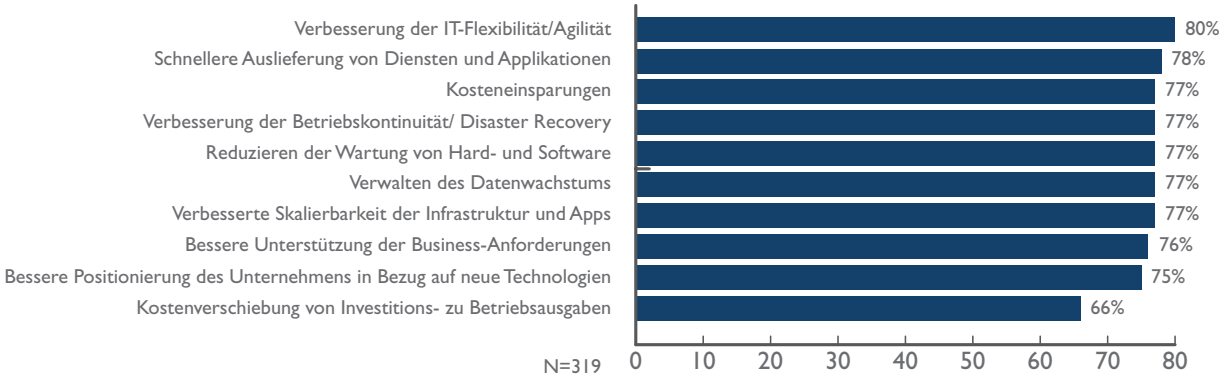
Ungeachtet der enormen Vorteile ist aber das Cloud-Computing mit einer Reihe von Herausforderungen behaftet, die nicht einfach unter den Tisch gekehrt werden können. Ein wichtiger Aspekt, der vielen Unternehmen und Endanwendern zu denken gibt, ist die Sicherheit, vor allem in Bezug auf Datenschutz, Privatsphäre und Kontrolle. In diesem Artikel befassen wir uns mit einigen der Sicherheitsbedenken für cloudbasierte Videokonferenzen und damit, wie Unternehmen diese Ängste mithilfe von Lösungen überwinden können, bei denen Sicherheit im Vordergrund steht.

SICHERHEIT – EINE HERAUSFORDERUNG

Videokonferenzen sind zu einem unabdingbaren Kommunikationsmittel für Tausende von Organisationen geworden, die nicht nur an Produktivitätssteigerungen und an einem Wettbewerbsvorteil interessiert sind, sondern ihre Betriebskosten reduzieren wollen, um ihre Profitmargen zu verbessern. Diese Unternehmen haben viele gute Gründe, ihre Videokonferenzlösung in der öffentlichen Cloud zu implementieren. Zu den wichtigsten Faktoren gehören sowohl kurzfristige taktische Überlegungen als auch längerfristige strategische Ziele. Die taktischen Treiber, etwa die Verschiebung von Investitionen (CAPEX) zu Betriebsausgaben (OPEX) und der reduzierte Verwaltungsaufwand, kommen den IT-Verantwortlichen entgegen, deren Budgets immer weiter schrumpfen. Die strategischen Treiber, etwa größere Agilität und bessere Unterstützung der sich ändernden Business-Anforderungen, reflektieren die dringendsten Anliegen der IT-Entscheider, die auf Transformation ausgerichtet sind. Auch wenn die Vorteile unbestreitbar sind, stehen viele Unternehmen aufgrund von Sicherheits- und Kontroll-Überlegungen einer Cloud-Videokonferenzlösung noch skeptisch gegenüber.

Aus den alljährlichen Befragungen von IT-Entscheidungsträgern, welche von Frost & Sullivan durchgeführt werden, geht hervor, dass mancherorts die Sicherheitsbedenken trotz der offensichtlichen Vorteile von Public-Cloud-Diensten noch sehr dominant sind. Abb. 1 zeigt den prozentualen Anteil von Public-Cloud-Nutzern aus einer kürzlichen Frost & Sullivan-Umfrage, die die Treiber nannten, die „sehr wichtig" für ihre Entscheidung zugunsten der Cloud für bestimmte Aufgaben waren. Auch wenn zahlreiche Faktoren die Entscheidung beeinflussten, so ist doch klar, dass die Kosten- und Budgetfaktoren, die früher im Vordergrund standen, nun durch Kriterien ergänzt werden, die weiter gefasste Business-Überlegungen betreffen.

Abb. 1: Als „sehr wichtig“ eingestufte Schlüsselkriterien zugunsten der Cloud

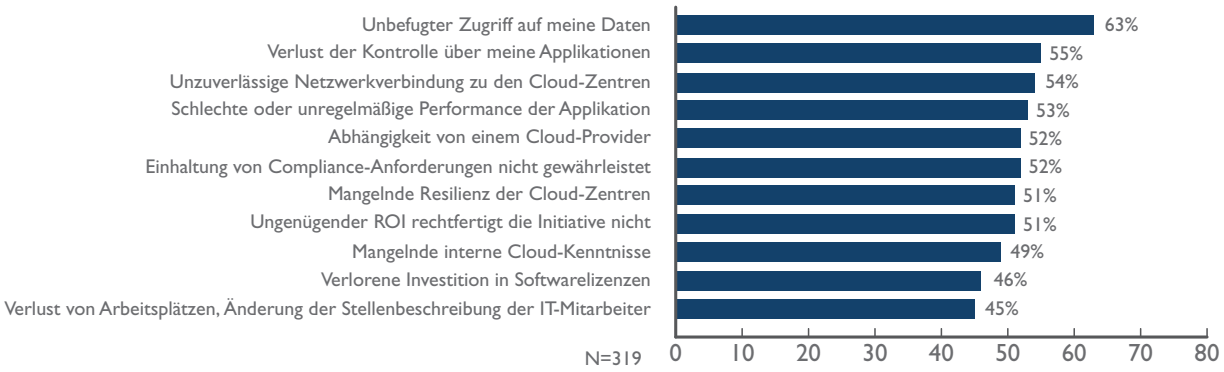


Source: Frost & Sullivan

In derselben Umfrage erwähnten die Befragten die bekannten Einwände bezüglich Sicherheit und Kontrolle als die Schlüsselfaktoren, die gegen eine Auslagerung auf die Public-Cloud sprachen (Abb. 2).

Da Cloud-Services die Nutzer mit „jedermann“ über jedes beliebige Gerät kommunizieren lassen, werden manche der Gespräche über das öffentliche Internet geführt. Deshalb fragen sich die User, wie sie ihre Daten und Applikationen, die in der gemeinsamen Public-Cloud ohne klar gezogene Grenzen angesiedelt sind, schützen können.

Abb. 2: Als „sehr wichtig“ eingestufte Schlüsselkriterien gegen die Cloud



Source: Frost & Sullivan

MOBILITÄT – EINE ZUSÄTZLICHE KOMPLIKATION

Bring-Your-Own-Device (BYOD) und Bring-Your-Own-Application (BYOA) ist ein Trend, der zu einer Veränderung führt, wie Business-User Produktivitäts-Apps erwerben und konsumieren. ,Während Mitarbeiter zufriedener und produktiver sind, wenn sie ihre eigenen Geräte und Applikationen nutzen dürfen, gehen BYOD und BYOA mit riesigen Sicherheitsproblemen für die IT-Verantwortlichen einher. Eine unkontrollierte Vermehrung von User-Geräten und -Anwendungen resultiert unweigerlich in mehr Versuchen, Verbindungen zwischen „nicht vertrauenswürdigen“ Geräten und dem Unternehmensnetzwerk herzustellen.

Mehr und mehr Applikationen, Geräte und eine Vielfalt von Netzwerken verbinden sich mit unternehmenseigenen Datenbanken, sodass es zunehmend schwieriger wird, die Sicherheit der inner- und zwischenbetrieblichen Zusammenarbeit zu wahren. Wenn die gewählte Cloud-Lösung die notwendigen Sicherheitsschichten und Zugriffskontrollmechanismen nicht bereitstellt, setzen Unternehmen nicht nur ihr Netzwerk einem beträchtlichen Risiko aus, sondern auch ihren Datenbestand. Plötzlich muss damit gerechnet werden, dass Kundendatenbanken und Anwendungen durch Zugriffe von Unbefugten oder durch nicht sichere Geräte gefährdet sind. Verlorene oder gestohlene Geräte und potenzielle Viren und andere Malware könnten eine echte Gefahr für die Unternehmensressourcen darstellen – eine durchaus berechtigte Sorge. All dies erfordert zusätzliche Sicherheitsmaßnahmen über viele Zugangspunkte, einschließlich Mobilgeräte, Applikationen und Netzwerke.

ÜBERLEGUNGEN ZUR GEHEIMHALTUNG

Bei Videokonferenzen werden geschäftskritische Informationen und Daten über betriebsinterne und betriebsfremde öffentliche und private Netzwerke übermittelt, wo sie anfällig gegen mögliche Sicherheitsverstöße sind.

Zu den wichtigsten Bedenken bezüglich Cloud-Sicherheit, die bei Videokonferenzen ins Gewicht fallen, gehören:

- ***Schutz der Informationen –*** Eine „Multi-Tenant"-Videokonferenz-Cloud bietet gemeinsame Nutzung von Applikationen und Ressourcen und birgt damit inhärente Risiken. Provider von cloudbasierten Videokonferenzen müssen sämtliche erforderlichen Schritte in die Wege leiten, um die Integrität der Daten zu wahren, die vor, während und nach der Besprechung ausgetauscht werden.

- ***Privatsphäre –*** Dienstanbieter müssen sicherstellen, dass alle geschäftskritischen Kundendaten (z.B. Kredikartennummern) verborgen oder verschlüsselt sind und dass nur berechtigte Nutzer Zugriff darauf haben. Darüber hinaus müssen die digitalen Identitäten und Anmeldedaten adäquat geschützt sein; dasselbe gilt für Daten, die der Provider über Kundenaktivitäten in der Cloud erfasst.

- ***Physische Sicherheit –*** Cloud-Videokonferenzen-Dienstanbieter müssen die physische Sicherheit der Datenzentren und der IT-Hardware gegen unbefugte Zugriffe und Diebstahl gewährleisten und mit Redundanz und Failover-Mechanismen mögliche Betriebsunterbrechungen auf ein absolutes Minimum beschränken.

- ***Endpunkt-Integrität –*** Da Videokonferenzdienste in der Cloud angestoßen und dann On-premise genutzt werden, müssen Sicherheit, Compliance und Integrität der Endpunkte Teil jeder Sicherheitserwägung sein.

- ***Identität- and Zugangs-Management –*** User haben mehrere Zugangspunkte. Lokale, Remote- und mobile User benötigen den einfachen Zugang zu Videokonferenzdiensten mit starken Authentifizierungskontrollen, die ihre Identität nicht gefährden.

DIE LIFESIZE ALTERNATIVE

Die Sicherheitsrisiken bei Videokonferenzen mögen vielfältig sein, doch mehrere Cloud-Dienste der nächsten Generation sind dabei, die richtigen Schritte zu unternehmen, um die Sicherheit zu verstärken und die Ängste der Kunden aus der Welt zu räumen. Lifesize Cloud, ein Cloud-Video-Dienst, der einfach zu nutzende und zuverlässig funktionierende Videobesprechungen, das Teilen von Dokumenten und Audiogespräche über beliebige Geräte ermöglicht, hat sich die Sorgen der Kunden zu Herzen genommen. Bereitgestellt über den IBM- und Amazon-Cloud-Backbone und implementiert in globalen Datenzentren, liefert Lifesize Cloud die Belastbarkeit, Kapazität und globale Anbindung, die sich Business-User wünschen. Eine umfassende Strategie in Sachen Sicherheit muss die am Cloud-Service beteiligten Anwender, Abläufe und Technologien integrieren. Zur Gewährleistung einer sicheren Zusammenarbeit per Video hat sich Lifesize für einen vielfältigen Ansatz entschieden.

- Verschlüsselung – Alle Kommunikation unter Lifesize Cloud-Nutzern ist vollständig mit 128-Bit AES (Advanced Encryption Standard) der Enterprise-Klasse für Medien und TLS (Transport Layer Security) für die Signalübermittlung verschlüsselt. An keiner Stelle des Systems hat ein Lifesize-Administrator Zugang zu den Medien. Es erfolgt keinerlei Aufzeichnung oder Speicherung.

- Datenzentren – Eine wichtige Sicherheitsüberlegung für Cloud-Service-Kunden ist es, zu wissen, welche Rechenzentren der Provider nutzt. Lifesize Cloud-Kunden können dank der IBM- und Amazon-Cloud-Backbones auf höchste Systemleistung, -zuverlässigkeit, -belastbarkeit und -sicherheit zählen. Außerdem werden sämtliche Datenzentren und Netzwerkstandorte regelmäßig überprüft und gegen physische Übergriffe geschützt.

- Authentifizierung – Die Verbindung zwischen Lifesize Cloud und den Lifesize Icon-Systemen wird bei der Bereitstellung über https authentifiziert. Registrierungen werden über TLS gesichert. Jeder User hat nur einen Account, über den er mit all seinen Geräten gleichzeitig eingeloggt sein kann. Eingehende Anrufe kann der User dann über das Gerät seiner Wahl entgegennehmen.

- Firewall/NAT Traversal – Nutzer müssen Endgeräte nicht außerhalb der Firewall platzieren, um die Kommunikation über Lifesize Cloud zu ermöglichen. Kollaboration via Cloud gestattet es den Usern, ihre Apps und Raum-Videosysteme hinter der Firewall zu behalten; das Traversal erfolgt dann über authentifizierte Server.

- Datenspeicherung – Die einzigen User-bezogenen Daten, die von Lifesize Cloud gespeichert werden, sind der vollständige Benutzername, die E-Mail-Adresse, das Kennwort, Telefon, Adresse und Firma. Kennwörter sind in der Datenbank verschlüsselt, es werden in der Cloud keine Kennwörter in Normaltext gespeichert.

- Rechnungstellung – Lifesize nutzt für Verkäufe über Vertriebskanäle Partner; von daher werden auf seinen Systemen keinerlei Rechnungsinformationen gespeichert.

- Account-Sicherheit – Die Nutzer müssen bei Verwendung eines Cloud-Dienstes bei der Zuweisung, dem Schutz und dem Ändern von Kennwörtern vorsichtig sein. Lifesize versendet eine Authentifizierungs-E-Mail, bevor ein Konto aktiviert wird. Jedes Konto (ob Admin oder Nutzer) ist kennwortgeschützt. Kennwörter und Authentifizierung sind verschlüsselt, so, wie die Kunden dies von einem sicheren Cloud-Dienst erwarten.

- Konferenz-Sicherheit – Mit Lifesize Cloud können die Anwender ihre Besprechungen mit einem Kennwort schützen und so eine weitere Sicherheitsstufe einführen. Zudem ist es möglich, während einer Konferenz jeden Teilnehmer ohne weiteres von der weiteren Teilnahme auszuschließen.
- Service-Verfügbarkeit – Lifesize Cloud wird in sicheren IBM-Datenzentren weltweit betrieben; Redundanz und Ausfallsicherheit sind gewährleistet. Im Fall einer Unterbrechung werden Anrufe auf einen anderen Server geleitet. Da die Systeme mit Backup-Funktion ausgestattet sind, sorgt die IT dafür, dass die User-Konfigurationen geschützt und auf dem aktuellsten Stand sind.
- Geschäftskontinuität und Disaster Recovery – Tritt in einem Datenzentrum oder Netzwerk-POP ein Problem auf, werden alle Lifesize-User sofort von einem anderen Datenzentrum übernommen. Der Dienst wird automatisch von einem Backup-Datenzentrum aus weitergeführt: Der Nutzer wählt sich erneut ein, und die Verbindung wird aufgebaut.

> „Wir unterhalten Büros in New York und San Francisco. Intern über Video zu kommunizieren, ist sehr viel besser als nur über das Telefon. Datensicherheit ist immer ein wichtiges Anliegen beim Arbeiten in der Cloud. Bei unseren Besprechungen geht es oft um sehr vertrauliche Dinge, und wenn die Informationen nach außen gelängen, könnte das unserem Geschäft schaden. Ein Aspekt, der uns an Lifesize wirklich gefällt, ist, dass wir die Kontrolle über die Endpunkte haben, über welche unsere Videogespräche übertragen werden. Dass alle unsere Video-Gespräche von Lifesize verschlüsselt werden, gibt uns eine große Sicherheit: Wir würden Lifesize nicht nutzen, wenn diese Verschlüsselungsfunktion nicht im Produkt integriert wäre. Lifesize zeigte uns auch weitere Möglichkeiten zur Erhöhung unserer Sicherheit, etwa durch eine bessere Konfiguration unserer Firewalls für die Videokonferenzen."
>
> — Trevor Hicks, Director of Technology, Wetherby Asset Management

> „Die typischen Sicherheitsbedenken im Zusammenhang mit Telekonferenzen, z.B. Authentifizierung und Verschlüsselung, haben sich bei uns ganz schnell verflüchtigt, nachdem wir auf Lifesize Cloud umgestiegen sind. Unser Vertrauen ist besonders stark, weil wir bei diesem Dienst unser Meetingraum-Videosystem hinter unserer Firewall behalten konnten und das Traversal über die authentifizierten Server läuft. Lifesize vereinfachte und verbesserte die Art und Weise, wie wir mit Hunderten von Mitarbeitern in unseren entfernten AdRoll Standorten kommunizieren, in entscheidender Weise. Inzwischen können sogar unsere technisch weniger bewanderten Mitarbeiter Meetings ganz ohne die Unterstützung durch unser IT-Personal starten und durchführen."
>
> — Steve Latour, Director of IT AdRoll

FAZIT

In immer schnellerem Tempo entscheiden sich Unternehmen für die Cloud. Gemäß Frost & Sullivan Research nutzen inzwischen 50% der US-amerikanischen Unternehmen Public-Cloud-Dienste; das sind mehr als drei Mal so viele wie noch vor einem Jahr. Videokonferenzen, die früher meist komplexe und teure Lösungen voraussetzten, werden immer mehr zu einer unverzichtbaren Anwendung, die zusehends in die Cloud verlagert wird.

Wie bei allen technologischen Änderungen sollten Kunden vor der Einführung von Cloud-Videokonferenzdiensten alle Vorteile und Risiken sorgfältig abwägen. IT, ein Bereich, der sich die Vorteile der neuesten Technologien und Prozesse in der Cloud zunutze macht, erwartet zu Recht, dass Sicherheit standardmäßig in einen Cloud-Videokonferenzdienst eingebaut ist. Ein ganzheitlicher Sicherheitsansatz ist eine unverzichtbare Forderung bei der Entscheidung von Unternehmen, die Public-Cloud-Dienste wegen ihrer höheren Effizienz und aus Kostengründen in Betracht ziehen.

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw

Silicon Valley
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

London
4 Grosvenor Gardens
London SWIW 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan ist der globale Partner für Unternehmen, wenn es um Wachstum, Innovation und Marktführung geht. Die Dienstleistungen Growth Partnership Services und Growth Consulting helfen dem Kunden, innovative Wachstumsstrategien zu entwickeln, eine auf Wachstum ausgerichtete Kultur zu etablieren und entsprechende Strategien umzusetzen. Seit über 50 Jahren entwickeln wir Wachstumsstrategien für Global-1000-Unternehmen, aufstrebende Firmen, den öffentlichen Sektor sowie Kunden aus der Investmentbranche. Ist Ihr Unternehmen gerüstet für die nächste große Welle von Branchenkonvergenz, revolutionären Technologien, intensiverem Wettbewerb, Mega-Trends, bahnbrechenden Best Practices, veränderter Kundendynamik und neuen aufstrebenden Volkswirtschaften?

Für Informationen zu Genehmigungen wenden Sie sich an:

Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041