



# Sichere Collaboration

Neue Arbeitswelt bringt neue Gefahren

Unterstützt durch

**mimecast**<sup>™</sup>

# Inhalt

Vorwort .....	2
COVID und die Auswirkungen auf Collaboration .....	3
Der klare Gewinner: Microsoft Teams .....	4
Flexibel, effizient, ohne Ortsbindung .....	5
Privat, geschäftlich oder beides? .....	6
Kein Einsatz ohne Herausforderungen .....	7
Mit den richtigen Maßnahmen die Risiken minimieren .....	8
Fazit .....	10
Weitere Informationen .....	11

## Vorwort

Die Pandemie hat das Jahr 2020 und Teile des Jahres 2021 fest im Griff gehabt. Die Auswirkungen betrafen dabei nicht nur Privatpersonen, sondern auch Unternehmen. Zur Kontaktreduzierung mussten schnell neue Wege gefunden werden, um Mitarbeitern eine Arbeitsumgebung zu schaffen, mit der sie auch räumlich getrennt weiterhin zusammenarbeiten können. Remote Work wurde das Maß der Dinge. Doch der verstärkte Einsatz von Collaboration-Tools ist auch Cyberkriminellen nicht verborgen geblieben. Dieser neue Angriffsvektor stellt für Cyberkriminelle ein lukratives Ziel dar.

Doch wie ist die Verbreitung gängiger Collaboration-Tools in den Unternehmen? Welche Auswirkungen hatte die Pandemie auf die Collaboration? Welche Gefahren und Chancen birgt der Einsatz von Collaboration-Tools? Und was kann getan werden, um die Gefahren zu minimieren?

Um diese Fragen zu beantworten, wurden im Rahmen dieser Studie 201 Entscheider oder stark am Entscheidungsprozess beteiligte Personen zu ihren Collaboration-Tools, den Chancen, Risiken und Zukunftsaussichten von Remote Work befragt. An der Befragung im Mai 2021 nahmen 201 Mitarbeiter aus mittleren und großen Unternehmen aus verschiedenen Branchen teil.

### Copyright

Diese Studie wurde von der techconsult GmbH verfasst und von Mimecast unterstützt. Die darin enthaltenen Daten und Informationen wurden gewissenhaft und mit größtmöglicher Sorgfalt nach wissenschaftlichen Grundsätzen ermittelt. Für deren Vollständigkeit und Richtigkeit kann jedoch keine Garantie übernommen werden. Alle Rechte am Inhalt dieser Studie liegen bei der techconsult GmbH. Vervielfältigungen, auch auszugsweise, sind nur mit schriftlicher Genehmigung der techconsult GmbH gestattet.

### Disclaimer

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen etc. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften. In dieser Studie gemachte Referenzen zu irgendeinem spezifischen kommerziellen Produkt, Prozess oder Service durch Markennamen, Handelsmarken, Herstellerbezeichnung etc. bedeuten in keiner Weise eine Bevorzugung durch die techconsult GmbH.

# COVID und die Auswirkungen auf Collaboration

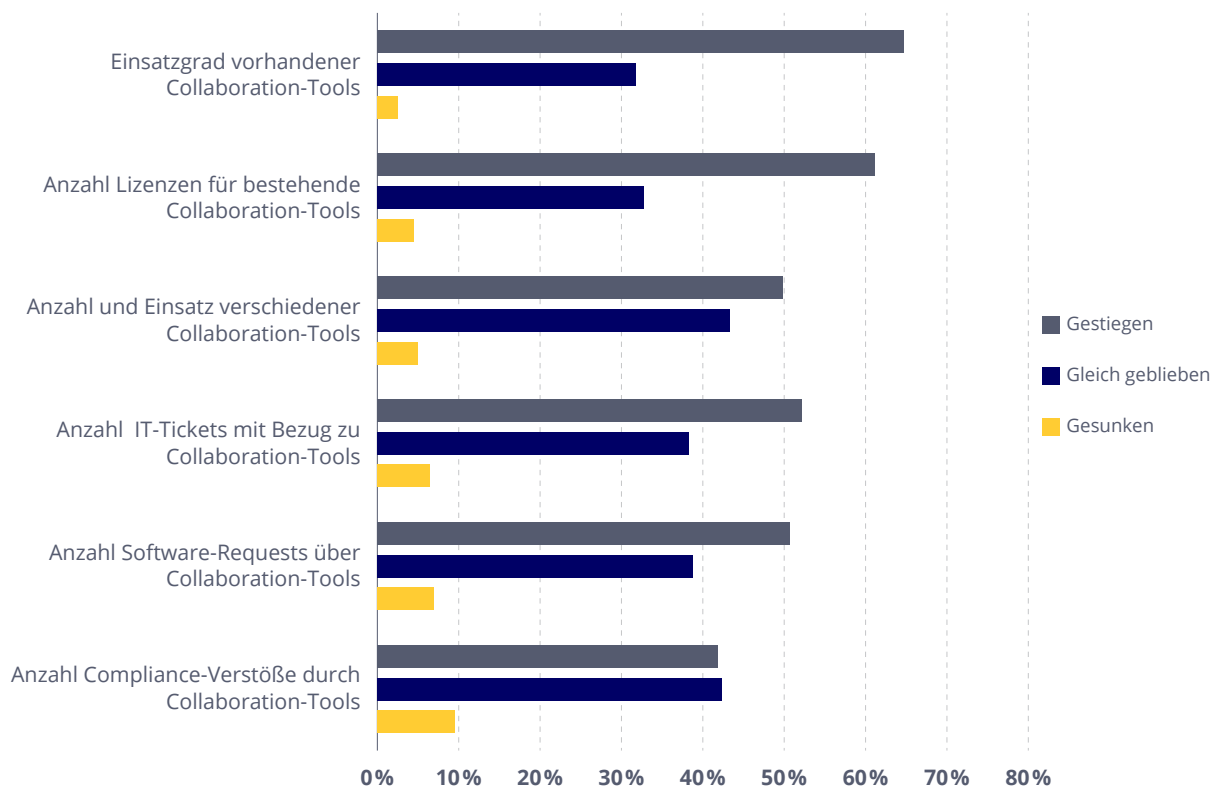
Das letzte Jahr stand global unter keinem guten Stern. Die COVID-19-Pandemie hatte die Welt fest im Griff. Nicht nur privat, sondern auch im Berufsfeld mussten Änderungen her, um der größten Krise seit Jahrzehnten zu begegnen. Für Unternehmen bedeutete dies, die Kontakte am Arbeitsplatz möglichst auf ein Minimum zu reduzieren. Um allerdings Menschen von zu Hause aus arbeiten zu lassen, bedarf es einer Infrastruktur, die für Remote Work geschaffen ist. Ein wichtiges Instrument stellen dabei Collaboration-Tools dar, mit denen Mitarbeiter ortsübergreifend nicht nur kommunizieren, sondern auch gemeinsam an Dokumenten arbeiten können.

Da ist es nicht verwunderlich, dass der Einsatzgrad von Collaboration-Tools nahezu explodiert ist. Allein in den vergangenen zwölf Monaten haben fast zwei Drittel der befragten Unternehmen einen spürbaren Anstieg des Einsatzes von Collaboration-Tools zu berichten gehabt. Knapp 60 Prozent der Unternehmen haben auch weitere Lizenzen für bestehende Collaboration-Tools erworben und die Hälfte der Unternehmen hat auch die Anzahl der verschiedenen eingesetzten Lösungen für Kollaboration erhöht.

Daraus lässt sich durchaus schließen, dass es ohne Collaboration-Tools nicht möglich gewesen wäre, in einer weltweiten Pandemie weiterhin effizient zu arbeiten. Und das haben die Unternehmen klar und deutlich erkannt.

Klarer Spitzenreiter in Sachen verstärkter Collaboration ist die Industrie. Dreiviertel aller befragten Industrieunternehmen gaben an, in den letzten zwölf Monaten mehr Lizenzen erworben zu haben und verstärkt mit Collaboration-Tools zu arbeiten. Das lässt darauf schließen, dass in klassischen Industrieunternehmen die Arbeit von zu Hause nur selten die Normalität war. Hier mussten innerhalb kürzester Zeit die Voraussetzungen geschaffen werden, um für die Mitarbeiter geeignete Home-Office-Arbeitsplätze bereitzustellen. Im Vergleich dazu: Nur vier von zehn Handelsunternehmen mussten im letzten Jahr neue Lizenzen erwerben. Hier waren Collaboration-Tools bereits vor der Pandemie verstärkt im Einsatz.

## Veränderungen während der Pandemie



Basis: 201 Unternehmen



## Der klare Gewinner: Microsoft Teams

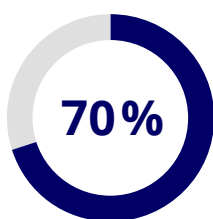
Natürlich gibt es eine Vielzahl von verschiedenen Collaboration-Tools, aus denen Unternehmen wählen können. Neben Jack-of-all-Trades-Lösungen wie Microsoft Teams gibt es auch Lösungen, die sich auf bestimmte Bereiche der Collaboration, wie das Filesharing oder die Videotelefonie spezialisieren.

Den mit Abstand größten Einsatzgrad über alle Branchen und alle Größenklassen hinweg erzielt Microsoft Teams. 70 Prozent der Unternehmen verwenden die allumfassende Collaboration-Lösung von Microsoft, um in ihrem Unternehmen effizient arbeiten zu können. Das kommt wenig überraschend: Denn Microsoft ist einer der weltweit führenden Anbieter von IT-Leistungen und damit in vielen Organisationen mit diversen Produkten bereits vertreten.

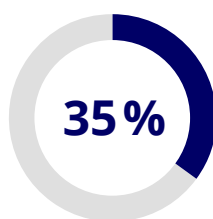
Auch das Zusammenspiel von Teams mit den gängigen Microsoft-Produkten wie Office 365 und das im Prinzip ganzheitliche Portfolio von Teams sorgen dafür, dass Teams die größte Verbreitung über sämtliche Branchen und Unternehmensgrößen aufweist. Gleichzeitig birgt die Spitzenreiterposition auch gewisse Gefahren. Denn Microsoft Teams wird durch den hohen Verbreitungsgrad ein sehr attraktives und lukratives Angriffsziel für Cyberkriminelle.

Dahinter rangiert Zoom, das in Zeiten der Pandemie einen regelrechten Lauf hatte. Die webbasierte Videoconferencing-Lösung war für viele Unternehmen zur richtigen Zeit am richtigen Ort. Ohne große Investitionen, sogar als Free-Variante, konnten Unternehmen ihre Meetings innerhalb kürzester Zeit ins Internet verlagern.

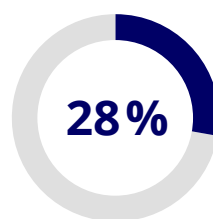
### Einsatzgrade gängiger Collaboration-Tools



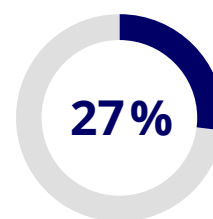
Microsoft Teams



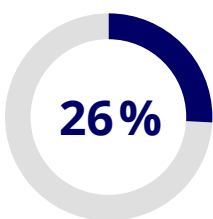
Zoom



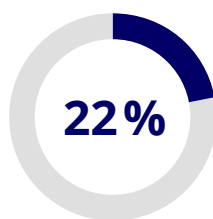
WhatsApp



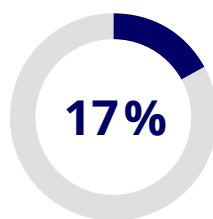
WebEx



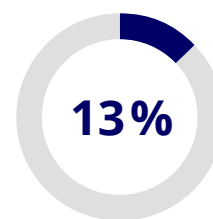
Skype for Business



OneDrive



GoToMeeting



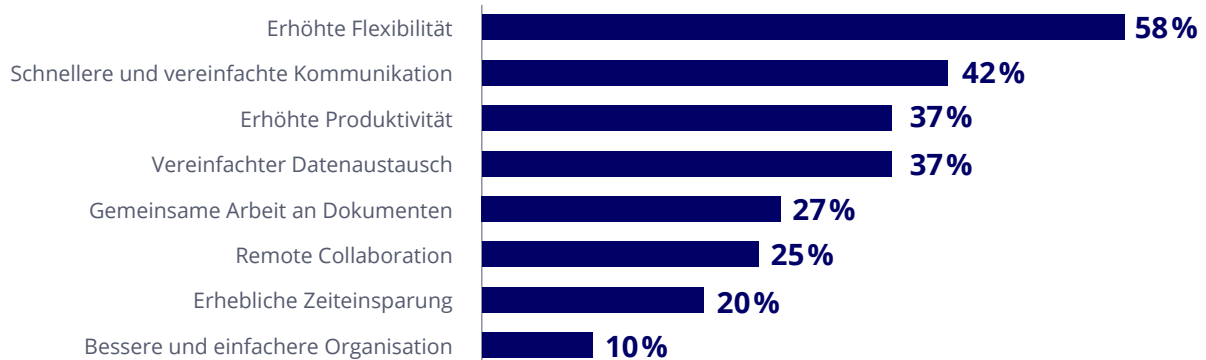
Slack

## Flexibel, effizient, ohne Ortsbindung

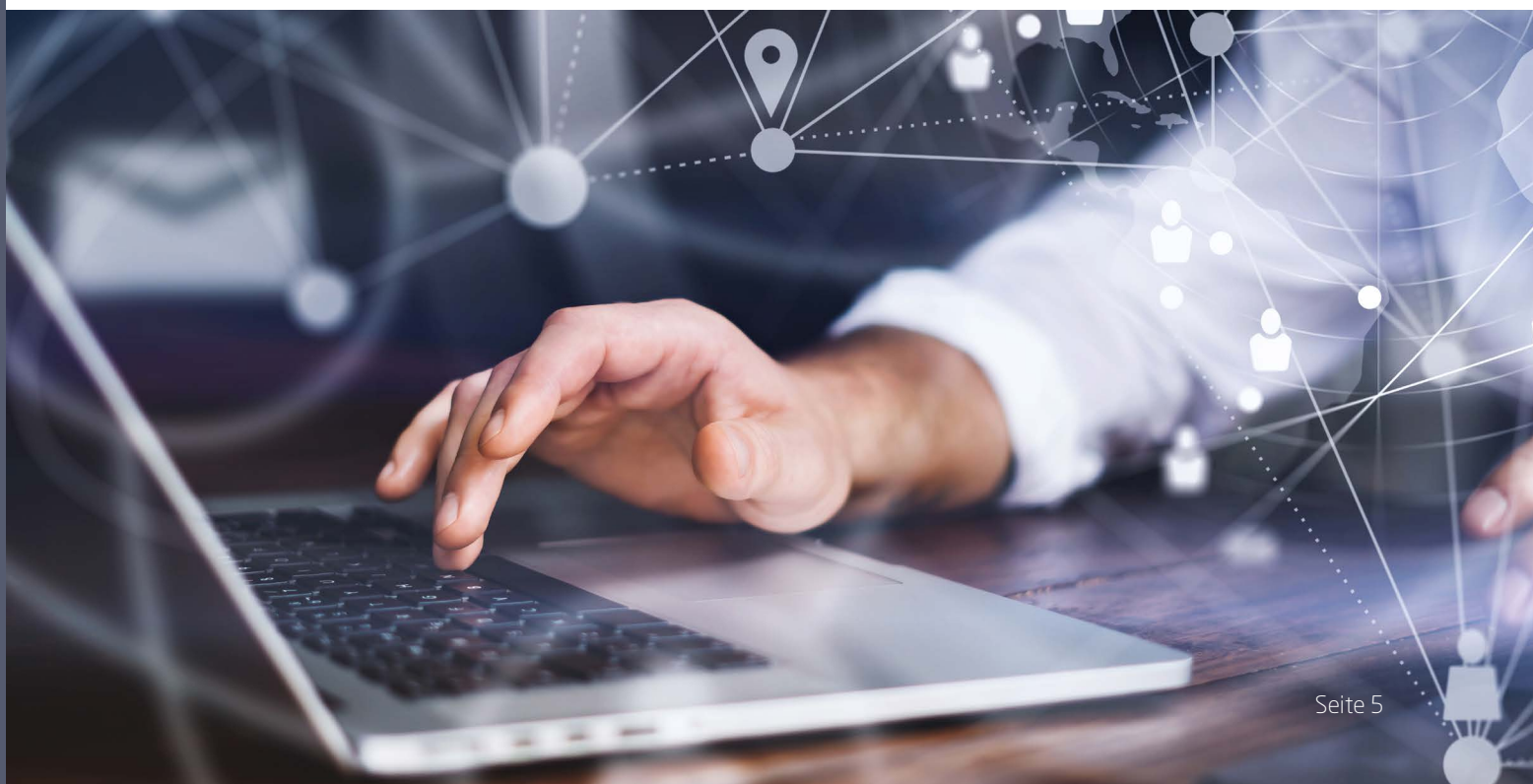
Die Veränderung in der Geschäftswelt macht Remote Arbeit und damit den Einsatz von performanten Collaboration-Lösungen unabdingbar. Aber Collaboration-Tools werden nicht nur eingesetzt, weil man muss, sie bringen zusätzliche Mehrwerte. Das bestätigen auch die befragten Unternehmen. Fast 60 Prozent der Unternehmen schätzen die durch den Einsatz von Collaboration-Tools gewonnene Flexibilität als besonders großen Vorteil ein. Diese Flexibilität führt dazu, dass weder der Ort noch die Uhrzeit oder der Tag eine Rolle spielen. Arbeit kann von überall, auch außerhalb der typischen Bürozeiten erledigt werden. Das lässt die Arbeit auch besser mit den persönlichen Lebensumständen verknüpfen. Kann man beispielsweise besser am Abend arbeiten, so arbeitet man einfach am Abend.

Mit einigem Abstand dahinter rangiert die beschleunigte und vereinfachte Kommunikation. Denn mit Collaboration-Software wird nicht nur mobiler Zugriff von jedem Ort ermöglicht: Mitarbeiter können beispielsweise über den kurzen Dienstweg über Projekte sprechen, ohne dass jeder Beteiligte sich im selben Büro aufhalten muss. Den geteilten dritten Rang nehmen der vereinfachte Datenaustausch sowie die erhöhte Produktivität ein. Dateien können „on the fly“ mit den Teammitgliedern geteilt werden oder auch Kommentare live eingesehen werden. Das spart lästiges Hin- und Herschieben von Dateien über E-Mails, was nicht selten mit langen Wartezeiten verbunden ist, bis die E-Mail beantwortet zurückgespielt wird.

### Vorteile von Collaboration-Tools



Basis: 201 Unternehmen | Mehrfachnennungen



## Privat, geschäftlich oder beides?

Natürlich lassen sich die Kommunikations- und Kollaborationslösungen nicht nur für betriebliches nutzen. Ein paar Katzenbilder hier, ein wenig Lästerei dort – was privat möglich ist, wird auch gerne mit den betrieblichen Collaboration-Tools gemacht. Doch die leichtsinnige Nutzung betrieblicher Collaboration-Tools für private Zwecke birgt Gefahren, die nicht zu vernachlässigen sind. Werden private Dateien, beispielsweise persönliche Fotos, über die Collaboration-Tools versandt, so können diese in Folge eines Angriffs durch Cyberkriminelle gestohlen und für kriminelle Zwecke missbraucht werden. Dasselbe gilt auch für das unverschlüsselte Teilen von sensiblen betrieblichen Dokumenten über Collaboration-Tools. Ohne die Möglichkeiten sensible Informationen im Büro zu besprechen, müssen große Mengen an sensiblen Informationen über die Collaboration-Kanäle ausgetauscht werden.

Glücklicherweise werden die Tools tatsächlich zu einem großen Teil betrieblich genutzt. Mehr als die Hälfte der Unternehmen gibt an, dass sowohl der Daten- und Informationsaustausch als auch die Kommunikation eher oder ausschließlich betrieblich sind.

Ein knappes Viertel gibt darüber hinaus an, dass sich private und betriebliche Aktivitäten die Waage halten. Bedenklich ist es beim restlichen Fünftel der Unternehmen, bei denen die Tools fast gar nicht für betriebliche Zwecke genutzt werden. In diesen Fällen wird man kaum noch von erhöhter Effizienz oder Produktivität profitieren. Die eingesetzten Collaboration-Tools sind dadurch nur Kostenfaktoren ohne Vorteile.

Bei größeren Unternehmen ist der Anteil an Mitarbeitern, die die Collaboration-Tools mehrheitlich für betriebliche Zwecke nutzen, auch deutlich höher, als dies bei kleineren Unternehmen bis 1.000 Mitarbeitern der Fall ist. In knapp zwei Drittel der größeren Unternehmen werden die Tools hauptsächlich geschäftlich genutzt, während es in kleineren Unternehmen circa 50 Prozent sind.

### Verwendungszwecke von Collaboration-Tools



#### Informations- und Datenaustausch



#### Kommunikation



## Kein Einsatz ohne Herausforderungen

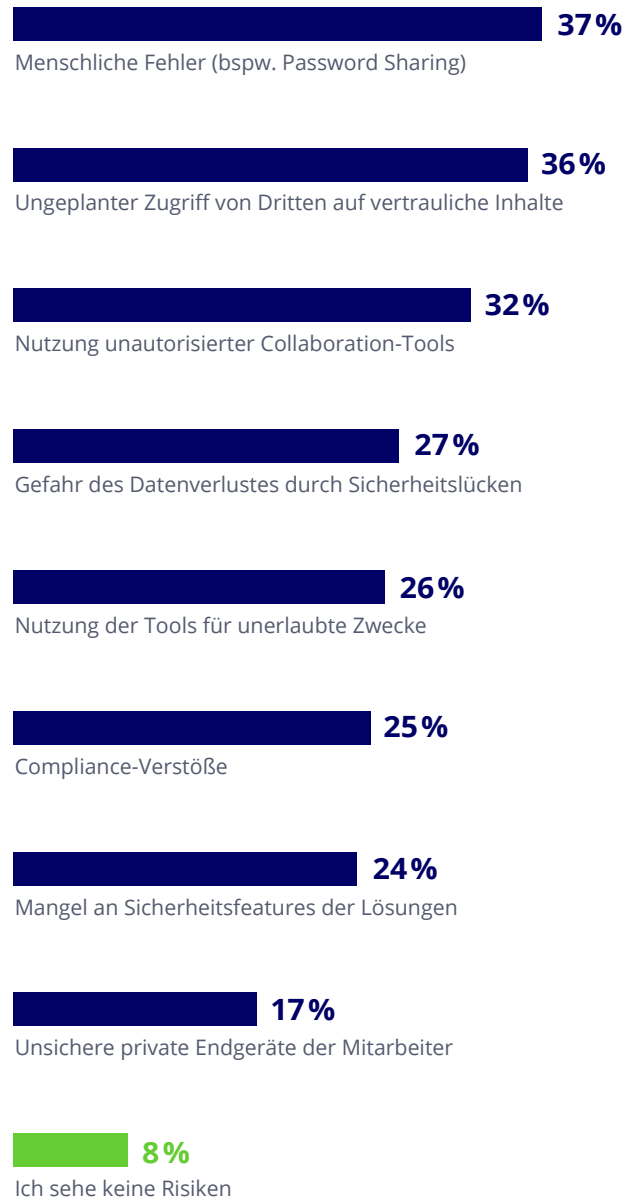
Der Einsatz von Collaboration-Tools birgt auch gewisse Risiken im Hinblick auf IT-Sicherheit. Schließlich sind diese Lösungen für einen Einsatz außerhalb der eigenen sicheren IT-Infrastruktur vorgesehen. Und außerhalb des Unternehmensnetzwerks fehlen oftmals die Sicherheitsmaßnahmen, wodurch menschliche Fehler nicht durch die Sicherheitsfunktionen abgedeckt werden können. Daher sehen auch 37 Prozent der Unternehmen in menschlichen Fehlern das größte Risiko im Einsatz von Collaboration-Tools. Diese menschlichen Fehler sind Dinge, die außerhalb jeglicher Sicherheitsmaßnahmen geschehen können. Beispiele dafür wären das Teilen von Passwörtern im Klartext mit Kollegen oder auch das Hereinfallen auf Phishingversuche. Die Bandbreite, an welchen Stellen Menschen Fehler in puncto IT-Sicherheit begehen können, ist groß.

Ebenfalls als hohes Risiko wird der ungeplante Zugriff von Dritten auf vertrauliche Inhalte eingeschätzt. Das kann da entstehen, wo externe Personen Zugänge zu den im Unternehmen eingesetzten Collaboration-Lösungen erhalten. Beispielsweise könnten für Projektpartner temporäre Zugänge zu einem bestimmten Projekt geschaffen werden. Wird an dieser Stelle aber geschlafen, kann es durchaus passieren, dass der Partner plötzlich Zugriff auf Dinge erhält, die er nicht sehen sollte.

An dritter Stelle folgt die Angst vor der sogenannten „Schatten-IT“. Diese entsteht meist dann, wenn Mitarbeiter in Fachabteilungen sich nach bestimmten Lösungen sehnen, diese jedoch nicht von der IT oder Geschäftsführung freigegeben oder implementiert werden. Und werden dann im Unternehmen solche Collaboration-Tools unautorisiert, „unter dem Radar“ der IT eingesetzt, birgt dies große Gefahren. Denn ausschließlich autorisierte Lösungen können mit allen Anforderungen, sei es Datenschutz, Compliance oder IT-Sicherheit konform gehen. Und nur, wenn die IT-Abteilung weiß, welche Lösungen im Einsatz sind, kann diese auch gezielt Sicherheitslücken schließen.

Die Spannbreite an Gefahren für das Unternehmen durch den Einsatz von Collaboration-Lösungen ist groß. Doch gibt es glücklicherweise verschiedene Maßnahmen, um diesen Herausforderungen zu begegnen.

### Herausforderungen beim Einsatz von Collaboration-Tools



Basis: 201 Unternehmen | Mehrfachnennungen

## Mit den richtigen Maßnahmen die Risiken minimieren

Um für einen sicheren Betrieb von Collaboration-Tools zu sorgen, können verschiedene Maßnahmen ergriffen werden. Wichtig dabei ist, ein Mittel allein sorgt nicht für einen sicheren Betrieb. Es ist eine Kombination von bestimmten Instrumenten, die einen gewissen Grundschutz liefern. Will man darüber hinaus gehen, kann man noch weitere ergänzende Methoden hinzuziehen.

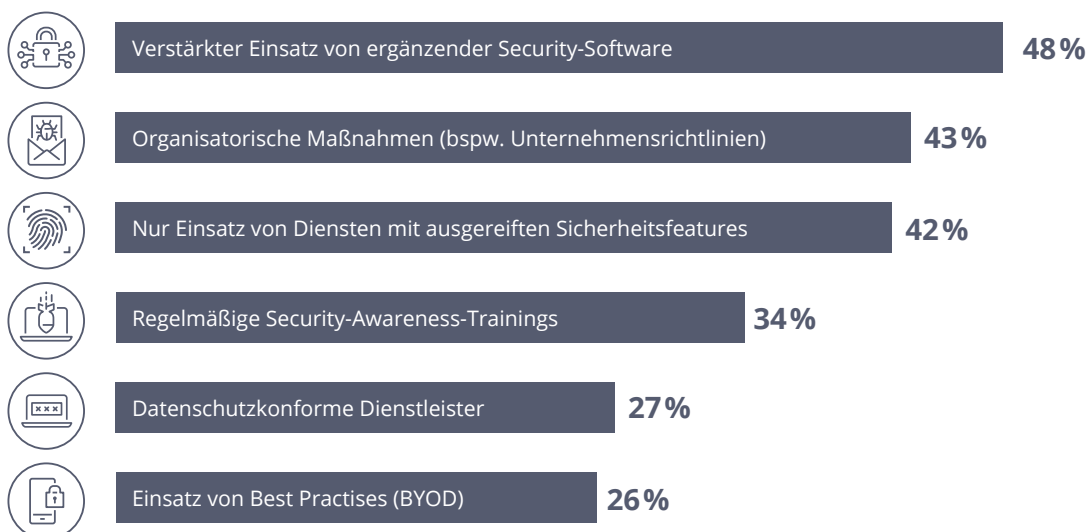
Von den Unternehmen wurde der verstärkte Einsatz von ergänzender Security-Software als wichtigste Maßnahme zum sicheren Betrieb von Collaboration-Tools identifiziert. Das können Lösungen für die Sicherheit des E-Mail-Verkehrs, des Endpunktschutzes, VPN-Tunnel oder auch spezielle Lösungen wie das Enterprise-Archiving für Collaboration-Tools sein. All jenes, das technologisch ist. Diese Maßnahmen lassen sich in der Regel am leichtesten implementieren, denn heutzutage können Security-Lösungen schnell und unkompliziert aus der Cloud bezogen werden, ohne größeren Aufwand für den Aufbau eigener Infrastruktur. So kann man bereits einen ersten Schutzwall errichten, der im Fall eines menschlichen Fehlers diesen ausbügeln kann.

Eine wichtige Stufe bei der Minimierung von Risiken ist für die Unternehmen die Schaffung von organisatorischen Maßnahmen um den Mitarbeitern schriftlich festgelegte Dos and Don'ts an die Hand zu geben.

Solche organisatorischen Maßnahmen können beispielsweise Unternehmensrichtlinien sein, wie die Collaboration-Tools eingesetzt werden dürfen oder wie man sich in Bezug auf seine Passwörter zu verhalten hat (sichere Passwörter, keine Weitergabe). Auch regelmäßige Security-Awareness-Trainings tragen einen großen Teil zur Sicherheit bei. Knapp ein Drittel der Unternehmen setzt diese Maßnahmen ein. Vergleichsweise oft werden Security-Awareness-Training in Unternehmen mit mehr als 5.000 Mitarbeitern eingesetzt. Das verwundert nicht: Denn je mehr Mitarbeiter ein Unternehmen hat, desto größer die Gefahr, dass menschliche Fehler im Bezug auf IT-Security auftreten, wie z.B. das Klicken schadhafter Links in Phishing Emails..

Ebenfalls hoch im Kurs steht der Einsatz von Diensten, die über ausgereifte Sicherheitsfeatures verfügen. Es gibt eine Reihe Tools, die Unternehmen einsetzen können, manche sogar für umsonst, manche zu premium Preisen. Man sollte beispielsweise niemals das Wählen, was am günstigsten ist oder was einem gerade im Mailpostfach von einem dubiosen Anbieter empfohlen wurde. Wichtig ist es, die verschiedenen Lösungen zu evaluieren und sich am Ende für die zu entscheiden, die alle gängigen Sicherheitsfeatures mitbringen, die man für seinen eigenen Betrieb benötigt. Nationale sowie internationale Zertifikate wie die ISO 27001-Zertifizierung oder ein Teletrust-Siegel sind gute Indikatoren dafür, dass man es mit einem seriösen Anbieter zu tun hat.

### Maßnahmen für sichere Collaboration





## Enterprise-Archiving - Ein Muss

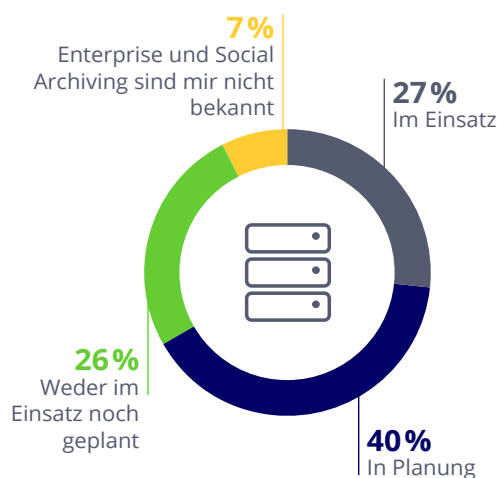
Da es ein immer größeres Datenwachstum gibt und die rechtlichen und regulatorischen Anforderungen immer komplexer werden, müssen Unternehmen für die digitale Archivierung von Dokumenten auf neue Ansätze bauen. Einer dieser Ansätze ist die Implementierung eines Enterprise-Archiving-Systems. Mit einem solchen Archivierungssystem können Unternehmen die Vielzahl an unterschiedlichen Unternehmensdaten aus unterschiedlichen Kanälen wie beispielsweise E-Mails, Dateien, Messaging-Daten, Inhalte aus sozialen Medien oder Share-Point-Daten verwalten und archivieren. Damit werden Unternehmen auch in die Lage versetzt, den von der DSGVO erforderten Compliance-Nachweis zum Schutz personenbezogener Daten zu liefern. Insbesondere wenn ein Unternehmen z.B. komplexen Regulierungen unterworfen ist, sollte die Archivierung sämtlicher Unternehmensdateien möglichst einfach und flexibel sein, um auch auf Veränderungen reagieren zu können. Aber auch für den Bereich e-Discovery, also dem Auffinden, Bearbeiten und Bereitstellen von Daten zur Unterstützung der Rechtsabteilung in Streitfragen, ist eine solche Lösung ein wichtiges und hilfreiches Instrument.

Derzeit verwendet nur ein Viertel der Unternehmen eine solche Lösung. Der Anteil der Unternehmen, die eine Archiving-Lösung verwenden, steigt mit der Unternehmensgröße an. Während nur 23 Prozent der Unternehmen bis 1.000 Mitarbeiter Archiving einsetzen, sind dies bei Unternehmen mit mehr als 5.000 Mitarbeitern sogar 39 Prozent.

## Remote-Arbeit bleibt auch in Zukunft

Der Ausblick für die Zukunft von Collaboration-Tools ist rosig. Mehr als die Hälfte der Unternehmen geht davon aus, dass der aktuelle Einsatzgrad von Lösungen zur digitalen Zusammenarbeit auch in Zukunft auf einem ähnlichen Niveau bleiben wird. Und weitere 37 Prozent gehen zudem noch einmal von einer weiteren Steigerung der Einsatzgrade aus. Nur die wenigsten Unternehmen glauben daran, dass es in Zukunft ein Absinken der Nachfrage nach Kollaborationslösungen geben wird. Das bedeutet, dass die Collaboration-Tools nicht nur eine temporäre Erscheinung sind, sondern dauerhaft bleiben. Und das bedeutet auch, dass die Sicherheitsvorkehrungen geschärft werden müssen. Cyberkriminelle haben als Folge der sich verändernden Geschäftswelt ihre Angriffsstrategien längst auf Cloud-Dienste und Remote-Mitarbeiter ausgerichtet. Und Collaboration-Tools sind da keine Ausnahme. Denn auch die Cyberkriminellen wissen um die Wichtigkeit von digitaler Zusammenarbeit und werden mit aller Macht versuchen, diesen Angriffsvektor auszunutzen. An der Absicherung der eigenen Kommunikations- und Kollaborationslösungen führt also kein Weg vorbei.

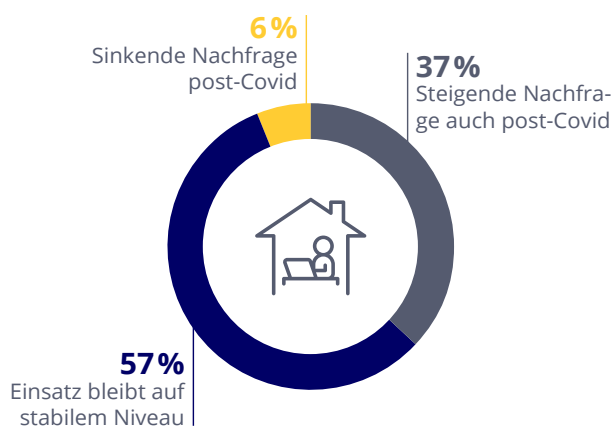
## Einsatzgrade von Enterprise Archiving



Basis: 201 Unternehmen

Doch bereits in Zukunft wird der Anteil insgesamt ansteigen. So planen rund 40 Prozent der Unternehmen zukünftig die Implementierung einer solchen Lösung. Damit würden in näherer Zukunft knapp drei Viertel der großen Unternehmen und knapp zwei Drittel der Unternehmen unter 5.000 Mitarbeitern eine Archiving-Lösung einsetzen.

## Erwartete Entwicklung von Collaboration-Tools



Basis: 201 Unternehmen

## Fazit

Collaboration-Tools sind in Unternehmen nicht mehr wegzudenken. Und sie werden auch weiterhin bestehen bleiben. Entweder auf dem jetzt herrschenden Niveau oder sie werden im Zuge des Ausbaus von Remote Work noch weiter ansteigen.

Weil dies der Fall ist, werden auch Cyberkriminelle nicht davor zurückschrecken, genau diese Lösungen zur Zusammenarbeit und ihre Nutzer gezielt anzugreifen. Denn die Tatsache, dass über Collaboration-Tools teilweise auch sehr persönliche Dateien oder hochsensible betriebliche Dateien versendet werden, macht Kollaborationslösungen zu einem attraktiven Angriffsziel.

Auch die stark zunehmenden Ransomware-Attacks, ausgelöst durch immer raffiniertere Phishing Emails werden vor solchen Online-Tools nicht halt machen. Da gilt es für Unternehmen, sich vor Datenverlust und Ausfallzeiten z.B. von Email-Systemen zu schützen.

Die sichere Verwendung von Collaboration-Tools kann auf unterschiedliche Weisen erfolgen, eine Kombination unterschiedlicher Maßnahmen ist dabei der beste Weg, um auch in Zukunft gegen Cyberangriffe auf die eigenen Collaboration-Tools gewappnet zu sein.

Unternehmen sollten sowohl die menschliche als auch die technische Seite in Angriff nehmen. Beispielsweise können regelmäßige Security-Awareness-Trainings Mitarbeiter in die Lage versetzen, die Gefahren ihres Handelns zu erkennen und bereits durch veränderte Handlungsweisen die Sicherheit zu verbessern. Ergänzend dazu sollte über den Einsatz entsprechender Sicherheitssoftware, die speziell für Collaboration angewandt wird, wie Enterprise-Archiving nachgedacht werden.

Kurz und knapp gesagt: Remote Work und Collaboration gelingen nur, wenn diese auch sicher sind. Daher sollte die Sicherheit beim Einsatz von Collaboration-Tools ganz oben auf der Liste der IT-Verantwortlichen stehen.



## Weitere Informationen

### Impressum

techconsult GmbH  
Baunsbergstraße 37  
34131 Kassel

E-Mail: [info@techconsult.de](mailto:info@techconsult.de)  
Tel.: +49-561-8109-0  
Fax: +49-561-8109-101  
Web: [www.techconsult.de](http://www.techconsult.de)

### Kontakt

Raphael Napieralski  
Analyst  
techconsult GmbH  
Baunsbergstr. 37  
D-34131 Kassel

E-Mail: [raphael.napieralski@techconsult.de](mailto:raphael.napieralski@techconsult.de)  
Tel.: +49-561-8109-0

(Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.)

## Über techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

## Über Mimecast

Mimecast (NASDAQ: MIME) entstand 2003 mit dem Fokus Unternehmen vor Cyber-Bedrohungen zu schützen. Dabei stehen unsere zehntausende Kunden täglich im Mittelpunkt und wir geben niemals auf Sicherheitsrisiken gemeinsam zu bewältigen. Unser skalierbarer Entwicklungsansatz schützt den Hauptangriffspunkt für Cyberattacken – E-Mail. Wir investieren kontinuierlich, um Markenschutz, Security Awareness Training, Web Security, Compliance und andere wichtige Funktionalitäten zu integrieren. Mimecast hilft, große und kleine Unternehmen vor bösartigen Angriffen sowie menschlichem und technischem Versagen zu schützen. Darin ist Mimecast führend und trägt so dazu bei, eine widerstandsfähige Welt zu schaffen.

Weitere Informationen finden Sie hier: [www.mimecast.com/de/](http://www.mimecast.com/de/).