techconsult
TECHNOLOGY MARKET ANALYSTS

DER GLOBALE EINSATZ VON KOLLABORATIONSLÖSUNGEN IN HYBRIDEN ARBEITSWELTEN

Wie Unternehmen mit Sicherheitsrisiken umgehen

Im Auftrag von

HORNETSECURITY

Informationen zur Studie

Erstellung durch

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: info@techconsult.de
Tel.: +49 561 8109 0
Fax: +49 561 8109 101
Web: www.techconsult.de

Erscheinungsdatum

10/2022

Autor

Ercan Hayvali

In Zusammenarbeit mit

HORNETSECURITY

Kontakt

Hornetsecurity GmbH
Am Listholze 78
30177 Hannover

E-Mail: info@hornetsecurity.com
Tel.: +49 511 515 464 0

Mehr erfahren

Sonstige Informationen

Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhaltsverzeichnis

Einleitung

Durch die Etablierung hybrider Arbeitsplatzkonzepte in den vergangenen Jahren wurden auch Kommunikations- und Kollaborationslösungen immer stärker in betriebliche Prozesse eingebunden. Für viele zählen Kollaborationslösungen wie Microsoft Teams deshalb zu den wichtigen Instrumenten zur Erledigung operativer Tätigkeiten. Durch den dadurch ermöglichten internen Austausch können Beschäftigte in Gruppen Projekte bearbeiten und Nachrichten und Dokumente austauschen. Dabei werden immer häufiger geschäftskritische und sensible Inhalte über Kollaborationslösungen geteilt. Somit müssen IT-Verantwortliche nicht nur den Schutz der IT-Infrastruktur und des Unternehmensnetzwerkes gewährleisten, sondern auch die Erreichbarkeit der Inhalte von Kollaborationslösungen sicherstellen.

Die Kommunikation in den Kollaborationslösungen findet jedoch häufig in einigen wenigen Kanälen statt. Trotz der Möglichkeit der Nutzung von privaten und öffentlichen Kanälen oder Gruppen neigen Beschäftigte dazu, den Großteil der Kommunikation über Direktnachrichten durchzuführen. Nicht selten werden hochsensible, private oder geheime Dateien und Informationen versendet. Dazu gehören auch IT-relevante Details und Passwörter. Zudem nutzen 75 Prozent der Beschäftigten die betrieblichen Kollaborationslösungen auch auf ihren privaten Endgeräten wie Smartphones oder Tablets. Diese Verschmelzung von privat und geschäftlich sowie die Verschiebung persönlicher Unterhaltungen in die digitale Welt stellt auf Dauer nicht nur die Beschäftigten, sondern auch die IT-Abteilungen vor große Herausforderungen.

Wie setzen Beschäftigte die Kollaborationslösungen im Detail ein und welche Inhalte werden besonders häufig geteilt? Welchen Einfluss hat die Schatten-IT auf die Security im Unternehmen und wie können die IT-Verantwortlichen damit umgehen? Welche Risiken und Herausforderungen ergeben sich durch derartige Lösungen und wie sehen dahingehend zukünftige Trends aus? Diese und weitere Fragen werde im Rahmen dieser umfassenden Studie untersucht und im Detail vorgestellt. Als Datenbasis dient eine international durchgeführte Befragung mit 540 IT-Verantwortlichen und Nutzern von Kollaborationslösungen aus Unternehmen mit mindestens 50 Mitarbeitern.

Hybrid Work als Arbeitsplatzmodell der Zukunft

Nicht zuletzt durch die Corona-Pandemie wurden Unternehmen und Mitarbeiter vor große Herausforderungen gestellt. Innerhalb kürzester Zeit haben sich Arbeitsplätze, Workflows und Kommunikationsgewohnheiten geändert und sich an die Gegebenheiten angepasst. Doch auch einige Jahre nach Pandemiebeginn wurden die als vorübergehend eingerichteten Änderungen zur Normalität. Dieser Wandel zeigt sich auch in der aktuellen Gestaltung der Arbeitsplätze.

So arbeiten rund 46 Prozent der Befragten im Rahmen eines hybriden Arbeitsplatzmodells nicht nur im Büro, sondern auch im Homeoffice. Dieses neuere Modell findet tendenziell in größeren Unternehmen häufiger Anwendung. So arbeitet lediglich ein Viertel (25 Prozent) der Befragten aus Unternehmen mit 50 bis 99 Mitarbeitern sowohl zuhause als auch im Office, wohingegen der Anteil bei Unternehmen mit 5.000 und mehr Mitarbeitern bei rund 58 Prozent liegt.

Darüber hinaus arbeiten rund 40 Prozent der Befragten vollständig im Büro oder sind wieder in das Präsenzbüromodell zurückgekehrt. Auch hier lassen sich größenklassenspezifische Unterschiede feststellen.

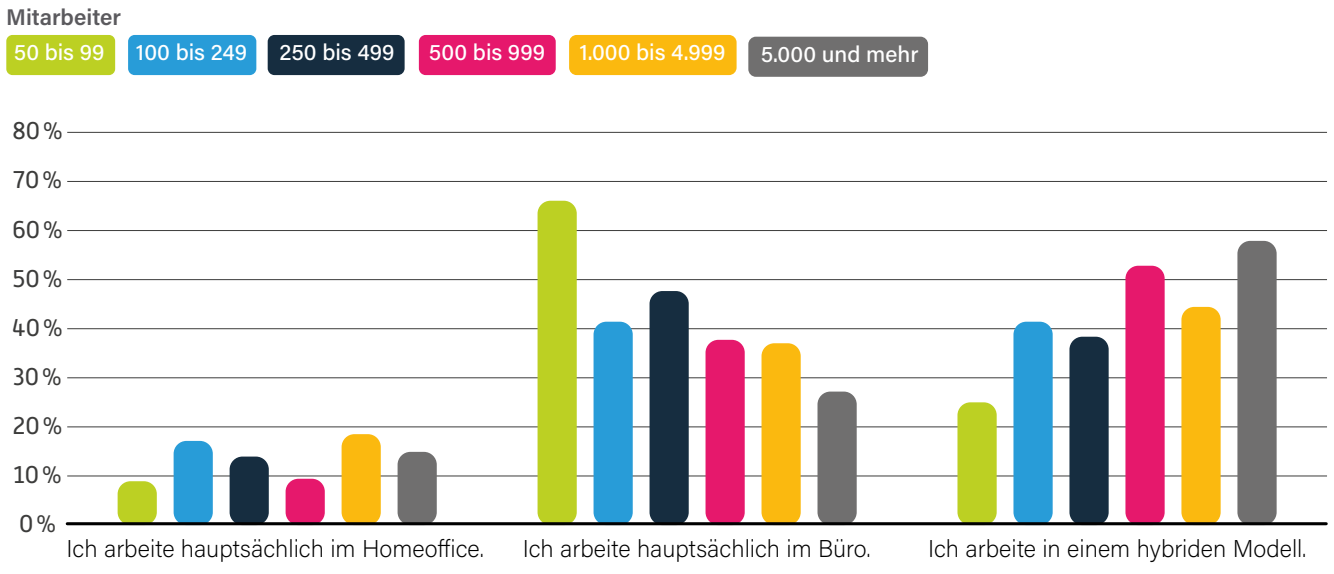
Zwei Drittel (66 Prozent) der Befragten in kleineren Unternehmen mit 50 bis 99 Mitarbeitern arbeiten vollständig im Büro, wohingegen der Anteil in Großunternehmen mit 5.000 und mehr Mitarbeitern bei nur 27 Prozent liegt. Insgesamt arbeiten somit lediglich 14 Prozent dauerhaft im Homeoffice.

Doch mit der neuen Arbeitsplatzkultur geht auch eine Änderung in der Art der Kommunikation einher. Galt noch vor Corona der direkte Austausch oder E-Mail-Verkehr als übliche Kommunikationskanäle, so sind es mittlerweile die Kollaborationslösungen wie Microsoft Teams, auf denen der Großteil des Informationsaustauschs abläuft. Mitarbeiter nutzen derartige Kollaborationslösungen somit nicht nur für den Datenaustausch, sondern auch zur täglichen kollegialen oder auch privaten Kommunikation.

Lediglich 14 Prozent der Befragten arbeiten vollständig im Homeoffice und 46 Prozent im Hybridmodell.

Aktuelles Arbeitsplatzmodell

Basis: 540 Unternehmen



Kollaborationslösungen als wichtiger Kommunikationskanal

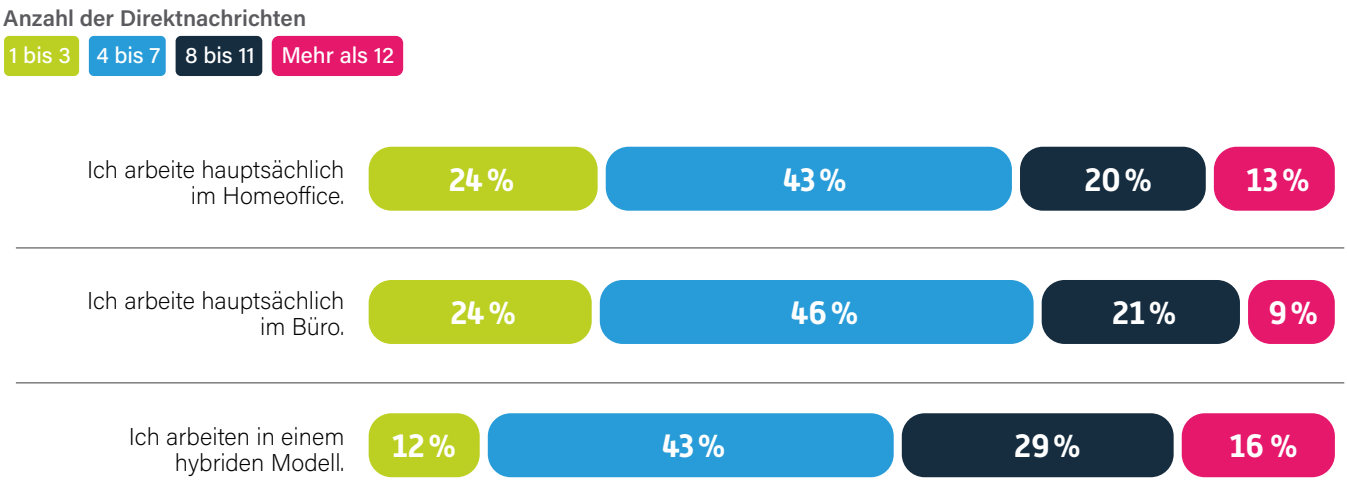
Der Wandel der Arbeitswelten zeigt sich nicht nur an den Orten, an denen gearbeitet wird, sondern auch am Miteinander der Beschäftigten. Wurde noch vor der Pandemie im Büro an der Kaffeemaschine oder beim gemeinsamen Mittagessen über private oder geschäftliche Themen gesprochen, hat sich diese Kommunikationskultur nun fast vollständig verschoben. Unterhaltungen oder kurze Absprachen werden nun überwiegend digital über beispielsweise Microsoft Teams durchgeführt und Besprechungen über Videomeetings abgehalten. Für Beschäftigte spielen Kollaborationslösungen somit eine große Rolle, um den Austausch von Informationen mit den Kollegen aufrechtzuerhalten. So geben rund 44 Prozent der Befragten an, an regulären Arbeitstagen mit vier bis sieben Personen über Microsoft Teams zu kommunizieren und fast ein Viertel (24 Prozent) haben sogar Kontakt mit acht bis elf Personen. Je nach Unternehmensgröße, Abteilung und Land kann sich die Anzahl natürlich unterscheiden. So wird insbesondere in Großunternehmen mit 5.000 und mehr Beschäftigten besonders häufig miteinander kommuniziert. Hier haben rund 45 Prozent täglich mit mindestens acht Personen Kontakt via Teams-Direktnachrichten, wohingegen der Anteil bei kleineren Unternehmen mit 50 bis 99 Mitarbeitern bei nur 21 Prozent liegt.

Durch Kollaborationslösungen auf privaten Endgeräten werden tendenziell mehr Nachrichten ausgetauscht

Jedoch hat auch das Arbeitsplatzmodell einen maßgeblichen Einfluss auf die Nutzung von Teams als Mittel zur direkten Kommunikation. Überraschenderweise tauschen Beschäftigte im Homeoffice tendenziell weniger Direktnachrichten mit Kollegen aus als Beschäftigte im Präsenzbüro oder im hybriden Arbeitsplatzmodell. Dies könnte insbesondere daran liegen, dass sich die Wege von Beschäftigten im Präsenzbüro häufiger kreuzen, man sich direkt austauscht und die Unterhaltungen auch digital fortsetzt, wohingegen der initiale Kontakt zu Kollegen aus dem Homeoffice seltener stattfindet. So schreiben rund 30 Prozent der Beschäftigten im Homeoffice und jeder Dritte (33 Prozent) im Präsenzbüro täglich mit mindestens 8 Kollegen, wohingegen der Anteil bei hybrid arbeitenden Beschäftigten bei 45 Prozent liegt.

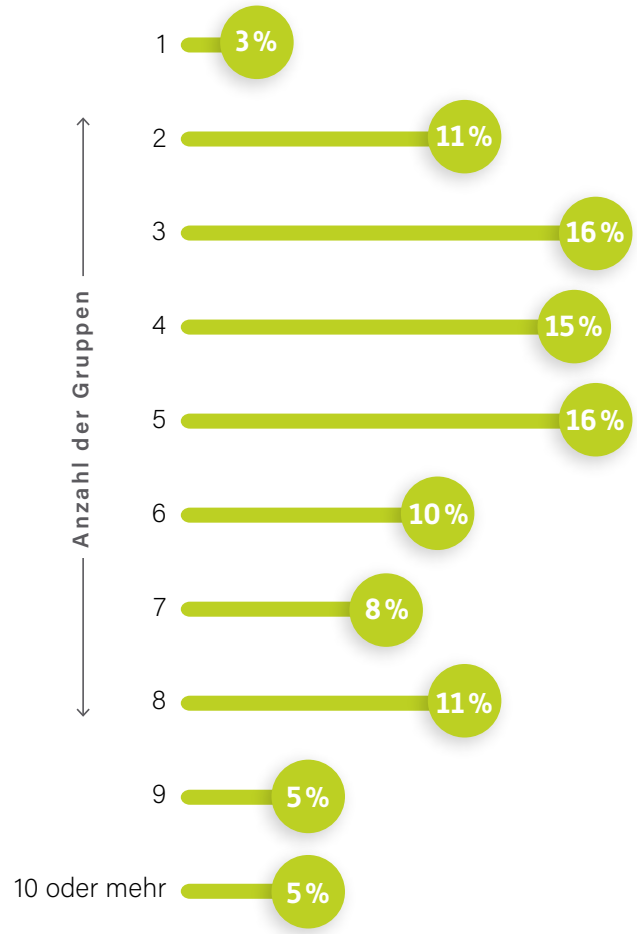
Anzahl der Direktchats an durchschnittlichen Arbeitstagen

Basis: 540 Unternehmen



Aktivität in Gruppen an durchschnittlichen Arbeitstagen

Basis: 540 Unternehmen



Der Nachrichtenaustausch zwischen Kollegen wird jedoch auch durch den Einsatz von privaten Endgeräten beeinflusst. So können Mitarbeiter auch auf privaten Geräten die Kollaborationslösung Microsoft Teams einrichten und so jederzeit Nachrichten empfangen und versenden. Rund drei Viertel (74 Prozent) der Befragten, die Teams nicht auf ihren privaten Endgeräten installiert haben, haben Nachrichtenkontakt mit vier oder mehr Kollegen. Dahingegen tauschen sich 84 Prozent der Befragten, die Teams auf privaten Endgeräten nutzen, mit mindestens vier oder mehr Kollegen täglich Nachrichten aus. Hier wird deutlich, dass private Endgeräte dazu beitragen können, die interne Kommunikation zu erhöhen. Jedoch könnte der Einsatz privater Endgeräte auch zu Security-Risiken führen. Denn privat genutzte und ungeschützte Endgeräte können sich mit Schadsoftware infizieren und diese über die Kollaborationssoftware auf das Unternehmensnetzwerk verteilen. Hier müssen IT-Abteilungen das Risiko durch sogenannte Schatten-IT verhindern und Backups der Daten, Nachrichten und Inhalte der Kollaborationslösungen durchführen.

Die Zusammenarbeit mittels Kollaborationslösungen kann auch in Gruppen erfolgen, in denen sich mehrere Mitarbeiter aufhalten und über Workflows, Projekte oder andere Themen austauschen können.

Durch die virtuelle Zusammenarbeit in Gruppen kann eine effiziente und produktive Kommunikation ermöglicht und die Qualität der Ergebnisse erhöht werden. Fast ein Drittel (31 Prozent) der Befragten ist an durchschnittlichen Arbeitstagen in bis zu drei Gruppen aktiv und 71 Prozent in bis zu sechs Gruppen. Trotz der größenklassen- und branchenspezifischen Unterschiede lässt sich durch die Streuung der Ergebnisse eine stets unternehmensspezifische Nutzung der Gruppenaktivitäten feststellen.

Wie bei den Direktnachrichten lässt sich auch bei der Intensität der Gruppennutzung ein Einfluss der privaten Endgeräte feststellen. So sind drei Viertel (75 Prozent) der Beschäftigten, die Teams auf privaten Endgeräten nutzen, in drei und mehr Gruppen aktiv. Dagegen ist nur mehr als jeder zweite Befragte (53 Prozent) ohne Microsoft Teams auf dem privaten Endgerät in mehr als drei Gruppen aktiv. Somit kann auch hier der Einsatz privater Endgeräte zu einer intensiveren Nutzung und Zusammenarbeit in Gruppen führen. Damit einhergehend müssen IT-Abteilungen auch dafür Sorge tragen, die Inhalte, Dateien und Chats innerhalb der Gruppen zu sichern und gegen möglichen Datenverlust zu schützen.

Direktnachrichten als bevorzugte Kommunikationsmethode

Durch die Verschiebung der operativen Tätigkeiten in die digitale Umgebung hat sich auch das Kommunikationsverhalten der Beschäftigten deutlich geändert. Dabei bietet Microsoft Teams als verbreitete Kollaborationslösung eine Vielzahl von möglichen Formen der Zusammenarbeit. So können Beschäftigte sich via Direktnachrichten kontaktieren, Dateien und Inhalte austauschen oder direkte Telefonate starten. Zudem können Kanäle für spezifische Projekte und Workflows erstellt werden, die entweder nur für eine eingeschränkte Nutzergruppe zugänglich sind oder als offener Kanal allen Beschäftigen offen steht. In diesen Kanälen lassen sich Dateien teilen, Inhalte und Meetings erstellen oder auch projektspezifische Nachrichten austauschen.

Insgesamt zeigt sich jedoch, dass Beschäftigte zur direkten Chatkommunikation neigen und diese den anderen Kanälen vorziehen. So stimmen 70 Prozent der Befragten der Aussage zu, dass sie mehr Direktnachrichten mit den Kollegen austauschen als Gruppennachrichten. Der bilaterale Nachrichtenaustausch gehört somit zu den verbreitetsten und meistgenutzten Kommunikationsformen der Kollaborationslösung Teams. Dies lässt sich über alle Unternehmensgrößenklassen hinweg auf ähnlich hohem Niveau beobachten.

Auch in projektbezogenen Gruppen haben die Beschäftigten die Möglichkeit des Austausches. Doch auch hier bevorzugen die Befragten mehrheitlich die bilaterale Direktkommunikation via Chatnachrichten. So stimmen 61 Prozent der Befragten der Aussage zu, dass sie trotz Gruppen eher Direktnachrichten bevorzugen, um mit Kollegen zu schreiben. Somit wird nicht nur per Direktnachrichten kommuniziert, wenn die Themen ausschließlich die kommunizierenden Personen betreffen, sondern auch bei Themen mit direktem Projektbezug mit anderen Beteiligten. Dies ist insbesondere in größeren Unternehmen ausgeprägt. So bevorzugen mehr als zwei Drittel (67 Prozent) der Beschäftigten aus Unternehmen mit 5.000 und mehr Mitarbeitern Direktnachrichten anstelle von Gruppennachrichten, wohingegen der Anteil in Kleinunternehmen mit 50 bis 99 bei lediglich 57 Prozent liegt.

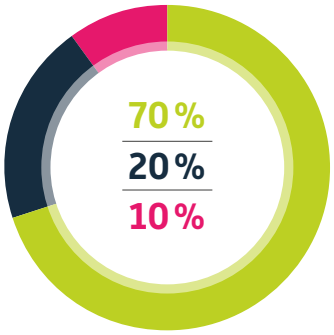
Darüber hinaus werden Direktnachrichten über Kollaborationslösungen wie Microsoft Teams auch für privaten Austausch genutzt. So führen der verbreitete hybride Ansatz und das Homeoffice dazu, dass Beschäftigte weiterhin Kontakt zu Kollegen halten und diesen über Teams pflegen. Dabei können dann auch nicht nur private Nachrichten, sondern auch private Dokumente, Dateien oder Bilder ausgetauscht werden. Rund 62 Prozent der Befragten geben an, dass sie Teams-Direktnachrichten auch für private Unterhaltungen nutzen. Dies lässt sich über alle Größenklassen hinweg beobachten, steigt jedoch mit der Unternehmensgröße an.

70 Prozent der Beschäftigten bevorzugen Direktnachrichten zur unternehmensinternen Kommunikation.

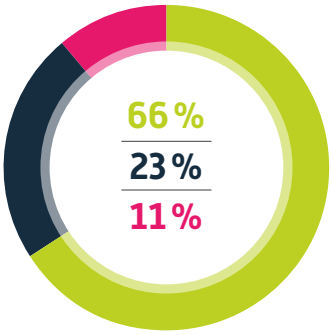
Nutzung von Kollaborationslösungen

Basis: 540 Unternehmen

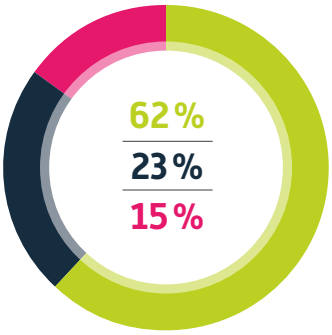
Stimme eher zu | Teils teils | Stimme eher nicht zu



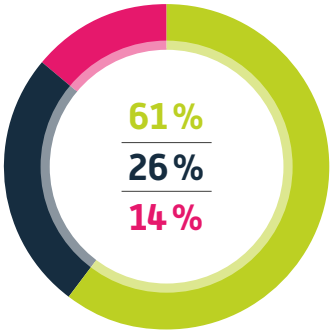
Ich sende viel mehr Direktnachrichten als Gruppennachrichten.



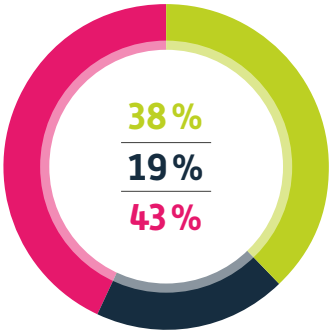
Ich sende viel mehr Direktnachrichten als Kanalnachrichten.



Ich verwende Direktnachrichten auch für private Unterhaltungen.



Trotz Gruppen bevorzuge ich Direktnachrichten, um mit Kollegen zu schreiben.



Ich sende auch geschäftskritische und interne Dokumente und Nachrichten an öffentliche Gruppen.

62 Prozent der Beschäftigten verwenden Direktnachrichten für private Unterhaltungen.

Es lässt sich zudem beobachten, dass die Nutzung von Teams auf privaten Endgeräten zu einem höheren Direktnachrichtenaufkommen durch privaten Austausch führt. So liegt der Anteil bei Beschäftigten mit Teams auf privaten Endgeräten bei 64 Prozent, wohingegen nur 58 Prozent der Beschäftigten ohne Teams auf den privaten Geräten private Nachrichten mit Kollegen austauschen. Dies birgt insbesondere dann unternehmensrelevante Security-Risiken, wenn die privaten Inhalte ungeprüft verteilt werden, ggf. Schadsoftware an Mitarbeiter verschickt wird, die dann eine Gefahr für das Unternehmensnetzwerk darstellen.

Deswegen sollten auch hier die IT-Verantwortlichen dafür sorgen, dass sämtliche Kollaborationsschnittpunkte durch Security-Lösungen überwacht und sämtliche Inhalte auch durch Backups gegen Verlust geschützt sind.

Bei der Nutzung von Gruppen und Kanälen auf Kollaborationsplattformen lässt sich erkennen, dass diese nicht so häufig eingesetzt werden wie Direktnachrichten. Insbesondere bei Kanälen, die zur Koordination und Bearbeitung von Projekten genutzt werden, lässt sich diese Tendenz erkennen. So geben mehr als zwei Drittel (67 Prozent) der Befragten an, eher Direktnachrichten als Kanalnachrichten zu versenden. Ähnlich wie bei der Nutzung von Gruppen neigen die Beschäftigten dazu, eher direkten Kontakt zu Kollegen via Direktchats zu suchen, um Informationen oder Inhalte auszutauschen.

Backups von Kollaborationslösungen erfolgskritisch

Für viele Unternehmen haben sich Kollaborationslösungen von einer Möglichkeit der ortsunabhängigen Arbeit hin zu einer Plattform für Projektmanagement und Zusammenarbeit entwickelt. Dabei werden nicht nur geschäftliche und private Nachrichten ausgetauscht, sondern auch Daten für die operative Arbeit sowie geschäftskritische Dateien versendet. So teilen 39 Prozent der Befragten geschäftskritische und interne Dokumente und Nachrichten nicht nur über Direktnachrichten, sondern auch über öffentliche Gruppen. Nutzen die Mitarbeiter Teams über private Endgeräte, so versenden sie eher kritische Dokumente über öffentliche Gruppen (43 Prozent) als jene, die Teams rein über die bereitgestellten Arbeitsmittel einsetzen (22 Prozent).

Bei den versendeten Nachrichten lassen sich neben den privaten Inhalten hauptsächlich operativ geschäftliche, interne und geschäftskritische Daten und Nachrichten unterscheiden. Dabei zeigt sich, dass die Beschäftigten Teams überwiegend zum Teilen von internen und geschäftskritischen Daten nutzen.

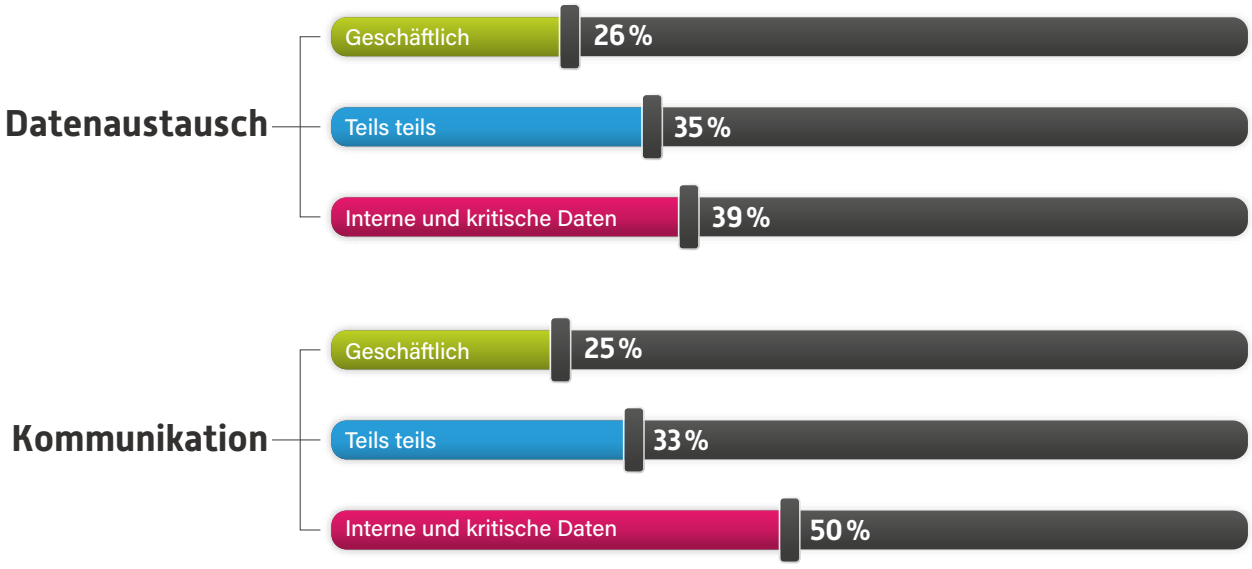
So versenden 39 Prozent der Befragten hauptsächlich geschäftskritische Dateien und jeder Zweite interne und geschäftskritische Nachrichten über die Kollaborationslösung Teams. Nur jeder vierte Befragte (25 Prozent) nutzt Teams zum Austausch von geschäftlichen Nachrichten und 27 Prozent zum Teilen von geschäftlichen Dateien.

Beschäftigte nutzen Teams auch als Speichermedium für geschäftskritische Nachrichten und Dateien, weshalb von allen Inhalten Sicherheitskopien erstellt werden sollten.

In Anbetracht dieser sensiblen Daten müssen IT-Verantwortliche besonders auf die Securitymaßnahmen innerhalb der Teams-Lösung und des Unternehmensnetzwerks achten. Denn immer wieder tauchen Sicherheitslücken auf, durch die sich Angreifer nicht nur Zugriff auf die gesamten Microsoft-Dienste verschaffen können, sondern auch auf geteilten geschäftskritischen und internen Nachrichten und Dokumente.

Hauptsächliche Nutzung von Kollaborationslösungen

Basis: 540 Unternehmen



Zudem erlauben derartige Sicherheitslücken den Angreifern das Löschen gesamter Chats, Dokumente und andere gespeicherter Dateien. Nutzen Unternehmen die „Teams", Kanäle und Gruppen innerhalb der Lösung als Speichermedium für unternehmens- oder projektrelevante Inhalte, so kann die Löschung der gespeicherten Inhalte zu großen Schäden innerhalb des Unternehmens führen. Aus diesem Grund gilt auch hier der Grundsatz des Backups. IT-Verantwortliche müssen stets dafür sorgen, dass jede Kommunikation und jeder Inhalt innerhalb der Kollaborationslösung gespeichert wird und wiederhergestellt werden kann.

75 Prozent der Befragten nutzen Microsoft Teams auch auf ihren privaten Endgeräten wie Smartphones oder Tablets.

Neben diesen externen Bedrohungen schützen Sicherheitskopien auch vor potenziellen internen Gefahren. Denn versehentliche oder vorsätzliche Löschvorgänge werden schnell im gesamten Netzwerk übernommen, wodurch kritische Daten verloren gehen oder auch vollständig vernichtet werden können. Die Ergebnisse zeigen deutlich, dass derartige Löschungen keine Seltenheit sind. So bestätigen 42 Prozent der Befragten, dass ihre IT-Verantwortlichen bereits Teams-Daten durch Backups wiederherstellen mussten. Dabei könnten genutzte private Endgeräte einen Einfluss auf die Gefährdung der Daten haben. Denn fast jeder zweite Befragte (47 Prozent) mit Teams auf dem privaten Endgerät hat bereits Erfahrung mit der Datenwiederherstellung von Teams gemacht, wohingegen der Anteil bei Befragten ohne Teams auf den privaten Endgeräten bei lediglich 26 Prozent liegt. Somit könnte auch hier das Zusammenrücken privat und geschäftlich genutzter Geräte zu einem Sicherheitsrisiko innerhalb des Unternehmens führen.

Dies wird insbesondere durch die Tatsache verstärkt, dass ein Großteil der Beschäftigten auch außerhalb der Arbeitszeit auf die Kollaborationslösung Teams zugreifen und sie nutzen kann. Denn drei Viertel (75 Prozent) der Befragten bestätigen, dass sie Microsoft Teams sowohl auf geschäftlichen als auch auf privaten Endgeräten wie Smartphones oder Tablets nutzen. Dieses hohe Niveau lässt sich in nahezu allen Unternehmensgrößenklassen und Ländern gleichermaßen beobachten. Diese Vermischung persönlicher und geschäftlicher Daten birgt zahlreiche Risiken, die es im Rahmen der Security- und Backup-Strategie zu berücksichtigen gilt. So könnten privat genutzt Apps durch weitreichende Berechtigungen auf geschäftskritische Daten aus Teams zugreifen. Da die IT-Abteilung keine Kontrolle über die privat genutzten Geräte hat, kann hier kein proaktiver Schutz gewährleistet werden. Auch bei Verlust oder Diebstahl von privaten Endgeräten können nicht nur Datenschutzverletzungen, sondern auch Risiken für das Unternehmensnetzwerk auftreten.

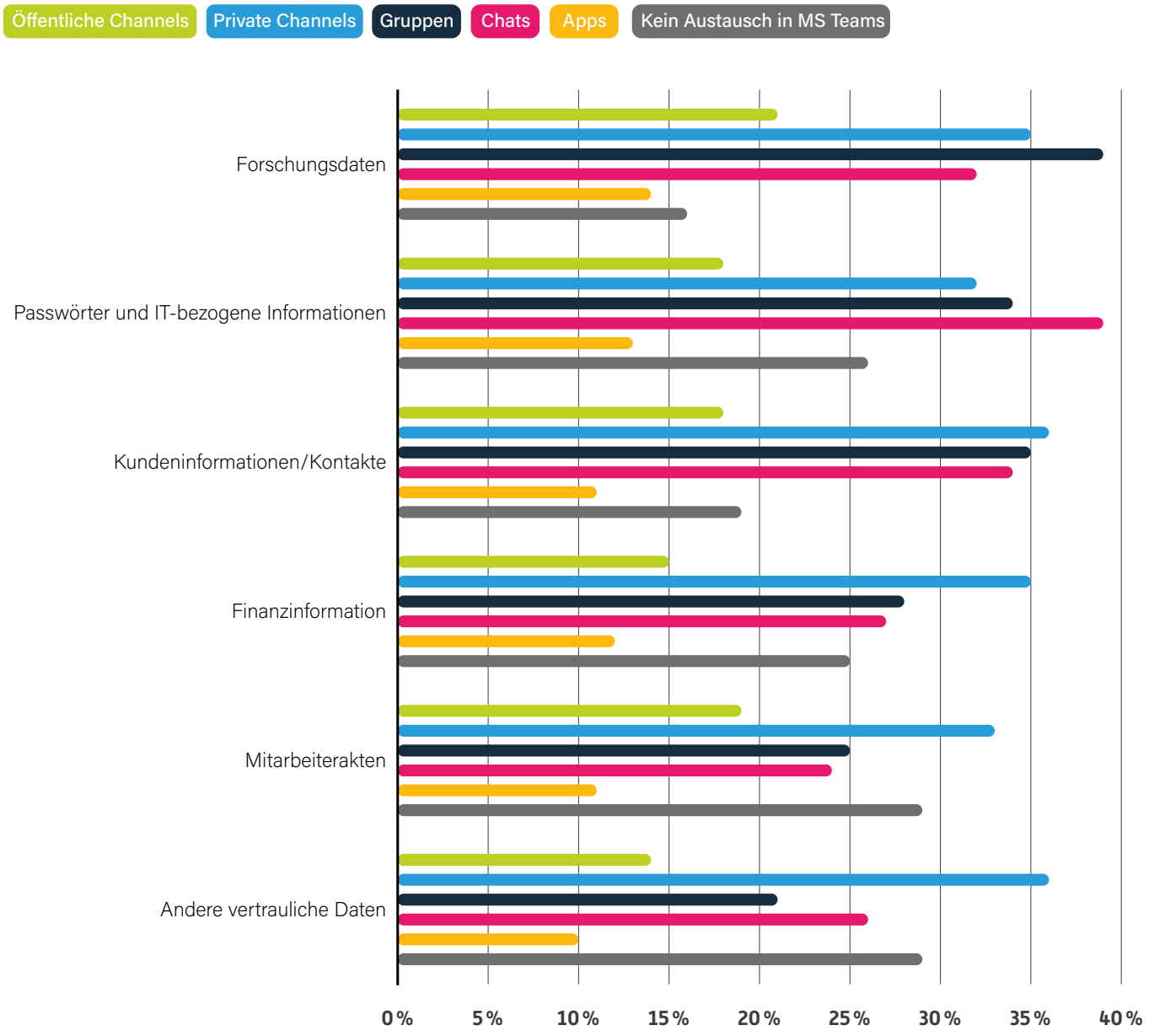
Mitarbeiter teilen sensible Daten über Chats

Der Austausch von Nachrichten und Dateien über Kollaborationslösungen kann eine Vielzahl von unterschiedlichen Inhalten umfassen. So können nicht nur geschäftsrelevante Nachrichten ausgetauscht werden, sondern auch sensible und teils geheime. So versenden 39 Prozent der befragten Beschäftigten geheime Passwörter und IT-relevante Informationen direkt über Teams-Chats an Arbeitskollegen.

Im Zuge der Verschiebung von Arbeitsschritten in die digitale Welt, hat sich auch der Umgang mit sensiblen Informationen geändert. Aus diesem Grund sollten Teams-Inhalte und Devices im Rahmen einer umfassenden IT-Security-Strategie abgesichert werden.

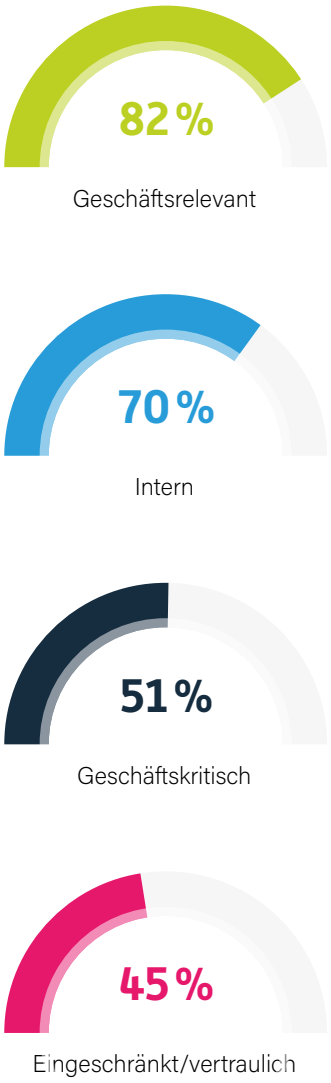
Austausch von Daten über unterschiedliche Teams-Formate

Basis: 540 Unternehmen



Versandhäufigkeiten unterschiedlicher Datentypen

Basis: 540 Unternehmen



Zudem werden auch Kundendaten und Kontaktlisten in Teams geteilt, insbesondere in privaten Kanälen (36 Prozent). Derartige private oder öffentliche Kanäle eignen sich vor allem für abteilungsspezifischen Informationsaustausch, z. B. innerhalb der Beschäftigten der Verkaufsabteilung. Aber auch Forschungsdaten und damit einhergehende Erkenntnisse werden von 39 Prozent der Befragten in Teams-Gruppen geteilt. Insgesamt zeigt sich, dass je nach Inhalt, Bedarf und Zielgruppe unterschiedliche Informationen innerhalb der Teams-Kommunikationskanäle verschickt werden. Dies stellt IT-Verantwortliche vor die Herausforderung, sämtliche Inhalte in Teams jederzeit abzusichern und im Bedarfsfall die Dateien wiederherzustellen.

Ein Blick aus einer Metaebene zeigt die unterschiedlichen Klassifizierungen der ausgetauschten Nachrichten. Insgesamt versenden 82 Prozent der Befragten häufig bis sehr häufig geschäftsrelevante und 70 Prozent interne Informationen und Nachrichten über Teams. Dazu gehört der alltägliche Austausch über operative Tätigkeiten und Workflows, die das Unternehmen oder Abteilungen betreffen.

Zudem teilt mehr als jeder zweite Befragte (51 Prozent) geschäftskritische Inhalte über Teams. Dazu können spezifische operative Daten, Kennzahlen oder Wettbewerbsinformationen zählen, die einen Einfluss auf die Entscheidungsfindung und strategische Ausrichtung des Unternehmens haben. Auffällig ist hierbei, dass Befragte mit Teams auf privaten Endgeräten (56 Prozent) deutlich häufiger geschäftskritische Inhalte teilen als Beschäftigte ohne Teams auf Privatgeräten (36 Prozent).

Eine weitere Art der versendeten Inhalte könnten vertraulicher Natur sein. So versenden 45 Prozent der Befragten häufig bis sehr häufig eingeschränkte oder vertrauliche Informationen über Teams. Ähnlich wie geschäftskritische Inhalte sind derartige Informationen dem Unternehmen selbst vorenthalten und würden ein hohes Risiko darstellen, sollten sie veröffentlicht oder der Konkurrenz in die Hände fallen. Derartige Informationen werden tendenziell häufiger in kleineren Unternehmen via Teams geteilt als in größeren. So liegt der Anteil bei Unternehmen mit 50 bis 99 Beschäftigten bei 54 Prozent, wohingegen in Großunternehmen mit 5.000 und mehr Beschäftigten lediglich 41 Prozent vertrauliche Informationen häufig bis sehr häufig teilen. Auch bei dieser Art von Inhalten lässt sich der Effekt privater Geräte beobachten. So teilt mehr als jeder zweite Beschäftigte (51 Prozent) mit Teams auf dem privaten Endgerät vertrauliche Informationen, wohingegen der Anteil bei Beschäftigten ohne Teams auf Privatgeräten bei lediglich 29 Prozent liegt. Kommt es zum Verlust oder Diebstahl der privaten Endgeräte, so können eingeschränkte und vertrauliche Daten öffentlich werden und dem Unternehmen schaden. Somit müssen auch hier die IT-Abteilungen proaktiv tätig werden und entsprechend darauf vorbereitet sein.

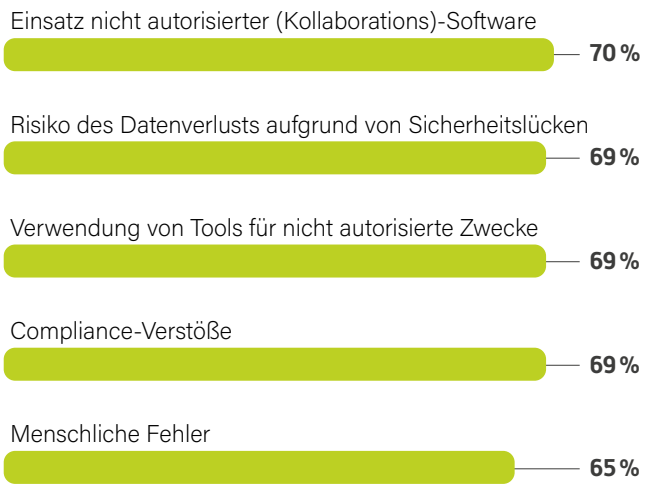
Datenverluste als Risikofaktor bei der Nutzung von Kollaborationslösungen

Obwohl der Einsatz von Kollaborationssoftware zahlreiche Vorteile bietet, lassen sich auch Risiken und Herausforderungen benennen, die es zu berücksichtigen gilt. So empfinden 70 Prozent der Befragten den Einsatz von nicht autorisierter Kollaborationslösungen und 69 Prozent die Verwendung von Tools für nicht autorisierte Zwecke als Security-Risiko für das Unternehmen. Nicht freigegebene Software oder Endgeräte, die als Schatten-IT am Unternehmensnetzwerk angeknüpft sind, können durch Sicherheitslücken und Fremdzugriff eine Gefahr für die Security darstellen.

Darüber hinaus sehen 69 Prozent das Risiko des Datenverlustes aufgrund von Sicherheitslücken als große Herausforderung beim Einsatz von Kollaborationslösungen. Unvorhergesehene Sicherheitslücken und Cyberangriffe können zum Ausfall der eingesetzten Lösungen zur Zusammenarbeit führen und wichtige Informationen und Daten des Unternehmens betreffen. Um diesen Herausforderungen gerecht zu werden bedarf es einer proaktiven Backup-Strategie, um sämtliche Inhalte dieser Lösungen zu sichern und im Bedarfsfall wiederherzustellen.

Die größten Security-Risiken und Herausforderungen

Basis: 540 Unternehmen | Summe von Top 1 und Top 2



Weitere genannte Risikofaktoren sind Compliance-Verstöße z. B. durch den Einsatz nicht lizenzierter Inhalte (69 Prozent) und menschliche Fehler (65 Prozent). Durch Unachtsamkeit kann es schnell passieren, dass relevante Inhalte und Informationen im Unternehmensnetzwerk oder auf Kollaborationsplattformen gelöscht werden. Dies kann dem Unternehmen großen Schaden zufügen oder zu Handlungsunfähigkeit führen.

Das tun Unternehmen um die Risiken zu minimieren:

- **56%** Regelmäßige Security-Schulungen
- **49%** Organisatorische Maßnahmen
- **45%** Verstärkter Einsatz von Sicherheitssoftware
- **34 %** Dienste mit ausgereiften Sicherheitsfunktionen
- **29 %** Dienstanbieter, die den Datenschutz einhalten
- **25%** Bewährte Verfahren für Bring Your Own Device
- **4%** Wir wissen nicht, wie wir Risiken minimieren können.

Um diesen potenziellen Risiken und Herausforderungen begegnen zu können, setzen 57 Prozent der Unternehmen auf regelmäßige Schulungen, um das Sicherheitsbewusstsein zu erhöhen. Denn viele Risiken sind hausgemacht und können durch entsprechende Sensibilisierung der Beschäftigten z. B. hinsichtlich des Umgangs mit unautorisierter Hard- und Software minimiert werden. Mehr als zwei Drittel (67 Prozent) der Befragten geben an, bereits für den Einsatz von Kollaborationslösungen sensibilisiert und geschult wurden zu sein. Damit einhergehend setzt fast jedes zweite Unternehmen (49 Prozent) auf organisatorische Maßnahmen und Richtlinien, um den Einsatz von Softwarelösungen zu kontrollieren und proaktiv möglichen Risiken entgegenzuwirken.

Ein weiterer Ansatz ist die Ausweitung der softwaregestützten Sicherheitsarchitektur. So setzen 45 Prozent der befragten Unternehmen verstärkt zusätzliche Security-Lösungen ein, um die Risiken und Herausforderungen im Umgang mit Kollaborationslösungen zu beseitigen.

Kollaboration ist mehr als nur ein Trend

Die vorgestellten Ergebnisse zeigen deutlich, dass die softwaregestützte Kollaboration einen wichtigen Bestandteil der modernen Arbeitswelten darstellt. Beschäftige nutzen täglich Lösungen wie Microsoft Teams zum kollegialen Austausch, zur Bearbeitung von Projekten oder zum Austausch von Informationen oder Dateien.

Insbesondere Direktnachrichten werden zur bilateralen Kommunikation bevorzugt, selbst wenn diese in Gruppen oder Kanälen abgehalten werden könnten. Zudem werden immer mehr Nachrichten und Dateien mit sensiblen Inhalten geteilt. Beschäftigte nutzen Microsoft Teams nicht nur um operativ geschäftliche Nachrichten auszutauschen, sondern auch sensible, geschäftskritische und geheime Inhalte zu teilen. Diese intensive und umfassende Nutzung derartige Lösungen führt dazu, dass ein Ausfall zu Produktivitätseinbußen oder zu größeren Schäden für das Unternehmen führen kann.

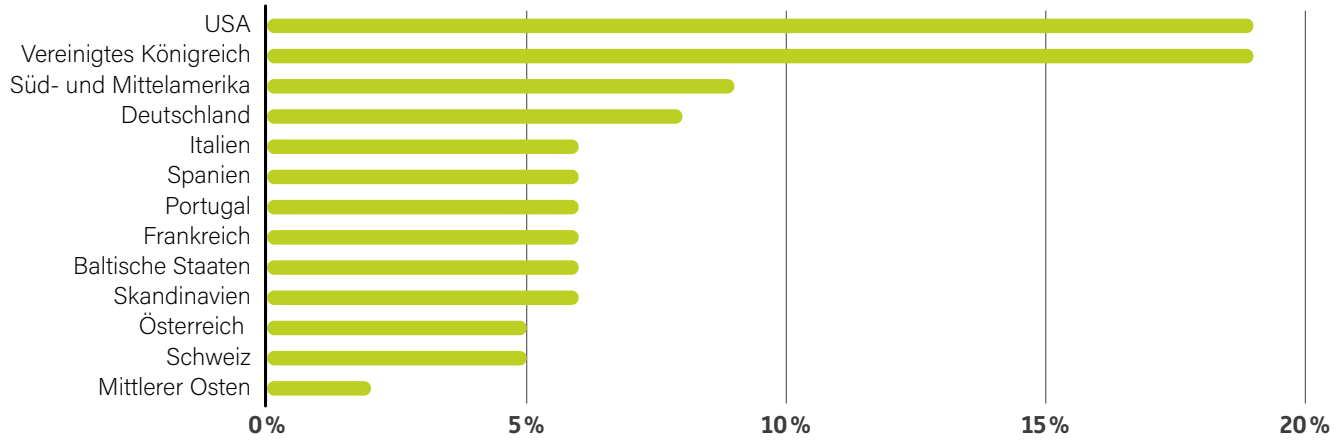
Somit müssen IT-Verantwortliche im Rahmen ihrer proaktiven Security-Strategie dafür Sorge tragen, dass sämtliche Nachrichten, Dateien und Inhalte der eingesetzten Kollaborationslösungen durch Sicherheitskopien geschützt werden. Diese Notwendigkeit wird auch dadurch verstärkt, dass betriebliche Software zur Zusammenarbeit immer häufiger auf privaten Endgeräten ausgeführt werden. Dies erhöht die Gefahr durch Cyberangriffe, Sicherheitslücken oder Datenverluste durch potenzielle menschliche Fehler.

Auch in Zukunft wird der Einsatz von Kollaborationslösungen zum Arbeitsalltag gehören und sogar noch stärker in Workflows und Prozesse eingebunden werden. Durch die Verbreitung des hybriden Arbeitsmodells werden derartige Lösungen wichtiger denn je. So prognostizieren zwei Drittel (66 Prozent) der Befragten, dass sie in Zukunft stärker auf Kollaborationslösungen setzen werden. Die ortsunabhängige Zusammenarbeit wird somit weiterhin einen festen Bestandteil der modernen Arbeitswelt darstellen mit Kommunikations- und Kollaborationslösungen als maßgebliche und relevante Instrumente.

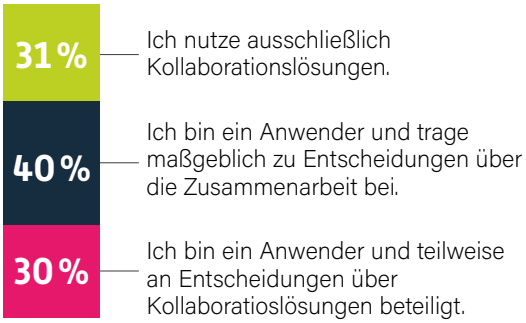
Stichprobe

Im Rahmen der vorliegenden Studie wurden im August 2022 insgesamt 540 Nutzer der Kollaborationslösung Microsoft Teams befragt. Die Befragten sind reine Anwender und Anwender mit maßgeblichen oder bedingten Entscheidungsbefugnissen hinsichtlich der Beschaffung und Gestaltung von Kollaborationslösungen. Es wurden nur Teilnehmer aus Unternehmen aller Branchen mit mindestens 50 Beschäftigten aus über 16 Ländern berücksichtigt.

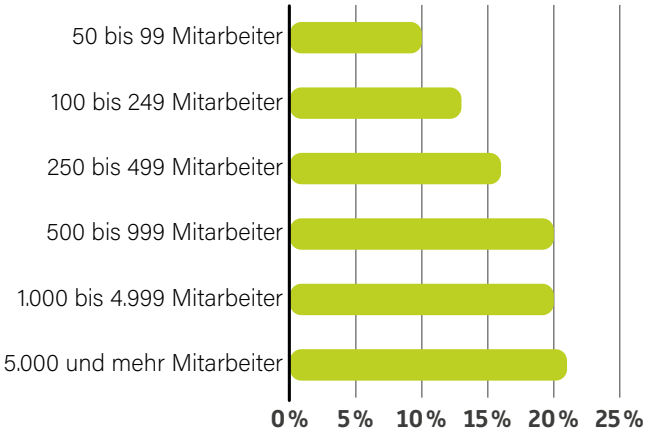
Unternehmenssitz



Zielgruppe



Mitarbeiter



Branche

15% Information und Kommunikation
13% Finanz- und Versicherungsaktivitäten
9% Andere Dienstleistungen
9% Herstellung
8% Berufliche, wissenschaftliche und technische Tätigkeiten
7% Groß- und Einzelhandel; Kfz-Werkstätten
6% Aktivitäten im Bereich Gesundheit und Sozialarbeit
6% Transport und Lagerung
5% Ausbildung
4% Verwaltungs- und Support-Dienstleistungen
4% Konstruktion
3% Öffentliche Verwaltung/Verteidigung; Sozialversicherung
2% Strom-, Gas-, Dampf- und Klimaversorgung
2% Beherbergungs- und Verpflegungsdienstleistungen
2% Kunst, Unterhaltung und Erholung
2% Immobilien
1% Wasserversorgung; Abwasser-, Abfallwirtschaft
1% Landwirtschaft, Forstwirtschaft und Fischereiwesen
1% Bergbau und Steinbrüche

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

Anbietervergleich

Microsoft Teams Backup-Lösungen

Im Zuge der quantitativen Untersuchung wurde zudem eine punktuelle Wettbewerbsbetrachtung und -analyse durchgeführt. Dabei wurde der Leistungsumfang von Teams-Backup-Lösungen ausgewählter Anbieter untersucht. Die folgende tabellarische Übersicht zeigt auf, ob und welche in der Studie thematisierten Teams-Kommunikationsformate im Rahmen der Backup-Lösungen unterstützt werden.

PROVIDER	Hornetsecurity	Acronis	AvePoint	Barracuda	Veeam	Skykick
USER CHATS	✓ Backed up	✗ Not backed up				
ONE TO ONE CHATS						
• Messages	✓	✗	✗	✗	✗	✗
• Attached Images	✓	✗	✗	✗	✗	✗
GROUP CHATS						
• Messages	✓	✗	✗	✗	✗	✗
• Attached Images	✓	✗	✗	✗	✗	✗
MEETING CHATS						
• Messages	✓	✗	✗	✗	✗	✗
• Attached Images	✓	✗	✗	✗	✗	✗
CHANNEL CONVERSATIONS						
PUBLIC CHANNEL CONVERSATIONS						
• Posts & replies	✓	✓	✓	✗	✓	✓
• Attached Images	✓	✗	✓	✗	✓	✗
PRIVATE CHANNEL CONVERSATIONS						
• Posts & replies	✓	✓	✓	✗	✗	✓
• Attached Images	✓	✗	✓	✗	✗	✗

Datum der Erstellung: 28.09.2022

Weitere Informationen

Kontakt für mehr Informationen

Ercan Hayvali
Analyst

Telefon: +49 561 8109 178
E-Mail: **ercan.hayvali@techconsult.de**

techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

Telefon: +49 561 8109 0
Fax.: +49 561 8109 101
Web: **www.techconsult.de**

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.

In Zusammenarbeit mit

HORNETSECURITY

Kontakt

Hornetsecurity GmbH
Am Listholze 78
30177 Hannover

E-Mail: **info@hornetsecurity.com**
Tel.: +49 511 515 464 0

Mehr erfahren

Über Hornetsecurity

Hornetsecurity ist ein führender E-Mail-Cloud-Security- und Backup-Provider, der Unternehmen und Organisationen jeglicher Größe weltweit absichert. Das preisgekrönte Produktportfolio deckt alle wichtigen Bereiche der E-Mail-Sicherheit ab: darunter Spam- und Virenfilter, Schutz vor Phishing und Ransomware, sowie rechtssichere Archivierung und Verschlüsselung. Hinzu kommen Backup, Replikation und Wiederherstellung von E-Mails, Endpoints und virtuellen Maschinen. Das Flaggschiffprodukt ist die marktweit umfangreichste Cloud-Sicherheitslösung für Microsoft 365. Mit über 400 Mitarbeitern an 12 Standorten verfügt das Unternehmen mit Hauptsitz in Hannover über ein internationales Netzwerk von mehr als 8.000 Channel-Partnern und MSPs sowie über 11 redundante, gesicherte Rechenzentren. Die Premium-Services nutzen mehr als 50.000 Kunden, darunter Swisscom, Telefónica, KONICA MINOLTA, LVM-Versicherung und CLAAS.

Presseanfragen

Bitte kontaktieren Sie uns unter **press@hornetsecurity.com**.

Eine Studie von

techconsult
TECHNOLOGY MARKET ANALYSTS

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**

Telefon: +49 561 8109 0
Telefax: +49 561 8109 101
Web: **www.techconsult.de**

In Zusammenarbeit mit

HORNETSECURITY