Krisensicher dank Cloud-Technologien

Welche Auswirkungen hat die Pandemie auf die IT-Infrastruktur deutscher Unternehmen?

IN ZUSAMMENARBEIT MIT

IONOS

Informationen zur Studie

ERSTELLT DURCH

techconsult
The IT Market Analysts

KONTAKT

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

IN ZUSAMMENARBEIT MIT

IONOS

Inhaltsverzeichnis

Vorwort

Manchmal muss man auch unangenehmen Dingen etwas Gutes abgewinnen. Für viele Unternehmen ist die Corona-Krise ein Katalysator für die Digitalisierung. Aktuelle Untersuchungen bestätigen, dass Unternehmen, die bereits auf innovative Technologien setzen, besser und schneller auf die Auswirkungen reagieren können und sich auch schneller erholen werden. Die Digitalisierung ist eine der wichtigsten Voraussetzungen, Arbeitsprozesse produktiver zu gestalten, effizientere Wertschöpfungsketten hervorzubringen und neue Geschäftsmodelle zu kreieren. Darüber hinaus sind digitale Prozesse die Grundlage für das Arbeiten im Home-Office. Die verhängten Kontaktbeschränkungen haben zu einer massiven Verlagerung der Büroarbeitsplätze ins Home-Office geführt. Inmitten der Krise zeigt sich, wie wichtig eine auf Remote Work eingestellte IT-Infrastruktur für die Unternehmen ist. Die IT der Unternehmen stand in der Verantwortung im Eiltempo eine sichere technische Infrastruktur bereitzustellen, die nicht nur nachhaltig ist, sondern sich auf situativ bedingte Veränderungen schnell einstellen kann.

Wie ist es den Unternehmen gelungen, zur Realisierung der großen Anzahl an Home-Office-Arbeitsplätzen seitens der IT-Infrastruktur ausreichende Kapazitäten bereitzustellen? Die veränderte Arbeitsweise hat die Anforderungen in den Unternehmen an ihr Server- und Netzwerkmanagement erhöht. Mit den alten, über die Jahre gewachsenen, starren und klassischen IT-Infrastrukturen ist der Wandel kaum möglich.

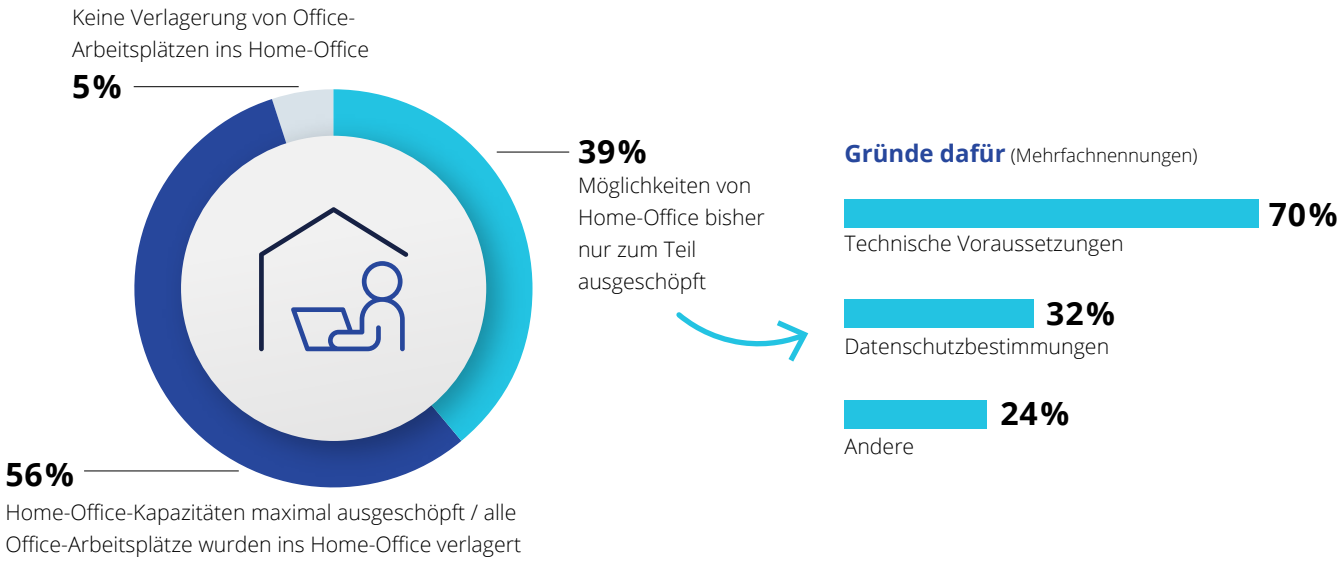
In vielen Unternehmen hat die Krise digitale Prozesse beschleunigt, zugleich wurden aber auch digitale Schwachstellen in der Digitalisierungsstrategie sichtbar. Wo klemmt es? Welche Probleme gibt es im Bereich IT-Operations- und Application-Management? Welche digitalen Maßnahmen wurden im Kontext der Home-Office-Regelungen von den Unternehmen ergriffen? Welche Auswirkungen hat es auf die IT-Infrastruktur der Unternehmen? Und welche Maßnahmen werden für eine sichere und datenschutzkonforme Remote-Arbeit ergriffen. Antworten auf diese und weitere Fragen gibt die Studie „Krisensicher dank Cloud-Technologien“, die von techconsult in Zusammenarbeit mit IONOS konzipiert und durchgeführt wurde.

Home-Office – Impulsgeber für digitale Lösungen

Im Verlauf der Pandemie haben die Unternehmen die Möglichkeiten für ihre Beschäftigten, von zu Hause zu arbeiten, immer mehr ausgeweitet. Gleichwohl ist das Potenzial noch nicht ausgeschöpft: Pandemiebedingt bieten inzwischen 95 Prozent der befragten Unternehmen Home-Office an. 56 Prozent der Betriebe haben ihre Home-Office-Möglichkeiten inzwischen voll ausgeschöpft.

Das bedeutet, alle vorhandenen Office-Arbeitsplätze wurden in das Home-Office verlegt. Knapp 40 Prozent der Unternehmen haben ihre Home-Office-Kapazitäten jedoch nur zum Teil ausschöpfen können, hier wäre theoretisch noch Potenzial vorhanden. Doch bei 70 Prozent der Unternehmen sind die technischen Voraussetzungen nicht gegeben und bei knapp jedem dritten Unternehmen lassen es die vorhandenen Datenschutzbestimmungen nicht zu.

Pandemiebedingte Verlagerung von Arbeitsplätzen ins Home-Office

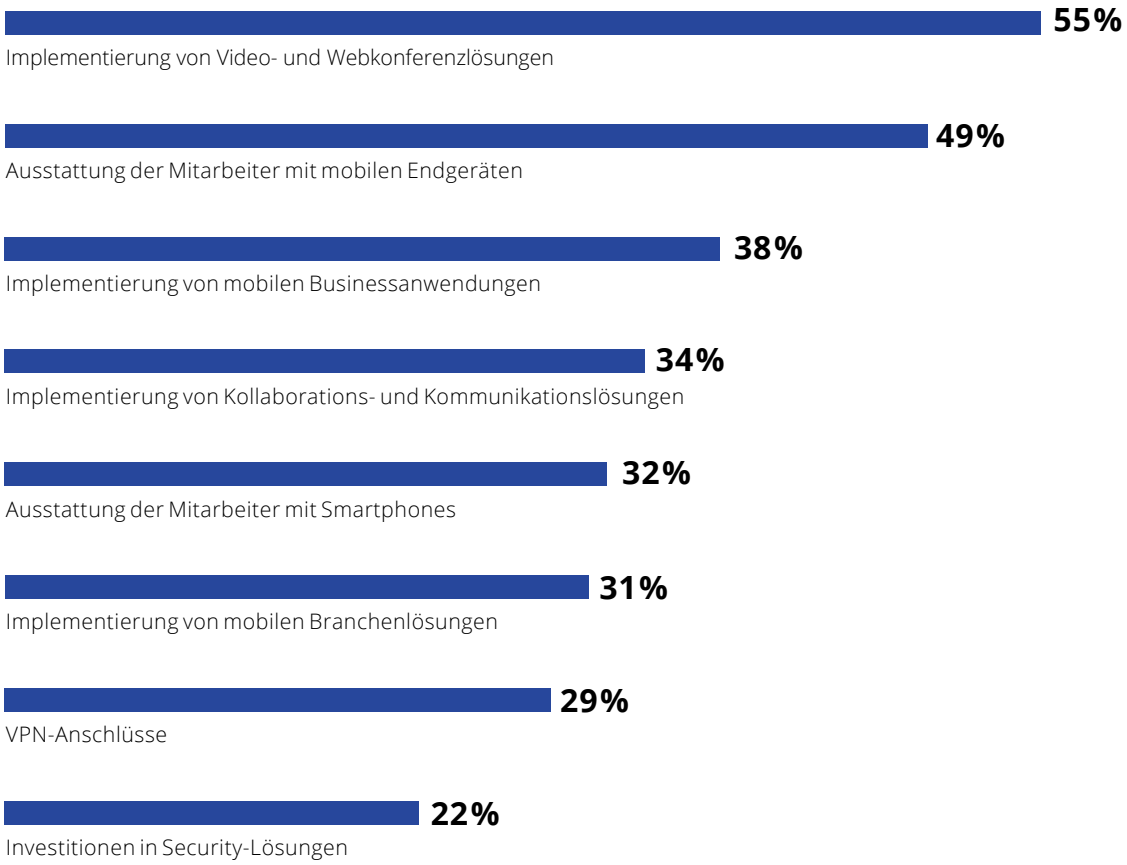


Es ist offensichtlich, durch Corona hat die Digitalisierung an Fahrt gewonnen. Jedes zehnte Unternehmen gab an, dass die Performance ihrer IT-Infrastruktur gegenüber der Zeit vor Corona zugelegt hat. Etwa die Hälfte der Unternehmen fühlt sich inzwischen zumindest gut aufgestellt. Nach dem Motto „Wer zögert, der verliert", haben viele Unternehmen digitale Projekte auf den Weg gebracht. In Windeseile wurde, wenn auch gezwungenermaßen, ein IT-Budget freigesetzt und in mobile Endgeräte und digitale Technologien für effiziente Remote-Arbeit investiert. Jedes zweite Unternehmen hat seine Mitarbeiter mit mobilen Endgeräten ausgestattet. Doch Geräte allein reichten nicht, es wurden auch die entsprechenden mobilen Anwendungen benötigt und eine sichere Anbindung an das Unternehmensnetz. Mehr als jedes dritte Unternehmen hat mobile Applikationen mit besonderer Ausrichtung auf Geschäftszwecke und bestimmte Branchen eingeführt. Kollaborations- und Kommunikationslösungen wurden weitflächig implementiert.

Durch Einschränkung von Präsenz-Meetings werden viele Besprechungen ersatzweise via Audio- und Videokonferenzen durchgeführt. Hierfür haben 55 Prozent der Unternehmen ihre Kapazität erhöht und entsprechende Lösungen eingeführt. Gleichzeitig waren IT-Verantwortliche herausgefordert, vor allem auch sichere Bedingungen für das Home-Office zu schaffen. VPN-Anschlüsse und Security-Lösungen sind weitere wichtige Bereiche, die im Kontext der neuen Arbeitsweisen priorisiert wurden.

> In vier von zehn Unternehmen hat die Corona-Krise die Einführung digitaler Prozesse beschleunigt bzw. vorhandene Prozesse einer Neugestaltung unterworfen.

Maßnahmen im Kontext von Home-Office



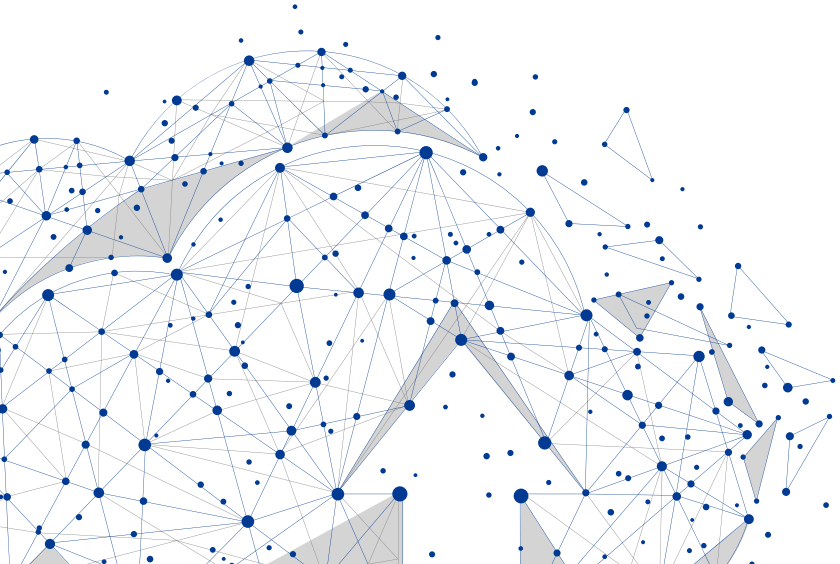
Filter: Wenn Arbeitsplätze ins Home-Office verlagert wurden | Mehrfachnennungen

Corona treibt Workloads in die Cloud

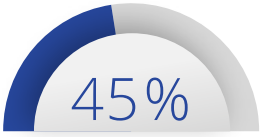
Anforderungen an das Server- und Netzwerkmanagement steigen

Für die schnelle Realisierung der großen Anzahl an Arbeitsplätzen im Home-Office bedarf es seitens der IT-Infrastruktur ausreichende Kapazitäten, sowohl was das Server- als auch Netzwerkmanagement betrifft. 43 Prozent der IT-Entscheider gaben an, auf die erhöhten Anforderungen nicht gut vorbereitet zu sein. Effizienz und Produktivität im Home-Office erfordern eine schnelle und stabile Internetanbindung. 45 Prozent der Befragten sehen im erhöhten Breitbandbedarf eine der größten Schwachstellen. Der Zugriff vom Home-Office auf Businessanwendungen und der Austausch großer Datenmengen benötigen große Bandbreiten und ein ausgefeiltes Bandbreitenmanagement, die entweder noch nicht flächendeckend zur Verfügung stehen oder auf das die vorhandenen Netze und heimischen WLANs erst vorbereitet werden müssen.

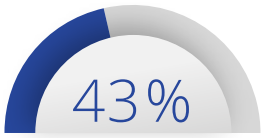
Für 43 Prozent der befragten Unternehmen stellt das Arbeiten im Home-Office ein erhöhtes Sicherheitsrisiko dar. Hier geht es zum einen um die Einhaltung der Sicherheitsvorschriften seitens der Beschäftigten, aber auch um technische Aspekte, beispielsweise bei der Einrichtung sicherer VPN-Verbindungen. Problematisch wird es vor allem, wenn User die Nutzung privater IT-Geräte (BYOD) in Betracht ziehen, weil dienstliche Geräte für die Verwendung im Home-Office nicht zur Verfügung stehen. Mobile Device Management (MDM) kann hier Abhilfe schaffen. Fehlende Rechen- und Speicherkapazitäten und eine veraltete Backend-IT-Infrastruktur sind weitere Probleme, die in jedem dritten Unternehmen im Kontext der Home-Office-Regelungen noch zu lösen sind. In Folge haben sich die Unternehmen vermehrt mit Cloud-Technologien beschäftigt und werden mehr Workloads in die Cloud verlagern.



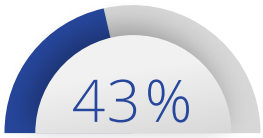
Probleme im IT Operations- und dem Application-Management



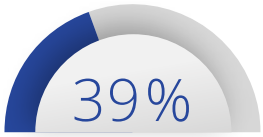
Erhöhter Bandbreitenbedarf



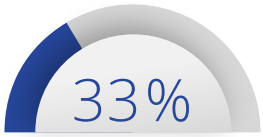
Erhöhte Sicherheitsrisiken



Erhöhte Anforderungen an das Server- und Netzwerkmanagement



Erhöhtes Speicheraufkommen



Fehlende Serverkapazitäten (Rechenleistungen)

Modernisierung der Backend-IT-Infrastruktur

Mehrfachnennungen

Migration in die Cloud nimmt Fahrt auf

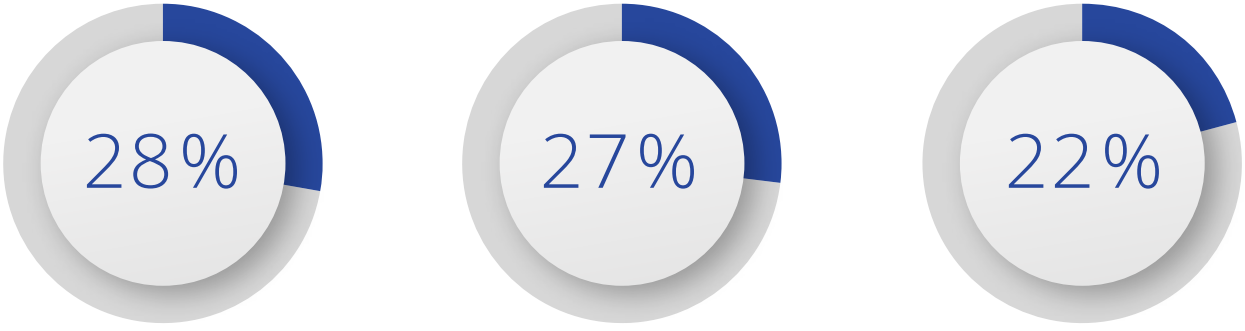
Maßgebliche Technologien auf dem Weg zum modernen Arbeiten sind Cloud-Infrastrukturen. Flexible und skalierende Cloud-Services bieten Unternehmen den in Zeiten der Pandemie nötigen Effizienzgewinn, ohne die Komplexität zu erhöhen. Sind die Services zudem noch datenschutzkonform und mit maximaler Sicherheit vor dem US CLOUD Act versehen, ist dies eine geeignete Umgebung, um die Migration in die Cloud zu beschleunigen.

> 87 Prozent der Unternehmen geben an, dass die erhöhten Anforderungen an das Server- und Netzwerkmanagement Einfluss auf die Cloud-Strategie haben.

Neue Arbeitsweisen bzw. das Festhalten vieler Betriebe an Home-Office, auch nach der Krise, lassen die Nachfrage nach Cloud-Technologien in den Unternehmen weiter ansteigen. IT-Entscheider haben erkannt, dass eine Migration der IT-Infrastruktur in die Cloud Möglichkeiten bietet, schnell auf geschäftliche Veränderungen zu reagieren, beispielsweise flexiblere Arbeitsweisen oder Veränderungen in der Personaldecke. Die Migration von Workloads in die Cloud trägt dazu bei, auch im Home-Office die nötige Produktivität zu gewährleisten.

Die Cloud stellt Services über das Internet zentral bereit. Kosten für Infrastructure-as-a-Service bzw. Platform-as-a-Service-Dienste fallen normalerweise nur für die tatsächliche zeitliche Nutzung an. Software-Nutzer beziehungsweise Software-Arbeitsplätze werden in der Regel monatlich oder jährlich abgerechnet. Die Anwendungen werden nicht im Rechenzentrum des Anwenders betrieben, sondern online abgerufen. Und auch Bereitstellung, Wartung und Aktualisierung liegen im Sinne der sogenannten Shared Responsibility teils in der Verantwortung des Anbieters und nur teils auf Anwenderseite. Unternehmen können damit schnell und einfach die Services nutzen und diese sowohl stationär als auch mobil einsetzen. 31 Prozent haben sich verstärkt mit cloudbasierten IT-Betriebsmodellen auseinandergesetzt. Jedes zweite Unternehmen wird 2021 den Fokus verstärkt auf Cloud-Dienste ausrichten. Dabei stellt sich für IT-Verantwortliche die Frage, wo Workloads ausgeführt werden sollen – ob in der Public Cloud, in der Private Cloud oder mit einer hybriden Lösung. Die Entscheidungen erfordern sorgfältige Prüfung und Recherche, da verschiedene Anwendungen unterschiedliche Anforderungen mit sich bringen. 28 Prozent der Unternehmen sehen kein Problem, sich die IT-Infrastruktur bei einem IT-Dienstleister mit anderen Unternehmen zu teilen. Sie verlagern mehr Workloads und Applikationen in die Public Cloud. 27 Prozent bevorzugen dagegen die Verfügbarkeit der Infrastruktur nur für ihr eigenes Unternehmen, sie schlagen vermehrt den Weg in die Private Cloud ein. Hybride Cloud Migrationsprojekte werden von 22 Prozent der Unternehmen vorangetrieben. Sie werden bestimmte Workloads vor Ort belassen und andere vermehrt in der Cloud ausführen. Ganz gleich, welche Cloud-Migration gewählt wird, Vorteile hat jede.

Einfluss von Home-Office auf Cloud-Strategie



Wir verlagern mehr Workloads und Applikationen in die Public Cloud

Wir verlagern mehr Workloads und Applikationen in die Private Cloud

Wir nutzen vermehrt Hybrides Cloudmanagement

Cloud-Technologien machen das Arbeiten komfortabel

Unternehmen können durch Cloud-Technologien schnell und einfach Software Services nutzen und diese für flexibles Arbeiten mobil einsetzen. Unabhängig von Ort und Gerät haben Beschäftigte zu jeder Zeit Zugriff auf ihre Daten und Geschäftsanwendungen. Neben der Flexibilität gibt es jedoch eine Reihe weiterer Vorteile, von denen vor allem IT-Entscheider profitieren. Die Cloud als hardwarelose Alternative sorgt für zügige Bereitstellung virtueller Rechen- und Speicherkapazitäten.

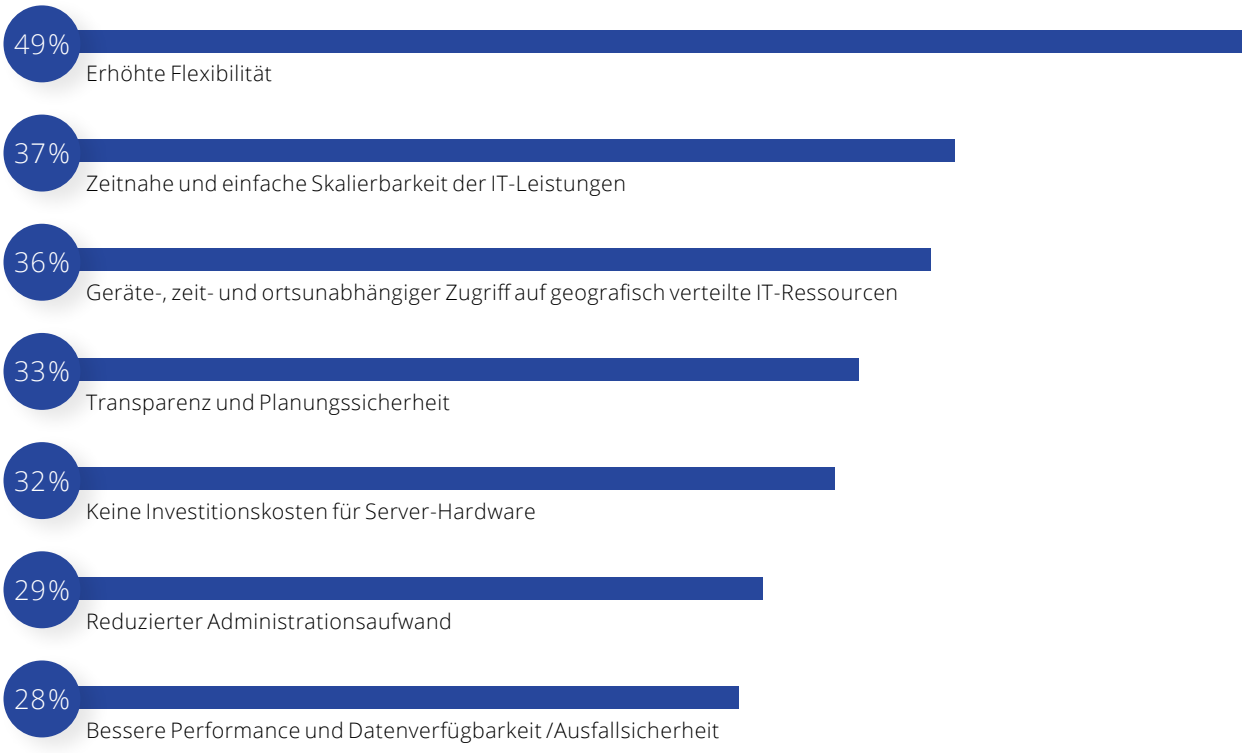
Weitere 37 Prozent der Befragten schätzen eine zeitnahe und einfache Skalierbarkeit der IT-Leistungen. Genannt werden auch: Transparenz und Planungssicherheit (33 Prozent), bessere Performance und Datenverfügbarkeit sowie Ausfallsicherheit. Hinzu kommen Kosteneinsparungen – teure Investitionskosten für interne Server-Strukturen entfallen. Auch die Bindung von Speicherkapazitäten ist nicht notwendig. Über Cloud-Dienstleister lassen sich IT-Leistungen nach Bedarf abrufen. Unternehmen, die sich der Cloud-Technologie breit öffnen, erzielen auf diese Weise Wettbewerbsvorteile, denn IT-Ressourcen lassen sich effizienter und gewinnbringender einsetzen.

29 Prozent der Befragten gaben an, dass Cloud-Infrastrukturen die IT im operativen Aufgabenbereich entlasten und dazu beitragen, den Administrationsaufwand zu reduzieren. Das IT-Team kann sich mehr mit modernen und ressourcenintensiven Technologien, wie beispielsweise Künstlicher Intelligenz, IoT oder Predictive Analytics beschäftigen und Innovationen vorantreiben.

Viele bisherige Studien haben gezeigt, dass bestehende Bedenken gegenüber der Datensicherheit und dem Datenschutz insbesondere den Einsatz von Public-Cloud-Technologien bremsten. Das scheint sich aufzulösen, ja sogar umzudrehen. 21 Prozent der Unternehmen sehen inzwischen gerade durch Cloud-Technologien die Sicherstellung der DSGVO-konformen Datenspeicherung gewährleistet. Bei Cloud-Anbietern sind der Unternehmenssitz und der Serverstandort entscheidend dafür, welches Recht zugrunde gelegt wird. Haben Cloud-Anbieter ihren Serverstandort in Deutschland, unterliegen alle darauf gespeicherten Daten dem strengen deutschen Datenschutz, der DSGVO.

Meistgenannte Vorteile von Cloud-Lösungen sind Flexibilität, einfache Skalierbarkeit und mobiler Zugriff.

Nutzen von Cloud-Technologien



Mehrfachnennungen

Home-Office – kein Selbstläufer

Problem Nummer eins – IT-Sicherheit

Die rasante Verlegung des Arbeitsplatzes von der Arbeitsstätte in das Home-Office ist nicht reibungslos verlaufen. Sie hat die IT-Verantwortlichen vieler Unternehmen vor Herausforderungen gestellt. Home-Office bedeutet nicht nur den Ort der Tätigkeit zu verlegen, sondern setzt Technologien und eine entsprechende IT-Infrastruktur voraus. Hinzu kommen Sicherheitslösungen und -konzepte. Die Studienergebnisse belegen: Die Corona-Krise ist in den Unternehmen ein Treiber der Digitalisierung, doch sie bringt zugleich auch Versäumnisse in der Digitalisierungsstrategie ans Licht.

> Jedes zweite Unternehmen gab an, dass die Corona-Krise Schwächen in ihrer Digitalisierungsstrategie aufgezeigt habe.

In nahezu jedem zweiten Unternehmen hapert es bei der Gewährleistung der IT-Sicherheit und der Erstellung von IT-Sicherheitskonzepten zur sicheren Einbindung der mobilen Geräte.

Ein weiterer Punkt ist der sichere Datenaustausch. Mitarbeiter im Home-Office müssen in der Lage sein, effizient und unkompliziert große Datenmengen sicher zu verschicken. Und das nicht nur innerhalb des Unternehmens, sondern auch im Austausch mit externen Geschäftspartnern. Dadurch hat sich in Windeseile die Nutzung von Cloud-Collaboration-Plattformen verbreitet. Doch dies hat nicht nur Vorteile, sondern birgt für viele auch Risiken.

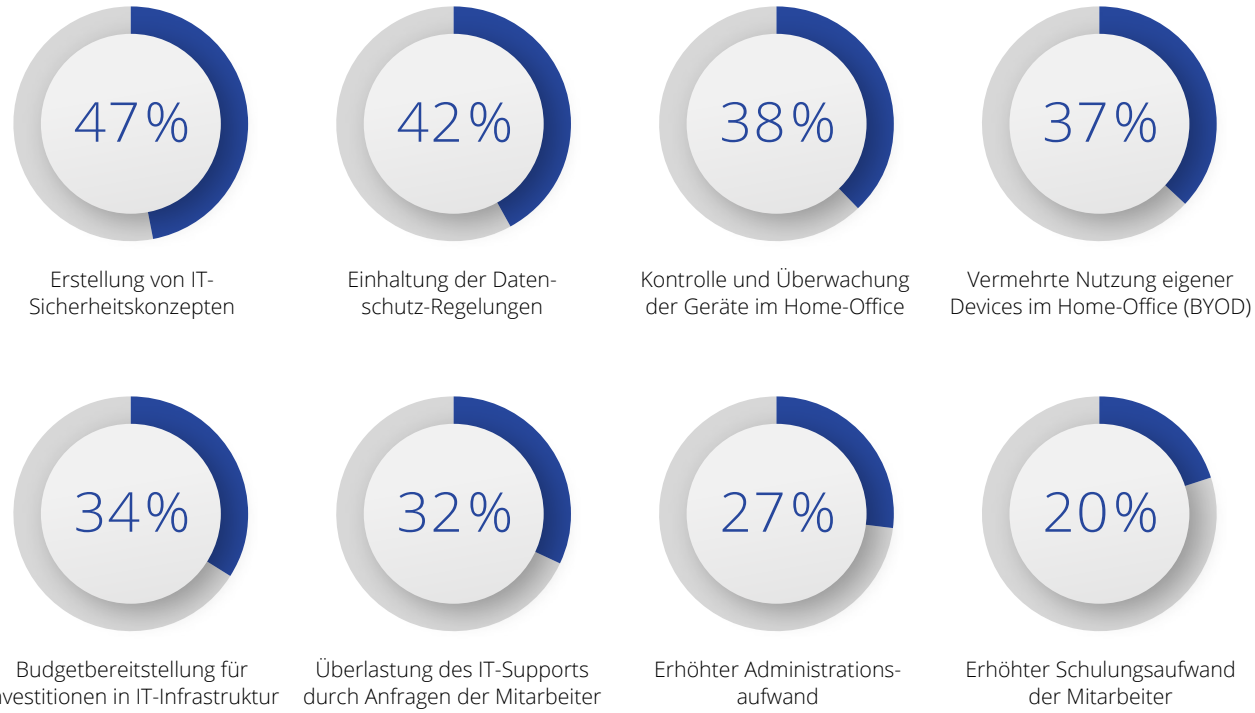
Der DSGVO-konforme Datenaustausch ist ein Nadelöhr für die virtuelle Zusammenarbeit. Insbesondere dann, wenn sich Unternehmen im Vorfeld nicht umfassend über die Plattformen informiert haben. 42 Prozent der Befragten schätzen die Einhaltung der Datenschutzregelungen bei vermehrter Nutzung von webbasierten Filesharing Tools und Kollaborationslösungen problematisch ein. Für IT-Administratoren ist es oft schwer, mit dem regen Datenaustausch Schritt zu halten. Durch Cloud-Speicher erhöht sich das Sicherheitsrisiko: Manche datenschutzrelevanten Abläufe sind den zwangsweise ins Home-Office verbannten Usern noch nicht im Detail vertraut. Schnell landen Daten und Informationen nicht nur bei den Mitarbeitern, sondern sind auch externen Personen versehentlich zugänglich.

Ein weiteres Problem stellen private Endgeräte dar. Viele Unternehmen haben zwar in mobile Endgeräte investiert, doch längst steht nicht jedem Mitarbeiter ein firmeneigenes mobiles Endgerät für die Arbeit im Home-Office zur Verfügung. Die Folge ist der Zugriff auf das private Gerät. 37 Prozent der IT-Entscheider sehen in der vermehrten Nutzung privater Computer und Mobiltelefone (BYOD) ein Problem. Kommen Privatgeräte für dienstliche Zwecke zum Einsatz, bedarf es einer BYOD-Strategie, die den sicheren Umgang mit den Geräten regelt und festlegt. Verantwortliche müssen abwägen, in welchem Maße diesen Geräten vertraut werden kann. Dabei ist unter anderem über Gerätetyp sowie Betriebssystem zu entscheiden, welche Mitarbeitergruppen welche Daten in welchem Umfang verarbeiten dürfen und welche Maßnahmen bei Verlust zu treffen sind. Die Anforderungen an die Absicherung privater IT-Systeme sind in speziellen Richtlinien und Maßnahmen festzuhalten. Diese sollten unter anderem Sicherheits-Updates, Virenschutzprogramme, VPN und Festplattenverschlüsselung beinhalten.

Darüber hinaus sind die Zugriffsberechtigungen bei privaten Systemen auf das erforderliche Mindestmaß zu reduzieren. Mobile Device Management (MDM) ermöglicht auch auf privaten Endgeräten ein sicheres Arbeiten - verschlüsselt und passwortgeschützt, indem es zum Beispiel bestimmte Workspaces einrichtet, in denen geschäftsrelevante Anwendungen, gekapselt vom eigentlichen Smartphone oder Tablet funktionieren.

In die Liste der Problemfelder reiht sich auch eine Überlastung des IT-Supports mit ein. Dies gaben 32 Prozent der Unternehmen an. Die Mehrbelastung resultiert aus einer Vielzahl von Problemen und Anfragen seitens der im Home-Office arbeitenden Mitarbeiter. Und davon gibt es reichlich: Beispielsweise, wenn die Technik hakt, die Videokonferenzschaltung nicht funktioniert oder das Internet ausfällt. 26 Prozent der IT-Entscheider fühlen sich durch einen Mehraufwand an Administration belastet, vor allem um die Cybersicherheit der Mitarbeiter im Home-Office sicherzustellen. Und 20 Prozent stellen durch fehlende Kenntnisse beziehungsweise digitale Kompetenzdefizite der Mitarbeiter einen erhöhten Schulungsaufwand fest.

Herausforderungen der Unternehmen durch vermehrte Remote-Arbeit



Mehrfachnennungen

Management- und IT-Security-Lösungen gefragter denn je

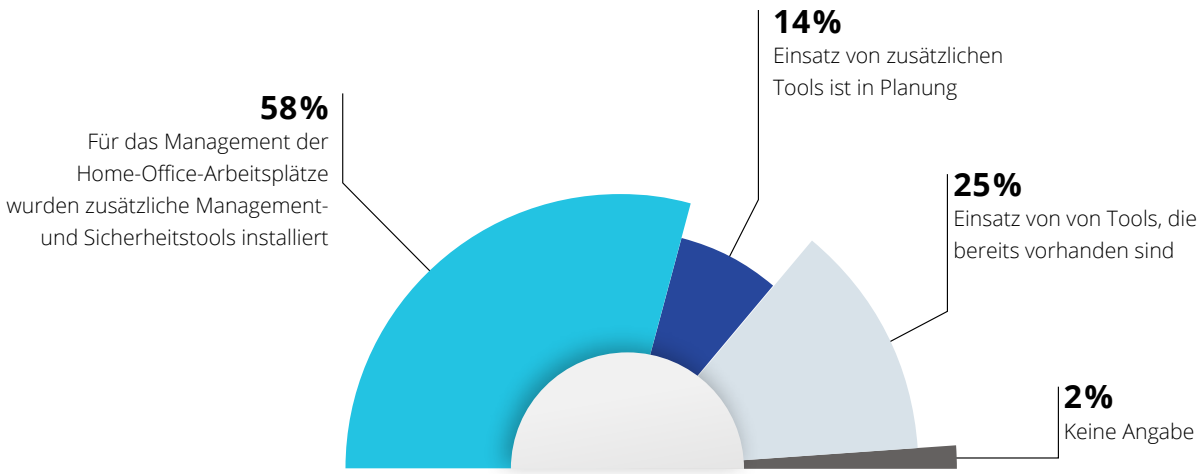
Die bisher eingesetzten IT-Management- und -Sicherheitslösungen reichen für die wachsenden Ansprüche nicht mehr aus. Unternehmen müssen es strikt vermeiden, dass sich Mitarbeiter mit ungesicherten privaten Endgeräten oder über ungesicherte Verbindungen ins Firmennetz einloggen. Fakt ist, die Umstellung auf Remote-Arbeit macht die Unternehmen anfälliger für Cyber-Bedrohungen und Gefahren durch Cyberkriminelle, deren Fantasie keine Grenzen kennt. Angreifer haben ihren Fokus längst auf die neuen Umstände umgestellt und versuchen beispielsweise gezielt mittels Social-Engineering-Kampagnen über schwach gesicherte mobile Endpunkte in Unternehmensnetzwerke einzudringen. Um sich gegen Cyber-Attacken und gezielten Missbrauch zu schützen und Angriffe zu verhindern, müssen sich Unternehmen verstärkt auf das Management der IT-Sicherheit fokussieren und entsprechende Sicherheitstools implementieren.

Den Ergebnissen nach waren zwar viele Unternehmen aktiv, aber es gibt noch deutlich Luft nach oben. 58 Prozent der Unternehmen haben für das Management der Home-Office-Arbeitsplätze in zusätzliche IT-Management- und Sicherheitstools investiert. 14 Prozent der Unternehmen sehen sich noch nicht umfassend geschützt und werden weitere zusätzliche IT-Sicherheitstools implementieren. Nur ein Viertel der Unternehmen fühlt sich trotz Remote-Arbeit ausreichend gesichert und greift auf die bereits bestehenden Sicherheitstools zurück.

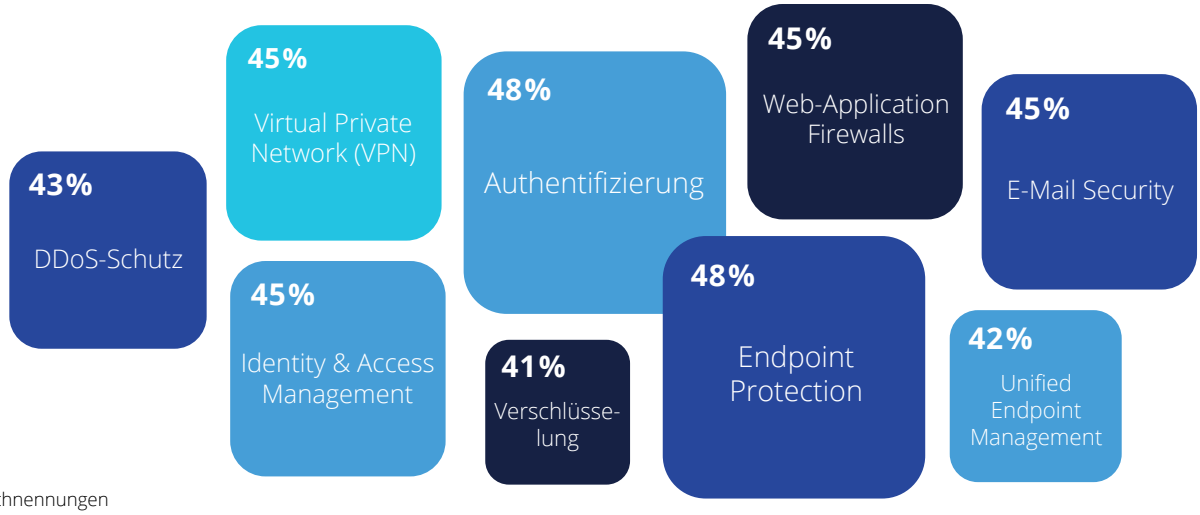
> Fast jedes zweite Unternehmen gab an, dass durch die Krise Management- und Security-Lösungen an Bedeutung gewonnen haben.

Für die Gewährleistung eines sicheren Fernzugriffs setzen Unternehmen verstärkt auf die Multifaktor-Authentifizierung (MFA). Mit dieser Methode macht man es Angreifern exponentiell schwieriger, sich Zugang zu fremden Konten zu verschaffen, auch wenn diese an das richtige Passwort gelangt sind. So würde nach dem normalen Login-Vorgang, ähnlich wie im Online-Banking, noch ein einmaliger Sicherheitscode zur Verifizierung nötig sein, beispielsweise über ein Hardware-Token, das eigene Smartphone oder gar mithilfe von Biometrie wie etwa einem Fingerabdruck. 48 Prozent legen den Fokus verstärkt auf Endpoint Protection. Mit der Anzahl an mobilen Geräten steigt gleichzeitig die Zahl potenzieller Einfallstore für Attacken.

Einsatz von Management- und IT-Sicherheitstools



Management und IT-Security-Lösungen, die durch Home-Office wichtiger geworden sind



Mehrfachnennungen

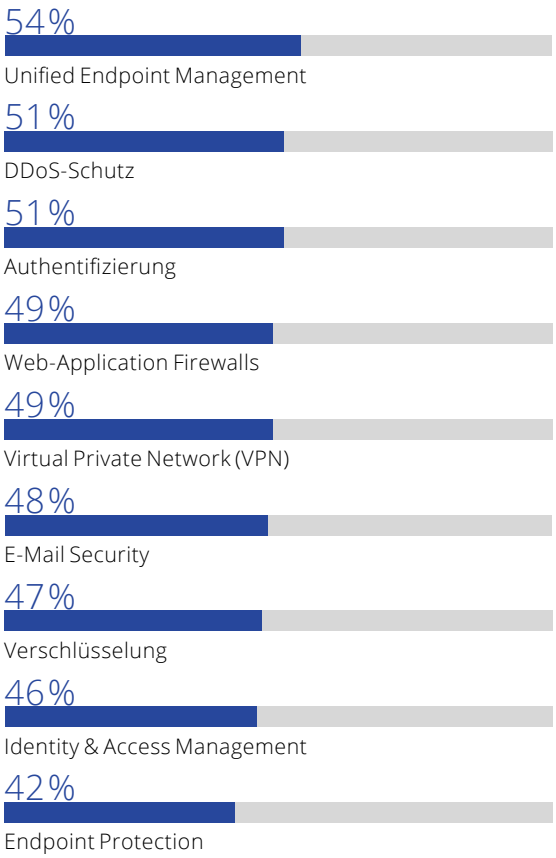
Das Unified Endpoint Management, die einheitliche Verwaltung von Geräten, macht es den IT-Abteilungen leichter, alle Geräte zu administrieren und abzusichern. Unified Endpoint Management sorgt auch für die Konformität der Geräte. Wichtig bei Home-Office-Regelungen ist die saubere Trennung von Privatem und Arbeitsbereich. Für IT-Entscheider ist es wichtig, beim Management der Geräte neben der Endgerätesicherheit auch die Endgerätesichtbarkeit und Endgeräte-Compliance zu verfolgen. Darüber hinaus haben weitere Methoden, wie Identity & Access Management, Firewalls, E-Mail Security oder DDoS Protection durch Corona an Bedeutung gewonnen.

Die Relevanz der Lösungen ist die eine Seite, die Umsetzung die andere. Niemand kann sich jederzeit in absoluter Sicherheit wiegen. Es gilt das maximal Mögliche für die Sicherheit des Unternehmens umzusetzen. Bei nahezu jedem zweiten Unternehmen zeigt sich Luft nach oben. Größte Defizite gibt es beim Management der Endgeräte. Doch auch bei allen anderen Lösungen gibt es reichlich Verbesserungspotenzial und noch jede Menge zu tun. Mängel treten auch bei der Umsetzung des DDoS-Schutzes und auch bei Authentifizierungslösungen auf. Gute Cloud-Anbieter bieten DDoS Protection und Monitoring bzw. Logging Services bereits per Default an.

Mit der Umsetzung von Verschlüsselungstechniken bzw. mit der Umsetzung von E-Mail-Security-Lösungen sind 47 Prozent unzufrieden. Angriffsvektoren gibt es viele.

Personen und Organisationen, die diese Vektoren mit immer ausgefeilteren Techniken ausnutzen, lauern an „jeder Ecke“. Unternehmen, die sich fahrlässig den Gefahren aussetzen, müssen mit schweren finanziellen Konsequenzen rechnen oder Schäden fürs Image befürchten.

Verbesserungspotenziale bei der Umsetzung

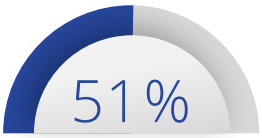


Mehrfachnennungen | Umsetzung „wenig zufrieden“ bis „sehr unzufrieden“

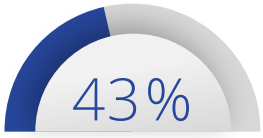
Sicherstellung datenschutzkonformer Remote-Arbeit

Nicht nur die IT-Sicherheit, auch der Datenschutz spielt bei Remote-Arbeit eine außerordentlich wichtige Rolle. 40 Prozent der befragten Unternehmen geben an, dass die Anforderungen an den Datenschutz und die Compliance komplexer geworden sind. Unternehmen setzen daher eine Reihe von Maßnahmen für datenschutzkonformes Arbeiten im Home-Office um. Jedes zweite Unternehmen führt Schulungen zum Datenschutz und zur Geheimhaltung durch. Die Schulungen sollten verschiedene Themen abdecken - von der Gestaltung des Arbeitsplatzes, dem abhörsicheren Führen von Video- und Webkonferenzen bis hin zum Umgang mit Daten – auch dem strikten Trennen von privaten und beruflichen Daten. 41 Prozent sensibilisieren verstärkt ihre Mitarbeiter und schärfen ihr Bewusstsein durch Aufzeigen möglicher Gefahren. Interne Richtlinien zur Datenhandhabung haben 36 Prozent der befragten Unternehmen erstellt. Diese beinhalten zum Beispiel das Verbot von Ausdrucken sensibler Dokumente. 43 Prozent haben einen Datenschutzbeauftragten ernannt. Er fungiert als interner Ansprechpartner im Unternehmen für Datenschutzfragen, bspw. wenn es um Meldungen von Datenpannen oder Geräteverlust geht. Neben umfangreichen Schulungsprogrammen für das Sicherheitsbewusstsein stehen auch technische Lösungen zur Verfügung. 38 Prozent der Unternehmen nutzen Richtlinien zum sicheren Umgang mit Passwörtern, wie zum Beispiel die Anzahl der Zeichen und Sonderzeichen, die Sperrung nach Fehlversuchen oder regelmäßige Wechselintervalle.

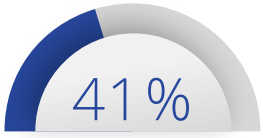
Maßnahmen für datenschutzkonforme Remote-Arbeit



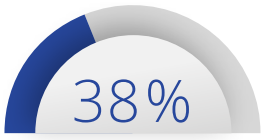
Schulung der Mitarbeiter zum Datenschutz und zur Geheimhaltung



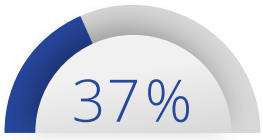
Ernennung eines Datenschutzbeauftragten/interner Ansprechpartner für Datenschutzfragen



Sensibilisierung der Mitarbeiter/ Schärfung des Gefahrenbewusstseins



Nutzung von Richtlinien oder technischen Maßnahmen für sichere Passwörter



Einschränkung von eigenständigen SW-Installationen

Mehrfachnennungen

Home-Office – gekommen, um zu bleiben

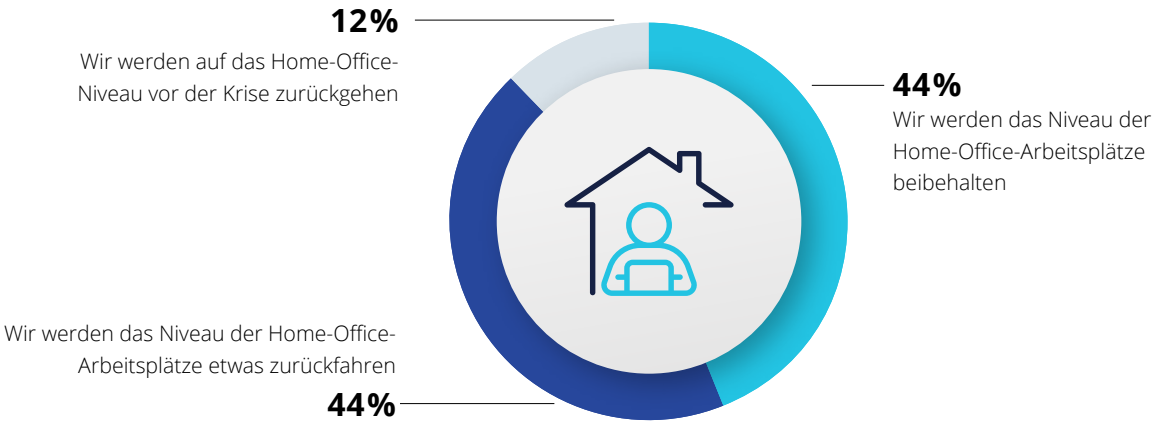
Eine logische Konsequenz aus der fortschreitenden Digitalisierung ist die neue Art und Weise des Arbeitens. Flexibleres Arbeiten und Home-Office-Modelle werden daher in vielen Unternehmen auch nach überstandener Pandemie weiter Bestand haben. Abgesehen von manchen Home-Office-Szenarien inklusive Homeschooling und Kinderbetreuung, wirkt sich mobiles Arbeiten für Arbeitnehmer und Arbeitgeber in der Regel vorteilhaft aus. Für Arbeitgeber entfallen lange Arbeitswege, sie profitieren von Kosten- und Zeitersparnis, von erhöhter Flexibilität und einer besseren Work-Life-Balance. Arbeitgeber können dagegen Miet- und Betriebskosten einsparen, steigern ihre Attraktivität und profitieren darüber hinaus von produktiveren Arbeitsweisen ihrer Mitarbeiter.

Nach langer Skepsis gegenüber Home-Office-Arbeitsplätzen haben inzwischen viele Arbeitgeber die Vorteile erkannt und wollen nach der Krise an diesen Modellen festhalten. Nahezu neun von zehn Unternehmen werden auch nach überstandener Pandemie ihren Mitarbeitern weiterhin Home-Office-Möglichkeiten bieten.

44 Prozent der Unternehmen geben an, das derzeitige Niveau an Home-Office beizubehalten, weitere 44 Prozent tendieren dazu, das hohe Level an Home-Office-Arbeitsplätzen nach der Pandemie wieder etwas zurückzufahren. Doch nur 12 Prozent der Betriebe werden auf das Niveau vor der Krise zurückgehen.

Im Rahmen der bereits genannten Herausforderungen und unter Berücksichtigung der zukünftigen Home-Office-Strategie werden die Unternehmen auch weiterhin den Schwerpunkt ihrer Investitionen auf Cloud-Technologien (41 Prozent), IT-Security-Lösungen (37 Prozent), mobile Endgeräte (37 Prozent) und Remote Access setzen. Ein gutes Viertel der Unternehmen plant Investitionen in Server- und Storage-Infrastruktur und in Daten-Backups.

Zukünftige Home-Office-Strategie



Fazit

Unternehmen haben die Krise als Chance genutzt, um die Digitalisierung voranzutreiben. Wer die Strukturen für Heimarbeit bereits vorher geschaffen hat, der konnte sich schnell an die neue Situation anpassen. Andere haben dagegen in notwendige Strukturen und in digitale Prozesse investiert, um die Geschäftsabläufe aufrechtzuerhalten.

Viele Unternehmen sind durch die Krise dazu übergegangen, die Weichen zu stellen, damit existierende bzw. zusätzliche digitale Prozesse auch außerhalb der Arbeitsstätte reibungslos funktionieren. Cloud-Technologien spielen dabei eine wesentliche Rolle. Die Cloud als hardwarelose Alternative für den Endanwender sorgt für zügige Bereitstellung virtueller Rechen- und Speicherkapazitäten. Zudem können Unternehmen auf diese Weise schnell und einfach Software Services nutzen und diese für flexibles Arbeiten mobil einsetzen. Der „langanhaltende Atem" der Pandemie zwingt viele Unternehmen Kosten zu sparen. Auch damit einhergehend werden sich viele Unternehmen mit Cloud-Modellen befassen und auf eigene kostenintensive Hardware verzichten.

Die flächendeckende Sicherstellung der Home-Office-Arbeitsplätze hat den Druck auf IT-Entscheider erhöht und sie vor zusätzliche Probleme gestellt. Dies betrifft sowohl die Digitalisierung der Office-Umgebung als auch das IT-Operations- und Application-Management. Eine der größten Herausforderungen ist und bleibt die Gewährleistung der IT-Sicherheit. Um all die Probleme zu meistern und die IT-Infrastruktur erfolgreich zu gestalten, bedarf es der Unterstützung und Expertise erfahrener und vertrauenswürdiger europäischer Dienstleister und Anbieter von Cloud-Infrastrukturen sowie Cloud Service, die mit dem Kunden auf Augenhöhe agieren und einen besonders persönlichen und fachlich hochstehenden Kundenservice bieten.

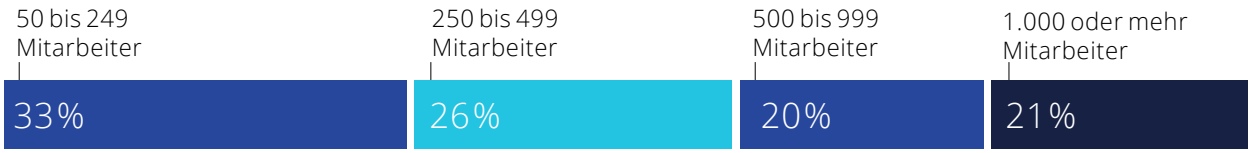
Cloud-Modelle werden sich in den Unternehmen weiter etablieren, ob mit oder ohne Pandemie. Im Zuge dieses Wandels der IT-Infrastruktur können sich für die Unternehmen auch zahlreiche neue Geschäftsmodelle entwickeln.

Studiendesign und Stichprobe

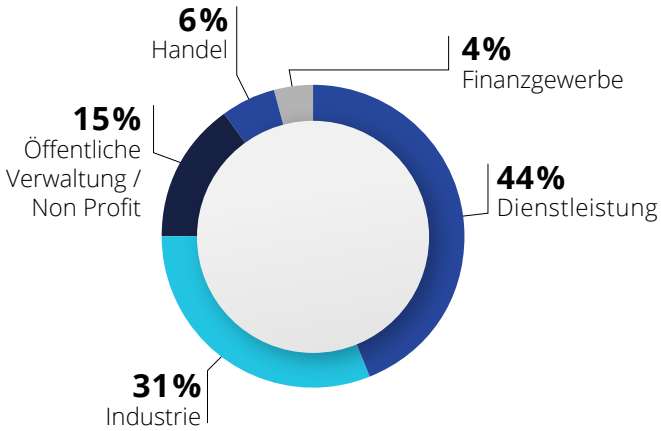
Die Studie „Krisensicher dank Cloud-Technologien“ wurde von der techconsult GmbH im Auftrag von IONOS konzipiert und durchgeführt. 204 Unternehmen wurden im deutschsprachigen Raum zum Einfluss der Corona-Krise auf die IT-Infrastruktur befragt. Die Befragung erfolgte über einen Online-Fragebogen.

Die Stichprobe umfasste Unternehmen ab 50 Mitarbeiter aller Branchen. Ansprechpartner waren in erster Linie IT-Leiter, IT-Fachbereichsleiter, sowie Entscheidungsträger für die IT-Infrastruktur und den Betrieb digitaler Arbeitsplätze geht.

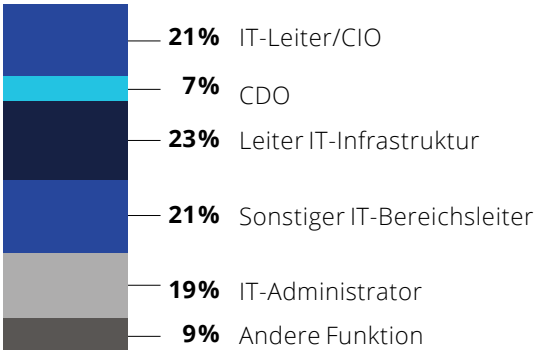
Mitarbeitergrößenklassen



Branchen



Ansprechpartner



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

Weitere Informationen

KONTAKT FÜR MEHR INFORMATIONEN

Verena Bunk
Senio Analyst

Telefon: +49 561 8109 141
E-Mail: **verena.bunk@techconsult.de**

Baunsbergstr. 37
techconsult GmbH
D-34131 Kassel

IMPRESSUM

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Web: **www.techconsult.de**
Telefon: +49 561 8109 0
Telefax: +49 561 8109 101

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 IONOS

IONOS ist mit mehr als acht Millionen Kundenverträgen der führende europäische Anbieter von Cloud-Infrastruktur, Cloud-Services und Hosting-Dienstleistungen. Das Produktportfolio bietet alles, was Unternehmen benötigen, um in der Cloud erfolgreich zu sein: von Domains über klassische Websites und Do-It-Yourself-Lösungen, Online-Marketing-Tools bis hin zu vollwertigen Servern und einer IaaS-Lösung.

IONOS Cloud ist die europäische Cloud-Alternative und Teil von IONOS. Das Produktportfolio umfasst eine IaaS Compute Engine mit eigenem Code Stack für Virtualisierung, Managed Kubernetes, eine Private Cloud powered by VMware sowie S3 Object Storage und gemanagten DDoS-Schutz für größere Betriebssicherheit. Mit diesem Angebot bietet IONOS etablierten mittelständischen und großen Unternehmen, regulierten Industrien, der Digitalwirtschaft und dem öffentlichen Sektor alle notwendigen Dienste und Services, um in und mit der Cloud erfolgreich zu sein.

IONOS ist Teil der börsennotierten United Internet AG (ISIN DE0005089031). Zur IONOS Markenfamilie gehören STRATO, Arsys, Fasthosts, home.pl, InterNetX, SEDO, United Domains und World4You.

1&1 IONOS SE
Elgendorfer Str. 57
56410 Montabaur, Germany

IONOS Cloud Kontakt
Telefon: +49 30 57700 850
Telefax: +49 30 57700 8598
E-Mail: **info@cloud.ionos.de**
Website: **https://cloud.ionos.de**

EINE STUDIE VON

techconsult
The IT Market Analysts

IN ZUSAMMENARBEIT MIT

IONOS