IDC PERSPECTIVE

Die Data-Protection-Strategie von Microsofts Office 365: Die Vernachlässigung von Datensicherung und -wiederherstellung stellt ein Risiko für Resilienz, Kontinuität und Produktivität dar

Archana Venkatraman

EXECUTIVE SNAPSHOT

ABBILDUNG 1

Executive Snapshot: Die Data-Protection-Strategie Microsofts Office 365

Thema dieser IDC Perspective ist die Data-Protection-Strategie für Microsofts Office 365 (O365). Office 365 wird in immer breiterem Umfang eingesetzt, da Großunternehmen rasch Tools für Produktivität und Zusammenarbeit auf Basis von Software as a Service (SaaS) einführen. Ihr Ziel dabei ist die Gewährleistung von Produktivität, digitaler Resilienz und Geschäftskontinuität in der Zeit nach der Coronapandemie. Damit übernimmt Microsoft Office 365 (O365) eine zentrale Rolle für das Geschäft. Folglich ist die Gewährleistung der Sicherheit der O365-Daten für IT-Sicherheit, Compliance und Geschäftskontinuität entscheidend. Keinen eigenen O365-Data-Protection- und -Recovery-Plan zu haben, ist eine riskante Datenstrategie.

Wichtigste Erkenntnisse

- O365 (oder Microsoft 365) umfasst viel mehr als E-Mails: Die Benutzer verwenden immer öfter auch Teams, SharePoint, OneNote und OneDrive. Dieser wachsende Einsatz von O365-Produkten bedeutet eine zunehmende Ausdehnung der Daten in der SaaS-Umgebung.
- Nur 23 % der von IDC befragten Unternehmen verwenden eigenen Angaben zufolge eine spezifische Datensicherung durch ~~Dritte~~ Drittanbieter für ihre O365-Umgebungen. Digital fortschrittliche Unternehmen verfügen eher über einen speziellen O365-Datenschutz als digitale Nachzügler.
- Ohne eine eigene Data-Protection-Strategie setzen sich Unternehmen Gefahren wie Ransomware, versehentlichen Datenlöschungen und anderen Formen von Datenverlusten aus ebenso wie Risiken in Bezug auf Compliance und Datenaufbewahrung sowie Risiken aus der SaaS-Einbindung.

Handlungsempfehlungen

- Bei Übernahme von Cloud-Diensten müssen Unternehmen das „Modell der gemeinsamen Verantwortung“ uneingeschränkt verstanden haben.
- Machen Sie die O365-Datensicherung zu einer wichtigen Priorität, um Resilienz und Geschäftskontinuität zu erhalten.
- Nutzen Sie die nativen Funktionen des SaaS-Anbieters und die Sicherheit auf Infrastrukturebene. Denken Sie dabei allerdings daran, diese durch eine Data-Protection-Architektur eines Drittanbieters zu verstärken, um die SaaS-Übernahme möglichst risikofrei zu gestalten.
- Stellen Sie sicher, dass eine Data-Protection-Strategie auf Enterprise-Niveau Daten über das gesamte fragmentierte Feld der IT hinweg abdeckt, einschließlich lokaler, Multi-Cloud-, SaaS- und Platform-as-a-Service (PaaS)-Umgebungen.

Quelle: IDC, 2020

Dezember 2020, IDC #EUR147031720

SITUATIONSÜBERBLICK

SaaS-Anwendungen wie Microsoft 365 (und die vorherigen Office 365-Versionen) werden als Grundlage für eine modernisierte Mitarbeitererfahrung betrachtet – mit Einführung neuer Möglichkeiten für die Zusammenarbeit und mit der Schaffung einer digitalen Arbeitsplatzarchitektur. E-Mail und Zusammenarbeit auf SaaS-Basis sind im Kontext der Fernarbeit wegen Corona besonders beliebt geworden. Den neuesten Finanzdaten von Microsoft zufolge (1. Quartal 2021) war das Cloud-Geschäft in diesem Quartal der Motor für ein schnelles Umsatzwachstum. Insbesondere der gewerbliche Umsatz mit Office 365 nahm um 21 % zu.

Der letzten Befragung von IDC von Endanwendern zufolge nutzen über 77 % der Unternehmen Microsoft Office 365. IDCs *European Software Survey* vom November 2020 ergab sogar, dass 90 % der Unternehmen in Industrieländern wie Großbritannien O365 einsetzen.

O365: mehr als nur E-Mails

Die Microsoft Office-Umgebung umfasst zahlreiche Anwendungen für Produktivität und Zusammenarbeit, u. a. Microsoft Exchange, Teams, OneDrive, OneNote und SharePoint. Teams ist dabei, sich rasch zu einem entscheidenden Hilfsmittel für die Zusammenarbeit aus dem Homeoffice zu entwickeln. Mehr als 115 Millionen Menschen nutzen Teams täglich (einem Microsoft-Blog vom 16. November 2020 zufolge). Unternehmen streben die Nutzung der Teams-Umgebung als Plattform für die Entwicklung unternehmensspezifischer Anwendungen und Dienste an.

Microsoft selbst sieht Teams als zentral für die O365-Innovation und verbessert das Angebot wie folgt:

- Annäherung von Power Platform an die Teams-Umgebung
- Möglichkeit zur Erstellung, Freigabe und Verfolgung von Daten durch die Benutzer direkt in Teams
- Bereitstellung von Tools für Entwickler (wie das Microsoft Teams Toolkit für Visual Studio und Visual Studio Code) als Basis für die Entwicklung ihrer Teams-Anwendungen

Teams ist überall. Microsofts Finanzbericht für das 4. Quartal 2020 zufolge haben mehr als 1.800 Unternehmen über 10.000 Teams-Benutzer und mehr als 70 Unternehmen haben über 100.000 Teams-Benutzer. Eine Branche, in der Teams immer häufiger eingesetzt wird, ist das Gesundheitswesen. Beispielsweise hat das britische Gesundheitssystem NHS Microsoft 365 gewählt, um 1,2 Millionen Mitarbeitern die neuestens Tools für Produktivität und Zusammenarbeit bereitzustellen – mit dem Ziel besserer Behandlungsergebnisse für Patienten. Zusätzlich hat sich der Benutzerstamm von Microsoft 365 E5 im Vergleich zum Vorjahr mehr als verdoppelt.

Mit dem wachsenden Einsatz von O365 nimmt auch die Datenmenge in dieser Umgebung zu.

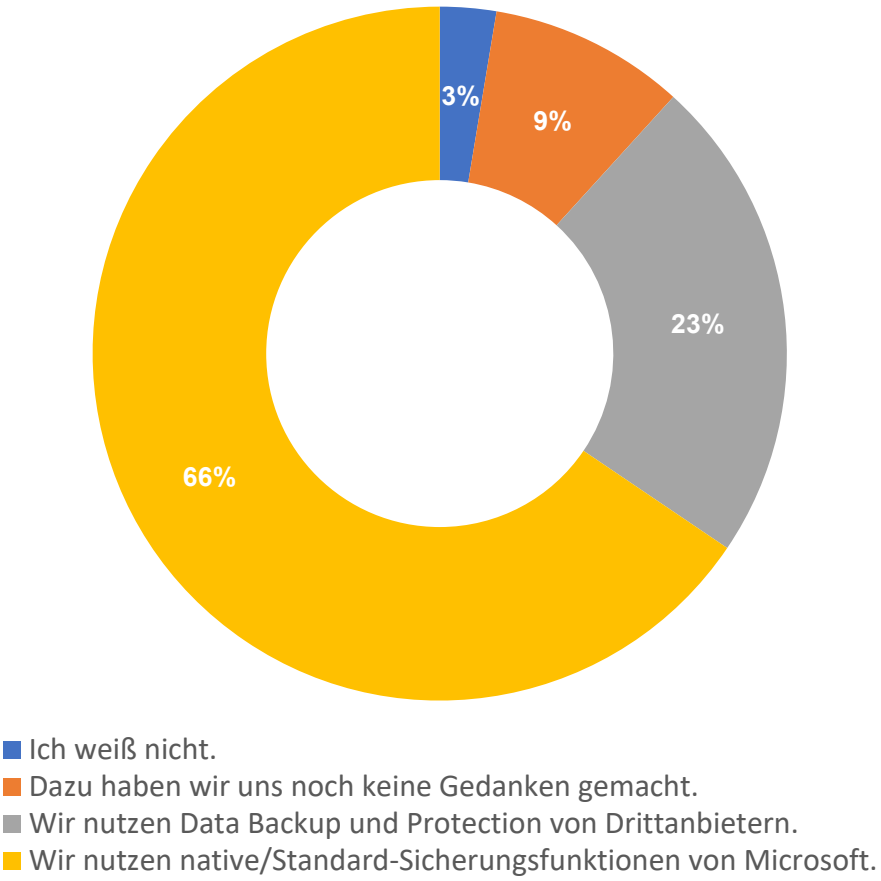
Dedizierte Datensicherung ist häufig ein nachträglicher Gedanke

Während O365 so schnell zentral für die Geschäftsproduktivität wird, bleibt eine Data-Protection-Strategie für die O365-Umgebung weiter ein nachträglicher Gedanke, wie in Abbildung 2 dargestellt.

ABBILDUNG 2

O365-Data-Protection-Strategie europäischer Unternehmen

F. Wie erfolgen Sicherung, Aufbewahrung und Wiederherstellung von Daten in O365-Umgebungen (Exchange, SharePoint, OneDrive, Teams etc.) in Ihrem Unternehmen?



Quelle: IDCs *European Software Survey*, November 2020 (n = 634)

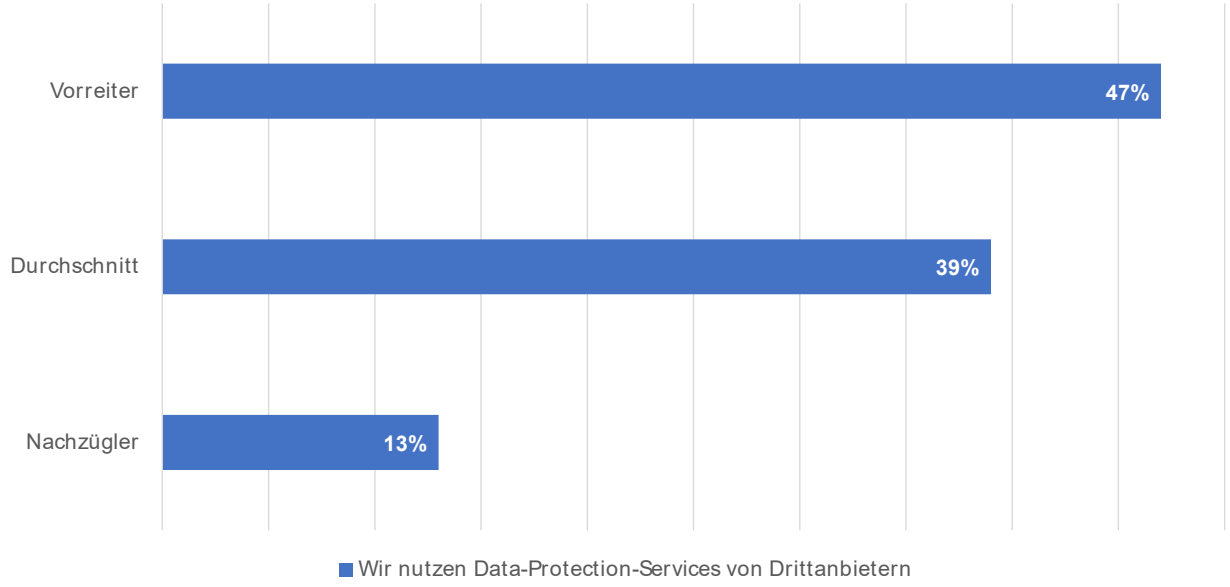
Die Befragungsergebnisse zeigen:

- Nur 23 % der von IDC befragten Unternehmen nutzen eigene Backup- und Recovery-Services von Drittanbietern, um ihre O365/M365-Umgebungen zu schützen.
- 77 % der M365- und O365-Nutzer verlassen sich auf die nativen Funktionen oder haben die Datensicherung ihrer cloud-basierten E-Mail- und Zusammenarbeitsumgebung bisher nicht in Erwägung gezogen.

Die Wahrscheinlichkeit, dass eine eigene SaaS-Data-Protection-Technologie zur Gewährleistung der Geschäftskontinuität und Datenwiederherstellung vorliegt, ist bei digitalen Vorreitern größer als in Unternehmen, die bei ihren digitalen Transformationsinitiativen weniger weit fortgeschritten sind (siehe Abbildung 3).

ABBILDUNG 3

Nutzung eigener Data-Protection-Services: digitale Vorreiter verglichen mit Nachzüglern



Quelle: IDCs *European Software Survey*, November 2020 (n = 634)

Hinsichtlich der Branchen galt, dass nur Befragte aus Banken und Versicherungen, Telekommunikation sowie von Serviceanbietern über robuste Data-Protection-Strategien für ihre O365- und M365-Umgebungen verfügten.

RAT FÜR TECHNOLOGIE-EINKÄUFER

Microsoft verbessert die Funktionen und die Sicherheit in seinen O365-Umgebungen ständig. Beispielsweise können mit neuen Funktionen wie Microsoft Endpoint Data Loss Prevention (DLP) Datenverluste auf Endgeräten leichter verhindert werden. Zudem wurden Funktionen für ein besseres Management von DLP-Warnhinweisen aufgenommen. Auch die SLAs für ausfallfreie Zeiten, Konsistenz und Verfügbarkeit werden laufend verbessert.

IDC ist der Überzeugung, dass die nativen Datensicherungsmöglichkeiten und die standardmäßige Datenaufbewahrung in O365 zwar eine gute Basis liefern, aber dennoch nicht alle Anforderungen an Compliance und Geschäftskontinuität abdecken.

Die tatsächliche Gefahr ist jedoch, dass viele Unternehmen die nativen Möglichkeiten als vollkommen ausreichend für die benötigte Datensicherung ansehen. Im Gespräch mit O365-Benutzern stellte IDC fest, dass viele Benutzer die Service-Level Agreements (SLAs) zur Verfügbarkeit von Microsoft mit einer Datensicherungsstrategie verwechseln. Andere sehen keine Notwendigkeit, über Datensicherung für die Cloud nachzudenken, weil es sich um eine „andersartige“ Technologie handelt.

Die Adaption von O365 ohne Datensicherung auf Unternehmensebene ist riskant

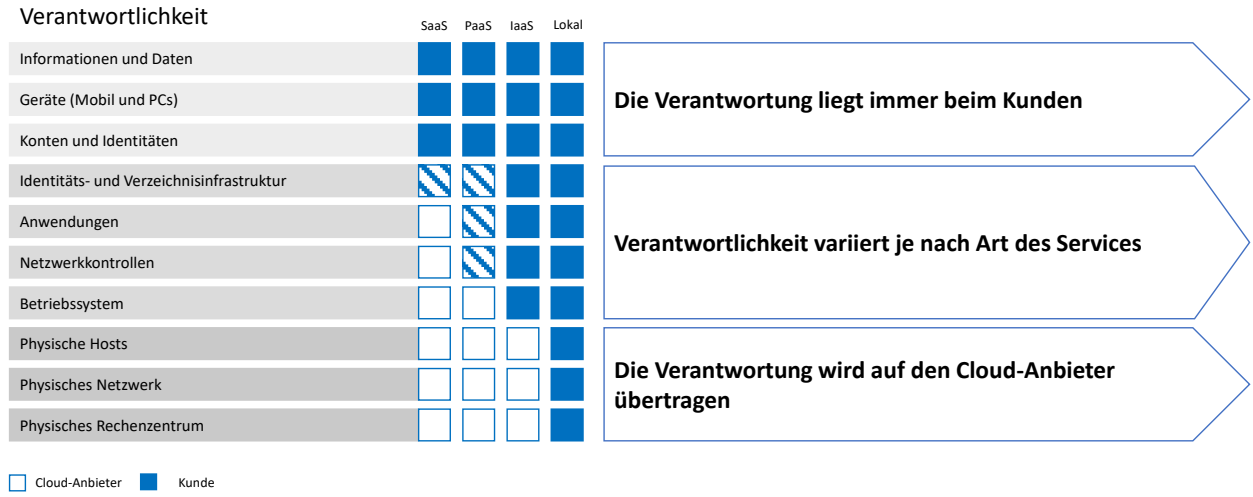
Unabhängig davon, ob die Daten lokal oder in der Cloud-Infrastruktur bzw. SaaS wie O365 vorliegen: Die Verantwortung für die Datensicherung liegt beim Kunden oder beim Dateneigentümer – also Ihnen.

Modell der gemeinsamen Verantwortlichkeit

Wenn Unternehmen öffentliche Cloud-Dienste einsetzen, müssen sie ein uneingeschränktes Verständnis des „Modells der gemeinsamen Verantwortlichkeit“ haben: also die Aufteilung der Verantwortlichkeiten auf einen Cloud-Anbieter (Auftragsverarbeiter) und einen Cloud-Benutzer (Datenverantwortlicher).

ABBILDUNG 4

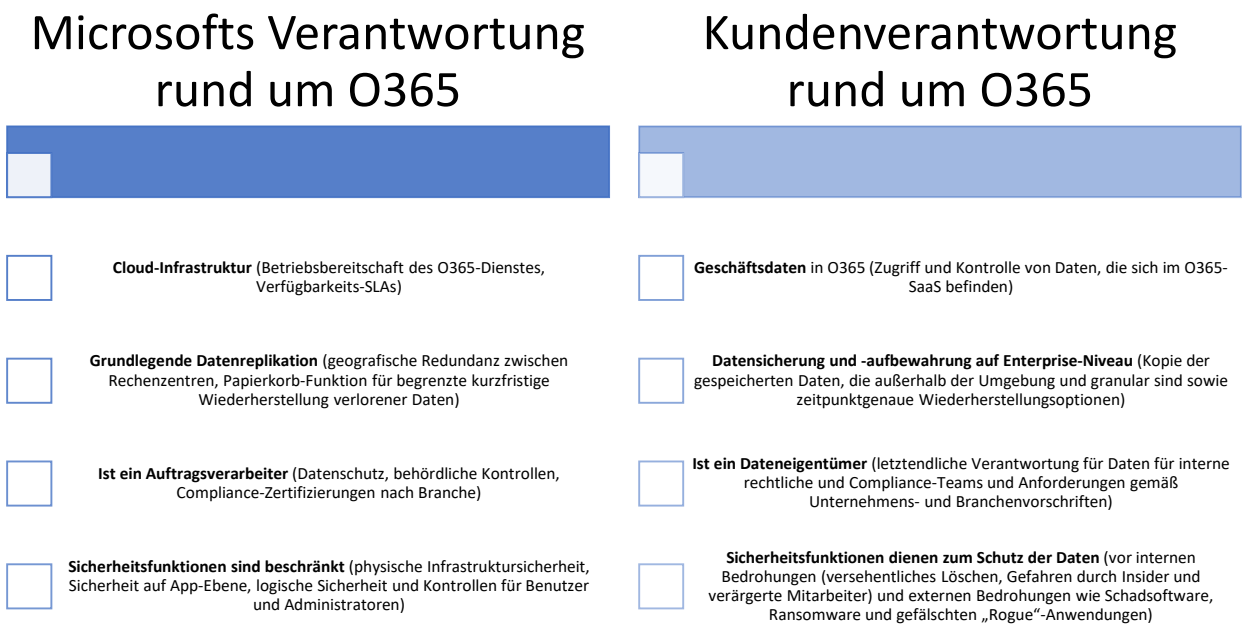
Modell der gemeinsamen Verantwortlichkeit in SaaS-, PaaS-, IaaS- und lokalen Umgebungen



Quelle: Microsoft, 2020

ABBILDUNG 5

Modell der gemeinsamen Verantwortlichkeit für Microsoft Office 365-Anbieter/-Kunden auf einen Blick



Quelle: IDC, 2020

Leitlinien für Cloud-Anbieter und Tipps für bewährte Verfahren

Der Microsoft-Servicevertrag empfiehlt die Datensicherung und -wiederherstellung durch Drittanbieter. Unter Abschnitt 6b, Serviceverfügbarkeit, heißt es:

> Wir bemühen uns, die Dienste am Laufen zu halten. Alle Online-Dienste leiden jedoch gelegentlich unter Störungen und Ausfällen. Im Fall eines Ausfalls oder einer Unterbrechung des Diensts sind Sie möglicherweise vorübergehend nicht in der Lage, Ihre Inhalte abzurufen. Es wird empfohlen, die Inhalte und Daten regelmäßig zu sichern, die Sie in den Diensten oder während der Verwendung von Drittanbieter-Apps und -Diensten speichern.

Native Funktionen für eDiscovery und Aufbewahrung für juristische Zwecke in M365 sind nicht äquivalent mit Datensicherung und -wiederherstellung

Die Funktionen der Aufbewahrung für juristische Zwecke von Microsoft 365 sind robust, aber sie können eine Datensicherungs- und -wiederherstellungsstrategie nicht vollständig ersetzen. Beispielsweise betonten Kunden in Gesprächen mit IDC, dass sie schnellen Datenzugriff und schnelle Datenwiederherstellung brauchen, um den Bedarf bei eDiscovery erfüllen zu können. Sie müssen Kosten und IT-Aufwand für die Wiederherstellung bestimmter Daten in unterschiedlichen Formaten und Geschwindigkeiten je nach Gerät berücksichtigen. Dabei kann die Verwendung einer nativen Funktion zur Aufbewahrung für juristische Zwecke Einschränkungen bedeuten: Möglicherweise ist sie für die Wiederherstellung versehentlich gelöschter Daten oder die schnelle Wiederherstellung in großem Umfang nicht geeignet. Eine eigene Datensicherung, die das gesamte Datenmanagement, inklusive SaaS-Daten, abdeckt, kann Unternehmen hinsichtlich der Aufbewahrung für juristische Zwecke umfassend unterstützen, wenn Daten über Enterprise-Workloads (auch O365-Daten) erfasst und Kosten kontrolliert werden können.

Bestehende Risiken

Da die Verantwortlichkeit und die unterstützende Technologie von Microsoft auf Infrastruktur, logische Sicherheit und Verfügbarkeit beschränkt sind, bedeuten fehlende Drittanbieter-Datensicherungspläne für Unternehmen folgende Risiken:

- **Datenverlust, versehentliche Löschung und Sicherheitsverstöße:** Auch O365 kann Opfer von Sicherheitsverstößen werden. Es ist durch interne Bedrohungen (z. B. versehentliche Datenlöschung, Eingriffe verärgerter Mitarbeiter oder Zugriff von ehemaligen Mitarbeitern) und externe Bedrohungen (z. B. Schadsoftware oder erpresserische Ransomware) gefährdet. IDCs *European Multicloud Survey* für 2020 zufolge waren für Kunden Ransomware, rasant steigende Kosten und die Sicherung von SaaS-Daten die wichtigsten Herausforderungen für die Datensicherung.
- **Risiken für Datenaufbewahrung und Einhaltung gesetzlicher Vorschriften:** Microsoft bietet die 90-tägige Aufbewahrung von Daten an. Allerdings erfüllt dies nicht die strengeren Datenspeicherungsvorgaben bestimmter Branchen wie Finanzdienstleistungen, Gesundheitswesen, Einzelhandel und der öffentlichen Hand. Datensicherung durch Drittanbieter kann Unternehmen helfen, eigene Aufbewahrungsvorgaben je nach geschäftlichen Anforderungen festzulegen und die europäischen Datenschutzbestimmungen einzuhalten.
- **Fehlende Kontrolle über die Daten in hybriden Umgebungen:** Die vollständige Überwachung von und Kontrolle über Daten ist eine Priorität der Geschäftsführung und ein erster Schritt hin zu einem datengesteuerten Unternehmen. Ohne Datensicherung haben Unternehmen keine Exit-Strategie oder die Freiheit hinsichtlich Risiken der Konzentration auf bestimmte SaaS-Anbieter.

RAT FÜR TECHNOLOGIE-EINKÄUFER

Wird Datensicherung nicht auf SaaS-Umgebungen wie M365 oder O365 ausgedehnt, gefährden Unternehmen ihre Daten durch Compliance-Probleme, Datenverlust, Sicherheitslücken und Risiken für die Geschäftskontinuität.

Datensicherung ist für schnell wachsende SaaS wie O365 nicht mehr optional – sondern für IT-Sicherheit und Kontrolle über die eigenen Daten Pflicht.

Die meisten Data-Protection-Anbieter haben Datensicherung und -wiederherstellungen für O365-Umgebungen im Angebot und bauen ihr Datensicherungsangebot ständig um weitere O365-Dienste aus. Bei Investitionen müssen Unternehmen sicherstellen, dass die von ihnen gewählte Datensicherungslösung Folgendes bietet:

- **Flexibilität und Auswahl:** Das Unternehmen sollte die Freiheit haben, vorhandene lokale Kapazitäten oder Cloud-Backup-Speicherorte für O365 zu nutzen.
- **Funktionen der Enterprise-Klasse:** Die Lösung sollte inkrementelle Sicherung, granulare Wiederherstellung, Automatisierung und richtlinienbasierte Aufbewahrung bieten.
- **Servicebreite:** Die Lösung sollte eine große Bandbreite von M365-Umgebungen sichern können, u. a. E-Mails, Teams, SharePoint etc.
- **Komplementäres Angebot zu O365:** Sie sollte tiefe Integration zwischen O365 und der vorhandenen Datensicherungsumgebung des Kunden bieten.
- **Innovation:** Zusätzliche Sicherheitsfunktionen wie Zugriffssteuerung, SaaS-Nutzungskennzahlen und Multifaktor-Authentifizierung für mehr Sicherheit sollten gegeben sein.
- **Skalierung:** Die Backuplösung muss die Möglichkeit der Skalierung in beide Richtungen ohne Kapitalkosten bieten, wenn sich der geschäftliche Bedarf und die Datennachfrage ändern und SaaS im Unternehmen breiter übernommen wird.

MEHR ERFAHREN

Ähnliche Recherchen

- *Western Europe Public Cloud IaaS Storage Market Forecast, 2019-2024: The COVID-19 Pandemic Keeps IaaS Storage Investments Resilient* (IDC #EUR146999320, November 2020)
- *Commvault Brings Metallic SaaS Data Protection to Europe Amid Growing Demand for Cloud-Based Backup* (IDC #IcEUR146988220, November 2020)
- *IDC FutureScape: Worldwide Data and Analytics 2021 Predictions* (IDC #US46920420, Oktober 2020)

Zusammenfassung

Thema dieser IDC Perspective ist die Data-Protection-Strategie von Microsoft für Office 365. Die Einführung von SaaS-Anwendungen, v. a. von Microsoft Office 365, nimmt an Fahrt auf. Die Nutzung weitet sich zudem über Exchange hinaus auf weitere Dienste wie SharePoint, OneDrive und Teams aus, um in der Zeit nach der Pandemie Möglichkeiten für Produktivität und Zusammenarbeit zu eröffnen.

„Obwohl O365 so zum Zentrum der Geschäftsproduktivität wird, bleibt eine Datensicherungs- und -wiederherstellungsstrategie ein nachträglicher Gedanke. Weniger als ein Viertel der O365-Benutzer verfügt über eine eigene Drittanbieter-Datensicherung für O365. Da das Datenvolumen in der O365-Umgebung sich immer weiter ausdehnt, müssen die Unternehmen eines verstehen – ganz unabhängig vom Speicherort der Daten ist der Benutzer für ihre Sicherung verantwortlich," so Archana Venkatraman, Associate Research Director, IDC European Datacenter. „Wenn Unternehmen keine eigene Sicherungs- und Wiederherstellungsstrategie für Daten haben, setzen sie ihre O365-Daten Gefahren wie Ransomware, Datenlöschung und Compliance-Risiken aus. Damit behindern sie ihre eigene Resilienz und Geschäftskontinuität."

Über IDC

International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation sowie der Verbrauchertechnologiemärkte. IDC unterstützt IT-Profis, Geschäftsleute und Investoren bei fundierten Entscheidungen über Geschäftsstrategien und den Einkauf von Technologie. Mehr als 1100 IDC-Analysten in mehr als 110 Ländern bieten globale, regionale und lokale Expertise zu Chancen und Trends in Technologie und Wirtschaft. Seit 50 Jahren bietet IDC strategische Einsichten, um unseren Kunden zu helfen, ihre wichtigsten geschäftlichen Ziele zu erreichen. IDC ist ein Tochterunternehmen von IDG, einem weltweit führenden Medien-, Forschungs- und Veranstaltungs-Technologieunternehmen.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, Großbritannien
+44 208 987 7100
Twitter: @IDC
idc-community.com
www.idc.com