März 2021

MARKTBERICHT

Einstieg in Office 365 Backup

Der globale Wandel zum externen Arbeiten vergrößert die Herausforderungen im Datenschutz. »

Barracuda
Your journey, secured.

Inhalt

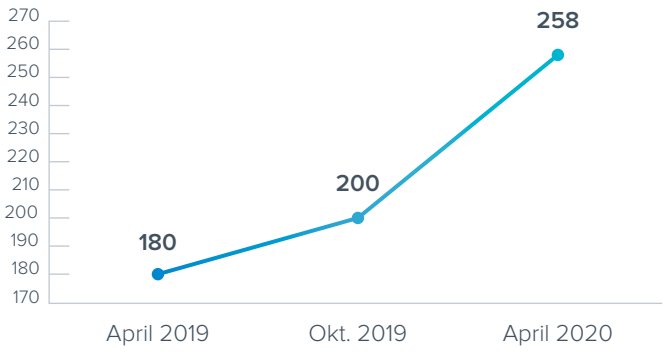
Einführung

Schutz der massiv ansteigenden Datenmengen in Office 365

Die Datenmenge in Microsoft Office 365 wächst rasant an und mit ihr der Bedarf, diese Daten zu schützen.

Office 365 verzeichnet gewaltiges Wachstum, besonders durch die aktuell extern arbeitenden Angestellten. Laut dem Blog „Thexyz“ stieg im März 2020 die Anzahl der Teams-Meeting-Minuten um 380% allein in den ersten 19 Tagen der Pandemie, und zwar von 560 Millionen auf 2,7 Milliarden pro Tag. Im vergangenen April gab es 258 Millionen Lizenzen und 75 Millionen aktive Teams-Benutzer täglich.

0365 Monatlich aktive User (Mio.)



Der durchschnittliche Zuwachs der monatlichen Office 365-Benutzer hat sich von Oktober 2019 bis April 2020 nahezu vervierfacht, was größtenteils an der gesteigerten Nutzung von externer Zusammenarbeit und Absprache im Homeoffice während der Pandemie liegt.

IT-Führungskräfte wissen, wie abhängig ihre Unternehmen von Office 365 sind, und dass sie ihre Lösungen schützen müssen. Oft ist jedoch unklar, welche Schutzfunktionen bereits nativ bei Office 365 enthalten sind.

Tatsächlich empfiehlt Microsoft seinen Kunden, Backup-Lösungen von Drittanbietern zu verwenden, denn das Unternehmen selbst garantiert Ihnen nur die Verfügbarkeit des Dienstes, nicht die Speicherung Ihrer Daten. Und da Microsoft keine nativen Speicherfunktionen bietet, erkennen die Kunden die Beschränkungen möglicherweise erst, wenn es ein Problem gibt.

Es kann auch vorkommen, dass die grundlegenden integrierten Funktionen von Microsoft den Ansprüchen der Kunden nicht gerecht werden; die Wiederherstellung mit nativen Tools kann schwierig und zeitraubend werden. Unternehmen, die ihre schnell wachsenden Datenmengen schützen wollen, haben Bedenken hinsichtlich der Vollständigkeit von Backup- und Speicherlösungen, der Sicherheit, der Compliance und natürlich der Benutzerfreundlichkeit der Lösung für die Bereitstellung und Verwendung.

In diesem Bericht sehen wir uns die Bedenken und Vorlieben von IT-Fachleuten bezüglich Office 365, Datensicherheit, Backup und Wiederherstellung, SaaS-Lösungen (Software-as-a-Service) und weiteren Themen an.

Methodik

Barracuda hat das unabhängige Marktforschungsunternehmen Centropy mit einer Umfrage unter IT-Entscheidungsträgern beauftragt, die für die Cloud-Infrastruktur ihres Unternehmens zuständig sind. Beteiligt waren **1.828 IT-Entscheidungsträger** in Unternehmen ab 50 Angestellten in den **USA, im EMEA- und APAC-Raum**. Die Umfrage wurde im Januar 2021 durchgeführt.

Zentrale Ergebnisse

ERKENNTNIS NR. 1

Datenschutz ist der Schlüssel zur Abwehr von Angriffen und Verlusten – von außen wie auch von Insidern.

Daten müssen vor Angriffen von außen, zum Beispiel mit Ransomware, und vor internem Verlust, beispielsweise durch versehentliches oder absichtliches Löschen geschützt werden. Die Umfrageteilnehmer legen für beide Szenarien großen Wert auf Datenschutz und Datensicherheit.

Ransomware-Angriffe kommen vielleicht nicht täglich vor, sind aber immer präsent. Angesichts der Ransomware-Themen in den Nachrichten verwundert das nicht, denn die meiste Berichterstattung befasst sich mit den Folgen und den Angriffsmethoden, lässt jedoch außen vor, worauf der Angriff abzielte. So soll verhindert werden, dass diese Informationen bei zukünftigen Angriffen genutzt werden.

Obwohl sie nicht wissen, worauf genau es die Angreifer abgesehen haben, waren sich die Befragten sehr wohl bewusst, dass Office 365 von Ransomware ins Visier genommen werden kann. 72% der Umfrageteilnehmer machten sich Sorgen über einen solchen Angriff. Die größten Sorgen waren in den USA zu finden (83%), die niedrigsten im EMEA-Raum (67%); der APAC-Raum lag mit 73% dazwischen.

Wenn wir berücksichtigen, dass über die Hälfte der Befragten schon einmal Opfer von Ransomware waren, überraschen diese Zahlen nicht. Auch die geografischen Daten passen in dieses Bild. Fast zwei Drittel der Befragten in den USA (64%) hatten bereits einen Ransomware-Angriff zu verzeichnen; im APAC-Raum waren es 55%, während es im EMEA-Raum gerade einmal 43% der Umfrageteilnehmer traf. Die schweren Folgen einer Unterbrechung der E-Mail-Anwendungen und anderer Lösungen für die Zusammenarbeit sind klar, besonders beim Ausmaß der externen Arbeit.

Ein weiterer Faktor, der die Sorgen um Ransomware weiter befeuert, ist der aktuelle Ransomware-Trend der Datenexfiltration. Dabei werden Daten gestohlen, bevor sie gesperrt werden, und anschließend an den Eigentümer zurück verkauft. Wenn der Dateneigentümer nicht bezahlt, verkauft man die Daten an den höchsten Bieter im Dark Web. Solche Datenpannen sind nicht nur potenziell rufschädigend, sondern oft auch teuer.

Beim Datenschutz sind Sicherheitsmaßnahmen gegen versehentliches oder absichtliches Löschen ein viel größeres Problem und ähnlich bedenklich. Fast 80% der Befragten möchten mehrere Schichten einer rollen-basierten Zugriffskontrolle, um den Zugang zu potenziell schädlichen Maßnahmen wie Datenlöschung und Bereinigung zu beschränken.

Ich mache mir Sorgen, dass Ransomware meine O365-Daten sperren/angreifen könnte.
72% stimmen zu (n=1.793)

Mein Unternehmen hatte bereits einen Ransomware-Angriff zu beklagen.
52% stimmen zu (n=1.741)

Mehrschichtige, rollen-basierte Zugriffskontrolle für Backup-Kopien ist mir wichtig.
79% stimmen zu (n=1.828)

Zentrale Ergebnisse

ERKENNTNIS NR. 2

Unternehmen möchten granulare Wiederherstellung und andere Funktionen, die mit den nativen Fähigkeiten von Microsoft nicht abgedeckt werden.

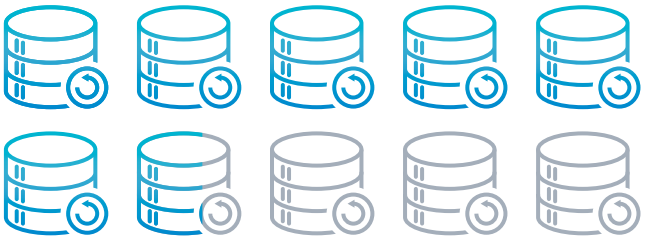
Überraschenderweise hat nur ein Drittel der Befragten eine Backup-Lösung eines Drittanbieters eingeführt. 67% verlassen sich immer noch auf die bei Microsoft integrierte Speicherung und Wiederherstellung gelöschter Ordner, obwohl diese Speicherrichtlinien komplex sind und keine Wiederherstellung einzelner Elemente ermöglichen. Dieser Anteil war am höchsten in den USA, wo 74% der Umfrageteilnehmer beim Backup ausschließlich auf Office 365 setzen. Im Vergleich dazu verfolgen im EMEA-Raum nur 61% der Befragten diesen Ansatz, im APAC-Raum sind es 70%.

Bemerkenswert ist die Feststellung von 81% der Umfrageteilnehmer, dass die Nutzung von Teams Fragen bei der Datenspeicherung aufwerfen würde. Im ersten vollen Monat der Pandemie vermeldete Microsoft beispielsweise einen Anstieg der Teams-Nutzung um 380%.

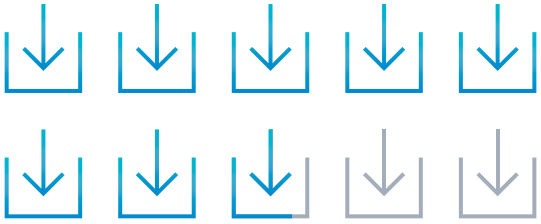
Über 80% der Befragten möchten eine Backup-Lösung, die auch Teams und freigegebene Dateien abdeckt. Außerdem erwarten sie von der Lösung für Office 365 unbegrenzten Speicherplatz und die Möglichkeit, Kopien der wiederhergestellten Elemente herunterzuladen.

Laut einem Bericht der IT Policy Compliance Group ist in drei Viertel der Fälle, bei denen die IT-Abteilung um Wiederherstellung gebeten wird, der Grund dafür ein versehentliches Löschen. Die Suche nach gelöschten Ordnern und die Verwendung der geführten Wiederherstellung von Microsoft sind zeitraubend, schwierig und fehleranfällig. In vielen Fällen muss das gesamte Verzeichnis wiederhergestellt werden, um ein gelöschtes Element zu finden, wobei wiederum neuere Daten überschrieben werden können und möglicherweise neue Probleme entstehen.

Für das Backup und die Wiederherstellung von Office 365-Daten verlasse ich mich ausschließlich auf die integrierten Funktionen von Office 365.
67% stimmen zu (n=1.779)



Mir ist eine granulare Wiederherstellung für Exchange, SharePoint, OneDrive und Teams wichtig.
77% stimmen zu (n=1.828)



Darum ist es nicht überraschend, dass Backup-Funktionen für Office 365-Daten einschließlich granularer Wiederherstellung sehr gefragt sind.

Fast genauso viele gaben an, ihnen sei die Wiederherstellung von E-Mail-Postfächern für andere Standorte oder Benutzer wichtig. Mit den nativen Funktionen von Microsoft lässt sich das nicht bewerkstelligen. Wenn jemand ein Unternehmen verlässt, steht nach 30 Tagen dort nur noch „gelöschter Benutzer“ und die damit verbundenen Daten können weder an einen anderen Ort noch einen anderen Benutzer gesendet werden.

Die Benutzerfreundlichkeit erstreckt sich auch auf die Anmeldung. 76% der Befragten gaben an, eine Lösung zu wollen, welche Single sign-on mit Azure Active Directory unterstützt.

Außerdem wünschen sich drei Viertel der Umfrageteilnehmer eine Lösung, mit der sie tägliche Berichte aller Backups, Wiederherstellungen und Exporte abrufen können. Das klingt vielleicht nicht nach bahnbrechenden Funktionen, doch die Nachverfolgung des Backups ist wichtig. Zum einen kann sie dabei helfen, Frühwarnzeichen verdächtiger Datenaktivitäten in Systemen zu erkennen.

...doch die Nachverfolgung des Backups ist wichtig. Zum einen kann sie dabei helfen, Frühwarnzeichen verdächtiger Datenaktivitäten in Systemen zu erkennen.

Zentrale Ergebnisse

ERKENNTNIS NR. 3

Datenschutz ist ebenso ein Sicherheitsanliegen wie auch eine regulatorische Frage.

Für viele Unternehmen hat der Aufbewahrungsort ihrer Daten sicherheitstechnische und regulatorische Auswirkungen. Diese Daten umfassen oft auch sensible Informationen, die geschützt werden müssen. Diese Schutzmaßnahmen müssen spezifische Verordnungen und Bestimmungen von Datenschutzbehörden erfüllen. Außerdem gibt es in verschiedenen Ländern Gesetze zur Datenaufbewahrung, die bestimmen, wie Daten über ihre Bürger oder Einwohner erfasst, benutzt und gespeichert werden dürfen. Diese Anforderungen umfassen Zeiträume für die Datenspeicherung und können auch Vorgaben beinhalten, dass bestimmte Daten auf Anfrage zu löschen sind.

Die Bestimmungen können je nach Land variieren, daher müssen die Unternehmen in Abhängigkeit vom Geschäftsgebiet verschiedene Anforderungen erfüllen – bei multinational aufgestellten Firmen keine leichte Aufgabe. In der Europäischen Union müssen zum Beispiel bestimmte Arten sensibler Daten an festgelegten physischen oder geografischen Orten gespeichert werden.

Nahezu 7 von 10 Befragten machen sich wegen dieser Compliance Sorgen. Verständlich, wenn die Bußgelder bei Verstößen entweder bis zu 20 Mio. € oder einen Prozentsatz der Jahresumsätze des letzten Jahres betragen können.

Ich mache mir Sorgen, ob meine Daten außerhalb meiner Region als Backup gesichert werden (Datenstandort).
69% stimmen zu (n=1.787)

Interessanterweise machen sich Befragte in den USA am meisten Sorgen (80%) darüber, ob ihre Daten außerhalb ihrer Region als Backup gesichert werden. Im Vergleich dazu äußerten 69% der Teilnehmer im APAC-Raum und 65% der Teilnehmer im EMEA-Raum diesbezüglich Bedenken. Der Grund dafür ist sehr wahrscheinlich die variierende Komplexität dieser Anforderungen in unterschiedlichen Regionen. In Frankreich und Deutschland sind die Bestimmungen zum Beispiel umfassender, während sie in den USA und Indien nur für bestimmte Branchen oder Datenarten gelten. Die Ergebnisse weisen darauf hin, dass in Ländern mit variierenden Regeln die Menschen sich größere Sorgen machen, da sie weniger Gewissheit hinsichtlich einer korrekten Handhabung haben.

Dasselbe Muster zeigt sich auch bei den Sorgen zum Datenschutz. Ganze 85% der Befragten in den USA stimmen zu, dass sie das Thema besorgt, während im APAC-Raum 75% der Befragten und im EMEA-Raum 64% der Befragten zustimmen. Das lässt vermuten, dass die IT-Führungskräfte in Ländern, die schon einige Jahre die DSGVO eingeführt haben, mehr Sicherheit im Umgang mit Datenschutzgesetzen haben. Im Vergleich dazu variieren die Datenschutzverordnungen in den USA immer noch von einem Bundesstaat zum nächsten, sodass dort IT-Führungskräfte wahrscheinlich mehr Bedenken zur Einhaltung dieses Stückwerks aus Bestimmungen und wechselnden Anforderungen haben.

Ich mache mir Sorgen um die Einhaltung von Datenschutzbestimmungen.
73% stimmen zu (n=1.802)

Zentrale Ergebnisse

ERKENNTNIS NR. 4

Unternehmen bevorzugen eine SaaS-Lösung, die schnell und einfach einzurichten und zu nutzen ist.

Unternehmen haben mit Office 365 eine bewusste und weitreichende Entscheidung für SaaS und die Cloud getroffen. Man könnte fast von einer Veränderung im Denken sprechen, wenn Unternehmen von einem lokalen Ansatz zu Cloud-Lösungen wie Exchange Online wechseln. Das Wachstum von Office 365 unterstreicht, wie fundiert und verbreitet diese Entscheidung ist.

Bei der Betrachtung von Lösungen haben IT-Führungskräfte nicht nur großes Interesse an SaaS-basierten Backups, sie erwarten auch eine nahezu unmittelbare Erfüllung ihrer Bedürfnisse. Knapp 8 von 19 wollen direkt nach der Registrierung ihre ersten Backups ausführen. Ein weiterer wichtiger Punkt für SaaS ist der Wunsch, keine eigene Hardware oder Software bereitstellen zu müssen. Fast drei Viertel der Befragten maß dieser Aussage große Bedeutung bei.

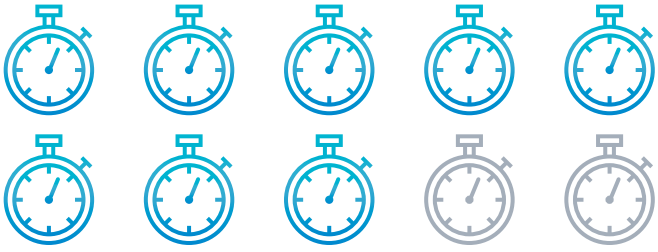
Die Umfrageteilnehmer möchten ihre Daten in der Cloud aufbewahren und 77% gaben an, ihre Office 365-Daten am liebsten in Azure speichern zu wollen. Leistung ist ein Grund und es überrascht somit nicht, dass 76% der Befragten auch der Meinung sind, dass eine enge Beziehung zwischen Microsoft und dem Backup-Anbieter essenziell ist. Die Befragten in den USA waren in diesen beiden Punkten am deutlichsten und stimmten zu jeweils 83% und 86% zu.

IT-Fachleute betonten auch die Attraktivität einer Komplettlösung gegenüber einer Reihe beliebter Lösungen, die separate Lizenzen für Backup und Cloud-Speicher verlangen. Neben den potenziell höheren Kosten bedeuten Einzellösungen auch mehr Verwaltungsaufwand, was Unternehmen möglichst vermeiden möchten.

SaaS-Backups für O365 – d. h., ohne Hardware- oder Software-Bereitstellung meinerseits – ist für mich wichtig.
74% stimmen zu (n=1.772)

Eine einfache Komplettlösung für Lizenzen – im Gegensatz zu einzelnen Lizenzen für Speicher- und Rechenlösungen – ist für mich wichtig.
79% stimmen zu (n=1.787)

Auf die Möglichkeit, mich zu registrieren und direkt mit dem Backup zu beginnen, lege ich großen Wert.
80% stimmen zu (n=1.805)



Fazit

IT-Führungskräfte weltweit suchen eine Cloud-native SaaS-Backup-Lösung für Office 365 mit großem Funktionsumfang und hoher Benutzerfreundlichkeit, die schnell eingerichtet und betriebsbereit ist.

Der Schutz der Office 365-Daten ist eine stetig wachsende Anforderung und Unternehmen suchen nach umfassenden, benutzerfreundlichen Backup-Lösungen. Das Wachstum der Office 365-Daten wird nicht nur durch die zunehmenden Benutzerzahlen verursacht, sondern auch durch die Art der externen Arbeit, die größtenteils auf SharePoint, OneDrive und Teams basiert.

Unternehmen fördern den Einsatz von Anwendungen zur Zusammenarbeit, da sie die Produktivität in diesem Umfeld steigern und auch beim Protokollieren der erledigten Arbeit helfen können. Allerdings sinkt dieser Wert rapide ohne ein Backup, denn die nativen Speicherfunktionen von Microsoft sind kein Backup. Kunden stellen oft einen Mangel notwendiger Funktionen für die Wiederherstellung und anderer Funktionen für das Tagesgeschäft fest.

Viele Unternehmen stellen fest, dass diese nativen Speicherfunktionen viel zu wünschen übrig lassen. Die Befragten zeigten eine starke Vorliebe für granulare Speicherung; die Möglichkeit, E-Mail-Postfächer von Benutzern für andere Standorte oder Benutzer wiederherzustellen; und mehrere Schichten rollen-basierter Zugriffskontrolle. Mehr als die Hälfte der Befragten wünscht sich diese Funktionen, verlässt sich allerdings immer noch auf die native Speicherung von Microsoft, die das nicht bieten kann.

Benutzerfreundlichkeit ist eine essenzielle Anforderung. Einfache Lizenzvergabe und schnelle Bereitstellung machen die Entscheidung für das Backup von einem Drittanbieter noch attraktiver und beseitigen mögliche Einstiegshürden. Gleichzeitig bilden Bedenken zu Datenschutz und Compliance weitere Anreize dafür, die richtigen Datenschutzmaßnahmen umzusetzen.

Schließlich ist auch die passende Plattform, die sich in ihre bestehende Microsoft-Infrastruktur einfügt, eine wichtige Voraussetzung für IT-Fachleute. Viele von ihnen sind von einer lokalen Microsoft-Umgebung umgezogen, als sie die Vorteile einer Cloud-nativen SaaS-Plattform erkannten. Die Vorteile der Datenspeicherung in der Cloud über den gesamten Lebenszyklus, darunter bessere Leistung, niedrigere Gesamtbetriebskosten und kein Wartungsaufwand, zeigen ein Verständnis vom Mehrwert der Cloud.

Benutzerfreundlichkeit ist eine essenzielle Anforderung. Einfache Lizenzvergabe und schnelle Bereitstellung machen die Entscheidung für das Backup von einem Drittanbieter noch attraktiver und beseitigen mögliche Einstiegshürden.

Anhang

ERKENNTNIS NR. 1

Datenschutz ist der Schlüssel zur Abwehr von Angriffen und Verlusten – von außen wie auch von Insidern.

Ich kenne ein Unternehmen, das einen Ransomware-Angriff erlitt und Schwierigkeiten mit der Wiederherstellung hatte.
66% stimmen zu (n=1.758)

ERKENNTNIS NR. 2

Unternehmen suchen nach einer umfassenden Backup-Lösung, die auch benutzerfreundlich ist.

Mir ist eine Backup-Lösung mit unbegrenztem Speicherplatz wichtig.
84% stimmen zu (n=1.794)

Mir ist es wichtig, E-Mail-Postfächer für einen anderen Standort oder Benutzer wiederherstellen zu können.
79% stimmen zu (n=1.828)

Die Möglichkeit, eine Kopie der wiederhergestellten Elemente herunterzuladen, ist mir wichtig.
84% stimmen zu (n=1.792)

Single sign-on mit Verzeichnisdiensten zur Verwaltung meiner Backup-Lösung ist mir wichtig.
76% stimmen zu (n=1.797)

Ich möchte tägliche Berichte meiner Backups, Wiederherstellungen und Exporte abrufen können.
75% stimmen zu (n=1.828)

ERKENNTNIS NR. 4

Unternehmen bevorzugen SaaS-Lösungen, die auf ihre vorhandene Infrastruktur für Office 365 aufbaut.

Ich lege Wert auf eine Backup-Lösung, die auf Azure läuft und Office 365-Daten in Azure speichert.
75% stimmen zu (n=1.828)

Mir ist eine enge Beziehung zwischen meinem Backup-Anbieter und Microsoft sehr wichtig.
76% stimmen zu (n=1.793)

Über Barracuda

Barracuda ist bestrebt, die Welt zu einem sichereren Ort zu machen und überzeugt davon, dass jedes Unternehmen Zugang zu Cloud-fähigen, unternehmensweiten Sicherheitslösungen haben sollte, die einfach zu erwerben, zu implementieren und zu nutzen sind.

Barracuda schützt E-Mails, Netzwerke, Daten und Anwendungen mit innovativen Lösungen, die im Zuge der Customer Journey wachsen und sich anpassen.

Mehr als 200.000 Unternehmen weltweit vertrauen Barracuda, damit diese sich auf ein Wachstum ihres Geschäfts konzentrieren können.

Weitere Informationen finden Sie unter barracuda.com.

Barracuda
Your journey, secured.