451 Research
Pathfinder Paper

November 2024

Einkaufsleitfaden : Datenschutz für Microsoft 365

In Auftrag gegeben von

veeam

S&P Global
Market Intelligence

Inhalt

Zusammenfassung **3**
Wichtigste Ergebnisse 3

SaaS-Datenschutz wird zunehmend zum Problem **4**

SaaS-Datenschutz von Drittanbietern ist auf dem Vormarsch **5**
Abbildung 1: SaaS-Kunden nutzen Drittanbieter von Backups 5
Gemeinsame Verantwortung 5
Drei verschiedene Möglichkeiten zur Umsetzung 6
Backup-Software 6
Backup-Dienst 6
Managed BaaS 6

Worauf Sie achten sollten **7**
Anpassung des Backup 7
Wiederherstellungskriterien 8
Services und Support 8

Künftige Aspekte **9**
Beziehung zum SaaS-Anbieter 9
Großes Plattformspektrum 9
Keine Anbieterbindung 10

Über den Autor **11**

Zusammenfassung

Microsoft 365 ist die Grundlage wichtiger Workloads der meisten Unternehmen, und die hohen Kosten für Ausfälle und Datenverluste haben die Bedeutung von Datenschutztools wie Backups drastisch erhöht.

Die SaaS-Bereitstellung (Software-as-a-Service) von Microsoft 365 bringt besondere Überlegungen und Herausforderungen mit sich, die Unternehmen bei der Bewertung von Datenschutzangeboten berücksichtigen müssen. In diesem Leitfaden werden die wichtigsten Funktionen erläutert, die Kunden bei der Bewertung von Backup-Angeboten berücksichtigen sollten, und es wird untersucht, wie die Entwicklung des SaaS-Marktes in naher Zukunft Entscheidungen über Hybrid- und Multicloud-Infrastrukturen beeinflussen könnte.

Wichtigste Ergebnisse

- **Ausfälle werden immer kostspieliger.** Die durchschnittlichen Kosten von Ausfällen sind in dieser jüngsten Studie stetig von 1,56 Millionen US-Dollar im Jahr 2022 auf 2,33 Millionen US-Dollar gestiegen. Etwa 47 % der Ausfälle kosten mehr als 1 Million US-Dollar, gegenüber 36 % in der Iteration dieser Studie im Jahr 2023. Ausfälle führen zu zahlreichen Folgen, darunter Produktivitätsverluste der Mitarbeiter, Datenverluste, Umsatzeinbußen und verlorene Kundentreue. Sicherheitsvorfälle, einschließlich Ransomware, waren eine der Hauptursachen für Ausfälle.
- **Der Schutz von SaaS-Daten entwickelt sich ständig weiter.** Ein Drittel (33 %) der Befragten nutzt Cloud-to-Cloud-Datenschutz von Drittanbietern für ihre SaaS-Daten, während 32 % sich beim Datenschutz auf ihren Cloud-Anbieter verlassen. Die Befragten nennen Microsoft 365 (67 %) am häufigsten als SaaS-Plattform, die einen Backup-Schutz benötigt, gefolgt von Google Workspace (46 %) und Salesforce (40 %). Nur 5 % der Befragten geben an, dass sie ihre SaaS-Anwendungen nicht sichern, was eine inkrementelle Verbesserung von 6 % im Jahr 2023 und 9 % im Jahr 2022 darstellt.

SaaS-Datenschutz wird zunehmend zum Problem

Die Häufigkeit und die Kosten von Ausfällen veranlassen Unternehmen, ihren Datenschutz und ihre Ausfallsicherheit zu verbessern. Der Datenschutz für SaaS-Workloads ist zu einem Hauptanliegen geworden, da Plattformen wie Microsoft 365, Salesforce und Google Workspace für die meisten Unternehmen wichtige Produktions-Workloads unterstützen.

Die aktuellen Trends haben den Datenschutz für SaaS für alle Unternehmen unerlässlich gemacht, unabhängig von der Größe.

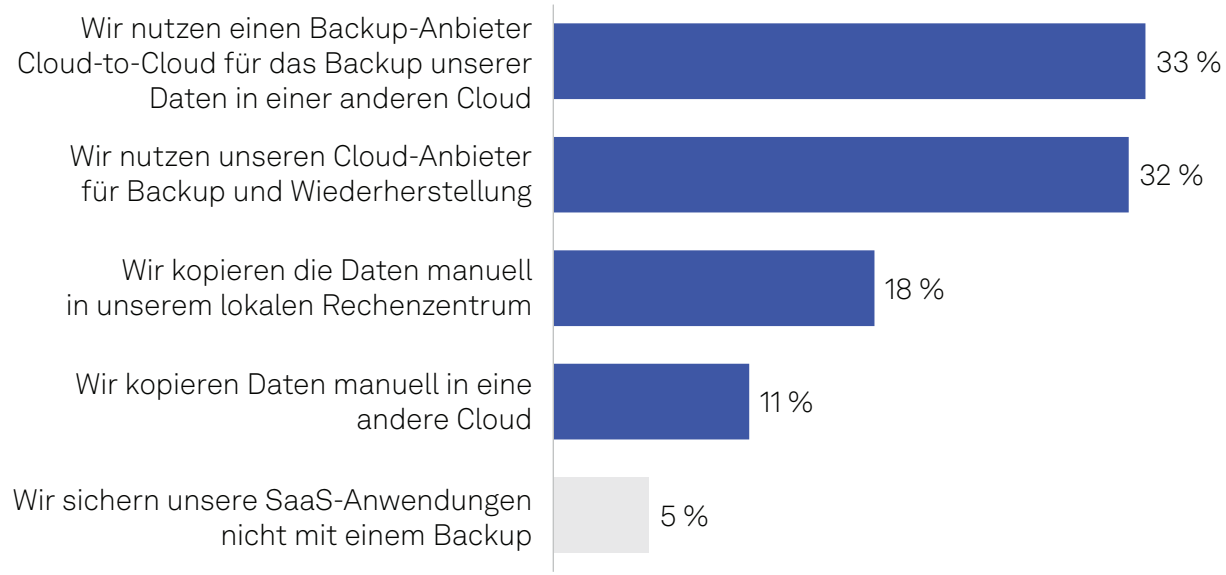
Ausfälle sind häufig und kostspielig: In den meisten Unternehmen kam es zu einem erheblichen Ausfall, der zu Datenverlust oder Produktivitätsverlusten der Mitarbeiter führte. Zwei Drittel (67 %) der Befragten haben schon einmal einen Ausfall erlebt, und mehr als 30 % haben in den letzten zwei Jahren einen Ausfall erlebt. Die Befragten geben an, dass die Kosten, die durch Ausfälle verursacht werden, von durchschnittlich 1,56 Millionen US-Dollar im Jahr 2022 auf 2,33 Millionen US-Dollar im Jahr 2024 gestiegen sind, was einem Anstieg von 49 % in den letzten zwei Jahren entspricht. Fast die Hälfte der jüngsten Ausfälle (47 %) kostete mehr als 1 Million US-Dollar, gegenüber 36 % im Jahr 2023.

Ausfälle von SaaS-Diensten und Sicherheitsvorfälle sind die Hauptursachen für Ausfälle: Ausfälle von SaaS- und Public-Cloud-Diensten verursachten ein Viertel der jüngsten Ausfälle bei den Umfrageteilnehmern, was den Bedarf an Verbesserungen der Ausfallsicherheit unterstreicht. Ein Backup eines Drittanbieters kann Probleme auf der Ebene des SaaS-Anbieters nicht beheben, jedoch könnte ein lokales Backup es den Mitarbeitern ermöglichen, wichtige Daten zu lokalisieren und darauf zuzugreifen, während die SaaS-Cloud nicht verfügbar ist. Sicherheitsprobleme wie Ransomware (28 %) sind eine weitere Hauptursache für Ausfälle. Daten und Workloads, die in SaaS ausgeführt werden, können durch einen Ransomware-Angriff oder einen anderen Sicherheitsvorfall gelöscht, verändert oder verschlüsselt werden, wenn SaaS-Anmeldeinformationen gestohlen werden.

Die Unternehmen sind auf der Suche nach Datenschutz-Tools für SaaS von Drittanbietern: Nur 5 % der Befragten geben an, dass sie SaaS-Workloads und SaaS-Daten nicht schützen. Ein Drittel der Unternehmen nutzt bereits Datenschutz-Tools von Drittanbietern, um Cloud-to-Cloud-Backups zu erleichtern, während ähnlich viele native Backup-Tools ihres SaaS-Anbieters verwendet (siehe Abbildung 1). Fast ein Drittel (29 %) kopiert Daten manuell in eine andere Cloud oder ein lokales Rechenzentrum, was etwas besser ist als kein Schutz, aber zu einem falschen Sicherheitsgefühl verleiten könnte. Manuelle Kopiervorgänge sind fehleranfällig, insbesondere wenn die selbst entwickelten Tools und Skripte nicht ordnungsgemäß gewartet werden oder wenn die Mitarbeiter, die die Skripte und Tools schreiben, das Unternehmen verlassen, ohne ihre Arbeit zu dokumentieren.

SaaS-Datenschutz von Drittanbietern nimmt zu

Abbildung 1: SaaS-Kunden nutzen Drittanbieter von Backups



Q. Was ist die primäre Datenschutzstrategie Ihres Unternehmens für SaaS-Anwendungen (z. B. Salesforce, Microsoft 365, Google Workspace [ehemals G Suite] usw.)?
xBasis: Alle Befragten (n=427).
Quelle: Voice of the Enterprise: Storage, Disaster Recovery 2024.

Gemeinsame Verantwortung

Bevor sich Unternehmen für ein Datenschutzangebot für Microsoft 365 entscheiden, sollten sie die Zuweisung der gemeinsamen Verantwortung zwischen einem Kunden und dem Anbieter oder Dienstanbieter berücksichtigen.

Unternehmen, die den Großteil der gemeinsamen Verantwortung übernehmen möchten, würden wahrscheinlich dazu neigen, eine lokale Bereitstellung mit Hardware und Software zu erwerben und zu implementieren, die sie kaufen und warten. Zu den Aufgaben des Unternehmens gehören in diesem Fall auch die Erstellung von Datenschutzrichtlinien, die Planung von Backups, Validierungstests für Backups, die Bereitstellung und der Support für die Endbenutzer.

Im Gegensatz dazu würden sich Unternehmen, die möglichst viel an gemeinsame Verantwortung auslagern möchten, wahrscheinlich für eine Managed Backup-as-a-Service (BaaS)-Bereitstellung entscheiden, bei der ihr Dienstanbieter die Implementierung, Bereitstellung und das Lebenszyklusmanagement der genutzten Server, Speichersysteme und Cloud-Speicherdienste übernimmt. Ein Managed BaaS-Anbieter würde auch den täglichen Betriebsaufwand im Zusammenhang mit der Bereitstellung, Validierung und dem Kundensupport für die Implementierung des Datenschutzes übernehmen. Der Kunde würde die Nutzung des Managed BaaS überwachen und Aktualisierungen planen.

Drei verschiedene Möglichkeiten zur Umsetzung

Es gibt grundsätzlich drei Möglichkeiten, Microsoft 365 zu schützen, und jede Methode bietet unterschiedliche Ebenen des Schutzes, der Unterstützung und der Datenkontrolle, um den Anforderungen eines Unternehmens gerecht zu werden.

Backup-Software

Für Unternehmen, die Erfahrung mit der Ausführung von On-Premises-Datenschutz haben, ist ein intern bereitgestelltes Backup-Softwarepaket möglicherweise die bevorzugte nahtlose Option. Unternehmen, die Erfahrung mit dem Betrieb älterer Backup-Infrastrukturen haben, haben eine flachere Lernkurve in Bezug auf die Bereitstellung, Wartung und Optimierung des internen Datenschutzes. Mit ihren Methoden und Richtlinien verringert sich der Bedarf an Schulungen für Mitarbeiter, und diese Unternehmen können vorhandene Speicherressourcen zur Konsolidierung der Backup-Daten nutzen und vermeiden zusätzliche Hardwarekäufe.

Backup-Dienst

Backup-Dienste ermöglichen es Kunden, ihre Microsoft 365-Konten schnell zu schützen, und wären wahrscheinlich für Unternehmen interessant, die nicht über die vorhandene Infrastruktur, die Prozesse und das erfahrene Personal verfügen, um Datenschutzdienste intern auszuführen. Mit Backup-Diensten können Kunden niedrigere Gesamtkosten durch gebündelte Lösungen erzielen, die über wichtige Funktionen wie unbegrenzten Backup-Speicher verfügen.

Dienstanbieter und Sicherungsanbieter bieten derzeit Sicherungsdienste an, und sie bieten in der Regel verschiedene Servicelevel an, die es Kunden ermöglichen, ihre Bereitstellungen basierend auf den Anforderungen der Microsoft 365-Konten anzupassen, die sie schützen. In der Regel sind Add-on-Dienste mit Premium-Funktionen wie beschleunigte Wiederherstellung von Ransomware sind in der Regel für zusätzlichen Schutz verfügbar, wenn gewünscht.

Bei Backup-Diensten werden Backup-Daten in der Regel in der Cloud-Speicherumgebung des Dienstanbieters gespeichert, die möglicherweise nicht für alle Arten von Kunden geeignet ist, unter anderem aufgrund von regulatorischen und datenrechtlichen Anforderungen.

Managed BaaS

Bei einer Managed Backup-as-a-Service (BaaS)-Bereitstellung stellt ein Dienstanbieter die Datenschutzinfrastruktur bereit und verwaltet sie, einschließlich der Backup-Server und des zugehörigen Backup-Speichers. Sicherungsdaten können in einer beliebigen Kombination aus einer lokalen Speicherinfrastruktur, dem Cloud-Speicherdienst des Dienstanbieters oder einer öffentlichen oder privaten Cloud-Umgebung gespeichert werden. Managed Service Provider (MSPs) bieten Fachwissen und Beratung für Unternehmen, die die Verwaltungs- und Betriebsverantwortung für Datenschutzdienste auslagern möchten. Unter den drei Bereitstellungsoptionen übernimmt Managed BaaS das größte Maß an Verantwortung für den Datenschutz, ist aber wahrscheinlich auch mit höheren Gesamtkosten und einem längeren Engagement im Vergleich zu einem Backup-Service verbunden.

Managed BaaS kann im Rechenzentrum oder in einer gemieteten Colocation-Umgebung eines Kunden eingesetzt werden, deshalb sind diese Lösungen attraktiv für Unternehmen in Compliance-sensiblen Branchen wie im Finanz- und im Gesundheitswesen, die möglicherweise nicht bereit oder in der Lage sind, ihre Daten in einer Public Cloud oder bei einem Backup-Dienstanbieter zu speichern.

Worauf Sie achten sollten

Obwohl der Bereich Datenschutz viele ausgereifte und innovative Angebote bietet, kann die Wahl der falschen Plattform die Daten und das Geschäft eines Unternehmens gefährden und zu höheren Kosten führen. Bei der Bewertung jeder Lösung sollten die gängigen bewährten Verfahren berücksichtigt werden. Ein Beispiel ist die 3-2-1-Regel, die vorschreibt, dass Unternehmen drei Kopien von Daten (einschließlich des Originals) speichern müssen, wobei Sicherungen auf zwei verschiedenen Medientypen und eine Kopie extern gespeichert werden müssen. Die Zunahme von Sicherheitsbedrohungen wie Ransomware und die kontinuierliche Weiterentwicklung der Compliance-Anforderungen sind ebenfalls wichtige Faktoren, die den Bedarf an unveränderlichem Speicher und fortschrittlichem Datenmanagement unterstreichen, um zu kontrollieren, wo und wie Daten gespeichert und abgerufen werden.

Bei der Entscheidung, wie Sie die Microsoft 365-Implementierung Ihres Unternehmens schützen möchten, sollten Sie die folgenden wichtigen Funktionen im Blick behalten:

Anpassung des Backups

Die Datenschutzlösungen von Microsoft 365 bieten eine Vielzahl von Anpassungsoptionen, um unternehmensspezifischen Anforderungen gerecht zu werden.

- **Speicherort des Backups:** Bei der Auswahl eines Backup-Dienstanbieters müssen Unternehmen wahrscheinlich die verfügbaren geografischen Speicheroptionen überprüfen, um sicherzustellen, dass die Unternehmensdaten in der am besten geeigneten Region gespeichert werden. Einige Unternehmen haben strenge Anforderungen an die Datenhoheit und Compliance, die sie möglicherweise daran hindern, Daten in bestimmten Ländern zu speichern.
- **Flexible Backup-Auswahl:** Der Geschäftswert und die Wichtigkeit von Daten und Endbenutzerkonten variieren innerhalb eines Unternehmens erheblich, und es ist möglicherweise nicht erforderlich, jedes Konto und jede Workload zu sichern. Eine flexible Backup-Lösung zwingt den Kunden nicht dazu, alle Bereiche des Unternehmens zu sichern, sondern ermöglicht es dem Kunden, einzelne Microsoft 365-Benutzer, Gruppen, SharePoint-Websites und Teams für das Backup auszuwählen.
- **Flexible Terminplanung:** Flexible Backup-Lösungen ermöglichen die Konfiguration des Datenschutzes, um den Anforderungen der Beteiligten gerecht zu werden. Wichtige Konten können z. B. so festgelegt werden, dass Sicherungen alle paar Minuten ausgeführt werden, während Konten mit weniger strengen Anforderungen für tägliche oder wöchentliche Schritte festgelegt werden können. Einige Angebote verfügen über konfigurierbare RPO-Einstellungen (Recovery Point Objective), die den Service Level Agreements (SLA) des Unternehmens entsprechen und die Daten begrenzen, die nach einem Vorfall verloren gehen könnten.
- **Anpassbare Aufbewahrung:** Flexible Lösungen bieten die Möglichkeit, den Aufbewahrungszeitraum für Backups anzupassen. In einigen Fällen, z. B. in stark regulierten Umgebungen, müssen Daten möglicherweise dauerhaft aufbewahrt werden. In anderen Fällen, z. B. in bestimmten finanziellen und rechtlichen Kontexten, möchte ein Unternehmen möglicherweise sicherstellen, dass Backups gelöscht werden, sobald die Daten nicht mehr benötigt werden.
- **Unveränderliches Speichermanagement:** Ein weiteres Schlüsselelement, insbesondere angesichts des zunehmenden Aufkommens von Ransomware, ist die Fähigkeit einer Backup-Plattform, unveränderliche Speicher zu verwalten, um Backups aufzubewahren und sie vor absichtlichem und unbeabsichtigtem Löschen oder Verschlüsseln zu schützen. Für Unternehmen, die ihre Backups in einem Public-Cloud-Speicherdienst speichern möchten, muss die Backup-Plattform Interoperabilität unterstützen, um die Aufbewahrungsdauer zu verwalten. Sicherheitsfunktionen wie die Multi-Faktor-Authentifizierung sollten ebenfalls verfügbar sein, um sicherzustellen, dass ein Eindringling die Unveränderlichkeit nicht einfach deaktivieren und Backups löschen kann.

Wiederherstellungskriterien

Sicherungen sind ohne Wiederherstellungsvorgänge ineffektiv. Unternehmen sollten bei der Bewertung der Wiederherstellungsfunktionen bestimmte Faktoren berücksichtigen:

- **Flexible Optionen zur Datenwiederherstellung:** Ein effektives Backup-Angebot muss Wiederherstellungsoptionen bieten, die den Anforderungen der Beteiligten entsprechen. In einigen Fällen kann eine granulare Datenwiederherstellung erforderlich sein, die es einem Kunden ermöglicht, eine bestimmte Datei, einen Ordner oder eine E-Mail-Nachricht wiederherzustellen, falls diese versehentlich gelöscht oder beschädigt wurde. Im Kontrast dazu kann für eine schnelle Wiederherstellung nach einem groß angelegten Vorfall wie einem Ransomware-Angriff eine Massenwiederherstellung erforderlich sein, um Daten mehrerer Benutzer oder sogar des gesamten Unternehmens wiederherzustellen.
- **Flexibler Wiederherstellungsstandort:** In einigen Fällen kann es wünschenswert sein, Daten an einem anderen Speicherort wiederherzustellen. Wenn beispielsweise ein gekündigter Mitarbeiter Nachrichten und Dateien vor seinem Ausscheiden gelöscht hat, möchte das Unternehmen diese Daten möglicherweise im Posteingang eines Vorgesetzten oder Compliance-Beauftragten oder in einer Dateifreigabe wiederherstellen.
- **Umfassende Anwendungsunterstützung:** Der Umfang des Supports für Anwendungen variiert je nach Backup-Angebot. Unternehmen werden wahrscheinlich eine Lösung wünschen, die alle Aspekte einer Anwendung schützt. Bei Teams würde eine fortschrittliche Backup-Plattform beispielsweise nicht nur die Daten innerhalb der Anwendung schützen, sondern auch Teams-Kanäle, Beiträge und Registerkarten, Teammitgliedschaften und andere relevante Einstellungen. Unvollständige Wiederherstellungen können zu Datenverlusten führen und Endbenutzer dazu zwingen, wertvolle Zeit mit der Neukonfiguration von Anwendungen in ihren bevorzugten Einstellungen zu verschwenden.
- **Erweiterte Suche:** Die Möglichkeit, Daten zu lokalisieren, ist für Wiederherstellungsvorgänge unerlässlich. Bei der Bewertung der Suchfunktionen einer Backup-Plattform sollten Unternehmen darauf achten, wie gut die Suchoberfläche mehrere Kriterien kombinieren kann, um Datensätze einzugrenzen und sich auf die spezifischen Daten zu konzentrieren, die wiederhergestellt werden müssen.
- **Self-Service-Wiederherstellung:** Die meisten Mitarbeiter und praktisch alle Wissensarbeiter sind täglich auf Microsoft 365 angewiesen. Self-Service-Wiederherstellungsportale ermöglichen es Kunden, den Abrufprozess zu initiieren, ohne dass ein menschliches Eingreifen erforderlich ist. Diese Funktion kann den betrieblichen Aufwand und die Anzahl der Anfragetickets zur Datenwiederherstellung, die an einen Helpdesk gesendet werden, erheblich verringern. Die Self-Service-Wiederherstellung kann auch dazu beitragen, dass Mitarbeiter Daten schneller wiederherstellen können, und kann nach Geschäftsschluss erfolgen, wenn weniger IT-Mitarbeiter verfügbar sind.

Services und Support

Das Niveau und die Qualität des technischen Supports sollten ebenfalls ein Faktor bei der Bewertung der Datenschutzoptionen von Microsoft 365 sein. In der Regel werden unterschiedliche Support-Level zu unterschiedlichen Preisen angeboten. Unternehmen sollten die technischen Supportfunktionen eines möglichen Anbieters während des Testzeitraums bewerten, der bis zu 60 Tage dauern kann. Für Unternehmen mit weniger strengen Anforderungen kann ein Standardvertrag für den technischen Support, der Aktualisierungen und Anrufe während der Geschäftszeiten ermöglicht, ausreichend sein. Für Unternehmen mit höheren Resilienzanforderungen kann der Premium-Support Erreichbarkeit der Support-Mitarbeitern rund um die Uhr bieten und auch SLA-Garantien enthalten, um die schnellsten Reaktionszeiten zu gewährleisten.

Künftige Aspekte

Die Datenschutzanforderungen eines Unternehmens in Bezug auf Microsoft 365 können sich ändern, wenn sich die Compliance- und Geschäftsanforderungen weiterentwickeln. Um auch zukünftig Datenschutz zu gewährleisten, sollten folgende Elemente berücksichtigt werden:

Beziehung zum SaaS-Anbieter

Unternehmen sind gut beraten, sich an Datenschutzanbieter und Dienstanbieter für Microsoft 365 zu wenden, die eine enge Beziehung zu Microsoft und dem Produktteam haben. Ein starker Anbieter von Datenschutzlösungen würde über eine Integration mit der API des SaaS-Anbieters verfügen und einen Produktentwicklungszyklus haben, der darauf ausgerichtet ist, neue Funktionen hinzuzufügen und die Plattform zu aktualisieren, um neue API zu nutzen und neue Arbeitslasten und Anwendungen zu schützen, wenn Microsoft 365 erweitert und weiterentwickelt wird.

Microsoft 365 Backup Storage ist ein wichtiger Dienst, den Microsoft entwickelt hat, um Backup-Anwendungen von Drittanbietern zu unterstützen, und Datenschutzplattformen sollten in der Lage sein, ihn zu unterstützen. Microsoft 365 Backup Storage befindet sich in der Cloud-Infrastruktur von Microsoft und deshalb kann der Dienst eine schnelle Wiederherstellung mit lokalen Wiederherstellungsgeschwindigkeiten bieten, was für die Einhaltung der Ziele bei den Wiederherstellungszeiten (RTO) unerlässlich ist, um den Client nach einem Vorfall schnell wieder einsatzbereit zu machen.

Die rasante Entwicklung und wachsende Bedeutung der KI-Funktionalität von Microsoft ist ein weiterer wichtiger Bereich, und Datenschutzanbieter sollten über Programme verfügen, die mit Microsoft Copilot arbeiten und zukünftige KI-Dienste integrieren und schützen.

Großes Plattformspektrum

Um den Datenschutz für alle relevanten Workloads zu vereinfachen, sollten sich Kunden für eine Datenschutzplattform entscheiden, die virtuelle Maschinen, physische Server, Speichersysteme (d. h. Network-Attached Storage) und andere wichtige Ressourcen und Dienste wie Microsoft Entra ID schützen kann. Mit der wachsenden Bedeutung von Cloud-native Workloads werden Unternehmen wahrscheinlich von Plattformen profitieren, die für Kubernetes konzipiert sind und die Skalierbarkeit dieser Architektur nutzen können.

Über Microsoft 365 hinaus möchten Unternehmen weitere SaaS-Plattformen wie Salesforce, Google Workspace und ServiceNow schützen. Mit dem Aufkommen neuer SaaS-Plattformen sollten Datenschutzanbieter über Roadmaps für Erweiterungen verfügen, um den Schutz dieser Anwendungen zu erhöhen, wenn sie an Bedeutung gewinnen.

Keine Anbieterbindung

Kunden sind gut beraten, Datenschutzangebote zu vermeiden, die mit der Bereitstellung von proprietärer Hardware und Software verbunden sind, auf die die Kunden warten müssen. Eine einheitliche Lösung mit End-to-End-Hardware- und Softwareintegration hat möglicherweise Vorteile für die Benutzerfreundlichkeit, die Abhängigkeit von einem einzigen Anbieter für Hardware und Software führt jedoch zu einer Bindung, die es in Zukunft schwieriger machen würde, auf ein anderes Angebot umzusteigen.

Auf der Hardwareseite ist es beispielsweise üblich, dass Kunden wettbewerbsfähige Angebote von Speicheranbietern einholen, um Kosten zu senken. Diese Hebelwirkung würde einer vollständig integrierten Lösung zum Opfer fallen und führt über die Lebensdauer der Bereitstellung zu höheren Ausgaben. Um der einfachen Bereitstellung und Einfachheit eines integrierten oder gebündelten Angebots gerecht zu werden, suchen Unternehmen möglicherweise nach Anbietern und Dienstanbietern mit umfassenden Supportprogrammen, die sie auch dann weiterhin auf hohem Niveau unterstützen, wenn eine Hardware- oder Softwarekomponente geändert oder hinzugefügt wird.

Die Bindung an einen Anbieter ist auch ein Thema bei der Bewertung von Dienstanbietern und Cloud-Speicherdiensten. Unternehmen sollten in Erwägung ziehen, mit einem Anbieter zusammenzuarbeiten, der keine harten Strafen für das Verlassen des Unternehmens erhebt. Kunden würden wahrscheinlich auch von der Zusammenarbeit mit einem Anbieter profitieren, der einen einfachen Wechsel von einem Bereitstellungsmodell zu einem anderen ermöglicht, z. B. einen Übergang von lokaler Software zu BaaS. Anbieter, die es Kunden ermöglichen, bei Bedarf von einem Cloud-Speicherdienst zu einem anderen zu wechseln, können Unternehmen dabei helfen, eine langfristige Anbieterbindung zu verhindern.

Über den Autor

Henry Baltazar

Research Director, Storage

Henry Baltazar ist Forschungsdirektor des 451 Research Storage-Kanals innerhalb von S&P Global Market Intelligence mit Schwerpunkt auf Datenspeicherung. In seiner derzeitigen Position analysiert Henry die Markttrends im Zusammenhang mit den Herausforderungen bei der Speicherung im Bereich Umwelt, Soziales und Unternehmensführung (ESG), der Modernisierung der Infrastruktur und der Ausfallsicherheit. Er veröffentlicht Berichte über Trends in den Bereichen Datenspeicherung, Disaster Recovery und Hybrid Cloud. Er wird in Publikationen wie der MIT Technology Review, Forbes und TechTarget häufig als Fachmann zitiert.

Henry kam durch die Übernahme von 451 Research im Jahr 2019 zu S&P Global Market Intelligence, wo er seit August 2006 als Analyst tätig ist. Nachdem er drei Jahre den Bereich Speicherforschung bei Forrester geleitet hatte, kehrte er 2015 zu 451 Research zurück, um die Aufgaben eines Direktors zu übernehmen und den Bereich Speicher zu leiten. Henry schloss sein Studium an der University of California, Berkeley, mit einem Bachelor in Umweltwissenschaften ab.

Über dieses Papier

Ein Pathfinder-Papier begleitet Entscheidungsträger auf Ihrem Weg zu Problemlösungen im Zusammenhang mit einer bestimmten Technologie oder einem Geschäftsfall. Es analysiert den geschäftlichen Nutzen einer Einführung und empfiehlt eine Reihe von Abwägungen und konkrete nächste Schritte im Entscheidungsprozess.

Über S&P Global Market Intelligence

Bei S&P Global Market Intelligence wissen wir um den Wert von präzisen, detaillierten und aufschlussreichen Informationen. Unser Team von Fachleuten arbeitet mit Kunden zusammen, um deren Perspektiven zu erweitern, mit Zuversicht zu arbeiten und Entscheidungen mit Überzeugung zu treffen. Wir bieten unübertroffene Einblicke und hochmoderne Daten- und Technologielösungen.

S&P Global Market Intelligence ist ein Geschäftsbereich von S&P Global (NYSE: SPGI). S&P Global ist der weltweit führende Anbieter von Kreditratings, Benchmarks, Analysen und Workflow-Lösungen für die globalen Kapital-, Rohstoff- und Automobilmärkte. Mit jedem Produkt, das wir anbieten, helfen wir vielen der renommiertesten Unternehmen der Welt, sich im wirtschaftlichen Umfeld zurechtzufinden, damit sie sofort mit der Planung für die Zukunft beginnen können. Weitere Informationen finden Sie unter www.spglobal.com/marketintelligence.

KONTAKTE

Nord- und Südamerika: +1 800 447 2273
Japan: +81 3 6262 1887
Asien und Pazifik: +60 4 291 3600
Europa, Naher Osten, Afrika: +44 (0) 134 432 8300

www.spglobal.com/marketintelligence
www.spglobal.com/en/enterprise/about/contact-us.html