Zerto

a Hewlett Packard Enterprise company

Einkaufsleitfaden über effektive Datensicherung

3 Schritte zur intelligenten Datensicherung, die jeder IT-Leiter kennen muss

Zerto
a Hewlett Packard Enterprise company

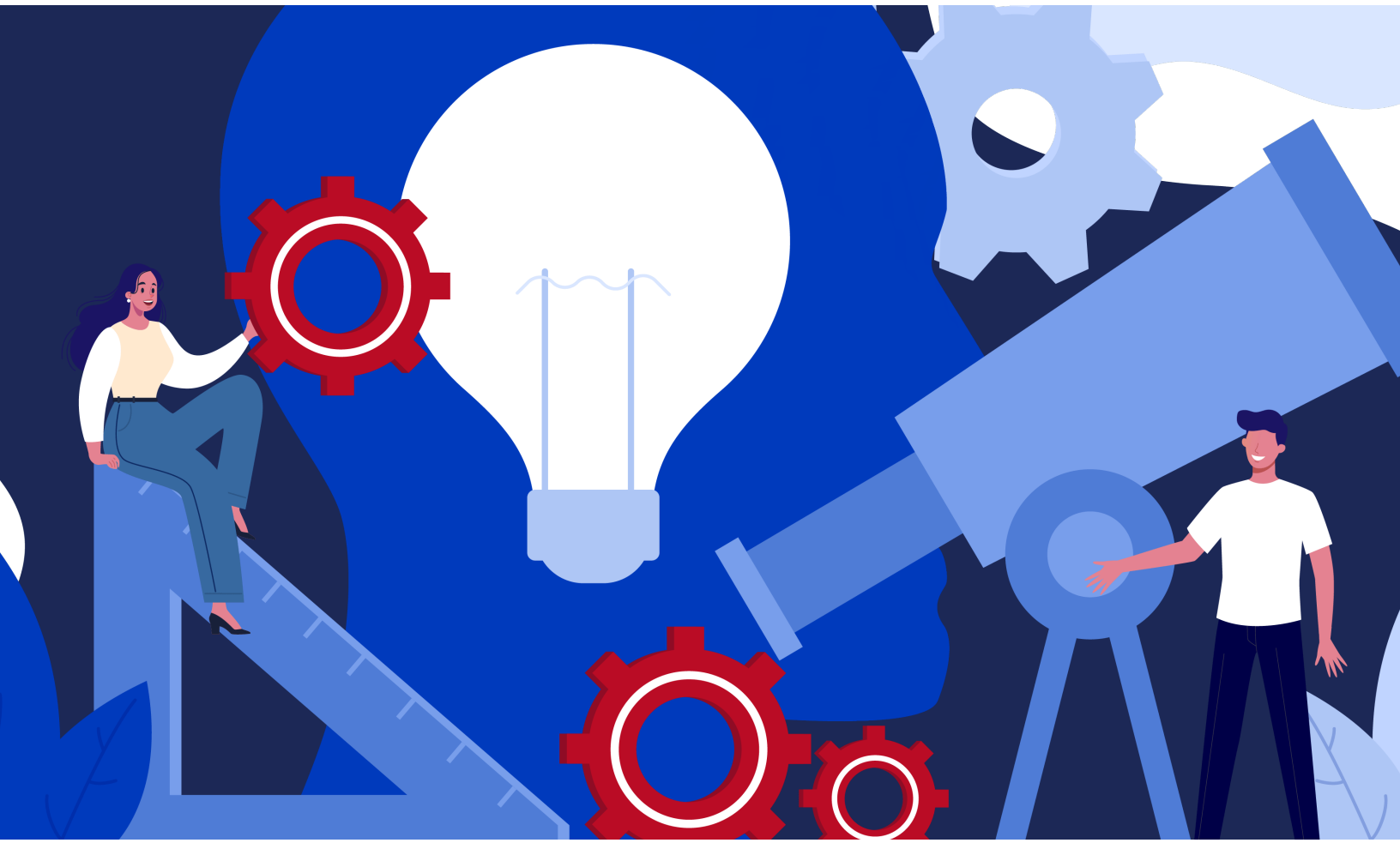
Inhalt

Einleitung

Da die Welt in ein neues digitales Zeitalter eintritt, sind die Bedeutung und der Wert digitaler Dienste und Daten größer als je zuvor. Vom Großunternehmen bis hin zum Mittelstand stehen IT-Teams unter wachsendem Druck, geschäftskritische Ressourcen in zunehmend komplexen IT-Umgebungen zu schützen. Die Aufrechterhaltung eines Always-On-Betriebs rund um die Uhr bei gleichzeitiger Sicherung und Aufbewahrung der genutzten Daten ist nicht nur erforderlich, um auf einem globalen Markt wettbewerbsfähig zu sein, sondern auch, um weltweit die gesetzlichen Vorschriften einzuhalten.

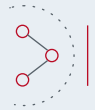
Die Entwicklung einer effektiven Datensicherungsstrategie beginnt damit, dass Sie die Schwachstellen Ihres Unternehmens in puncto Datensicherung kennen müssen. Ausfallzeiten und Datenverluste können eine Vielzahl von Ursachen haben, von traditionellen, ungewollten Naturkatastrophen bis hin zu herbeigeführten, absichtlichen Katastrophen. Im letzten Jahrzehnt haben sich Cyberangriffe zu einer der größten Bedrohungen für Daten und IT-Dienste entwickelt. Unabhängig von der Ursache können die Kosten für Ausfallzeiten oder Datenverluste beachtlich sein und Unterbrechungen, die Stunden, Tage oder sogar Wochen andauern, können die Kundenzufriedenheit unwiderruflich einbrechen lassen und den Ruf eines Unternehmens irreparabel schädigen.

Mit der richtigen Datensicherungsstrategie und den richtigen Lösungen zur Unterstützung dieser Strategie können Daten und IT-Dienste vor Ausfallzeiten und Datenverlusten geschützt werden. Dieser Leitfaden soll Ihnen helfen, die Schwachstellen zu durchblicken, die sich auf Ihr Unternehmen auswirken können, die Arten der verfügbaren Datensicherungslösungen kennenzulernen und zu verstehen, wie diese Überlegungen Ihnen helfen können, die richtigen Lösungen zum Entwickeln einer effektiven Datensicherungsstrategie zu wählen.



Allgemeine Terminologie

Die folgenden Begriffe werden häufig im Bereich Datensicherung verwendet:

	Begriff	Definition
	**Wiederherstellungszeit (Recovery Time Objective, RTO)**	Die gewünschte Zeitspanne zwischen einer Unterbrechung und der Wiederherstellung des Zugangs zu Daten und Diensten
	**Wiederherstellungspunkt (Recovery Point Objective, RPO)**	Der gewünschte Zeitpunkt, ab dem Daten wiederhergestellt werden können, nachdem sie durch eine Unterbrechung verloren gegangen sind
	**Kontinuierliche Datensicherung (Continuous Data Protection, CDP)**	Echtzeit-Datenreplikation, die protokollierte Wiederherstellungspunkte und Orchestrierung von Anwendungen für eine flexible Wiederherstellung kombiniert
	**Disaster Recovery (DR)**	Schnelle Wiederherstellung nach einer Unterbrechung oder Katastrophe, die Systeme und Daten offline nimmt
	**Backup**	Regelmäßiges Kopieren von Daten zur langfristigen Aufbewahrung und Wiederherstellung
	**Cyber-Resilienz**	Wiederherstellung nach einem Cyberangriff wie einem Ransomware-Angriff, bei dem Dienste und Daten verschlüsselt werden
	**3-2-1-Regel**	Eine Datensicherungsstrategie, die drei Kopien der Daten auf zwei verschiedenen Medien umfasst, darunter eine Kopie an einem entfernten Standort zum Schutz vor einer standortweiten Katastrophe
	**Unveränderlichkeit**	Daten werden in einen schreibgeschützten Zustand versetzt, der selbst von einem Systemadministrator nicht geändert werden kann, um sie vor Cyberangriffen zu schützen
	**Air Gapping**	Isolierung eines Datensatzes oder eines Reinraums vom Netzwerk und Internet, um sie vor Angreifern von außen zu schützen
	**Zero Trust**	Ein sich weiterentwickelnder Satz von Cybersicherheitsgrundsätzen, der das alte Paradigma „Vertrauen ist gut, Kontrolle ist besser“ durch „Vertraue niemandem, kontrolliere jeden“ ersetzt, um die Notwendigkeit einer proaktiven, tiefgehenden Verteidigung und extrem wachsamer Prozesse zu verstärken

So gehen Sie den Kaufprozess an

Beginnen wir damit, den Kauf von Datensicherungslösungen in drei verschiedene Schritte zu unterteilen:

1. **Sie müssen Ihre Schwachstellen in puncto Datensicherung kennen**
2. **Untersuchen und dokumentieren Sie Ihre Anforderungen**
3. **Legen Sie Ihre Kaufkriterien fest**

1 Sie müssen Ihre Schwachstellen in puncto Datensicherung kennen

Wir alle sind in gewissem Maße auf Daten und digitale Dienste angewiesen, um Geschäfte zu tätigen. Daher können Unterbrechungen jedes Unternehmen in jeder Branche betreffen. Unternehmen stehen vor wichtigen Herausforderungen wie diesen:

*Die durchschnittliche Lösegeldzahlung hat sich fast verdoppelt, von **812.380 US-Dollar im Jahr 2022 auf 1.542.333 US-Dollar im Jahr 2023**[1]*

- **Wie kann ich einen Always-On-Betrieb aufrechterhalten?** Ob online oder vor Ort, ob Ihr Betrieb rund um die Uhr oder nur von 9 bis 17 Uhr geführt wird – während der Geschäftszeiten können Sie sich keine Unterbrechung leisten. Umsatz- und Produktivitätsverluste sowie Vertrauensverluste aufseiten Ihrer Kunden können Ihren Betrieb ernsthaft beeinträchtigen. Der Ausfall von Anwendungen und Computersystemen kann den E-Commerce, die Kommunikation, die Produktionslinien oder eine beliebige Anzahl von Diensten lahmlegen, auf die Ihre Kunden angewiesen sind. Lange Wiederherstellungszeiten, die mit veralteten Datensicherungslösungen einhergehen, können Ihrer Marke und Ihrem Ruf schaden.
- **Wie kann ich Datenverluste verhindern?** Ihre Daten sind für Ihr Unternehmen von entscheidender Bedeutung und ein Verlust des Datenzugriffs bedeutet eine Unterbrechung hinsichtlich Produktivität und Umsatz. Nicht falls, sondern wenn etwas schiefgeht, müssen Sie in der Lage sein, Ihre Daten schnell und präzise wieder online zu bringen, bevor es sich auf Ihr Endergebnis auswirkt. Datenverluste können aus vielen Gründen auftreten, z. B. durch menschliches Versagen, Softwarebeschädigung, Naturkatastrophen, Hardwareausfälle und Cyberangriffe wie Ransomware-Angriffe. Ein Verlust von ein paar Stunden kritischer Daten während Spitzenzeiten kann verheerend sein. Nur Sie kennen den wahren Wert Ihrer Daten für Ihr Unternehmen.
- **Ist eine Wiederherstellung nach einem Cyberangriff wie einem Ransomware-Angriff möglich?** Obwohl die Cybersicherheit für die Verhinderung von Angriffen von entscheidender Bedeutung ist, ist keine Vorbeugungsmaßnahme zu 100 % wirksam. Cyberangriffe werden von Jahr zu Jahr raffinierter und gehen weit über das bloße Verschlüsseln von Daten und die Forderung von Lösegeld für den Verschlüsselungscode hinaus. Ransomware-Angriffe zielen immer häufiger auf die Wiederherstellungslösungen selbst ab und Angreifer finden sogar Wege, unveränderliche Wiederherstellungsdatenkopien zu umgehen, indem sie die Frist für unveränderliche Backups künstlich ablaufen lassen. Wiederherstellungslösungen erfordern mehrere Ebenen von Optionen, um wirksam zu sein.
- **Wie kann ich die Vorschriften und Standards der Branche einhalten?** Es treten immer mehr staatliche Vorschriften zur Datensicherung und Datensicherheit in Kraft und die Branchen haben es sich zur Aufgabe gemacht, strengere Standards einzuführen, an die sich alle Unternehmen halten sollen. Die Nichteinhaltung staatlicher Vorschriften kann zu Geldstrafen und strafrechtlichen Konsequenzen führen, die sehr kostspielig sein können, während die Nichteinhaltung von Branchenstandards Ihre Geschäftsfähigkeit und den Ruf Ihrer Marke beeinträchtigen kann.
- **Welche Komplexitäten in meiner IT-Umgebung erschweren die Datensicherung?** IT-Umgebungen sind nicht mehr die monolithischen, ortsgebundenen Rechenzentren, die sie einmal waren. Heute erstrecken sie sich in der Regel über mehrere Clouds, lokale Rechenzentren und entfernte Standorte und umfassen auch cloudbasierte Software-as-a-Service-Anwendungen (SaaS-Anwendungen). Der Einsatz mehrerer verschiedener Datensicherungslösungen auf unterschiedlichen Plattformen erfordert mehr Fachwissen und Verwaltungsschnittstellen, ganz zu schweigen von den zahlreichen Support-Telefonnummern, die bei einem Vorfall anzurufen sind.

Je nach Art der betroffenen Daten und Dienste, der Größe des Unternehmens und der Art der Branche oder des Geschäfts können Ihre Schwachstellen sehr unterschiedlich aussehen. Nur Sie kennen das Ausmaß der Schwachstellen für Ihr Unternehmen – und die potenziellen Kosten, die entstehen, wenn Sie Ihren Betrieb für Stunden oder Tage unterbrechen müssen oder wenn Sie Daten gemessen in Stunden oder Tagen verlieren.

[1] „Ransomware-Bericht 2023: Sophos-Bericht ‚State of Ransomware'"

2 Untersuchen und dokumentieren Sie Ihre Anforderungen

Sobald Sie Ihre Schwachstellen in puncto Datensicherung zusammengefasst haben, ist es an der Zeit, die Anforderungen für Ihre Datensicherungsstrategie festzulegen. Untersuchung und Dokumentation sind entscheidend, um sicherzustellen, dass jeder in Ihrem Unternehmen im Einklang mit Ihren Zielen handelt.

- **Dokumentieren Sie Ihre IT-Umgebung.** Dokumentieren Sie jedes Ihrer IT-Systeme und dessen Wichtigkeit für Ihren Geschäftsbetrieb, um festzustellen, welche Ebene an Datensicherung sie benötigen. Dokumentieren Sie auch die verschiedenen Plattformen, Hardware-, Speicher-, Software- und Netzwerksysteme, die Ihre Datensicherungslösungen unterstützen und von ihnen unterstützt werden müssen.
- **Dokumentieren Sie Ihre Datensicherungsstrategie und Ihren Datensicherungsplan.** Dokumentieren Sie die gewünschten RTO- und RPO-Werte für jede Workload-Ebene in Ihrer IT-Umgebung, unabhängig davon, ob sie in Sekunden und Minuten oder in Stunden und Tagen gemessen werden. Dokumentieren Sie das Personal, das für die Umsetzung und Verwaltung des Datensicherungsplans verantwortlich ist, einschließlich der Incident-Response-Teams. Dokumentieren Sie nicht nur zu Umsetzungszwecken, sondern auch für laufende Tests Ihrer Datensicherungspläne, einschließlich Tests von DR, Backups und Reaktion auf Cyberangriffe.
- **Recherchieren und dokumentieren Sie Vorschriften und Branchenstandards.** Nehmen Sie sich Zeit, die Vorschriften zur Datensicherung im Allgemeinen und die branchenspezifischen Vorschriften sowie alle relevanten Branchenstandards, die Ihr Unternehmen eingeführt hat, zu verstehen. Wenn Sie diese kennen und ordnungsgemäß dokumentieren, können Sie fundierte Kaufentscheidungen treffen und sicherstellen, dass die von Ihnen erworbenen Lösungen die Vorschriften einhalten.

Mit diesem Schritt erhalten Sie eine klare, gründliche Übersicht über Ihre Datensicherungsanforderungen, die Ihnen wiederum bei der Prüfung Ihrer Optionen als Entscheidungshilfe dient. Mit den richtigen Informationen an der Hand können Sie sicherstellen, dass die von Ihnen gewählte Lösung auf Ihre Bedürfnisse zugeschnitten ist.

3 Legen Sie Ihre Kriterien für den Kauf von Datensicherungslösungen fest

Die Datensicherung sollte nahezu alle Workloads und Daten in Ihrem Unternehmen auf einem bestimmten Schutzniveau abdecken. Um Ihre Datensicherungsstrategie zu optimieren, sollten Sie jeden dieser zentralen Lösungsbereiche berücksichtigen:

Disaster Recovery

Die Fähigkeit, Daten nach einer Unterbrechung schnell wiederherzustellen, damit Ihr Unternehmen zumindest kritische Abläufe so schnell wie möglich wieder aufnehmen kann

Backup

Die Möglichkeit, Kopien von Daten zu erstellen, die über lange Zeiträume aufbewahrt werden können, um die Vorschriften einzuhalten oder um weniger kritische Systeme nach einer Unterbrechung wiederherzustellen

Cyber-Resilienz

Die Fähigkeit, nach einem Cyberangriff wie einem Ransomware-Angriff, bei dem wichtige Systeme und Daten beeinträchtigt werden, so schnell wie möglich eine Wiederherstellung herbeizuführen

Zusätzliche Lösungsschwerpunkte können für Ihre Branche spezifisch sein, dieser Leitfaden ist jedoch auf die Kaufkriterien für diese drei Bereiche ausgerichtet.

Backup als Disaster Recovery

Obwohl die Begriffe oft synonym verwendet werden, ist es wichtig, den Unterschied zwischen Backup und Disaster Recovery (DR) zu kennen. Das Backup ist bezüglich der Aufbewahrung optimiert, während DR bezüglich der Leistung optimiert ist – und beide haben ihren Platz in der Datensicherung.

Eine Backup-Lösung kann manchmal die Anforderungen an RPO und RTO für isolierte Ereignisse erfüllen, aber für tatsächliche Katastrophenszenarien, die ganze Standorte betreffen, sind die Wiederherstellungsfunktionen Ihrer Backup-Lösung unzureichend, um Daten innerhalb von Minuten oder sogar Stunden wiederherzustellen. Wenn es darum geht, Ihr Unternehmen wieder voll produktiv zu machen, eignen sich Backups besser für die langfristige Datenaufbewahrung als für Rund-um-die-Uhr-Wiederherstellungsdienste. Bei Backups wird die maximal tolerierbare Ausfallzeit nicht sinnvoll berücksichtigt.

Die beiden wichtigsten und kritischen Anwendungsfälle für Backups in einer modernen Datensicherungsstrategie sind:

- Langfristige Aufbewahrung zur Archivierung und Einhaltung der Vorschriften
- Wiederherstellung von Workloads auf niedrigeren Ebenen, bei denen RPOs und RTOs gemessen in Stunden oder Tagen akzeptabel sind

In Anbetracht dessen ist das Backup ein entscheidender Bestandteil der Datensicherung, da weder Disaster-Recovery-Lösungen noch Cyber-Resilienz-Lösungen darauf ausgelegt sind, Daten langfristig aufzubewahren, und beide eher für den Schutz kritischer, übergeordneter Geschäftssysteme konzipiert (und preislich angesetzt) sind.

Wichtige Kaufkriterien

Die Auswahl einer Datensicherungslösung – oder mehrerer Lösungen – ist ein komplizierter Prozess, der mit größeren und komplexeren IT-Infrastrukturen nur noch komplizierter wird. Um den Prozess zu vereinfachen, enthält dieser Leitfaden wichtige Kaufkriterien, die Sie bei der Wahl einer Datensicherungslösung berücksichtigen sollten.

RTO

Wenn Ihre kritischen Geschäftssysteme offline gehen, können Sie es sich dann erlauben, stundenlang zu warten, um Daten von einem Backup oder über das Internet wiederherzustellen? Wenn nicht, visieren Sie möglicherweise eine Wiederherstellungszeit von nur ein paar Minuten an. Der schnellste Weg, einen solchen RTO-Wert zu erreichen, erfolgt in der Regel nicht durch eine Datenwiederherstellung, sondern einen Failover an einem Standby-DR-Standort. In diesem Szenario sind alle Wiederherstellungsdaten bereits vorhanden und warten darauf, als laufender Workload wiederhergestellt zu werden, und können innerhalb von Minuten hochgeladen werden.

Herkömmliche Lösungen für die Datensicherung wie Backup oder Speicherreplikation allein können Anwendungen und Daten nicht schnell genug wiederherstellen. Disaster Recovery schließt diese Lücke. Auch wenn die Dienste während des Failover an einem entfernten Standort in einem reduzierten Zustand laufen, sind sie dennoch in Betrieb. Ihr Unternehmen kann in diesem Zustand bis zur vollständigen Wiederherstellung des primären Produktionsstandorts wieder betriebsbereit sein.

RPO

Welche Menge an Daten dürfen Sie verlieren, wenn eine Unterbrechung auftritt und es zu Datenverlust kommt? Bei herkömmlichen Datensicherungslösungen wie Backups oder Snapshots können seit dem letzten brauchbaren Checkpoint für die Wiederherstellung Stunden von Daten verloren gehen. Aber für Ihre kritischsten Systeme und deren Daten wollen Sie wahrscheinlich so wenig Datenverlust wie möglich – ein RPO gemessen in Sekunden.

Backups und Snapshots können keine RPO-Werte im Sekundenbereich liefern. Nur bei der Echtzeitreplikation werden die Daten schnell genug verschoben, wenn sie sich ändern, um sie in Sekundenschelle zu schützen. Allerdings sind nicht alle Replikationslösungen gleich. Die einfache Replikation von Datenblöcken in Echtzeit garantiert weder Datenkonsistenz noch bietet sie flexible Wiederherstellungsoptionen. Um die Wiederherstellung wirklich zu gewährleisten, müssen konsistente Checkpoints für die Wiederherstellung erstellt werden. Und um einen RPO-Wert im Sekundenbereich zu gewährleisten, müssen diese Checkpoints für die Wiederherstellung alle paar Sekunden erstellt und in einem Journal aufgezeichnet werden.

Anwendungen können die Replikation noch schwieriger machen, wenn sie aus mehreren separat replizierten Workloads bestehen. Bei Anwendungen muss die Replikation über die zu einer Anwendung gehörenden Workloads hinweg konsistent sein, um die Wiederherstellung zu einem zeitlich konsistenten Checkpoint über alle Workloads hinweg sicherzustellen. Andernfalls können Anwendungen nicht gestartet werden und die Ausfallzeiten dauern an, bis die Anwendung wieder in einen konsistenten Zustand versetzt werden kann. Der von einer Replikationslösung erstellte aufgezeichnete Checkpoint muss die Gruppierung der Anwendungsworkloads berücksichtigen, um eine Wiederherstellung mit einem RPO-Wert im Sekundenbereich zu gewährleisten.

Echtzeit-Replikation und alle paar Sekunden aufgezeichnete Checkpoints für die Wiederherstellung sind zwar ideal, aber nicht auf jeder Plattform verfügbar. Auf einigen Infrastrukturplattformen ist die periodische, snapshotbasierte Replikation möglicherweise die einzige – und damit beste – Replikationsoption, die Ihnen zur Verfügung steht. Bei der Vielzahl von vorhandenen Cloud-Infrastrukturen gibt es unterschiedliche Optionen und es ist wichtig zu wissen, welche auf den von Ihnen verwendeten Plattformen verfügbar sind.

Plattform-Unterstützung

Wenn Sie mehrere Computerplattformen wie VMware, Hyper-V, Amazon EC2 oder Azure VMs nutzen, kann es schwierig sein, eine Lösung zu finden, die alle Ihre Plattformen unterstützt. Zahlreiche Datensicherungslösungen unterstützen nur einen einzigen Hypervisor oder eine einzige Cloud-IaaS-Plattform (Infrastructure as a service). Je nach Ihrer IT-Umgebung ist es möglich, mehr als eine Lösung zu verwenden, was unter Umständen notwendig ist, aber Ihre gesamte Datensicherungsstrategie verkompliziert. Die Verwendung von Lösungen mehrerer Anbieter, für die unterschiedliche Fachkenntnisse erforderlich und mehrere Supportnummern verfügbar sind, macht jeden Teil des Datensicherungsplans komplexer.

Die Suche nach einem einzigen Anbieter, der alle Ihre Plattformen unterstützt, kann den Kaufprozess sowie Ihren Bedarf an Support, Lizenzierung und Schulung erheblich vereinfachen bzw. reduzieren. Berücksichtigen Sie die Möglichkeit, dass Sie Ihrer IT-Umgebung in Zukunft eine weitere Plattform hinzufügen werden, und ob die von Ihnen gewählte Lösung auch diese Plattform unterstützt. Prüfen Sie sorgfältig, welche Lösung(en) Ihnen am besten dabei hilft (helfen), den gewünschten RTO- und RPO-Wert über alle Ihre Plattformen hinweg zu erreichen.

Hardware-/Speicherunterstützung

Einige Datensicherungslösungen sind reine Softwarelösungen, während andere ihre eigene Hardware umfassen. In beiden Fällen werden bestimmte Hardware- oder Speichertypen unterstützt oder auch nicht. Lösungen, die nur bestimmte Hardware oder Speichermedien unterstützen, können dazu führen, dass Sie in Zukunft weitere Hardware und Speichermedien kaufen müssen.

Eine hardware- und speicherunabhängige Lösung, bei der es sich in der Regel um eine reine Softwarelösung handelt, kann eine vielfältige Hardwareumgebung unterstützen und bietet Ihnen mehr Auswahlmöglichkeiten bei der Hardware, wenn Sie Ihre Umgebung in Zukunft erweitern möchten. Auch hier sollten Sie sich überlegen, welche Lösungen Ihre Anforderungen am besten erfüllen und Ihnen dabei helfen, die allgemeinen Datensicherungsziele in Ihrer gesamten IT-Umgebung zu erreichen.

Scale-Out-Architektur

Der Bedarf an Daten und digitalen Diensten nimmt weiter zu. IT-Umgebungen werden immer größer, um diesem Bedarf gerecht zu werden, und auch Datensicherungslösungen müssen horizontal skalierbar sein und gleichzeitig eventuelle Unterbrechungen minimieren. Jede Lösung kann durch einfaches Hinzufügen weiterer Komponenten horizontal skaliert werden, aber je mehr Komponenten Sie hinzufügen, desto komplexer kann die Lösung bezüglich Verwaltung und Unterstützung werden. Die Unterstützung von Tausenden von Workloads mit einer agentenbasierten Lösung bedeutet, dass Tausende von Agenten installiert und verwaltet werden müssen. Bei einer hardwarebasierten Appliance-Lösung haben Sie möglicherweise Dutzende von Hardware-Appliances zu verwalten.

Jede Lösung kann demonstriert werden, wobei nur eine Handvoll Workloads geschützt werden muss. Es ist wichtig zu untersuchen, ob eine bestimmte Lösung, wenn sie in größeren Umgebungen und im großen Maßstab eingesetzt wird, noch in der Lage ist, die gewünschten Wiederherstellungszeiten und Wiederherstellungspunkte zu erreichen. Lösungen, die ohne Agenten auskommen und eine nahtlose Bereitstellung und Verwaltung von Scale-Out-Ressourcen ermöglichen, können eine mühelose und effiziente Skalierung möglich machen.

Automatisierung/Orchestrierung

Manuelle Schritte zählen zu den Hauptfaktoren, die die Wiederherstellungszeit verlängern. Die Automatisierung und Orchestrierung der Wiederherstellung verkürzt die Wiederherstellungszeit erheblich, insbesondere bei der Wiederherstellung einer großen Anzahl von Workloads. Stellen Sie sich vor, Sie müssten Hunderte von Workloads wiederherstellen und dabei mehrere manuelle Schritte für jeden einzelnen Workload durchführen. Dadurch würde sich die Wiederherstellungszeit um Stunden statt um Minuten verlängern.

Die Automatisierung von Wiederherstellungsschritten und die Orchestrierung der Wiederherstellung von Dutzenden oder Hunderten von Workloads auf einmal ist der Schlüssel zur Minimierung der Wiederherstellungszeit. Die automatisierte Wiederherstellung ist besonders wichtig für die Koordinierung der Wiederherstellung auf Grundlage von Abhängigkeiten zwischen Anwendungen und verbundenen Anwendungen, die aus mehreren Workloads bestehen. Automatisierung und Orchestrierung sollten Teil der Disaster-Recovery-Lösung sein, um eine schnelle Wiederherstellung und eine Wiederherstellungszeit von wenigen Minuten zu erreichen.

One-to-Many-Architektur

Wie die 3-2-1-Regel zeigt, bieten mehrere Kopien mehr Informationssicherheit, und das gilt ohne Frage auch für DR. Sie benötigen mehrere Datenkopien, um eine rechtzeitige Wiederherstellung zu gewährleisten, denn Katastrophen können mehr als nur Ihren primären Betrieb beeinträchtigen. Die Fähigkeit einer Lösung, Ihre Anforderungen an RPO und RTO zu erfüllen, kann beeinträchtigt werden, wenn Sie nur eine einzige Wiederherstellungskopie der Daten zur Verfügung haben und diese Kopie beschädigt ist. Ziehen Sie eine Lösung in Betracht, die Daten gleichzeitig für zwei verschiedene Wiederherstellungsziele schützen kann. Diese Kopien der Wiederherstellungsdaten können lokal und remote, vor Ort oder in der Cloud sein – je nachdem, was Ihnen den besten Schutz und die besten Wiederherstellungsoptionen für Ihre Daten bietet.

Analysen und Berichterstellung

Es ist wichtig, dass Sie leicht erkennen können, ob Ihre Datensicherungslösung Ihre Anforderungen erfüllt, sowohl hinsichtlich der Einhaltung von Vorschriften als auch der Sicherheit. Die Anzeige von Datensicherungsanalysen und die Erstellung von Berichten darüber kann für die Unterrichtung von Stakeholdern oder staatlichen Kontrollstellen über Erfolge oder Probleme von entscheidender Bedeutung sein.

Die Überwachung des Zustands und der Effektivität Ihrer Datensicherungslösungen mittels Analysen hilft bei der Identifizierung potenzieller Probleme und ermöglicht Ihnen eine bessere Planung der Wiederherstellung auf Grundlage der Ergebnisse von DR-Tests und der Trends dazu, wie schnell Daten über Wiederherstellungspunkte gesichert werden. Je größer Ihre IT-Umgebung ist, desto wertvoller ist die umgebungsweite Analyse für die Überwachung der Datensicherung.

DR-Tests

Keine Disaster-Recovery-Lösung ist effektiv, wenn sie nicht regelmäßig getestet werden kann. In der Vergangenheit war das Testen von Disaster-Recovery-Plänen so schwierig, dass viele Unternehmen trotz bester Absichten Schwierigkeiten hatten, ihre Disaster-Recovery-Pläne auch nur einmal im Jahr zu testen. Diese Tests zogen oft Unterbrechungen nach sich: Das Unternehmen musste häufig Live-Systeme offline nehmen, um die Wiederherstellung ordnungsgemäß zu testen.

Die Möglichkeit, Tests ohne Unterbrechung des Geschäftsbetriebs durchzuführen, ist eine wesentliche Voraussetzung für häufige Tests. Unabhängig davon, ob Sie die Wiederherstellung eines einzelnen Workloads, einer Anwendung oder eines ganzen Standorts testen, sollte Ihre Lösung Ihnen ermöglichen, Tests mit Zuversicht und ohne Unterbrechung des Geschäftsbetriebs durchzuführen.

Erweiterbare Architektur

Erweiterbare Optionen wie APIs in Datensicherungslösungen können Ihnen die Möglichkeit zur Integration in einheitliche Verwaltungslösungen und Nutzung dieser Lösungen bieten. Diese Integrationen können dabei helfen, Daten in einheitliche Verwaltungsansichten zusammen mit anderen Systemen, wie z. B. Cybersicherheit, einzubringen, um einen besseren Einblick in potenzielle Bedrohungen zu erhalten und den Zugang für eine einheitliche Kontrolle und externe Automatisierung zu ermöglichen.

Lösungen, die eine API-first-Architektur verwenden, legen in der Regel alle Kontrollen offen, einschließlich der Sicherheitsmaßnahmen für die Integration in Tools und Dienste von Drittanbietern. Die Flexibilität einer erweiterbaren Architektur bietet mehr Optionen für die Verwaltung und Überwachung in Ihrem Unternehmen.

Flexible Wiederherstellungsoptionen

Unterbrechungen treten in vielen Formen und Ausmaßen auf. In manchen Fällen müssen Sie nur eine einzelne Anwendung wiederherstellen, in anderen Fällen dagegen einen ganzen Standort oder mehrere Standorte. Die Möglichkeit der Wiederherstellung auf granularer Ebene ermöglicht eine flexible betriebliche Wiederherstellung – von einzelnen Dateien oder Ordnern bis hin zum Failover ganzer Standorte, wenn die Unterbrechung dies rechtfertigt.

Ein Failover der betroffenen Workloads und nicht des gesamten Standorts kann die Wiederherstellungszeit verkürzen und das Failback bei Bedarf erleichtern. Außerdem kann es für den täglichen IT-Betrieb nützlich sein, einzelne Dateien wiederherstellen zu können, ohne andere Systeme zu unterbrechen. Je mehr Optionen Sie für die Wiederherstellung haben, desto besser können Sie auf Unterbrechungen jeder Größenordnung reagieren.

Sichere Backups

Als Kopien ganzer Workloads können Backups attraktive Ziele für unbefugte Eindringlinge oder Cyberangriffe wie Ransomware-Angriffe sein, die auf deren Löschung abzielen. Ihre Fähigkeit, diese Backups mit integrierter Verschlüsselung, konfigurierbarer Unveränderlichkeit und doppelter Autorisierung zu schützen, ist ein entscheidender Faktor für die Aufrechterhaltung der Sicherheit Ihrer Backups während ihres gesamten Lebenszyklus.

Backup-Häufigkeit

Wie oft Backups durchgeführt werden können, ist eine wichtige Überlegung, insbesondere für die Tier-2-Workloads, die Backups als primäre Wiederherstellungslösung verwenden. Obwohl tägliche Backups für viele Tier-2-Workloads ausreichend sein können, sind bei einigen häufigere Backups erforderlich, möglicherweise sogar alle vier Stunden. Die Möglichkeit, Backups nach benutzerdefinierten, workloadspezifischen Zeitplänen durchzuführen, bietet ein hohes Maß an Flexibilität bei der Entwicklung einer Datensicherungsstrategie.

Effizienz der Backup-Speicherung

Backups und ihre langfristige Aufbewahrung können eine Menge Speicherplatz in Anspruch nehmen. Obwohl Backups aus Gründen der Kosteneffizienz oft sicher im Speicher niedrigerer Stufen abgelegt werden können, kann die Reduzierung des Speicherplatzes Ihrer Backups durch integrierte Komprimierung und Deduplizierung die Speicherkosten im Laufe der Zeit erheblich senken. Dies ist besonders wichtig, da die Menge der in IT-Systemen gesammelten und gespeicherten Daten weiterhin rapide zunimmt.

Software-as-a-Service-Backups (SaaS)

Es ist wichtig zu verstehen, dass Sie bei der Umstellung auf cloudbasierte Anwendungen wie Microsoft 365 immer noch Daten sichern müssen. SaaS-Anbieter sichern die auf ihrer Plattform erstellten Daten nicht automatisch. SaaS-Backup- und Wiederherstellungslösungen erstellen zusätzliche Kopien von SaaS-Anwendungs-Backups und speichern diese an separaten, sicheren Orten. Einige können auch partielle Backups oder Snapshots für zusätzlichen Schutz und Komfort erstellen.

Ziehen Sie eine komplette Backup-Lösung für Ihre lokalen, Cloud- und SaaS-Anwendungsdaten in Betracht – oder verwenden Sie separate Backup-Tools für jede Anwendung. In jedem Fall sollten Sie sicherstellen, dass Ihre SaaS-Daten zusammen mit den übrigen Daten vor Ort und in der Cloud gesichert werden.

Erkennung von Cyberangriffen

Cybersicherheitslösungen sind so konzipiert, dass sie Eindringlinge erkennen. Was aber, wenn ein Eindringling von der Cybersicherheitslösung nicht erkannt wurde und ein Angriff auf Ihre Daten und Anwendungen bereits im Gange ist? Eine Datensicherungslösung, die erkennen kann, wann ein Angriff begonnen hat, kann Ihrem Incident-Response-Team helfen, schneller zu handeln, um den Angriff zu isolieren und zu beheben, was die Wiederherstellungszeit verkürzt.

Backups können auf potenzielle Malware oder verschlüsselte Daten gescannt werden, die auf einen begonnenen Angriff hindeuten, aber es kann Stunden dauern, bis sie entdeckt werden. Die Möglichkeit, Datenänderungen in Echtzeit anzuzeigen – wie bei der Echtzeitreplikation in einer Disaster-Recovery-Lösung – kann dazu beitragen, Sie innerhalb von Sekunden nach Beginn eines Angriffs zu alarmieren, so dass Ihr Incident-Response-Team schnellstmöglich gewarnt wird. Die Kombination dieser Erkennung mit anderen von Cybersicherheitssystemen gemessenen Kennzahlen wie die Netzwerkaktivität kann diesen Teams helfen, den Ausgangspunkt und den Aktionsradius eines Angriffs schnell ausfindig zu machen.

Unveränderlichkeit

Sicherungs- und Wiederherstellungsdaten jeder Art, einschließlich replizierter Daten für die Disaster Recovery, sind anfällig für Cyberangriffe, insbesondere wenn die Angreifer Administratorrechte für die Wiederherstellungslösung erlangen. Die Möglichkeit, unveränderliche Kopien der Wiederherstellungsdaten zu erstellen, ist von entscheidender Bedeutung, um sicherzustellen, dass die Daten wiederhergestellt werden können, wenn die Wiederherstellungslösung beeinträchtigt ist.

Obwohl die Wiederherstellung über eine unveränderliche Kopie der Daten in der Regel langsamer und nicht ideal ist, ist sie immer noch besser als einem Angreifer Lösegeld zu zahlen und damit weitere Angriffe zu provozieren. Die Unveränderlichkeit ist eine der einfachsten Möglichkeiten, den Schutz der Daten vor Ransomware zu erhöhen.

Zero-Trust-Architektur

Da Angreifer es zunehmend auf Wiederherstellungslösungen abgesehen haben, ist die Sicherheit Ihrer Wiederherstellungslösung von entscheidender Bedeutung, um Angreifer daran zu hindern, Ihre Wiederherstellungsfähigkeit zu beeinträchtigen. Wiederherstellungslösungen sollten konfigurierbar sein und Optionen bieten, die auf den Grundsätzen der Zero-Trust-Architektur beruhen, einschließlich des am wenigsten privilegierten Zugangs, rollenbasierter Zugangskontrollen, sicherer Anwendungen und routinemäßiger Sicherheitsupdates.

Obwohl keine Sicherheitsvorkehrungen zu 100 % wirksam sein können, kann die Fähigkeit, Angreifer durch Sicherheitsmaßnahmen abzuschrecken, sowohl die Schwere als auch die Häufigkeit von Angriffen mindern. Jede Wiederherstellungslösung, die sich innerhalb von Produktionssystemen befindet, stellt in gewissem Maße eine Zielscheibe für Eindringlinge dar, aber mit der entsprechenden Sicherheit kann die Angriffsfläche der Lösung minimiert werden.

Cyber-Vault

Cyberangriffe wie Ransomware-Angriffe können zu einem Weltuntergangsszenario führen, bei dem alle Websites und Systeme beeinträchtigt oder verschlüsselt sind. Ein Cyber-Vault kann selbst in derartigen Weltuntergangsszenarien Schutz bieten, da die Daten in einer isolierten Umgebung per Air Gap geschützt werden, in der sie unveränderlich sind und nur lokal von einer Person direkt im Rechenzentrum verwaltet werden können. Leider sind nicht alle Vaults wirklich isoliert oder mit Air Gap versehen. Einige sind cloudbasiert, wobei die Verwaltungsebene des Vaultspotenziellen Hackern ausgesetzt ist.

Um sicherzustellen, dass die Daten wiederhergestellt werden können, müssen sie physisch per Air Gap abgeschirmt und vom Netzzugang isoliert sein. Ähnlich wie ein Tonband, das durch Entnahme und Lagerung in einem sicheren Bereich physisch und luftdicht gesichert werden kann, darf ein Vault nur für das Management persönlich im Rechenzentrum zugänglich sein. Der Vorteil eines Vaults gegenüber einem Tonband besteht darin, dass der Vault eine isolierte Speicher- und Datenverarbeitungsumgebung enthält, in der die Daten für forensische Zwecke schnell und sicher wiederhergestellt werden können.

Die Online-Bereitstellung von Daten und Anwendungen in einer speziellen Reinraumumgebung kann den Wiederherstellungsprozess erheblich verkürzen – von Monaten auf Tage. Bei einem Tonband oder anderen isolierten Datenbackups allein kann der Wiederherstellungsprozess für die Übertragung der Daten Wochen dauern. In einem Szenario, in dem die Daten vollständig beeinträchtigt sind, kann ein Vault die Wiederherstellung für Incident-Response-Teams beschleunigen, so dass kein Lösegeld gezahlt werden muss sowie Zeit und Kosten für den Wiederherstellungsprozess gespart werden.

So gehen Sie beim Kauf vor

Nehmen Sie die auf dem Markt verfügbaren Datensicherungslösungen unter die Lupe und ermitteln Sie, ob sie die von Ihnen festgelegten Kriterien erfüllen. Es gibt mehrere Möglichkeiten, dies anzugehen, und jede davon ist kostenlos:

Stellen Sie Recherchen an

Stellen Sie zu einer bestimmten Lösung mit Hilfe Ihrer eigenen Experten Recherchen an – unabhängig von der Kommunikation mit dem Anbieter der Lösung. Beauftragen Sie Dritte mit der Validierung von Rechercheergebnissen.

- Analystenberichte können Lösungen spezifisch bewerten oder bevorzugte Lösungstypen für relevante Anwendungsfälle aufzeigen.
- Kundenrezensionen und -referenzen können Aufschluss über den Erfolg von Kunden und deren Probleme mit den Lösungen geben.

Setzen Sie sich mit Lösungsanbietern in Verbindung

Überprüfen Sie Ihre eigenen Nachforschungen direkt beim Anbieter und lassen Sie sich von ihm Einblicke in Ihren speziellen Anwendungsfall geben.

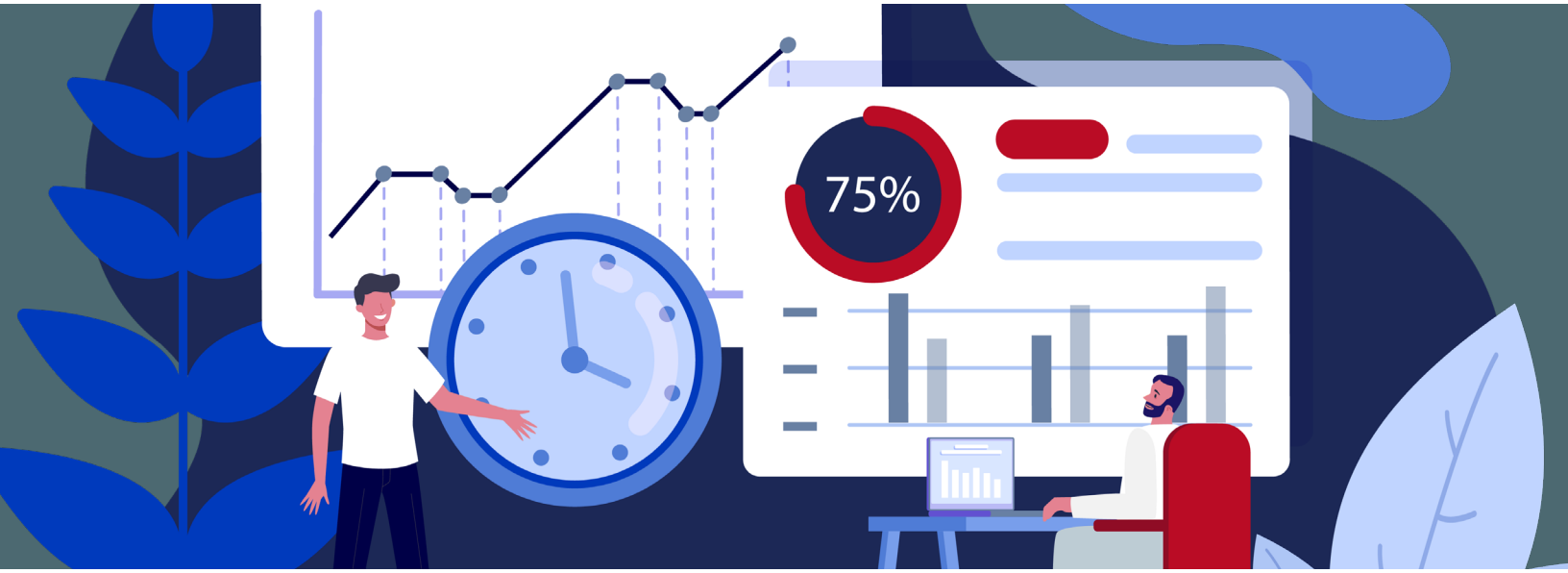
- Lösungsarchitekten können bei der Entwicklung einer Lösung helfen, die speziell auf die Anforderungen und Kriterien Ihres Unternehmens zugeschnitten ist.
- Demonstrationen können Einblicke in die Verwaltungsfähigkeiten und -funktionen geben.

Bewerten Sie die Lösung

Lassen Sie Ihre eigenen Experten und Stakeholder die Lösung testen, um Optimierungen und mögliche Schwachstellen nachvollziehen zu können. Bewertungen können auf unterschiedliche Weise durchgeführt werden:

- On-Demand-Testlabore sind oft in virtualisierten oder Cloud-Umgebungen verfügbar, um die Lösung in einer geschlossenen Umgebung zu testen.
- Mit einer Testlizenz können Sie sie direkt in Ihrer eigenen Infrastrukturumgebung testen.
- Proof of Concept (PoC) kann zur Bewertung bestimmter, für Ihr Unternehmen relevanter Anwendungsfälle verwendet werden.

Neben der Berücksichtigung der Funktionen der verschiedenen Lösungen als Kaufkriterium müssen auch den Kosten, der Lizenzierung und den verfügbaren Servicemodellen für die Lösungen Rechnung getragen werden.



Führen Sie eine Analyse der Gesamtbetriebskosten durch

Die Gesamtkosten einer Datensicherungslösung können die Kosten für die Lizenzierung der Lösung, die Kosten für die unterstützende Infrastruktur/Hardware, die Implementierungskosten, die Wartungskosten und andere indirekte Kosten für die Überwachung und Verwaltung der Lösung umfassen.

Betrachten Sie die drei Arten von Lizenzmodellen, die üblicherweise mit Datensicherungslösungen angeboten werden:

- **Dauerlizenzen** – Sie kaufen die Lösung als Kapitalaufwand im Voraus mit laufenden Support- und Wartungsgebühren.
- **Abonnementbasierte Lizenzen** – Sie zahlen für die Nutzung der Lösung über einen bestimmten Zeitraum, wobei die Kosten über die Laufzeit des Abonnements als Betriebsausgabe verteilt werden können.
- **Nutzungsbasierte Lizenzen** – auch „Pay-as-you-go“ genannt, aber der Preis richtet sich danach, wie viele Workloads oder TB an Daten geschützt werden, so dass die Kosten je nach Verbrauch/Nutzung nach oben oder unten skaliert werden können.

Ermitteln Sie, welche zusätzliche Infrastruktur oder Hardware zur Unterstützung der Lösung benötigt wird, z. B. zusätzliche Netzwerk-, Speicher- und Rechenressourcen sowie Kosten für Rechenzentren und Kühlung. Vergessen Sie nicht, die Kosten für die Implementierung einzubeziehen, unabhängig davon, ob sie intern oder über professionelle Services durchgeführt wird. Hinzu kommen die laufenden Kosten für die Verwaltung und Überwachung der Lösung und die Durchführung von Wiederherstellungstests.

So komplex dies auch erscheinen mag, so sollten Sie doch mehrere Preis- und Lizenzierungsoptionen prüfen, um herauszufinden, welche am besten zu Ihrem Budget und der Art und Weise passt, wie Ihr Unternehmen IT-Ressourcen nutzen möchte (d. h. als Investitions- oder Betriebsausgabe).

Selbermachen vs. Managed Service Provider (MSP)

Wenn Ihnen die Gesamtkosten für Kauf, Implementierung und Verwaltung der Datensicherung nicht zusagen, können Sie einen Managed Service Provider (MSP) beauftragen, der den Dienst für Sie bereitstellt und betreibt. Ein wesentlicher Vorteil einer verwalteten Lösung besteht darin, dass Sie für jeden Teil Ihrer Umgebung die besten Lösungen nutzen können, ohne mehrere Produkte oder Dienste konfigurieren und verwalten und sich in ihre Nutzung einarbeiten zu müssen. Der MSP kann eine Lösung konfigurieren, die speziell auf Ihre Bedürfnisse zugeschnitten ist und Ihrer Datensicherungsstrategie entspricht.

Es gibt drei vorherrschende Modelle für Datensicherungsdienste, die MSP anbieten:

- **Datensicherung in einer von einem MSP gehosteten Cloud** – Ihre Produktionsumgebung befindet sich vor Ort, während die geschützten Wiederherstellungsdaten für die Wiederherstellung extern in einer von einem MSP gehosteten Cloud gespeichert werden. Dies ist ideal, wenn Sie noch keinen externen Speicherort für die Datensicherung haben und diesen auch nicht selbst einrichten möchten.
- **Datensicherung über die von einem MSP gehostete Cloud** – Ihre Produktionsworkloads und -daten werden vom MSP gehostet und Ihr lokaler Standort wird zur Speicherung Ihrer Wiederherstellungsdaten verwendet. So haben Sie vollen Zugriff auf und volle Kontrolle über Ihre Wiederherstellungsdaten, falls es beim MSP zu einer Unterbrechung kommt.
- **In der Cloud des MSP gehostete Datensicherung und Produktion** – der MSP hostet Ihre Produktionsworkloads und -daten in einer Cloud und Ihre Wiederherstellungsdaten in einer separaten Cloud. Das ist ideal, wenn Sie nicht über das nötige Fachwissen verfügen oder die Infrastruktur nicht selbst verwalten möchten.

Die Inanspruchnahme eines MSP entlastet Ihr Unternehmen vollständig vom täglichen Betrieb. Es entbindet Sie nicht von der Verantwortung, die Sie weiterhin tragen. Dies ist im Wesentlichen eine vollständige Auslagerung der Datensicherung an einen Dritten. Sie müssen sich keine Gedanken über das Design, die Kapazität oder darüber machen, ob sie läuft oder nicht, und auch nicht darüber, ob jemand sie genau überwacht, da Sie das Know-how des Serviceanbieters in Anspruch nehmen.

Führen Sie eine ROI-Analyse durch

Um die Kosten für die Datensicherung zu rechtfertigen, reicht es oft aus, die Kosten für Ausfallzeiten und Datenverluste aufzuzeigen, die ohne die Möglichkeit einer einfachen oder schnellen Wiederherstellung entstehen. Stunden- oder tagelange Ausfallzeiten und/oder Datenverluste können sich schnell summieren, ebenso wie die Kosten für die Inanspruchnahme externer Wiederherstellungsdienste, wenn es zu einer Unterbrechung kommt. Das Kosten-Nutzen-Verhältnis einer Wiederherstellung innerhalb von Minuten und eines Verlusts weniger Sekunden von Daten kann den Wert einer Datensicherungslösung oft schon bei einem einzigen Vorfall demonstrieren. Viele Unternehmen haben der Datensicherung nach einer solchen Unterbrechung Priorität eingeräumt.

Zusammenfassung

Die Daten und digitalen Dienste, auf die wir täglich angewiesen sind, sind ständig von Unterbrechungen bedroht, sei es durch Naturkatastrophen, Unfälle oder bösartige Angriffe. Unternehmen wie das Ihre stehen vor zahlreichen Herausforderungen bei der Entwicklung einer Datensicherungsstrategie, um solche Unterbrechungen zu minimieren. Ihr Unternehmen ist einzigartig und nur Sie kennen die besonderen Herausforderungen, die Sie mit Ihrer Strategie bewältigen müssen, genau.

Es gibt viele Datensicherungslösungen, die in Ihre Datensicherungsstrategie integriert werden können, und die Auswahl einer solchen Datensicherungslösung erfordert eine sorgfältige Prüfung Ihrer Anforderungen. Die Berücksichtigung der in diesem Leitfaden beschriebenen Kriterien wie RTO, RPO, Skalierbarkeit, Tests usw. kann Ihnen bei Ihren Kaufentscheidungen helfen und Sie in die Lage versetzen, die besten Lösungen für Ihre Datensicherungsanforderungen auszuwählen.

Am Ende dieses Leitfadens finden Sie eine Checkliste, die Ihnen dabei helfen soll, die im vorigen Abschnitt genannten Kaufkriterien im Auge zu behalten sowie die Schritte, die Sie unternehmen müssen, um sich auf den Kaufprozess vorzubereiten. Ziel ist es, Sie bei der Auswahl der besten Datensicherungslösung für die Anforderungen Ihres Unternehmens zu unterstützen und Sie auf mögliche Unterbrechungen vorzubereiten. Weitere Informationen zu spezifischen Datensicherungslösungen finden Sie in den folgenden Ressourcen.

Zusätzliche Ressourcen

Whitepaper: Modern Data Protection: What Is It and Why Should You Care? (Moderne Datensicherung: Was ist das und warum sollte Sie das interessieren?) – Zerto

Leitfaden: Key Considerations for a Disaster Recovery Strategy (Schlüsselüberlegungen zu einer Disaster-Recovery-Strategie)

Whitepaper: Recovery Is the Cornerstone of Ransomware Resilience (Wiederherstellung ist der Eckpfeiler der Ransomware-Resilienz) – Zerto

Whitepaper: Verständnis für die Notwendigkeit einer kontinuierlichen und sicheren Datensicherung (hpe.com)

Mehr erfahren

RITM0109203

Ihre Checkliste zum Kauf von Datensicherungslösungen

Zerto
a Hewlett Packard Enterprise company

Checkliste zum Kauf von Datensicherungslösungen

Den Kaufprozess angehen

Schritt 1 Identifizieren Sie Ihre Schwachstellen	☐	Ausfallzeiten, die den Geschäftsbetrieb unterbrechen
	☐	Datenverluste, die zu Unterbrechungen und Produktivitätsverlusten führen
	☐	Nicht darauf vorbereitet sein, nach einer Cyberattacke Daten schnell wiederherzustellen
	☐	Schwierigkeiten bei der Einhaltung der Vorschriften
	☐	Komplexität der IT, die die Implementierung und Verwaltung erschwert
Schritt 2 Recherchieren, Planen und Dokumentieren	☐	Dokumentieren Sie Ihre IT-Umgebung
	☐	Dokumentieren Sie Ihre Datensicherungsstrategie und -pläne
	☐	Recherchieren und dokumentieren Sie Vorschriften und Branchenstandards
Schritt 3 Legen Sie Ihre Kriterien für den Kauf von Datensicherungs-lösungen fest	☐	Bietet die Lösung RTOs im Minutenbereich?
	☐	Bietet die Lösung RPOs im Sekundenbereich?
	☐	Unterstützt die Lösung Ihre kritischen Infrastrukturplattformen, einschließlich der Cloud?
	☐	Verfügt die Lösung über eine Scale-out-Architektur?
	☐	Unterstützt die Lösung Ihre Hardware und Ihren Speicher?
	☐	Bietet die Lösung Automatisierung und Orchestrierung?
	☐	Unterstützt die Lösung eine One-to-Many-Architektur?
	☐	Bietet die Lösung unterbrechungsfreie DR-Tests?
	☐	Verfügt die Lösung über flexible Wiederherstellungsoptionen?
	☐	Ist die Lösung als verwalteter Service (DRaaS) verfügbar?
	☐	Bietet die Lösung sichere Backup-Formate?
	☐	Entspricht die Backup-Häufigkeit Ihren Anforderungen an den RPO-Wert?
	☐	Verfügt die Lösung über effiziente Speicherfunktionen wie Komprimierung und Deduplizierung?
	☐	Kann die Lösung Daten in der Cloud sichern?
	☐	Bietet die Lösung eine Erkennung von Ransomware-Angriffen?
	☐	Erfolgt die Erkennung in Echtzeit oder basiert sie auf der Überprüfung von Backups?
	☐	Bietet die Lösung Optionen für die Unveränderlichkeit von Wiederherstellungsdaten?
	☐	Ist die Wiederherstellungslösung durch eine Zero-Trust-Architektur geschützt?
	☐	Bietet die Lösung einen wirklich isolierten Tresor als Schutz?
So gehen Sie beim Kauf vor	☐	Stellen Sie Recherchen zu den Funktionen der Lösung an
	☐	Suchen Sie nach Analystenberichten
	☐	Suchen Sie nach Kundenbewertungen/-referenzen
	☐	Arbeiten Sie mit einem Lösungsarchitekten des Anbieters zusammen
	☐	Bewerten Sie die Lösung durch Tests oder PoC
	☐	Führen Sie eine Analyse der Gesamtbetriebskosten durch
	☐	Soll die Lösung intern implementiert werden?
	☐	Soll ein MSP beauftragt werden?
	☐	Führen Sie eine ROI-Analyse durch

Mehr erfahren

RITM0109203