arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Tipps für eine optimale Datenverwaltung beim Umstieg auf ein hybrides Rechenzentrum

Von Florian Malecki, Executive Vice President Marketing, Arcserve

Hybride Rechenzentren sind immer mehr im Kommen. Der Grund: Mit einem hybriden Rechenzentrum können Unternehmen ihre Daten besser verwalten, sowohl vor Ort als auch in einer privaten oder öffentlichen Cloud. Diese Flexibilität ist heute von entscheidender Bedeutung, denn Unternehmen müssen sich sowohl mit neuen IT-Trends als auch wachsenden Bedrohungen auseinandersetzen, beispielsweise Ransomware-Attacken. Diese sind für Unternehmen jeder Größenordnung eine enorme Herausforderung. Ein hybrides Rechenzentrum bietet eine anpassungsfähige, flexible IT-Umgebung, die es Unternehmen ermöglicht, nicht nur auf Ransomware, sondern auch auf andere Probleme schnell und effektiv zu reagieren, und zwar im laufenden Betrieb.

Ein hybrides Rechenzentrum bietet ein Plus an Sicherheit, Leistung, Zuverlässigkeit, Agilität, Skalierbarkeit und Kosteneinsparungen. Aber das ist leichter gesagt als getan, denn die Datenbereitstellung für hybride Rechenzentren ist durchaus komplex. Zwar ermöglicht sie es Unternehmen, Daten und Workloads nach Bedarf effizienter zu speichern und zu verschieben und dabei eine bessere Kontrolle über sensible Daten zu erlangen. Gleichzeitig erhöhen sich aber auch die Komplexität und der Verwaltungsaufwand von Servern, Speicher, Netzwerken und Software.

So sind Unternehmen beispielsweise selbst dafür verantwortlich, ihre Daten und Anwendungen sowohl in der Cloud als auch vor Ort zu schützen. Sie müssen in der Lage sein, Daten und Anwendungen in der Cloud oder vor Ort wiederherzustellen, unabhängig davon, wo das Unternehmen die Daten und Anwendungen ursprünglich gehostet hat. Außerdem gilt es, die Sicherung

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

und Wiederherstellung in der hybriden Umgebung zu steuern und zu verwalten.
Auf drei Aspekte sollten die Unternehmen besonders achten, wenn sie ihre Daten in einem hybriden Rechenzentrum erfolgreich verwalten und schützen wollen.

1. Zentralisierte Datensicherung

Für eine erfolgreiche Datensicherung in einem hybriden Rechenzentrum ist ein zentralisiertes Backup-Management unerlässlich. Um effektiv zu sein, muss die Backup-Lösung deshalb über eine zentralisierte Backup-Verwaltungskonsole verfügen. Viele Anbieter von Sicherungssoftware integrieren diese in die Verwaltungskonsole des Cloud-, Hypervisor- oder Betriebssystemanbieters. Das vereinfacht zwar einerseits die Verwaltung von Backups als Teil des Betriebs in einer bestimmten Umgebung, aber ein Cloud-, Hypervisor- oder Betriebssystem-zentrierter Ansatz zur Verwaltung ist in einem hybriden Rechenzentrum nicht praktikabel. Stattdessen kann eine separate, zentralisierte Konsole die Datensicherung in einem hybriden Rechenzentrum besser verwalten. Anwender und Administratoren können auf diese Art und Weise die Sicherung und Wiederherstellung von Workloads überwachen und verwalten, unabhängig davon, ob diese vor Ort oder in der Cloud ausgeführt werden. Ebenso wichtig ist, dass es zentrale Richtlinien gibt, die man dann auf die einzelnen Umgebungen überträgt.

2. Workload-Mobilität

In einer hybriden Umgebung befinden sich die Workloads in der Cloud, vor Ort oder an beiden Plätzen. Eine Datenschutzlösung muss daher für die Sicherung mehr als nur den Ort identifizieren. Sie muss auch die Umgebung erkennen, in der die Daten wiederhergestellt werden. Das ist entscheidend, damit eine Lösung alle notwendigen Schritte für die erfolgreiche

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Wiederherstellung vornehmen kann. Diese Fähigkeit zur Sicherung und Wiederherstellung von Daten in einer Cloud- sowie einer On-Premises-Umgebung ist unerlässlich. Machbar ist das mit Lösungen, die zunächst die physischen Maschinen sichern und sie dann auf einer virtuellen Maschine wiederherstellen – entweder in der Cloud oder vor Ort. Die optimale Lösung sollte aber auch mit der Cloud, dem Hypervisor sowie den Betriebssystem-APIs integriert sein, um entsprechende Backups und Wiederherstellungen vornehmen zu können.

3. Schutz vor Ransomware

Da sich immer mehr Unternehmen auf ihre Backups verlassen, nehmen die Cyberkriminellen zunehmend auch Backup-Software ins Visier, vor allem bei Ransomware-Attacken. Wenn es ihnen gelingt, Backups oder die Backup-Software zu kompromittieren, haben sie bessere Chancen, bei der Lösegelderpressung erfolgreich zu sein. Daher sollte die in einem hybriden Rechenzentrum eingesetzte Backup-Software über Schutzmechanismen zur Abwehr derartiger Angriffe verfügen. Die Backup-Lösung sollte deshalb alle, die Zugriff wünschen, zunächst authentifizieren und dann autorisieren.
Mit verfügbaren Multifaktor-Authentifizierungstools kann die Sicherungssoftware die Identität von Nutzern überprüfen und diese Identitäts- und Zugriffsverwaltung nutzen, um deren Aktivitäten zu überwachen. Sie kann sogar die Zustimmung mehrerer Personen verlangen, bevor bestimmte Aufgaben ausgeführt werden dürfen, wie etwa das Löschen einer Sicherung oder die Änderung des Sicherungsplans. Darüber hinaus sollte Backup-Software auch die Möglichkeit bieten, unveränderliche Speichertechnologien zu verwalten.
Bei der unveränderlichen Speicherung werden die Sicherungen in einem lesbaren, aber nicht veränderbaren Format gespeichert. Das verhindert, dass Ransomware diese verschlüsseln kann. Außerdem sollte eine Sicherungs-

arcserve®
Protect what's priceless.

8855 Columbine Road, Suite #150
Eden Prairie, Minnesota 55347
Phone: +1 844 639 6792

Software über moderne Air-Gapping-Technologien verfügen, denn diese sind eine bewährte Methode zum Schutz von Backups und vor Ransomware. Sie trennen Backups entweder logisch oder physisch von der Produktionsumgebung. Bei einem logischen Air-Gapping befindet sich der unveränderliche Speicher in der Cloud oder vor Ort. Bei physischem Air-Gapping können Unternehmen ihre Daten auf Festplatten oder Bändern sichern, die physisch von der Produktionsumgebung getrennt werden können.

Fazit

Hybride Rechenzentren bieten Unternehmen viele Vorteile, darunter ein Maximum an Flexibilität sowie die Möglichkeit, Daten vor Ort, in der Cloud oder sogar an beiden Stellen zu hosten. Aber diese Flexibilität verändert die Dynamik der Datensicherheit. Es kann sein, dass Sicherheitslösungen, die vor Ort oder in der Cloud gut funktionieren, beim Einsatz in einem hybriden Rechenzentrum Schwachstellen haben. Unternehmen benötigen daher einen neuen Ansatz, um die Anforderungen an die Datensicherheit in einem hybriden Rechenzentrum zu erfüllen.

Unternehmenskontakt
Jock Breitwieser
Arcserve
+1 408.800.5625
jock.breitwieser@arcserve.com

Agenturkontakt
TC Communications
Arno Lücht
+49 8081 9546-19
Thilo Christ
+49 8081 9546-17
arcserve@tc-communications.de
www.tc-communications.de