arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Tests, Orchestrierung und Vorbereitung sind die wesentlichen Säulen der Datenresilienz

Von René Claus, EMEA MSP Sales Director bei Arcserve

Cyberangriffe stellen Unternehmen weltweit vor große Probleme. Nicht nur, dass durch den Datenverlust selbst durchaus beträchtliche Kosten anfallen können, sondern es entstehen auch sehr hohe Kosten aufgrund von Ausfallzeiten. Gartner schätzt, dass Ausfallzeiten bis zu 5.600 US-Dollar pro Minute kosten können, und Statista stellt fest, dass im vierten Quartal 2021 die durchschnittliche Ausfallzeit nach einem Ransomware-Angriff in den USA 20 Tage betrug. Die Kosten eines Angriffs gehen aber weit über den finanziellen Verlust hinaus, denn auch der Ruf des Unternehmens steht auf dem Spiel. Wenn Unternehmen nicht in der Lage sind, die Bedürfnisse ihrer Kunden zu erfüllen, wird die Marke beschädigt, und es kann schwierig sein, die Reputation wiederherzustellen.

Glücklicherweise haben Unternehmen aber verschiedene Möglichkeiten, sich zu schützen. Der effektivste Ansatz zur Minderung der Kosten eines Angriffs ist die Investition in eine orchestrierte Sicherungs- und Wiederherstellungsarchitektur, die die Ausfallsicherheit der Daten gewährleistet. Wenn Unternehmen über eine solche Architektur verfügen, sind sie auf jede potenzielle Katastrophe vorbereitet, nicht nur auf einen Cyberangriff, sondern auch auf eine Naturkatastrophe wie beispielsweise eine Überschwemmung. Mit einem gut definierten Plan und den erforderlichen Tools können Unternehmen die Auswirkungen minimieren und den Betrieb reibungslos aufrechterhalten.

Eine von Arcserve durchgeführte weltweite Umfrage zeigt, dass 77 Prozent der IT-Entscheidungsträger in orchestrierte Sicherungs- und Wiederherstellungsarchitekturen investieren, um die Ausfallsicherheit ihrer Daten zu gewährleisten. Diese Investition zahlt sich aus, denn Backup und Wiederherstellung sind von grundlegender Bedeutung für jeden Datensicherheitsplan. Sie geben Unternehmen die Möglichkeit, eine potenziell katastrophale Situation zu vermeiden.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Testen, Orchestrierung und Vorbereitung: 3 wichtige Elemente für die Datenresilienz

Bei einem Zwischenfall treten zahlreiche Variablen und Unbekannte auf. Solide Backup- und Disaster-Recovery-Richtlinien bereiten Unternehmen darauf aber nur dann wirkungsvoll vor, wenn sie ein regelmäßiges Testprogramm in ihre Richtlinien aufnehmen. Mit DR-Tests (Datenresilienz-Tests) können Organisationen die Verfahren ermitteln und dokumentieren, die für die Wiederherstellung des Geschäftsbetriebs und der Systeme im Falle eines Zwischenfalls erforderlich sind. Danach können sie diese Verfahren validieren und potenzielle Lücken in Bezug auf die Richtlinien und das Personal schließen. Nur durch angemessene Tests können diese kritischen Aspekte identifiziert und berücksichtigt werden.

Die Orchestrierung, d. h. die Automatisierung zur Beschleunigung der End-to-End-Wiederherstellung, ist der zweite Aspekt der Ausfallsicherheit. Im Wesentlichen bestimmt die Orchestrierung die optimale Reihenfolge für das Hochfahren verschiedener, miteinander verbundener Systeme während einer Wiederherstellung. Sie umreißt die optimale Reihenfolge, in der die Systeme wiederhergestellt werden sollten, identifiziert alle Zwischenschritte, die für die Validierung in jeder einzelnen Phase erforderlich sind, und gewährleistet eine reibungslose und geordnete Wiederherstellung.

Das letzte Element ist die Vorbereitung. Als Analogie dient hier eine Brandschutzübung in einem Bürogebäude. Während der Übung macht ein Alarm die Mitarbeiter auf die Bedrohung aufmerksam. Fluchtwegschilder weisen sie an, die Treppe statt des Aufzugs zu benutzen und sich an von der Organisation festgelegten sicheren Orten zu versammeln. Die Vorbereitung zur Datenresilienz funktioniert auf die gleiche Weise. Die Mitarbeiter führen regelmäßig Übungen durch, um sicherzustellen, dass jeder die notwendigen Maßnahmen und Abläufe kennt.

RPO, RTO und zulässige Ausfallzeiten

Vielen Unternehmen schenken ihren Sicherungs- und Wiederherstellungsaufgaben nicht die Aufmerksamkeit, die sie verdienen. Sie führen vielleicht DR-Tests durch, wenn sie neue Backup-Software oder Speicherserver einrichten, versäumen es aber,

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

laufende Tests durchzuführen. Unternehmen müssen regelmäßige Backup-Tests durchführen, sei es vierteljährlich, jährlich oder zeitgleich mit wichtigen Ereignissen wie einer Fusion, der Einführung eines neuen IT-Systems oder der Erweiterung der Belegschaft. Best Practices schreiben vor, dass es wichtig ist, festzulegen, wann ein Disaster-Recovery-Test durchgeführt werden sollte, um ein Worst-Case-Szenario beim Eintritt einer Katastrophe zu vermeiden.

Idealerweise sollten Unternehmen eine umfassende Strategie für Backup-Tests entwickeln, und es gibt einige Schlüsselelemente, die sie dabei berücksichtigen sollten. Zwei primäre Strategieelemente sind das Wiederherstellungspunktziel (RPO) und das Wiederherstellungszeitziel (RTO). Ein Unternehmen kann sein RPO durch die Höhe des Datenverlustes bestimmen, den es im Falle eines Vorfalls maximal tolerieren kann – es geht um die Zeitspanne, die während eines Vorfalls vergehen kann, bevor die Menge der verlorenen Daten die vorab definierte Toleranzgrenze überschreitet. Aus dem RPO ergibt sich die Häufigkeit der Datensicherung, ob beispielsweise stündlich, einmal täglich oder alle sieben Tage.

Die RTO ist die Zeit, die für die Wiederherstellung eines voll funktionsfähigen Betriebs nach einem Vorfall zur Verfügung steht. Die Wiederherstellung ist der Unterbrechungszeitraum, der Auswirkungen auf das Neugeschäft, die Mitarbeiter und den täglichen Betrieb hat. Unternehmen sollten ihre Annahmen deshalb bezüglich der Auswirkungen von Unterbrechungen und der zulässigen Wiederherstellungszeit im Rahmen ihrer Teststrategie validieren.

In der Arcserve-Studie geben 83 Prozent der Befragten an, dass eine Ausfallzeit von 12 Stunden oder weniger für kritische Systeme akzeptabel ist, bevor es zu messbaren negativen Auswirkungen auf das Geschäft kommt. Dennoch sind nur 52 Prozent der Befragten in der Lage, einen schwerwiegenden Datenverlust innerhalb von 12 Stunden oder weniger zu beheben, während 29 Prozent der befragten Unternehmen angeben, dass sie ihre Daten nicht innerhalb eines Tages wiederherstellen könnten.

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Diese Umfrageergebnisse zeigen eine Kluft zwischen den Erwartungen und den tatsächlichen Fähigkeiten. Unternehmen sollten sich darauf konzentrieren, ihre Datenwiederherstellungsfähigkeiten zu verbessern, um dieses Problem zu beheben und ihre akzeptablen Ausfallzeiten anzugleichen. Dies kann die Implementierung robusterer Sicherungs- und Wiederherstellungslösungen und die Verbesserung von Notfallwiederherstellungsplänen beinhalten. Dazu gehört auch, dass die Prozesse regelmäßig getestet und aktualisiert werden, um ihre Wirksamkeit zu gewährleisten. Indem sie diese Lücke schließen, können Unternehmen die negativen Auswirkungen von Datenverlusten besser abmildern und Ausfallzeiten minimieren und so ihren Betrieb und ihren Ruf schützen.

Fazit

Cyber-Bedrohungen sind heute allgegenwärtig. So stellt IBM in seinem Bericht „Cost of a Data Breach 2022“ fest, dass 83 Prozent der Unternehmen im vergangenen Jahr mehr als eine Datenschutzverletzung erlitten haben. Organisationen sollten also vorbereitet sein und handeln. Dies bedeutet, potenzielle Bedrohungen zu verstehen, Risiken zu mindern und Strategien für die Wiederherstellung zu entwickeln. Eine solche proaktive Haltung kann den entscheidenden Unterschied ausmachen, wenn es darum geht, dass ein Unternehmen eine Katastrophe möglichst unbeschadet übersteht.

Wie aus zahlreichen Ransomware-Vorfällen zu sehen ist, haben unvorbereitete Unternehmen oft mit schwerwiegenden Folgen zu kämpfen, die bis zum völligen Bankrott führen können. Auf der anderen Seite haben Unternehmen, die der Vorbereitung Priorität einräumen, bessere Chancen, Katastrophen zu überstehen und sich davon zu erholen. Die Vorbereitung ist ausschlaggebend dafür, ob ein Unternehmen nach einem Vorfall wieder auf die Beine kommt oder in den Ruin stürzt.

Folgen Sie Arcserve auf LinkedIn oder Twitter und lesen Sie unsere neuesten Artikel zum Thema Datenschutz und -management im Arcserve Blog.

###

arcserve®
Protect what's priceless.

380 Data Drive, Suite 510
Draper, Utah 84020
Phone: +1 844 639 6792

Über Arcserve

Arcserve gehört weltweit zu den Top-5-Herstellern von Datensicherungslösungen und bietet als Anbieter von Unified Data Resilience Lösungen eine einheitliche Plattform für die Ausfallsicherheit von Daten an. Das Unternehmen stellt das breiteste Spektrum an Best-in-Class-Lösungen für die Verwaltung, den Schutz und die Wiederherstellung aller Datenumgebungen zur Verfügung. Die Lösungen von Arcserve eignen sich für KMUs und Großunternehmen, unabhängig von deren Standort und der Komplexität der Infrastruktur. Sie beseitigen die Komplexität und bieten gleichzeitig erstklassigen, kosteneffizienten, flexiblen und massiv skalierbaren Datenschutz und Sicherheit für alle Datenumgebungen. Dazu gehören On-Prem-, Off-Prem- (einschließlich DRaaS, BaaS und Cloud-to-Cloud), hyperkonvergente und Edge-Infrastrukturen. Dank der fast drei Jahrzehnte langen Erfahrung des Unternehmens mit preisgekrönten IP-Lösungen und der kontinuierlichen Konzentration auf Innovation können Partner und Kunden, darunter MSPs, VARs, LARs und Endbenutzer, sicher sein, dass sie den schnellsten Weg zu Daten-Workloads und -Infrastrukturen der nächsten Generation finden. Arcserve ist ein zu 100 Prozent channelorientiertes Unternehmen, das in über 150 Ländern vertreten ist und mit 19.000 Vertriebspartnern die kritischen Datenbestände von 235.000 Kunden schützt.
Erfahren Sie mehr unter arcserve.com und folgen Sie Arcserve auf Twitter oder LinkedIn.

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