PRESSEMITTEILUNG

Schluss mit den Backup-Mythen

eperi räumt mit Fehleinschätzungen zum Thema Datensicherung auf

Pfungstadt, 6. Juni 2023 – Die Relevanz und Wertigkeit von Daten rückt immer stärker in den Fokus wirtschaftlichen und gesellschaftlichen Handelns. Infolgedessen wird auch die zuverlässige Datensicherung und -wiederherstellung wichtiger. Genau der richtige Zeitpunkt, um ein paar weitverbreitete Backup-Mythen zu entlarven.

1. **Daten müssen nur gesichert werden, um sie im Katastrophenfall wiederherstellen zu können**
   Dieser Mythos wird tagtäglich widerlegt. Der Verlust von Daten gehört inzwischen zum Alltag der Unternehmen und es muss keineswegs zwingend eine Katastrophe, wie etwa ein Hochwasser, ein Feuer oder ein Ransomware-Angriff sein, damit Daten verloren gehen. Viel häufiger werden Daten aus Unachtsamkeit oder aufgrund technischer Probleme beschädigt oder gelöscht. Und ein solcher Datenverlust betrifft auch nicht zwingend nur den Server, sondern vielfach auch die Endgeräte der Mitarbeitenden. Grundsätzlich jedoch gilt, dass die Ursache für den Datenverlust zweitrangig ist. Wichtig ist ausschließlich, dass eine topaktuelle Sicherheitskopie sämtlicher Daten vorhanden ist, damit diese wiederhergestellt und möglichst unterbrechungsfrei weitergearbeitet werden kann.

2. **Der Cloud-Anbieter ist für die Sicherheit der Daten im Cloud-Backup verantwortlich**
   Auch dieser Irrglaube ist weitverbreitet und sorgt dafür, dass Cyberkriminelle oft ein leichtes Spiel haben. Fakt ist, dass die Verantwortung für die Sicherheit und den Schutz der Daten ausschließlich beim Cloud-Nutzer, sprich dem Unternehmen, liegt. Vielfach herrscht Unwissenheit darüber, welche Schutzmaßnahmen von Cloud-Anbietern überhaupt bereitgestellt werden. Zumeist gehen die Cloud-Nutzer davon aus, dass die Datensicherheit und der Datenschutz ausschließlich Sache des Cloud-Anbieters sind, was zu einem falschen Sicherheitsempfinden führt. Denn tatsächlich ist es einzig und allein die Pflicht des Nutzers sicherzustellen, dass seine Daten adäquat geschützt sind. Erschreckend ist, dass bei einer Befragung unter deutschen Führungskräften herauskam, dass 58 Prozent davon ausgehen, dass der Cloud-Anbieter die Infrastruktur, Anwendungen und Daten in der Cloud-Umgebung schützt.

3. Es gibt keinen Unterschied zwischen Datensicherung und -Wiederherstellung

   Diese Einschätzung ist falsch, denn beide – sowohl die Datensicherung als auch deren Wiederherstellung - sind für die Geschäftskontinuität von Bedeutung. Dennoch gibt es Unterschiede: Bei der Datensicherung stehen der Schutz und die sichere Aufbewahrung der Daten im Vordergrund. Im Gegensatz dazu geht es bei der Datenwiederherstellung darum, möglichst schnell gesicherte Daten abzurufen und auf Systemen wiederherstellen zu können. Folglich ist sowohl eine zuverlässige Datensicherung als auch die schnelle Datenwiederherstellung entscheidend für die Geschäftskontinuität eines Unternehmens.

4. Ein wöchentlicher Backup-Rhythmus ist ausreichend

   Einen solchen Rhythmus kann man verfolgen, allerdings ist es dann mit der Datensicherheit nicht weit her. Fakt ist, dass in der Zeit zwischen der letzten Erstellung des Backups und dem Verlust der Daten viel passieren kann. Deshalb gilt: Je kürzer die Abstände zwischen den Backups sind, desto geringer ist der potenzielle Datenverlust im Ernstfall. Der kürzeste Backup-Rhythmus ist das sofortige Backup bei jeder noch so kleinen Datenveränderung – das „kontinuierliche Backup“. Nur durch eine permanente und konsequente Datensicherung in kurzen Intervallen können lange Produktionsausfälle, große Imageschäden und vieles mehr vermieden werden. Zum Glück scheint sich dieser Gefahr schon ein Großteil der Unternehmen bewusst zu sein. Laut einer Umfrage unter 3.000 IT-Entscheidern planen 57 Prozent bis Ende des Jahres konkrete Maßnahmen, um eine moderne Datensicherung zu gewährleisten.

5. Backup-as-a-Service ist unsicherer als eine on-premise Datensicherung im Rechenzentrum

   Das Gegenteil ist der Fall: Mit der Cloud als Ziel für verteilte Datenablagen ist das Risiko eines Datenverlustes geringer als bei einer ausschließlichen on-premise Sicherung. Deshalb ist es wichtig, die Cloud in eine skalierbare und agile Backup-Strategie zu integrieren. In einer datengetriebenen Welt bringen wachsende Datenmengen auch neue Anforderung an die Datensicherung mit sich und Backup-as-a-Service ist dabei das führende Zukunftsmodell. Durch die Georedundanz liegt das Backup geographisch an einem anderen Ort, was automatisch das Risiko verringert, dass Daten durch unvorhergesehene Ereignisse wie Naturkatastrophen, technische Defekte oder menschliche Fehler verloren gehen. Außerdem verfügen Back-up-as-a-Service-Lösungen über moderne Verschlüsselungstechnologien, so dass die Daten auch dann geschützt sind, falls ein Backup in die falschen Hände geraten sollte.

6. Die native Verschlüsselung eines Cloud-Backup-Anbieters ist ausreichend

   Nein, nur mit einer starken Verschlüsselung, die vor der Übertragung in die Cloud greift, sind Daten wirklich sicher. Anderenfalls hat der Backup-Anbieter Zugriff auf Klartextdaten und das sollte vermieden werden. Wichtig ist an dieser Stelle zu klären, unter welchen Umständen öffentliche Behörden aus Drittländern Zugriff auf personenbezogene Daten von EU-Unternehmen erhalten dürfen. Um diesen Konflikt zu vermeiden, setzen viele US-Cloud-Anbieter auf EU-Tochterunternehmen, welche die Daten dann in der EU speichern. Aber auch mit diesem Konstrukt lässt sich nicht verhindern, dass ein Tochterunternehmen auf Druck einer amerikanischen Muttergesellschaft EU-Daten auch für US-Behörden freigibt. Problematisch ist zudem, dass EU-Bürger nicht das Recht haben, der Datenverarbeitung zu widersprechen - sprich es können keine Betroffenenrechte wahrgenommen werden, wie bei der DSGVO. Sensible Daten sollten deshalb unbedingt vor dem Transfer in die Cloud verschlüsselt werden und personenbezogene Daten sollten es auch während der Verarbeitung und Speicherung über die Landesgrenze hinweg bleiben.

Wie sich zeigt sind die modernen Backup-Möglichkeiten nicht nur besser als ihr Ruf, sondern ihre Nutzung ist längst überfällig. Umso wichtiger ist es, sich von alten Vorstellungen – um nicht zu sagen Vorurteilen – zu trennen und beherzt auf moderne Technologien zu setzen.

Über die Eperi GmbH:

eperi - Datenschutz ist unser Ansatzpunkt
Wir glauben, dass Datenschutz ein grundlegendes Menschenrecht ist. Unser Ziel ist es, dass Menschen zu jeder Zeit die Kontrolle über ihre Daten behalten. Ohne Kompromisse und mit der besten Technologie. Mit dem Kunden im Mittelpunkt haben wir eine Lösung geschaffen, die für den Benutzer unsichtbar ist und gleichzeitig die höchsten Sicherheitsstandards erfüllt.
Mit der eperi Lösung profitieren Unternehmen von allen Vorteilen der Cloud-Nutzung, wie bspw. einer effizienten unternehmensweiten Kollaboration – und bleiben dabei rechtssicher gemäß weltweiter Datenschutzgesetze. eperi besitzt mehrere internationale Patente für seine innovative Multi-Cloud Technologie, die einen konkurrenzlosen Datenschutz für SaaS Anwendungen, individuelle Applikationen und Dateien bietet. Der Kunde behält die alleinige Kontrolle über alle sensiblen Daten, da keine unverschlüsselten Daten in die Cloud gesendet werden.
Wir ermöglichen die Cloud – einfach, sicher, individuell, DSGVO-konform!

Pressekontakt eperi
Eperi GmbH
Sabine Jost
Gutenbergstraße 4-6
64319 Pfungstadt
Tel: +49 (0)6157 95639 16
E-Mail: sabine.jost@eperi.com
Web: www.eperi.com

Pressekontakt Agentur
TC Communications
Thilo Christ
Tel: +49 171 6220610
Alexandra Schmidt
Tel: +49 170 3871064
E-Mail: eperi@tc-communications.de