DIE KRUX MIT DEM BACK-UP UND DESSEN STRATEGISCHE BEDEUTUNG

Durch die Abhängigkeit nahezu aller Geschäftsprozesse von der IT sind Back-up und Restore elementare Bestandteile einer Business-Continuity-Strategie. Damit Unternehmen auf Nummer sicher gehen, können Back-up-Services entscheidende Hilfe leisten.

Autor: Corinna Tripp

Redaktion: Axel Pomper

➤ Die Sicherung von Daten ist seit der verantwortungsvollen Nutzung von Computern eine alltägliche und normale Sache – sollte man meinen. Doch die rasante Entwicklung der IT im Zusammenspiel mit der seit Jahren andauernden Datenexplosion hat zur Folge, dass viele Unternehmen ein Problem mit ihrer Datensicherung haben. Erstens kann oftmals nicht mit Sicherheit davon ausgegangen werden, dass Back-ups auch wirklich für ein Restore taugen. Zweitens sind viele Back-ups nicht in der Lage, die Daten sehr schnell in einem Schadensfall wieder auf die Produktivsysteme zu bringen und damit einen wichtigen Beitrag zur Business Continuity zu leisten. Drittens wird das Back-up von unglaublich vielen Daten, die sich oftmals auf verteilten Speichersystemen befinden, immer teurer, sofern nicht eine kluge Strategie beispielsweise für Back-up-Medien, ein Storage Tiering oder Cloud-Speicher angewendet wird. Und viertens werden die IT-Administratoren durch ein problematisches Back-up weit über Gebühr belastet. Allem zum Trotz ist das Back-up seit der sich zuspitzenden Gefahrenlage durch Ransomware noch wichtiger geworden, ist es doch die Versicherung gegen eine bösartige Verschlüsselung von Daten durch Cyber-Kriminelle. Es besteht Handlungsbedarf. Eine Möglichkeit, das Back-up und Restore besser und sicherer zu gestalten, sind Managed Services in Verbindung mit Back-up as a Service (BaaS). Hierbei liegt die erste Kopie meist im Unternehmen, das zweite Back-up bei einem Service Provider oder in der Cloud.

Komplexes ganz einfach mit Back-up Assessment

Virtualisierte Welten, IT in der Cloud und die ständige Verfügbarkeit der Daten und Systeme setzen moderne Back-up-Lösungen voraus, die auch wirklich funktionieren. Die Gewissheit, ob ein Back-up – gleich ob traditionell im Unternehmen oder gemeinsam mit einem BaaS-Partner – auch wirklich funktioniert und im Notfall eine schnelle und umfassende Hilfe gewährt, gehört geprüft. Dies ist Teil eines Back-up Assessments. Dabei werden die installierten Back-up-/Restore-Lösungen auf Herz und Nieren getestet und die Ergebnisse mit den Service Level Agreements (SLAs) des Unternehmens abgeglichen. Spezialisten prüfen die Leistungsfähigkeit und Zuverlässigkeit der Datensicherung und Restore-Vorgänge. Der Tool-basierte Test und der daraus folgende Report sollen Unternehmen individuell aufzeigen, ob die angestrebte Sicherheit mit der installierten Back-up-Lösung eingehalten wird und ob sowohl die rechtlichen als auch un-

ternehmensspezifischen Pflichten für die Datensicherung und deren Wiederherstellung erfüllt sind. Im Falle einer Abweichung gibt der Report Hinweise darauf, wo das Unternehmen seine Backup-Strategie oder die Lösungen für das Back-up und Restore anpassen sollte.

Nach dem Assessment wird das Back-up-Restore von den Spezialisten inklusive Management individuell ausgestaltet. Ein BaaS lässt sich sehr individuell planen und sich bei Veränderungen der Voraussetzungen vergleichsweise leicht anpassen. Die Palette der Möglichkeiten reicht von partiellen Back-ups über Sekundär-Sicherungen von Inhouse-Back-ups bis hin zur kontinuierlichen und kompletten Sicherung in unterschiedlichen Lokationen. Meist werden die Services in mehreren Stufen auf- und ausgebaut: Die erste Kopie des Back-ups wird dabei oft im Unternehmen gespeichert. Die benötigte Infrastruktur samt Wartung und Betrieb kann der Service Provider übernehmen. Damit ist vielen Unternehmen wesentlich geholfen, denn über das Remote Infrastructure Management (RIM) erfolgen alle nötigen Schritte vollautomatisch, vom Monitoring bis hin zum aktiven Eingriff durch den Servicepartner. In einem nächsten Schritt werden zusätzliche Kopien des Back-ups zum Servicepartner beziehungsweise in dessen Infrastruktur gespiegelt. Hier kommen vielfach Cloud-Technologien zum Einsatz, sofern diese mit den Anforderungen und Gesetzen kompatibel sind. Technologien wie eine Deduplizierung können für eine schnelle Datenübertragung ins Back-up-Zentrum sorgen, wo die Daten je nach vereinbartem Service Level auf passenden Medien gespeichert sind. Hierbei ist zu beachten, dass ein Restore von großen Datenmengen selbst über eine leistungsstarke Internetleitung kaum in akzeptabler Zeit realisierbar ist. Daher ist es sinnvoll auf einen Provider zu setzen, der den direkten Zugang in dessen Rechenzentrum gewährt. Hier kann im Notfall eine Kopie des Back-ups auf transportable Speichermedien gezogen werden, um dieses schnell für einen Restore zurück in die Firmenzentrale zu bekommen. Auf einer weiteren Stufe kann das Unternehmen gemeinsam mit dem Servicepartner eine Desaster-/Recovery-Strategie anstreben. Neben der reinen Datensicherung sorgt der Partner für die passende Strategie, damit das Unternehmen im Notfall möglichst keinen oder nur geringen Schaden davonträgt und die Business Continuity gewährleistet ist.

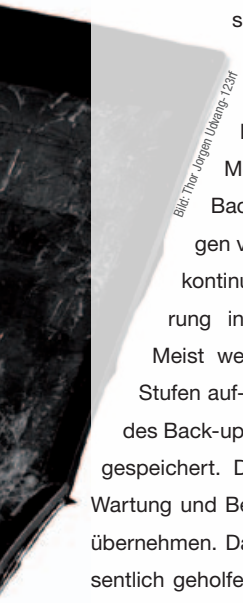

Bild: Thor_Jorgen Udvang-123rf

BACK-UP IST WEIT MEHR ALS NUR DIE SICHERUNG VON DATEN. BACK-UP IST DIE VERSICHERUNG IM SCHADENSFALL, UM GRÖSSEREN SCHADEN UND ÄRGER VOM UNTERNEHMEN FERNZUHALTEN.

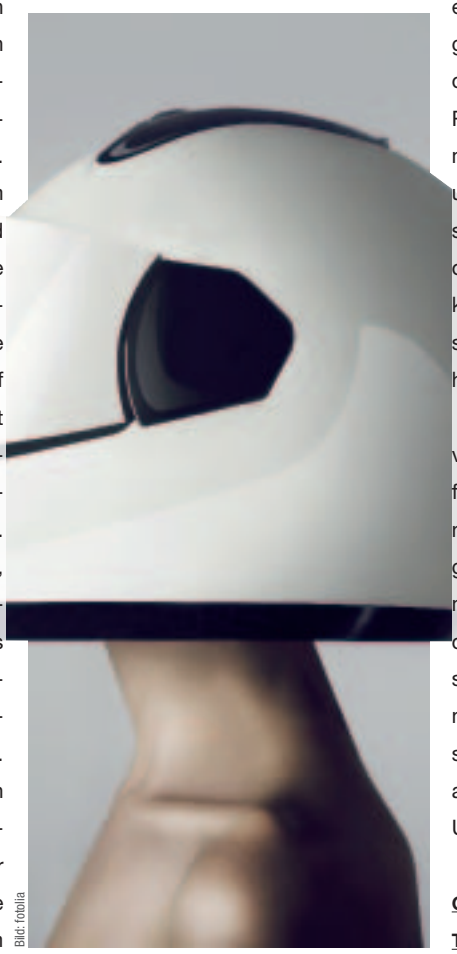

Bild: fotolia

Besondere Anforderungen an BaaS

Als wäre es nicht schon genug Arbeit und Aufwand, die Daten eines Unternehmens für den Fall von technischen Schäden oder gegen Diebstahl zu sichern, kommen seit geraumer Zeit auch noch die lästigen Cyber-Kriminellen mit ihrer Ransomware hinzu. Die Schadsoftware trifft große und kleine Unternehmen gleichermaßen, da Kriminelle keinen großen Unterschied machen. Erpressungen und Geldforderungen von einer entsprechenden Anzahl kleinerer und mittelgroßer Betriebe kann ebenso lukrativ sein wie die Erpressung von Großunternehmen. Egal wie, der fragwürdige Erfolg von Cyber-Kriminellen ist Fakt. Doch ein gutes Back-up, das auch diesen Schadensfall mit ins Kalkül zieht, ist neben der klassischen Security eine wirkungsvolle Absicherung. Ein guter BaaS-Partner wird dies berücksichtigen und das Back-up entsprechend auslegen. Ein Unternehmen ist auch bei einem Fall von Ransomware sicher, wenn sichergestellt ist, dass alle Daten auf einem anderen Medium unverschlüsselt vorliegen. Zudem ist dabei die Zeitspanne zwischen dem letzten Back-up und der Aktivierung der Ransomware entscheidend. In vielen Unternehmen ändern sich Datensätze auf den File-Servern und in den Datenbanken im Sekundentakt oder schneller. Ein Back-up, das mehrere Stunden oder gar Tage alt ist, ist daher wenig nützlich. Eine kontinuierliche Sicherungsstrategie ist daher sinnvoll, um Datensätze möglichst aktuell wiederherzustellen.

Back-up ist weit mehr als nur die Sicherung von Daten. Es ist die Versicherung im Schadensfall, um größeren Schaden und Ärger vom Unternehmen fernzuhalten. Dass Back-up in seinem gesamten Umfang heute keine Nebenaufgabe mehr ist, sollte mittlerweile allen IT-Verantwortlichen klar sein. Die Möglichkeit, diese Sicherung strategisch im Unternehmen einzusetzen, können sich große Unternehmen intern leisten. Die selbe Sicherheit kann in vielen Fällen Back-up as a Service auch für mittelständische und kleinere Unternehmen bieten.

Corinna Tripp ist Marketing Manager bei MTI Technology