

DATENSICHERUNGEN:

Für Betriebe unverzichtbar

Der Begriff „Backup“ bezeichnet im IT-Kontext eine Sicherheitskopie. Zu den gängigsten Speichermedien zählen externe Festplatten, Netzwerkspeicher (auch „NAS“ genannt) oder Cloud-Lösungen. Ausschlaggebend für die Wahl der passendsten Lösung für Unternehmen sind unter anderem die regelmäßig anfallende Datenmenge, die erforderliche Häufigkeit von Backups und das Einhalten gesetzlicher Rahmenbedingungen in puncto Datensicherheit. Eine gute Backup-Strategie beinhaltet zudem eine Failover-Lösung, wie beispielsweise weitere Speicherlaufwerke in anderen Brandzonen innerhalb eines Gebäudes oder an anderen Standorten ... von Timo Stute



TS6400
TeraStation-Gruppe



Seit Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Mai 2018 sind Unternehmen in der Pflicht, die Datenschutzprinzipien „Privacy by Design“ und „Privacy by Default“ umzusetzen, und für den Schutz der (Mitarbeiter-)Daten verantwortlich. Sie haben sicherzustellen, daß keine personenbezogenen Informationen in die Hände unbefugter Dritter gelangen, dürfen Daten nur im zwingend erforderlichen Maße erheben und müssen diese nach der Bearbeitung wieder löschen. Verstöße können empfindliche Bußgelder nach sich ziehen, so belegte etwa die Berliner Datenschutzbeauftragte die Deutsche Wohnen kürzlich mit einem Bußgeld von 14,5 Millionen Euro. Eine ebenso große Bedrohung wie der Datendiebstahl stellt ein Datenverlust dar. Im Falle eines Festplattendefekts, eines Gebäudebrands oder eines Angriffs durch Ransomware-Programme, mit denen Hacker ungefragt Dateien verschlüsseln und erst gegen eine Lösegeldzahlung wieder freigeben, können Backups bares Geld wert sein. Denn schlimmstenfalls zieht ein Datenverlust zeitintensive und kostspielige Maßnahmen nach sich, um die verlorenen Dateien neu zu beschaffen und anzulegen. Die Dringlichkeit geeigneter Gegenmaßnahmen untermauert eine Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aus dem Jahre 2018. Darin gaben 53 % der Befragten an, bereits Opfer eines Datenverlusts geworden zu sein.

Doch wie sieht die ideale Backup-Lösung aus?

Zwar punkten USB-Sticks und externe Festplatten als kostengünstige Lösung, eine zuverlässige Sicherungsstrategie erfordert jedoch den aufwendigen Paralleleinsatz mehrerer Speicher und deren Verteilung auf verschiedene Lagerplätze. Eine komfortable Alternative bieten Clouds

wie Dropbox oder Google Drive. Dadurch stehen die Daten an jedem internetfähigen Gerät zur Verfügung, allerdings geben Unternehmen ihre Daten aus der Hand und können sich nie gänzlich sicher sein, wer darauf Zugriff hat. Die Einrichtung einer professionellen Server-Infrastruktur läßt demgegenüber keine Wünsche offen, die damit einhergehenden Kosten sind jedoch allenfalls für große Betriebe zu stemmen. Eine sogenannte Hybrid Cloud kombiniert mehrere Ansätze und deren Vor- sowie Nachteile: Während sensible Informationen auf dem eigenen Server bleiben, erfolgt nur die Speicherung wenig kritischer Daten bei einem öffentlichen Cloud-Dienst.

NAS = Network Attached Storage

Die kosteneffizienteste und flexibelste Backup-Lösung für kleine und mittelständische Betriebe stellen Netzwerkspeicher, sogenannte NAS, dar. Zu den Vorteilen zählt etwa die einfache Einrichtung und Administration über eine bedienerfreundliche Nutzeroberfläche im Browser, die problemlos ohne einen ausgebildeten IT-Fachmann vor Ort gelingt. Dank eigener Rechenlogik funktioniert das NAS wie ein kleiner Server und bietet nicht nur allen PCs im Netzwerk Zugriff auf den Speicher, sondern erlaubt auch eine flexible Festlegung von Zugriffsberechtigungen. Im Inneren arbeiten mehrere Festplatten (mindestens zwei), die in einem sogenannten RAID betrieben werden. Die Abkürzung steht für „Redundant Array of Independent Disks“ und bezeichnet eine Methode, um mehrere Speicherlaufwerke zu einer Anordnung zusammenzufassen, die schneller und zuverlässiger ☞

als eine einzelne, große und teure Festplatte arbeitet. Für den Nutzer selbst erscheint das Gerät aber nur als ein einzelnes, normales Laufwerk. Der Vorteil der Technologie liegt in der fehlertoleranten Konfiguration: Die auf dem NAS abgelegten Daten werden automatisch dupliziert und über mehrere Festplatten hinweg gespeichert. Fällt ein Laufwerk in einem RAID aus, sind die Daten immer noch auf den restlichen, intakten Medien vorhanden und verfügbar. Die unterschiedlichen RAID-Stufen weichen im Hinblick auf die Fehlertoleranz und Leistung voneinander ab. So bietet ein RAID 1, das zwei interne Festplatten erfordert, die höchste Zuverlässigkeit und Geschwindigkeit, reduziert jedoch den zur Verfügung stehenden Speicherplatz auf die Hälfte. Für vier oder mehr Festplatten bietet sich ein RAID 5 oder RAID 6 an: Dabei können eine (RAID 5) beziehungsweise zwei (RAID 6) Festplatten ohne Datenverlust ausfallen, gleichzeitig steht dem Nutzer deutlich mehr Speicherplatz zur Verfügung. Ein NAS ist problemlos erweiterbar: Je nach Gerät lassen sich nachträglich weitere Festplatten hinzufügen. Alternativ besteht die Möglichkeit, weitere NAS in das Netzwerk zu integrieren.

Voll-Backup

Es existieren verschiedene Strategien, um eine Sicherung anzulegen. Die aufwendigste Methode ist das Voll-Backup, das stets alle Dateien komplett sichert. Das bietet zwar den größten Schutz, dauert aber auch lange. Beim differenziellen Backup hingegen erfolgt nur zu Beginn eine Komplettsicherung. Danach werden Teil-Backups angefertigt, die jeweils alle Daten enthalten, die seit dem letzten Voll-Backup geändert oder hinzugefügt wurden. Der Vorteil ist, daß für eine Daten-Wiederherstellung nur das anfängliche Voll-Backup und die neueste Teil-Speicherung benötigt werden. Diese Methode beansprucht aber auch viel Speicherplatz und Zeit. Bei der inkrementellen Sicherung erfolgt zu Beginn zwar ebenfalls eine Voll-Sicherung, fortan jedoch nur noch eine Speicherung der Änderungen seit dem letzten Teil-Backup. Das geht schnell, aber für die Datenwiederherstellung sind alle Teilsicherungen notwendig. Ist eine nicht mehr vorhanden, fehlen bestimmte Daten. Regelmäßige, zeitintensive Backups leisten einen wichtigen Beitrag, um den eigenen Datenbestand vor der steigenden Anzahl an Ransomware-Attacken zu schützen.

Snapshots = Momentaufnahmen

Demgegenüber kann das Anfertigen von Snapshots (Momentaufnahmen) auf dem NAS selbst sowie Snapshot-Backups auf anderen Geräten, wie sie die

aktuelle NAS-Generation der Buffalo TeraStation 6000-Serie ermöglicht, eine besonders schnelle Abhilfe schaffen, falls wichtige Dokumente eines Unternehmens durch Schadsoftware verschlüsselt wurden und nicht mehr zugänglich sind. Bei klassischen Backups handelt es sich um physische Kopien von Dateien, Snapshots hingegen speichern Informationen darüber, wann welcher Teil einer Datei geändert wurde – und zwar entlang eines Zeitstrahls in zahlreichen Versionen. Im Falle des versehentlichen Löschens, Überschreibens oder der Verschlüsselung durch Ransomware ist es somit möglich, zur letzten oder einer beliebigen, vorherigen Version zurückzuspringen, um wieder den Zustand von vor der Verschlüsselung herzustellen.

Bei einem Snapshot-Backup handelt es sich um einen besonderen Ansatz von Buffalo, der beide Methoden kombiniert. Dadurch lassen sich etwa die Daten von einem NAS auf ein zweites Modell kopieren. Der Vorteil: Ein Snapshot-Backup sichert alle Dateien in ihrem Zustand beim Start des Vorgangs, sodaß es möglich ist, während des laufenden Prozesses damit weiterzuarbeiten. Ein traditionelles Backup kann das nicht leisten, denn hier werden die Daten nacheinander gesichert. Befindet sich dabei eine Datei gerade in Bearbeitung, hat das möglicherweise eine fehlerhafte Übertragung zur Folge. Da Snapshots ressourcen- und platzsparend funktionieren, empfiehlt es sich, diese mehrfach pro Arbeitstag auszuführen, um im Problemfall auf möglichst viele Versionen der Datenbestände zurückgreifen zu können.

Grundsätzlich läßt sich also festhalten, daß auch kleine und mittelständische Unternehmen, ebenso wie große Firmen, eine zuverlässige Speicher- und Backup-Lösung benötigen, die im Vergleich aber kostengünstiger sein muß und sich einfach ins Netzwerk integrieren und verwalten läßt. In unseren Augen ist für diese Betriebsgruppe ein NAS die aktuell ideale Lösung. <<



Timo Stute, Team
Leader Sales
Central Europe bei
Buffalo EU B.V.
Alle Bilder: Buffalo

IMPRESSUM

Computern im Handwerk/ handwerke.de

gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten“ Wissens- und Technologie-Transfer.

Herausgeber: Horst Neureuther

© Copyright: **CV München
CV Computern-Verlags GmbH
Goethestraße 41, 80336 München**

Telefon 0 89/54 46 56-0

Telefax 0 89/54 46 56-50

Postfach 15 06 05, 80044 München

E-Mail: info@cv-verlag.de

redaktion@cv-verlag.de

www.handwerke.de

Geschäftsleitung:

Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:

Dipl.-Vw. Heide Tschinkel-Neureuther

e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle

Mitarbeiter in dieser Ausgabe:

Tobias Heller, Björn Lorenz, Horst Neureuther (verantw.), Gundo Sanders, Timo Stute, Sarah Tietjen

Anzeigenvertretung:

Medienmarketing SANDERS

Tel. 0 72 03/50 27 270

Mail: gsanders@mm-sanders.de

Layout:

AD&D Werbeagentur GmbH,
Silvia Romann, Dietmar Kraus

Druck: Niederösterreichisches
Pressehaus Druck- und Verlagsgesellschaft m.b.H., St. Pölten

Druckauflage: 52.500

Tatsächliche Verbreitung:
51.521 (III/19)



Auflage und Verbreitung kontrolliert.

35. Jahrgang

Erscheinungsweise: 10 x jährlich

Abo-Preis:

29,- € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €

Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679

Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 37 vom 01.11.2019.

Titelkopf: © Fotolia.de/yellow