VOM SOLARWINDS-BLOG

Ein Leitfaden zum Entwickeln einer Backup-Strategie für kleine Unternehmen

von Nick Cavalancia

Nick Cavalancia ist ein unabhängiger Autor und kein Mitarbeiter von SolarWinds.
19. Oktober 2016

Ich bin seit mehr als 25 Jahren in der IT-Branche tätig und komme dort oft mit Fachleuten aus allen möglichen Spezialgebieten in Kontakt. Wenn ich über Backups rede (was recht häufig geschieht), gehe ich entsprechend davon aus, dass mein Gesprächspartner mit den Grundlagen vertraut ist.

Aber gerade in kleinen oder mittelständischen Unternehmen ist das nicht immer so einfach. Dort übernehmen Sie so viele verschiedene Aufgaben in der IT, dass die Datensicherung nur eine von vielen ist. Da ist manchmal ein kleiner Anstoß in die richtige Richtung vonnöten.

Wie also planen Sie Ihre Backup-Strategie für ein kleines Unternehmen am besten?

In den letzten zwei Jahren habe ich zahlreiche Artikel zum Thema Backup und zum „Wie" und „Warum" geschrieben. All diese Artikel nun zu durchforsten, wäre sicher etwas mühselig für Sie, deshalb fasse ich das Wesentliche daraus in einer einzigen Handreichung zusammen.

Ich habe die einzelnen Punkte als Fragen formuliert, die Sie sich vielleicht selbst schon gestellt haben und die ich dann Schritt für Schritt durchgehe. Sie können also jederzeit direkt zu der Frage springen, die für Sie relevant ist.

WARUM MÜSSEN DATEN ÜBERHAUPT GESICHERT WERDEN?

Wenn Sie diese Frage absurd finden, können Sie gleich ein paar Zeilen überspringen. Aber es gibt auch heute durchaus noch Unternehmen – und zwar nicht nur Kleinbüros und Homeoffices –, die noch immer keine Backups durchführen. Die Datensicherung ist aus folgenden Gründen unerlässlich:

1. Wenn ein kritischer Teil Ihrer Geschäftsumgebung ausfällt, können Sie keinen Umsatz machen.
2. Kunden erwarten heutzutage von Unternehmen jeder Größe ständige Verfügbarkeit.
3. Ohne eine Backup-Strategie dauert es nicht nur wesentlich länger, beschädigte Datensätze oder ausgefallene Anwendungen und Systeme wiederherzustellen, es dauert auch länger, die Geschäftstätigkeit wieder auf Normalniveau zu bringen.

WARUM KANN ICH NICHT EINFACH EIN SYNCHRONISIERUNGSTOOL VERWENDEN?

Ich selbst nutze einen Cloud-Synchronisierungsanbieter zum Backup wichtiger Dateien – allerdings nur für meinen persönlichen Laptop. Natürlich können Sie die Dateien und Ordner Ihres Dateiservers mit Google Drive/OneDrive/Dropbox/usw. synchronisieren. Aber damit haben Sie noch nicht den gesamten Server gesichert. Für die einfache Sicherung von Dateisätzen sind Synchronisierungstools eine prima Sache. Sie ersetzen aber keinen echten Backup, aus dem Sie Ihren Geschäftsbetrieb wieder vollständig herstellen können.

WELCHE ART BACKUP IST DIE RICHTIGE FÜR MICH?

Es gibt zahlreiche Optionen und jeder Anbieter preist natürlich das eigene Produkt als das einzig Wahre an. Als Erstes müssen Sie sich fragen: Was ist für Ihr Unternehmen wichtig – die Wiederherstellung von Dateien, die zügige Wiederaufnahme des Betriebs oder die kontinuierliche Verfügbarkeit? Diese Frage kann ich Ihnen nicht beantworten. Nur Sie selbst können sagen, was für Ihr Unternehmen am wichtigsten ist.

Dann stellt sich natürlich die Frage, wo Ihre Backups gespeichert werden sollen. Das kann vor Ort sein, in der Cloud oder auch in einer Hybrid-Cloud-Architektur. All diese Lösungen haben Vor- und Nachteile. Wenn Sie alles auf ein Pferd setzen und sich für die Sicherung ausschließlich vor Ort oder ausschließlich in der Cloud entscheiden, besteht die Gefahr, dass genau diese Option ausfällt – durch einen Standortausfall oder eine Unterbrechung der Internetverbindung. Beim Hybrid-Cloud-Backup können Sie synchronisierte Sicherungskopien an beiden Orten aufbewahren. Damit sind Sie für so ziemlich alles gewappnet.

WAS MUSS GESICHERT WERDEN?

Ganz klar: *Alles*! Der Sinn und Zweck der Disaster Recovery in einem kleinen Unternehmen ist die Fähigkeit, nach jedem Zwischenfall möglichst zügig weitermachen zu können. Am einfachsten geht das mit Image-Backups. Dabei wird jeweils das gesamte System (ob physisch oder virtuell) als ein einziger Datensatz gesichert (mehr dazu später).

Wahrscheinlich haben Sie noch keine richtige Backup-Strategie, sonst würden Sie das hier nicht lesen. Über die Sicherung Ihrer allerwichtigsten Server und Dienste müssen Sie aber allemal nachdenken.

WELCHE BACKUP-METHODEN GIBT ES?

Die Backup-Methoden lassen sich im Prinzip in zwei Kategorien aufteilen: Backups auf Dateiebene und Backups auf Image-Ebene. Dateiebenen-Backups sind hervorragend zur Sicherung von Dateien und Ordnern auf Ihrem Dateiserver geeignet. Sie können auch zur Sicherung von Datenbanken bestimmter Anwendungen genutzt werden. Anwendungsspezifische Backups (bei denen bereits bekannt ist, was für die jeweilige Anwendung gesichert werden muss) vereinfachen Dateiebenen-Backups, da alle für die Wiederherstellung einer Anwendung relevanten Datensätze automatisch erfasst werden.

Image-Backups eignen sich besonders für die Gesamtsicherung eines kompletten Systems. Bei einem Image-Backup haben Sie außerdem Zugang zu einer raschen Wiederherstellung (sowohl lokal als auch remote) mithilfe eines Modells für kontinuierliche Wiederherstellung. Dabei wird jedes Mal, wenn ein Backup durchgeführt wird, auch eine Wiederherstellung des Backups durchgeführt.

WAS SOLL GESICHERT WERDEN?

Was gesichert werden muss und welche Methode am besten geeignet ist, hängt technisch betrachtet eng damit zusammen, welche Bedrohungen am wahrscheinlichsten sind. Wenn Sie sich darüber nicht im Klaren sind, ist das Ganze wie Kofferpacken, ohne zu wissen, wohin die Reise geht. Sie müssen also zunächst die Bedrohungen ermitteln, vor denen Sie Ihr Geschäft schützen müssen. Daraus ergibt sich dann, was genau gesichert werden muss. Wenn Sie sich beispielsweise nur darum sorgen, dass Dateien gelöscht werden könnten, dann ist ein Image-Backup etwas übertrieben. Wenn Sie sich aber vor einem umfassenden Standortverlust schützen möchten, sind Dateiebenen-Backups der einzelnen Server nicht besonders sinnvoll, da die Wiederherstellung viel zu lange dauern würde.

WELCHE WIEDERHERSTELLUNGSZIELE GIBT ES?

Für alle Datensätze, Anwendungen und Systeme, die wiederhergestellt werden sollen, müssen Sie ein paar Parameter festlegen. Dazu bietet die Branche hilfreiche Kriterien. Als Erstes müssen wir uns das Recovery Time Objective (RTO) ansehen, also die Zeitspanne, die bis zur Wiederherstellung vergehen darf. Dann haben wir das Recovery Point Objective (RPO). Darunter wird der maximale akzeptierte Datenverlust verstanden, der sich aus der Zeitspanne zwischen den Sicherungen ergibt (z. B. Verlust von Daten aus 15 Minuten). Und schließlich gibt es noch die MTPoD (Maximum Tolerable Period of Disruption). Diese gibt an, welche Ausfalldauer zulässig ist, bevor die Betroffenen unruhig werden. Anders gesagt, wird damit angegeben, wie lange es dauert, bevor das Geschäft wirklich unter dem Ausfall leidet.

Diese Werte müssen Sie für jeden Sicherungssatz ermitteln. Beginnen Sie dabei mit dem Wichtigsten und arbeiten Sie sich nach unten durch. Der Grund? Wenn Sie beispielsweise für die Unternehmenswebsite ein RTO von 10 Minuten und ein RPO von lediglich 15 Minuten ermittelt haben, könnten Sie zum Beispiel von den derzeitigen Dateiebenen-Backups auf eine kontinuierliche Wiederherstellung auf Image-Ebene umsteigen. Sehen Sie, wie sich alles nach und nach zu einem Bild fügt?

WIE ERSTELLEN SIE EINEN DISASTER-RECOVERY-PLAN FÜR EIN KLEINUNTERNEHMEN?

Im Plan sollten zunächst alle Datensätze aufgeführt sein sowie die Notfälle, gegen die Sie sich wappnen möchten. Sehen Sie sich dann jeweils die Überschneidung dieser zwei Aspekte an. Sie müssen konkret festlegen, welcher Datensatz zu sichern ist und wie die Wiederherstellung erfolgen soll. Das können Sie bis hin zu jedem erforderlichen Einzelschritt ausfeilen, allerdings muss das nicht sein. Zumindest sollten Sie aber den Wiederherstellungstyp, den wiederherzustellenden Datensatz, eventuell zu beachtende Abhängigkeiten (z. B. Active Directory) und nach der Wiederherstellung durchzuführende Schritte festhalten.

SIE TESTEN DAS ALLES AUCH, ODER?

Vielleicht schwirrt Ihnen schon ein wenig der Kopf ob all dieser Optionen und der Aufgaben, die ich Ihnen allein zur richtigen Datensicherung aufgegeben habe. Und jetzt sollen Sie das Ganze auch noch testen?

Dies ist der schwierigste Schritt, denn einen Notfall zu simulieren und dann die Wiederherstellung daran zu testen, kostet Zeit und Ressourcen. Es ist aber auch der wichtigste Schritt – denn wenn Sie den Plan nicht testen, wissen Sie nicht, ob er überhaupt funktioniert. Das absolut minimale Testszenario wäre, den Plan mit dem Team, das an der Wiederherstellung beteiligt wäre, durchzugehen. Spielen Sie alle Schritte durch und besprechen Sie, was schieflaufen könnte und was dann zu tun wäre. Optimalerweise führen Sie tatsächlich eine Wiederherstellung auf einem anderen Server oder Standort durch und prüfen, ob sich die vorhandenen Backups problemlos zur Wiederherstellung nutzen lassen.

KÖNNEN SIE DAS SELBER MACHEN?

Gut möglich, dass all das hier Beschriebene (Backup-Strategie, Planung und Testen) über Ihr Fachwissen oder Ihre verfügbare Zeit hinausgeht. Doch es gibt zahlreiche IT-Dienstleister, die Backup-Dienste anbieten und Ihnen dabei unter die Arme greifen können.

SCHRITT FÜR SCHRITT ZU EINER BESSEREN BACKUPSTRATEGIE FÜR KLEINE UNTERNEHMEN

Wenn Sie die Tipps dieses Backup-Leitfadens befolgen, sind Sie Ihrem Ziel schon wesentlich näher: einen produktiven Geschäftsbetrieb zu gewährleisten, der allen Katastrophen widersteht. Mit einer soliden Backup-Strategie sind auch kleine Unternehmen viel besser aufgestellt, mit dem Verlust von Daten, Anwendungen oder ganzen Systemen klarzukommen.