WEBSITE-BACKUPS MIT BORDMITTELN

goneo Internet GmbH Marienwall 27, 32423 Minden

WEBSITE-BACKUPS MIT BORDMITTELN

SICHERHEITSKOPIEN VON WEBINHALTEN UND WEBAPPLIKATIONENEN HERSTELLEN, PRÜFEN UND BEI BEDARF WIEDER ZURÜCKSICHERN.

INHALTSVERZEICHNIS

WAS ERFÄHRT MAN IN DIESEM TEXT?

Wir beschäftigen uns auf den folgenden Seiten mit der Frage, wie sich Backups von kompletten Websites (im Sinne von Webauftritten) möglichst effizient anfertigen lassen. Dabei versuchen wir, hauptsächlich „Bordmittel" zu benutzen, also Tools und Features, die im Wesentlichen zur Grundausstattung eines klassischen Webhostingpakets gehören. Als Nutzer (Kunde) hat man meist FTP-Zugriff (File Transfer Protocol), in manchen Fällen ist auch eine Verbindung per SSH (Secure Shell) möglich. Die meisten kleinen bis mittelgroßen Websites werden heute durch eine Datenbank wie MySQL oder MariaDB unterstützt. Die meistgenutzten Open Source Webanwendungen setzen die Skriptsprache PHP und die Unterstützung einer Datenbank voraus, wobei die Verbreitung von WordPress außerordentlich hoch ist. Mehr als 20 Prozent aller Sites sollen auf WordPress basieren.

Auch die Backupstrategie spielt eine wichtige Rolle und wir beschäftigen uns mit der Frage, wie im Ernstfall, bei Datenverlust, reagiert werden sollte, wo die Backups aufbewahrt werden sollten und wie man sich auf den Ernstfall vorbereiten kann.

AN WEN RICHTET SICH DIESER TEXT?

Backups von Festplatten, die in Desktop-PCs oder Notebooks verwendet werden, spielen hier nur eine sehr untergeordnete Rolle. In diesem Text, der sich an Webseitenbetreiber richtet, die Sicherheitskopien vorhalten wollen, wird beschrieben, wie sich vollständige Backups von Websites herstellen lassen, aus denen man die Webanwendung wieder rekonstruieren kann.

Die meisten Prozeduren, die hier beschrieben werden, sind allgemeingültig. Auch wenn goneo als Beispiel für ein Hostingunternehmen genannt wird, bei dem Kunden Webseiten einrichten und betreiben können, sollten die Hinweise auch für andere Unternehmen dieser Art gelten.

Dieser Text soll dem Leser einen Überblick über die Möglichkeiten bieten, wie Sicherheitskopien von Webanwendungen samt Datenbankinhalten angefertigt und zur Wiederherstellung, zum Beispiel bei Datenverlust verwendet werden können.

Leser, die eine Webseite betreiben, die auf einem sogenannten Shared Server untergebracht ist, zu dem eine FTP-Verbindung aufgebaut werden kann, werden vermutlich am meisten profitieren.

DISCLAIMER

Die Informationen in diesem Text wurden mit großer Sorgfalt recherchiert und überprüft. Dennoch sind Irrtümer nicht ausgeschlossen. Das Befolgen bzw. Anwenden der Hinweise erfolgt auf eigene Gefahr. Es kann keine Gewährleistung für die Richtigkeit, Vollständigkeit oder Aktualität der beschriebenen Verfahrensweisen, Beschreibungen und Funktionsweisen übernommen werden. Keine Haftung für Schäden an Datenverarbeitungsanlagen oder Verlust von Daten, die möglicherweise aus der Anwendungen der hier vorgestellten und beschriebenen Verfahrensweisen resultieren.

Bei den Begriffen Anyconnect, AVI, Contao, Cyberduck, Drupal, JavaScript, Joomla, FileZilla, Flash, FLV, JPG, MAC OS, Microsoft, MySQL, MySQLDumper, ownCloud, OS X, PDF, PHP, Sqlite, Total Commander, TYPO3, Windows, WinSCP, WordPress, WS-FTP lite, XCloner handelt es sich um Markennamen, an denen Rechte bestehen, die von den jeweiligen Inhabern gehalten werden.

EINIGE ALLGEMEINE WORT ÜBER BACKUPS

WAS VERSTEHT MAN ALLGEMEIN UNTER EINEM BACKUP?

Wir verstehen hier Backup als eine automatische oder manuelle Sicherung von Daten aller Art. Bei diesen Daten kann es sich um ausführbaren Programmcode handeln, um das abgespeicherte Ergebnis einer Arbeit mit einem Textverarbeitungsprogramm oder eine Tabellenkalkulation oder auch um Bilder, Videoclips oder viele andere Dateiarten.

Mit dem Begriff Backup bezeichnet man im Allgemeinen sowohl den Prozess des Herstellens einer Sicherheitskopie von Daten als auch die Sicherheitskopie selbst.

In anderen Lebensbereichen oder Branchen wird der Begriff Backup ebenfalls verwendet, allerdings oft auch mit einer anderen Konnotation: So kann Backup auch „Beistand" oder „Unterstützung" bedeuten. Gelegentlich meint man mit Backup auch ein zweites System, das zum Einsatz kommt, wenn das erste bzw. das primäre ausfällt.

WARUM BRAUCHT MAN BACKUPS?

Da grundsätzlich jedes technische System ausfallen kann, ist es ratsam, im Sinne einer Vorsorge regelmäßig Sicherheitskopien der Datenbestände herzustellen oder, allgemein formuliert, einen Ersatz vorzuhalten.

Doch nicht nur durch technische Defekte entsteht der Bedarf nach Backups. Auch menschliche Fehler können zu Datenverlust führen. Das ist zum Beispiel dann der Fall, wenn eine Anwendung geschlossen wird, bevor die Datei, die man damit erzeugen wollte, abgespeichert wurde. Zwar haben die Softwarehersteller unter Umständen Sicherungsmechanismen eingebaut, doch allein durch Gewöhnung und automatisiertes Handeln klickt man auch die Warnfenster schnell mal weg. Warum solche menschlichen Fehler entstehen ist zwar gut erforscht, allerdings gibt es letztlich kein wirksames Mittel, menschliche Fehler komplett zu verhindern. Eine Strategie mit dieser Fehlerwahrscheinlichkeit umzugehen, ist Vorsorge zu betreiben, eben durch Backups.

Nicht zu vergessen: Nicht nur durch Fehlbedienung, auch durch unentdeckte Fehler im Programm können Daten zerstört werden. Das geht bis hin zu einem Datenverlust durch Zerstörung des Dateisystems. Keiner der Anbieter von Open Source Content Management Systemen wird Garantien für eine korrekte Funktionsweise seines Systems geben.

Es ist klar, dass das Herstellen von Sicherungskopien Mühe und Zeit erfordert. Wahrscheinlich liegt es daran, dass man diesen Aufwand zunächst als verzichtbar ansieht und das Backup aufschiebt. Je nach Umfang der Datenmenge dauert es auch eine gewisse Zeit, ehe das Backup erstellt ist. Für die Herstellung der Sicherungskopien muss der Computer einen Teil seiner Rechenkapazität aufwenden, was sich möglicherweise in einer deutlich verlangsamten Verarbeitungs- und Reaktionsgeschwindigkeit für andere Anwendungen

niederschlägt. Auch dieser Effekt trägt dazu bei, dass Backups nicht zu den beliebtesten Aufgaben gehören, die man sich am Rechner vorstellen kann.

Viele Menschen schätzen den Wert eines Backups anfänglich also eher als gering ein. Bedeutungsvoll wird ein Backup allerdings dann, wenn tatsächlich ein Schadenfall mit Datenverlust auftritt.

Welches Risiko tatsächlich durch die Möglichkeit eines technischen Versagens gegeben ist, lässt sich für viele Systeme durchaus angeben, ist aber aufgrund der Daten, die man zu einer validen Abschätzung braucht, recht aufwendig.

So kann man sich bei technischen Geräten auf die Zeit zwischen Ausfällen beziehen und die sogenannte Mean Time Between Failures (MTBF) ermitteln. Dies ist bei neuen Geräten kaum möglich, wenn diese noch nicht ausgefallen sind. Zudem braucht man recht viele Beobachtungen, um zu verlässlichen Mittelwerten zu gelangen. Tatsächlich findet sich in Datenblättern zu Festplatten ein MTBF-Wert. Dies ist ein unter Laborbedingungen ermittelter Wert. Zudem wird auch ein Wert für Power-On-Hours (PHO) angegeben. Bei vielen Platten liegt dieser um die vier Jahre. Ein weiterer wichtiger Anhaltspunkt kann die jährliche Ausfallrate sein, annual failure rate, kurz AFR genannt.

Diese statistischen Angaben, die aus empirisch ermittelten Daten gewonnen wurden, lassen erkennen, dass es keine Sicherheit für Ihre Daten auf den Festplatten gibt. Das Risiko ist stets größer als 0,000 Prozent. Die Frage ist also nicht, ob es zu einem Datenverlust kommt, sondern wann. Leider lassen sich dafür nur Wahrscheinlichkeiten angeben.

Bei einem System wie einem Desktop-PC könnte man nun die Fehlerwahrscheinlichkeiten addieren. Jedes Komponente kann ausfallen: Die Festplatte, der Controller, die Hauptplatine, der Prozessor, die Speicherbausteine, das Netzteil usw. Das ist bei Servern, die für den Hostingbetrieb eingesetzt werden, nicht anders. Unter anderem deswegen werden Verfügbarkeitszeiten angegeben, die typischerweise in Größenordnungen von 99,8 bis 99,9 Prozent im Jahresmittel liegen. Ausfälle werden in diesem Bereich oft mit Umschalten auf ein redundantes Backupsystem oder durch Tausch der Hardware kompensiert, so dass die Ausfallzeit insgesamt gering bleibt.

Wichtig ist, sich zu vergegenwärtigen, dass grundsätzlich ein Risiko besteht, dass ein Gerät oder eine technische Komponente eine Fehlfunktion entwickelt, die zu einem Datenverlust führen kann.

Auf der anderen Seite ist klar, dass man die Kosten eines Backups dem Risiko gegenüber stellen muss, allein schon aus ökonomischen Gründen: Backups kosten Zeit, Nerven und Geld (man benötigt schließlich Speicherplatz). Und es gibt wichtige und unwichtige Daten.

Dies gilt im Übrigen auch für Daten, die auf der heimischen Festplatte abgespeichert sind. Auch PC, Notebook, Smartphone und Tablets können kaputt gehen (oder auch verloren gehen). Daher haben viele Betriebssysteme Backuptools eingebaut. Je nach System nerven einige Popups oder Hinweise, dass man doch bitte schön ein Backupmedium anschließen solle oder einen Zeitplan festlegen müsse. In vielen Fällen werden die Backups erstellt, indem die Daten auf

eine externe Festplatte kopiert werden. Gegebenenfalls kann man diese kopierten Daten komprimieren, um Platz zu sparen oder auch verschlüsseln.

In einigen Fällen ist auch eine Sicherungskopie in die Cloud möglich. In diesem Fall wird die Kopie der Daten auf einem Server abgelegt, der sich irgendwo befindet. In den meisten Fällen wissen Sie nicht wo. Es bleibt Ihnen nichts anderes übrig als dem Speicheranbieter zu vertrauen.

Wichtiger wird es zudem, sich gegen Datenverluste zu schützen, die aufgrund krimineller Aktivitäten entstehen, also zum Beispiel durch Hacking oder andere „Cyberangriffe".

Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt ein Datensicherungskonzept im Rahmen des IT-Grundschutzes.

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b01/b01004.html

AUTOMATISCHE BACKUPS DES ANBIETERS

Für den Fall eines Ausfalls der technischen Anlagen schützen sich die Anbieter von Hostingdienstleistungen vor Datenverlust, indem täglich vollständige Backups der auf den Kundenservern gespeicherten Informationen angelegt werden. Es werden in der Regel mehrere Backupgenerationen vorgehalten, so dass im Bedarfsfall Daten wieder hergestellt werden können.

Zudem werden die Server auch mit redundanten Plattenspeichern betrieben (RAID), so dass auch hier mehr Sicherheit gegeben ist als beim heimischen Rechner oder beim Büro-PC.

Grundsätzlich können die Anbieter auch einzelne Datenbestände zurücksichern, die auf dem Webspace von Kunden und in den Datenbanken liegen. Dies ist aber meist mit manuellem Aufwand verbunden, so dass extra Kosten fällig werden können. Eigene Backups sind also dringend anzuraten.

USERSEITIGE BACKUPS

Die meisten Betreiber von Serverfarmen empfehlen Kunden, selbst regelmäßig Backups anzulegen. So kann man selbst jederzeit bei Bedarf auf verlorengegangene Datenbestände zurückgreifen. Ein Datenverlust kann übrigens nicht nur durch technischen Ausfall entstehen, sondern auch zum Beispiel dadurch, dass man Daten versehentlich überschreibt.

Im einfachsten Fall können Webseitenbetreiber per FTP und einem geeigneten Programm wie FileZilla die Dateien, die im Verzeichnis auf dem Server gespeichert sind, herunterladen und gegebenenfalls komprimiert auf einer Festplatte ablegen.

Die Inhalte von MySQL-Datenbanken können mit einem Tool wie MySQLDumper gespeichert werden. Diese kostenlose Anwendung lässt sich per goneo clickStart schnell installieren und kann so eingestellt werden, dass Sicherungen der Datenbankinhalte gepackt auf ein vorbestimmtes Verzeichnis abgelegt werden. Die gepackte Datei kann dann heruntergeladen werden. Umgekehrt kümmert sich

MySQLDumper auch um die Wiederherstellung der Datenbank, wenn dies nötig werden sollte (dazu mehr im Kapitel über MySQLDumper).

WICHTIGKEIT VON SICHERHEITSKOPIEN

Wie sinnvoll regelmäßige Datensicherungen sind, wird erst richtig deutlich, wenn sie benötigt werden. Dabei muss es noch nicht einmal unbedingt zum technischen Ausfall gekommen sein. Gerade im Umgang mit Website-Daten kann es schnell passieren, dass Daten unbeabsichtigt vom User überschrieben, aber dennoch benötigt werden. Hier ist ein eigenes Backup immer hilfreich, um schnell und einfach den vorherigen Zustand wieder herzustellen. Es sollten mehrere Generationen an Backups aufbewahrt werden.

DATENSCHUTZ

Im Idealfall lässt sich aus den kopierten Daten das vollständige System wieder herstellen (das ist ja schließlich Sinn und Zweck eines Backups). Die kopierten Daten müssen also geschützt werden, so wie Originaldaten auch. Man darf nicht vergessen, dass unter Umständen personenbezogene Daten Dritter mitgesichert wurden. Das ist dann der Fall, wenn über die Website Daten von Usern erhoben worden sind, zum Beispiel für Newsletter-Registrierungen oder Anmeldedaten für ein Blog oder Forum.

Es kann daher sinnvoll oder erforderlich sein, die gesicherten Daten verschlüsselt abzuspeichern. Hierbei lauert aber eine Gefahr: Ein Hardwareschaden ist im Regelfall glücklicherweise ein seltenes Ereignis. So kann es passieren, dass ein vor längerer Zeit festgelegtes Passwort, mit dem die Daten verschlüsselt worden sind, in Vergessenheit gerät. Auch wenn man das Passwort niederschreibt und an einem vermeintlich sicheren Ort deponiert, besteht Verlustgefahr, die mit der Zeit größer wird. Ohne dieses Passwort sind die gesicherten Daten nicht wieder herstellbar und machen das Backup nutzlos.

Zudem können die Backupmedien, also die Datenträger gestohlen oder verloren werden. Ein USB Stick fällt schnell mal aus der Tasche, auch eine externe Festplatte bleibt schnell mal irgendwo liegen und kommt abhanden. Nichtehrliche Finder – und damit muss man rechnen - könnten unverschlüsselte Daten für ihre Zwecke verwenden.

Das gilt übrigens auch für alte Datenträger, die als Backupmedium benutzt worden sind. Wenn diese nicht mehr gebraucht werden, sollte man auch alte Daten löschen. Das gilt auch für Dateien, die sich auf Cloudspeicherplätzen oder ausrangierten Festplatten befinden.

VERSCHIEDENE BACKUPSTRATEGIEN

Es gibt verschiedene Strategien bei der Herstellung von Backups. Sie können den kompletten Datenbestand sichern (Vollbackup), einen Teil davon (partielles Backup) oder den Teil des gesamten Bestands, der sich seit der letzten Sicherung geändert hat (inkrementelles Backup bzw. differenzielles Backup). Gerade wenn die Datenbestände größer werden, ist ein regelmäßiges vollständiges Backup zwar wünschenswert, aber nicht immer praktikabel.

VOLLBACKUP

Wird der komplette Datenbestand gesichert, spricht man von einem Vollbackup. Es liegt nach dem Sicherungslauf eine vollständige Kopie der Daten vor. Aus einem Vollbackup lässt sich, wenn keine Probleme aufgetreten sind, der Zustand des Systems vor einer Havarie wieder herstellen. Nur die Änderungen, die zwischen Backupzeitpunkt und Schadenszeitpunkt an den Daten vorgenommen worden sind, sind verloren.

Das Vollbackup ist eine recht einfache, aber auch sehr speicherplatzintensive und zeitfressende Variante eines Backups. Es dauert einfach - je nach Backupmedium – eine gewisse Zeit, ehe alle Daten kopiert sind. Und während dieses Vorgangs können sich schon wieder Dateien verändert haben.

Das passiert in Zusammenhang mit Websitedaten dann, wenn während des Kopierens User über das Internet auf die Website zugreifen und zum Beispiel in einem Blog Kommentare hinterlassen, Voting vornehmen und ähnliche Interaktionen unternehmen. Will man sicher gehen, dass eine 1:1 Kopie erstellt wird, müsste man für die Dauer des Sicherungslaufs den Zugriff sperren. Das senkt natürlich die Qualität der Nutzungserfahrung und sollte daher vermieden werden.

PARTIELLES BACKUP

Oftmals reicht es, einen Teil des gesamten schützenswerten Datenbestands zu sichern. So könnte man zum Beispiel bei einer Webseite nur den Teil der Daten sichern, der nicht auf andere Art wiederherstellbar wäre.

Dies kommt eventuell im Falle von Content Management Systemen (CMS) in Betracht. Das CMS muss man nicht sichern, da es aus anderer Quelle im Bedarfsfall wieder hergestellt werden kann. Anders liegt der Fall, wenn das System sehr verändert oder an bestimmte Bedürfnisse angepasst worden ist. Zu sichern sind dann alle Dateien, die von den Originaldateien abweichen. Dazu gehören bei einem CMS auch die Templatedateien oder Konfigurationsdateien.

Dass die Daten, die durch die Nutzerinteraktion und den Betrieb entstanden sind zu sichern sind, versteht sich. Dies klingt einfacher als es ist, denn oftmals ist es gar nicht so einfach zu erkennen, welche Datenbestände hier wichtig und entscheidend sind und welche nur temporär angelegt worden sind. Dazu gehören Daten, die zum Zwecke der Geschwindigkeitssteigerung der Seitenauslieferung automatisch erzeugt worden sind (Caching) oder die letzten Suchanfragen der

integrierten Suche beinhalten. Natürlich könnte man diese Daten sicherheitshalber einfach mitsichern, doch sind, wie oben geschildert, Sicherungsläufe zeitaufwändig und verbrauchen Ressourcen wie Speicherplatz.

Ein weiterer Aspekt verdient Beachtung: Es kann sein, dass man selbst nicht die neuste Version des CMS einsetzt. Die Gründe dafür sind vielfältig. Versucht man dann, die aktuellste Version einzuspielen, um sie mit geretteten Nutzerdaten zu betreiben, die mit einer Vorgängerversion erzeugt worden sind, kann man auf Probleme stoßen. Auch die Datenbankstruktur ändert sich im Laufe der Versionsgeschichte, da neu hinzugekommene Funktionen entsprechende Daten speichern, die früher gar nicht anfielen.

Nicht unwichtig sind Daten, die automatisch angelegt werden und von der Anwendung zum Zwecke der Fehlersuche oder Webanalyse erstellt wurden. Auch hier muss entschieden werden, ob diese Dateien besonders zu schützen sind.

INKREMENTELLES BACKUP

Werden nur Daten gesichert, die seit der letzten Vollsicherung hinzugekommen sind, spricht man von einem inkrementellen Backup. Die einzelnen hinzugekommenen Dateien werden sozusagen gesammelt bis man wieder ein Vollbackup anlegt.

Für einen manuellen Backupbetrieb empfiehlt sich das inkrementelle Backup nicht, da man bei Content, der auf Webservern bereit liegt, selten volle Übersicht über die veränderten oder hinzugekommenen Daten hat.

Nutzt man Software, um Sicherungskopien herzustellen, ist ein inkrementelles Backup oft Mittel der Wahl. Da nicht alle Daten gesichert werden müssen, kann man mit weniger Zeit für den Durchlauf auskommen und braucht nicht so viel Sicherungsspeicherplatz.

Allerdings muss auch das Backupprogramm sozusagen Buch darüber führen, welche Dateien schon gesichert sind, verändert wurden und neu kopiert werden müssen. Das Ergebnis, die Sicherungsdateien, sind also in der Struktur komplexer. Zudem muss man zur Rekonstruktion alle Backupmedien, die für dieses inkrementelle Backup verwendet wurden, zur Hand haben. Auch das inkrementelle Backup ist anfangs ein Vollbackup. In Abständen wird dann wieder ein Vollbackup erstellt und anschließend werden wiederum nur die Inkremente gesichert.

DIFFERENZIELLES BACKUP

Das differenzielle Backup funktioniert ähnlich. Hier werden zum initialen Vollbackup die geänderten bzw. hinzugekommenen Dateien gesichert. Das heißt, das Vollbackup wird mit den geänderten Dateien ergänzt, bis wieder ein Backup ansteht.

Auch hier spart man Sicherungsspeicherplatz und Zeit. Allerdings muss man für eine Rekonstruktion sowohl das Vollbackup und die Datenträger mit den geänderten Dateien haben.

KOMBINATION VON STRATEGIEN

Eine optimale Strategie wird aus einer Kombination von Vollbackup, partiellem Backup und inkrementellen oder differenziellen Backup bestehen: Das Vollbackup sollte in zeitlich größeren Abschnitten erstellt werden, zum Beispiel monatlich oder wöchentlich. Ein Teilbackup empfiehlt sich dann täglich, wobei ein inkrementelles Backup sich für noch kürzere Zeitabschnitte empfiehlt.

Wie groß die zeitlichen Abstände jeweils sind, muss anhand der tatsächlichen Änderungsfrequenz der Daten entschieden werden, nicht zuletzt aber auch anhand der Überlegung, welche Prioritäten dem Backup eingeräumt werden.

Vor umfangreichen Änderungen, etwa vor dem Einspielen neuer Softwareerweiterungen, neuer Versionen oder Hardwareänderungen sollte man ein Vollbackup anlegen. Auch nach diesen Änderungen sollte man ein neues Vollbackup erstellen, da man eventuell Hardwareänderungen nicht mehr so einfach rückgängig machen kann. Dies gilt auch für neue Versionen von Software, für die der alte Lizenzcode nach einer gewissen Zeit nicht mehr gültig ist und die gesicherte Version und zurückgespielte Version aufgrund dessen den Dienst versagt.

Es sollten mehrere Generationen von Backups aufbewahrt werden. Wie viele dies konkret sein sollten, müsste man ebenfalls anhand der Änderungsfrequenz und des Risikos entscheiden. Unter Umständen wird ein Datenverlust durch schadhafte Software verursacht, wobei ein eingeschleppter Virus oder Trojaner das Problem sein kann. Oft lässt sich im Nachhinein nicht mehr feststellen, wann die zerstörerische Wirkung eingesetzt hat oder wann der Virus sich einnisten konnte. Ältere Backups erweisen sich in solchen Fällen oft als hilfreich.

BACKUPMEDIEN

Grundsätzlich unterscheiden sich die Datenträger in Preis, Kapazität und Geschwindigkeit. Hinzu kommt noch die Haltbarkeit, wobei eine möglichst lange Haltbarkeit eine Voraussetzung ist, um einen Datenträger überhaupt als Backupmedium einsetzen zu können.

Datenträger, die als Backupmedien Verwendung finden, müssen nicht wie Datenträger im produktiven Betrieb besonders schnell sein. Hier kommt es mehr auf die Kapazität an, genauer gesagt auf die Dichte im Sinne von möglichst viel Speicherplatz pro Einheit oder Volumen. Der Preis pro Speichereinheit geht oft damit einher. Dieser ist aber meist das zweitwichtigste Kriterium.

Im einfachsten Fall werden Daten kopiert und unter einem anderen Namen auf der gleichen Festplatte abgelegt. Damit hat man bereits ein (Teil-)Backup.

Dies ist nicht besonders sicher, da eben diese Festplatte ausfallen kann. Also empfiehlt sich, zur Erhöhung der Sicherheit der Daten, die Ablage auf einem anderen Medium, also im zweiteinfachsten Fall auf einer anderen Festplatte.

Die Preise für Festplatten sind gesunken, so dass sich Festplatten tatsächlich als Backupmedium gut eignen. Je nach zu sichernder Datenmenge kann eine externe Festplatte, die sich dann auch noch an einem sicheren Ort aufbewahren lässt, eine gute Möglichkeit sein.

Weitere denkbare Medien sind die CD-ROM oder die DVD. Beide sind in der Kapazität stark begrenzt und eignen sich eher als Austauschdatenträger denn als Backupmedium. Die Daten müssen auch mit einem Brenner aufgebracht werden. Dabei beobachtet man ein langsames Verschwinden dieser Medien. Notebookhersteller verzichten bereits häufig auf den Einbau entsprechender Hardware. Man muss also damit rechnen, in wenigen Jahren keine Geräte mehr zu finden, die CDs oder DVDs lesen könnten.

Ein ähnliches Schicksal steht den Bandlaufwerken bevor, die man gerne zur massenhaften und dauerhaften, archivartigen Sicherung von Daten verwendet hat. Magnetbänder waren viel billiger als Festplatten, dafür aber um einiges langsamer. In der Praxis trifft man diese Art der Sicherung und Archivierung zunehmend seltener an.

Eine recht häufig verwendete Art, Sicherungskopien zu speichern, ist, die Dateien mit den Sicherungen auf einem entfernten Server abzulegen („in der Cloud"). Je nach Wertigkeit, Wichtigkeit oder Brisanz der Daten kann dies eine gute Alternative sein. Dabei muss man jedoch beachten, dass man nicht mehr weiß, wo genau die Daten gespeichert werden und wer Zugriff darauf hat. Zudem gibt es keinesfalls eine Garantie, dass dort die Daten vor Zerstörung sicher sind. In der Regel werden solche Daten auf Storageservern gespeichert, die auch nichts anderes darstellen als einen Verbund von Festplatten. Zwar nutzen entsprechende Anbieter wiederum Sicherungssysteme, um die Daten zu schützen, doch wie diese Maßnahmen genau aussehen, ist selten dokumentiert. Vor einem Verlust der Zugangsdaten oder der Schlüssel für die Verschlüsselung sollte man sich hüten.

Außerdem ist selten klar erkennbar, wer Zugriff auf diese Daten hat oder welche rechtlichen Bedingungen gelten. Server können gehackt werden, Daten können

gestohlen werden. Einen höheren Sicherheitslevel erreicht man, indem man die Sicherungsdaten verschlüsselt in der Cloud abspeichert, ohne dass der Anbieter des Speicherplatzes Kenntnis über die Verschlüsselung oder den Schlüssel hat. So ist das Abspeichern in der Cloud recht bequem, wenn die Risiken akzeptabel sind. Dann bleibt nur och Vorsorge für den Fall zu treffen, dass der Speicheranbieter sich aus dem Markt verabschiedet, das Geschäftsmodell ändert oder die Zugriffsmöglichkeiten einschränkt.

AUFBEWAHRUNG: WOHIN MIT DEN BACKUP-DATENTRÄGERN?

Sollte es sich um physikalische Datenträger handeln, also um Festplatten, Bänder oder Sticks, empfiehlt es sich, diese an einem anderen Ort als die im laufenden Betrieb befindlichen Datenträger aufzubewahren. Der Zugang zu den Sicherungsdatenträgern sollte geschützt und kontrolliert sein. Wichtig ist, dass die Datenträger vor schädlichen Umwelteinflüssen wie Feuchtigkeit, Hitze, Staub und so weiter geschützt gelagert werden. Mehrere, räumlich getrennte Aufbewahrungsorte minimieren die Gefahr, dass durch einen Schadensfall aufgrund höherer Gewalt wie einer Überschwemmung oder eines Feuers alle Backups zerstört werden.

Es hat sich als hilfreich erwiesen, einzelne Backupmedien gesondert zu beschriften und eine Systematik dabei anzuwenden. Auch wenn die Medien rollieren, ist es wichtig, immer Kenntnis davon zu haben, welches Backup oder welcher Teil eines Backups sich auf einem einzelnen Datenträger befindet. Man muss dafür Sorge tragen, dass sich die Datenträger nicht fälschlicherweise überschrieben werden. Ein gutes Beschriftungssystem (oder Dateibenennungssystem) ist dann wertvoll, wenn im Falle eines Falles Daten zurückgesichert werden müssen. Die schnelle Auffindbarkeit des aktuellsten Backups ist dann wesentlich.

So könnte man für jeden Tag der Woche einen Datenträger vorsehen, wobei das Set an Datenträgern mit den Aufschriften „Montag", „Dienstag", „Mittwoch" und so weiter markiert ist. Gleiches lässt sich für Monats- oder Quartalsbackups adaptieren.

Bei einer Speicherung in die Cloud lassen sich die Namen der Sicherungsdatei entsprechend vergeben.

Es ist sicher sinnvoll, mehrere Sicherheitskopien zu haben und diese an mehreren Stellen aufzubewahren. So werden im Falle einer Überschwemmung oder eines Brands nicht alle Datenträger zerstört. So kann man eventuell einen Satz der Datensicherung im Büro auf einer Festplatte aufbewahren, einen anderen zuhause. Bei wichtigen Daten könnte man auch an einen Safe oder ein Bankschließfach denken. In der Regel haben Backupsätze von Webseiten und Webapplikationen nicht den Umfang von Datensicherungen eines Notebooks oder Desktopcomputers, wo Daten in Terabyte-Größenordnung anfallen. Ein Gigabyte an Webseitendaten ist schon recht groß. Es gibt natürlich Ausnahmen, zum Beispiel im Falle von Fotowebseiten (Galerien) oder Videocommunities. In diesen Fällen könnte man überlegen, diese Mediendateien, die dann ja oft den eigentlichen und nicht unerheblichen Wert darstellen, ohnehin zwei- oder dreimal vorzuhalten.

Bei Onlineshops wäre es ratsam, diese auf zwei getrennten Servern aufzusetzen, so dass im Havariefall schnell umgeschwenkt werden kann. Dies bedeutet natürlich doppelt so viel Hostingaufwand, so dass im Einzelfall entschieden werden muss, ob sich das lohnt. Hinzu kommen ja noch nicht unaufwendige Prozesse der permanenten Synchronisation der Datenbestände.

BACKUPS VON WEBSITES MIT BORDMITTELN

Im Zusammenhang mit Websites hat man es mit für gewöhnlich drei Arten von Daten zu tun, die sicherungswürdig sind. Welche Art, Größe und Anzahl von Dateien tatsächlich gesichert werden müssen, hängt natürlich vor allem von der Webanwendung ab. Ein frisch installiertes WordPress wird weniger Dateien beinhalten und weniger Speicherplatz belegen als ein über die Jahre gewachsenes System. Zudem ist es ein großer Unterschied, ob man es mit einem Shop, einem CMS wie Joomla oder einer Speicheranwendung wie ownCloud zu tun hat.

ANWENDUNGS- UND INHALTSDATEIEN SICHERN

Es handelt sich zum einen um Dateien, die als Webdokumente angesehen werden können. Dazu gehören Dateien im HTML-Format, die im Grunde Textdateien sind, Bild- und Grafikdateien in den einschlägigen Formaten, oft im JPG-, PNG- oder GIF-Format. Eventuell kommen noch Audio- und Videodateien (in den Formaten AVI, FLV, MP4 oder verwandten Formaten) hinzu. Nicht unüblich sind auch Dateien, die zum Herunterladen angeboten werden, oftmals im PDF-Format. Daneben ist noch eine Reihe anderer Inhaltsformate denkbar.

Hinzu kommen Dateien, die in Zusammenhang mit HTML-Dateien die Ansicht im Browser erzeugen oder Funktionen ermöglichen. Es handelt sich oft um JavaScript-Dateien, die die Endung „.js" tragen oder um PHP-Dateien mit der Endung „.php".

Zudem gibt es einige Sonderdateien, die für die Webserversoftware von Bedeutung sind. Dazu gehören die oft anzutreffende Dateien .htaccess und php.ini.

Im Falle von Webapplikationen wie WordPress, Joomla, Typo3, Drupal oder anderen Anwendungen verwischt die Grenze zwischen Anwendungsdaten und Inhaltsdaten. Auf Servern, die mit dem Internet verbunden sind und vorrangig Webdokumente ausliefern sollen, finden wir neben den klassischen eigentlichen Webdateiformaten HTML, CSS, JS, JPG, GIF und vielleicht auch noch Flash viele Dateien vom Typ PHP. Diese beinhalten ausführbaren Skriptcode, der vom Webserver nicht direkt zum Browser geliefert wird, sondern vom Server interpretiert wird und in Zusammenhang mit HTML-, CSS-, JavaScript-Dateien etc. und vor allem Datenbankinhalten ein HTML-Dokument entstehen lässt, dass dann an den Browser geschickt wird, um den HTML-Code mit CSS-Vorschriften und JS-Befehlen zu rendern, wie man sagt.

Idealerweise könnte man nun alle diese HTML-, CSS-, JS-, JPG-, GIF- und PHP-Dateien als Anwendungsdaten klassifizieren, die sich nicht so häufig ändern und alles, was in der Datenbank steckt als Inhaltsdaten, die man relativ oft sichern muss, weil sie sich schnell verändern.

In der Praxis werden aber Inhalte wie Bilder und herunterladbare Dokumente nicht in der Datenbank gespeichert, sondern in ihrer eigentlichen Form auf dem Webspace. So können zum Beispiel JPG-Dateien Teil des Templates (der Vorlage) sein oder auch Teil des Inhalts eines Beitrags. Dies lässt sich dann eigentlich nur durch das Verzeichnis, in dem die Datei liegt, zuordnen. Da jedoch solche

Templates manchmal personalisierbar sind und userabhängige Dateien in ein Verzeichnis mit den Beitragsbildern gespeichert werden, ist der Unterschied nicht immer klar. Das sollte beachtet werden, wenn man überlegt, partielle Backups anzulegen.

Nun könnte man überlegen, ob man Anwendungsdaten – also das „nackte" WordPress oder Joomla – überhaupt sichern möchte, da dies ja aus allgemein zugänglichen Quellen wieder herstellbar ist. Dabei muss man aber beachten, dass in diesen Quellen meist nur die aktuellste Version angeboten wird. Ältere Versionen muss man bisweilen aufwendig suchen. Auch wenn man an den Originaldateien eine Änderung vorgenommen hat – es reicht auch schon eine Umbenennung – oder eine gezielte Ergänzung von Konfigurationsdateien, wäre es durchaus ratsam, auch die Applikationsdaten zu sichern.

DATENBANKINHALTE SICHERN

Die meisten Webapplikationen verwenden Datenbanken, um Inhalte zu speichern. Ein sehr prominenter Vertreter ist die Datenbanktechnologie MySQL. Die Daten in einer Datenbank liegen nicht als solche in einem Verzeichnis in Form einer Datei auf dem Server, sondern werden in einer anderen Struktur gespeichert.

Für den Betreiber einer Webseite ist es vergleichsweise einfach, die einzelnen Inhaltsdateien zu erkennen, welche Inhalte in einer Datenbank liegen, erschließt sich nicht so leicht.

Als Alternative zu MySQL begegnet man ab und zu Sqlite, eine „leichtgewichtige" Alternative zur Speicherung von Inhaltsdaten in einer Datenbankstruktur. Im Unterschied zu MySQL erzeugt die Verwendung von Sqlite eine Datei, die wie die Anwendungsdaten auf dem Webspeicherplatz angelegt wird und ebenso wie alle anderen Webdateien heruntergeladen werden kann. Ein prominenter Vertreter von Anwendungen, die mit Sqlite auskommen ist die Open Source Onlinespeicherlösung ownCloud, die in der Community-Grundinstallation Sqlite als Datenbanklösung defaultmäßig vorschlägt.

E-MAIL-INHALTE SICHERN

Auch Mailinhalte werden nicht dort gespeichert, wo sich die Inhaltsdateien oder Datenbankinhalte befinden. Dennoch gehören auch eingegangene und versendete Mails zu den Daten, die unbedingt gesichert und aufbewahrt werden müssen.

Für den Fall, dass man eine eigene Webmailer-Applikation auf dem Webspeicherplatz installiert und betreibt, muss man diese Applikation in Sachen Sicherung wie ein CMS behandeln. Eine prominente Open Source Mailanwendung für den Webserver ist Roundcube.

BACKUPS ERSTELLEN – SO GEHT MAN VOR

Eine Sicherung von Website-Dateien manuell auszuführen, ist im Vergleich zu den implementierten Backuproutinen wie wir sie zum Beispiel in Windows oder OS X haben, nicht besonders komfortabel. Man muss diese Backups selbst anlegen und mehrere Schritte ausführen.

Allerdings erhält man auf diese Weise ein Backup, mit dem man als Webseitenbetreiber umzugehen weiß.

Es gibt (kommerzielle) Tools, die diese Aufgaben übernehmen können, aber im Falle einer Havarie mit Datenverlust kann es passieren, dass auch das Sicherungssystem, das die Daten zurücksichern könnte, zerstört wurde. Es müsste dann eventuell neu beschafft werden oder erneut auf dem Server installiert werden, ehe der eigentliche Rücksicherungsprozess funktionieren kann.

WEBDOKUMENT MIT FILEZILLA SICHERN ODER EINEM ANDEREN FTP-PROGRAMM

Um eine Sicherung der Datenbestände auf dem Webspeicherplatz (Webspace) vorzunehmen, empfiehlt sich die Verwendung eines FTP-Programms wie FileZilla, das unter einer offenen Lizenz verfügbar ist und daher nichts kostet. Es ist für Microsoft Windows, Mac OS X und Linux verfügbar. Mit diesem Programm überträgt man für gewöhnlich oft auch die Daten zum Server, wenn man ein neues CMS aufsetzen will, Bilder oder anderes Material hoch lädt.

Das Prinzip der Sicherung ist einfach: Man lädt einfach alle Dateien, die sich auf dem Webspeicherplatz befinden herunter und speichert diese auf der eigenen Festplatte (oder auf einem an das System angeschlossenen Speichermedium).

Es gibt natürlich viele andere FTP-Programme, die man gelegentlich auch als FTP Clients bezeichnet (im Sinne einer Client-Server-Nomenklatur). Auf dem Server läuft ein Dienst, der entsprechend FTP-Server bezeichnet wird. Dieser Dienst arbeitet parallel zum Dienst „Webserver" (meist Apache) und kann sowohl Daten zum Serverspeicherplatz transportieren als auch Daten herunterladen. Der Zugang zum Speicherplatz des Server muss mit einem Nutzernamen und einem Passwort gesichert sein, da sonst jeder beliebig Dateien hochladen und verändern könnte. Es gibt zwar auch eine Konfiguration, die man anonymes FTP nennt, da hier keine Anmeldeinformationen eingegeben werden müssen. Im FTP-Programm kann man diese Bezeichnung möglicherwiese bei einer Bezeichnung für eine Option finden, allerdings wird im Hosting-Betrieb immer mit Anmeldeinformationen gearbeitet. Diese Anmeldeinformationen benötigt man zwingend, um eine Sicherheitskopie per Download, so wie wir es im Folgenden beschreiben, anzufertigen.

Andere bekannte, kostenlos verfügbare FTP-Programme heißten Cyberduck (für MacOS), Free FTP, WS-FTP-light, Total Commander, WinSCP, Anyconnect. Es gibt aber viele weitere. Zudem ermöglichen auch die Dateimanager vieler Betriebssysteme mit entsprechender Konfiguration einen Verbindungsaufbau und Dateitransfer via FTP. Allerdings beherrschen nicht alle FTP-Clients eine automatische Konfiguration des Verbindungsaufbaus, so dass bestimmte Einstellungen häufig manuell angepasst werden müssen. Oft stellt sich die Frage,

ob zum Beispiel der sogenannte aktive oder passive Modus verwendet werden soll (meist führt der passive zum erfolgreichen Verbindungsaufbau, wenn sich der Rechner mit dem FTP-Client hinter einer Firewall mit Adressübersetzung befindet, funktioniert aber nicht bei jeder Netzwerkkonfiguration).

Etwas, was die meisten FTP-Programme gemeinsam haben, ist die zweigeteilte Ansicht eines Dateibrowsers: Links werden meist die lokalen Dateibestände angezeigt, also die Daten auf der Festplatte im Notebook oder Desktop-PC. Rechts werden die Dateien aufgelistet, die sich auf dem Serverspeicherplatz befinden.

Dies sei nun am Beispiel von FileZilla genauer gezeigt.

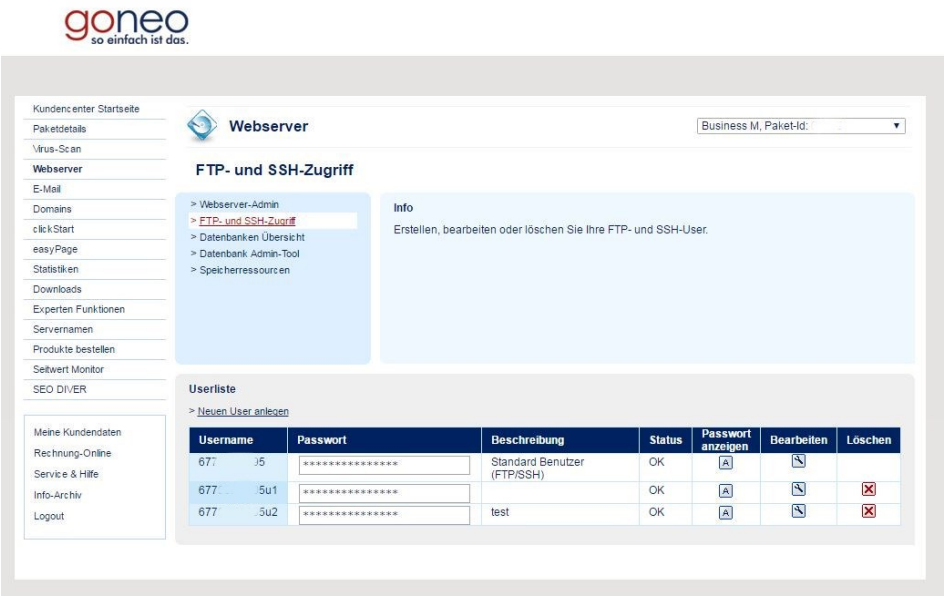
SO FUNKTIONIERT FILIZIILLA

Bevor überhaupt Dateien, die sich auf dem Server befinden, angezeigt werden können, ist eine Verbindung herzustellen. Bei FileZilla geschieht dies wie bei allen anderen FTP-Clients auch durch die Angabe

- des Servers (das ist oft, aber nicht immer der Domainname, den man als Kunde im Zusammenhang mit dem Webauftritt verwendet, eventuell ergänz durch ein vorangestelltes „ftp." und der Angabe des Protokolls in der Form „ftp://"),
- des FTP-Benutzernamens (je nach Anbieter und Leistungspaket sind auch mehrere FTP-Benutzernamen mit unterschiedlicher Zugriffsberechtigung möglich),
- des für diesen FTP-Benutzernamen geltenden Passworts.

ZUGANGSDATEN FINDEN

In den meisten Fällen lässt sich bei Webhostern wie goneo der FTP-Benutzername im Kundencenter oder wie die Administrationssektion auch immer genannt wird, erfahren und eventuell ändern. goneo-Kunden finden diese Informationen im Kundencenter. Nutzer anderer Anbieter bekommen diese Daten in ähnlicher Weise mitgeteilt.



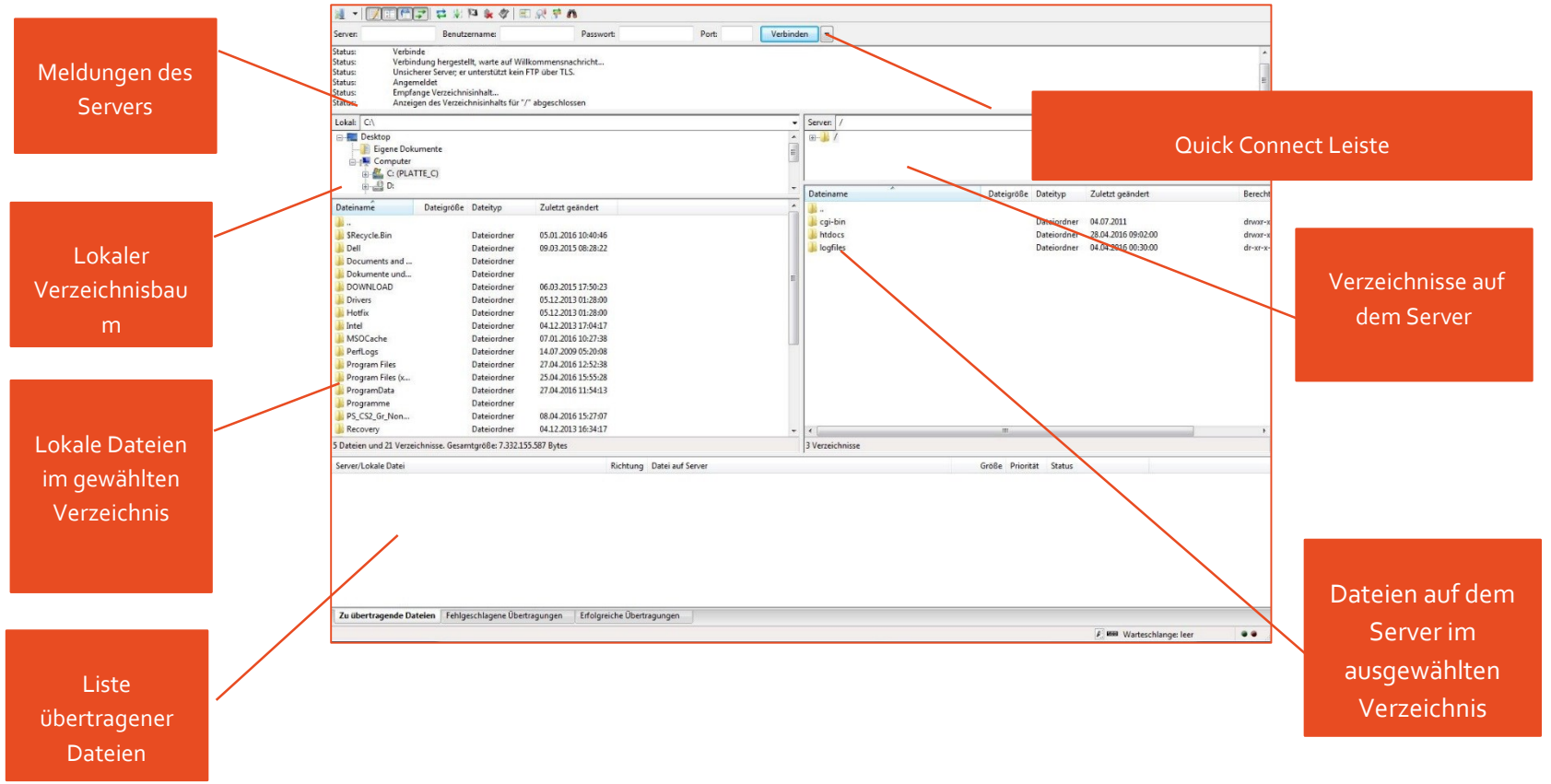
Geändert werden kann auch das Passwort.

Diese Angaben benötigt man zum Aufbau der FTP-Verbindung mit dem Server.

Bei FileZilla geht dies am einfachsten, indem man Server, FTP-Username und Passwort in die „Quick-Connect"-Leiste eingibt und auf „Verbinden" klickt.

Moderne FTP-Anwendungen wählen den Dateiübertragungsmodus automatisch.

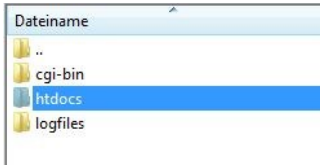
In der Standardansicht sieht das Hauptbedienfester von FileZilla wie folgt aus.



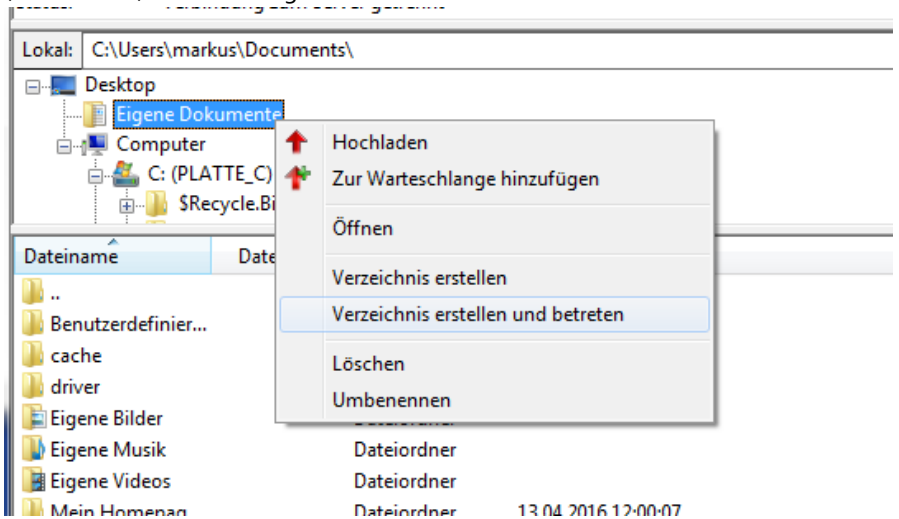
Es gibt im FTP die Unterscheidung, ob die Datei per ASCII Zeichen oder binär übertragen werden soll.

Nach der Verbindungsherstellung wird alles, was sich im Verzeichnis htdocs befindet heruntergeladen. Dazu markiert man das Verzeichnis htdocs und erteilt den Downloadbefehl per Klick (in FileZilla Rechtsklick und Auswahl „Herunterladen"). Das Programm fragt dann eventuell noch nach dem gewünschten lokalen Speicherort.

Meistens werden die Dateien in das lokale Verzeichnis heruntergeladen, das im linken Teil angezeigt wird. Natürlich kann man den Speicherort ändern. Es empfiehlt sich für eine Sicherungsspeicherung, ein neues Verzeichnis zu erstellen.



Auch dies lässt sich mit einem Befehl aus dem Kontextmenü in FileZilla (Rechtsklick) bewerkstelligen.



An dieser Stelle ein Hinweis: Es gibt Webanwendungen, die bei der Installation Dateien eine Ebene über dem sogenannten „Document root" ablegen wollen. Diese Dateien müssen also mitgesichert werden. Typo3 und Contao sind solche Webanwendungen, die aus Sicherheitsgründen einen Teil der Anwendungsdaten außerhalb von Verzeichnissen installieren, die man per Browser aus dem Internet erreichen kann, wohl aber per FTP.

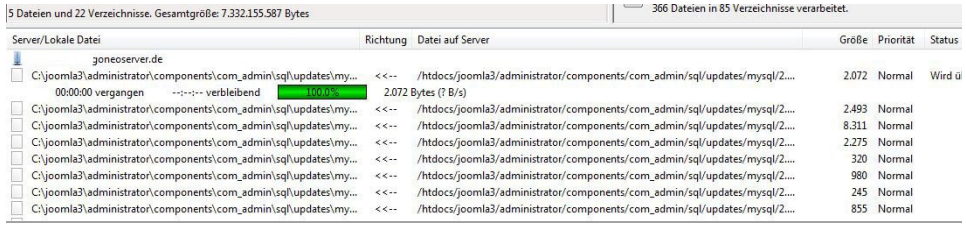
Mittels des FTP-Programms wird nun eine 1:1 Kopie der Dateistruktur auf der Festplatte erzeugt. Man kann den Fortschritt des Herunterladens im unteren Teil des FileZilla-Fensters verfolgen. Andere FTP-Clients verwenden möglicherweise andere Darstellungen.

Es kann vorkommen, dass aus verschiedenen Gründen eine Datei nicht heruntergeladen werden kann. FileZilla ordnet diese Datei dann einer Gruppe „Fehlgeschlagene Übertragungen" zu. FileZilla wird, wenn es entdeckt, dass eine Datei mit gleichem Namen im Speicherort bereits vorhanden ist, mit einem Dialogfenster regieren und dem Nutzer die Entscheidung überlassen, wie nun weiter verfahren werden soll.

Besondere Aufmerksamkeit verdienen die „Sonderdateien" wie .htaccess (mit Punkt vor dem Dateinamen). Beide müssen nicht zwingend vorhanden sein, aber dass .htaccess existiert ist bei der Verwendung eines Content Management Systems wie WordPress oder Joomla sehr wahrscheinlich.

Leider verstecken sich die Dateien gerne (genau dies soll eigentlich auch der vorangestellte Punkt bewirken), je nach Einstellung des FTP-Programms. Man sollte diese Dateien sichtbar machen, damit man sicher geht, auch diese Dateien zu kopieren. Das FTP Programm bietet eine entsprechende Einstellungsmöglichkeit.

Da mittels FTP (File Transfer Protocol) das Herunterladen dateiweise erfolgt, dauert der Prozess eine ganze Weile, je nach Anzahl der Dateien und Verzeichnisse, deren Größe und der Verbindungsgeschwindigkeit (Bandbreite).



Nach Abschluss hat man ein vollständiges Backup der Websitedateien auf der Festplatte.

Es empfiehlt sich zu überprüfen, ob alle Dateien und Verzeichnisse ohne Fehler heruntergeladen wurden.

EXKURS: WAS IST FTP?

Eine einfache und effiziente Möglichkeit, Daten vom lokalen Computer auf den Server zu übertragen, bietet das File Transfer Protocol, kurz FTP. So bringt man ganz allgemein Texte, Fotos, Videos usw. zur Veröffentlichung ins Internet.

Das FTP-Protokoll gehört zu einer ganzen Familie von typischen Internetprotokollen und ist neben HTTP, IMAP,POP3, SMTP und UDP sicher eines der meistverwendeten Anwendungsprotokolle im Internet.

Mit FTP lassen sich Dateien vom Client zum Server übertragen. In diesem Szenario spricht man vom Hochladen. Der umgekehrte Weg, also die Übertragung vom Server zum Client nennt man Herunterladen. In der Praxis handelt es sich beim Client hier typischerweise um einen PC oder auch ein Notebook, während im Hosting-Umfeld der Server zumeist in einem größeren Rechnerverbund innerhalb eines Rechenzentrums untergebracht ist.

Mit dem Befehlssatz, den FTP zur Verfügung stellt, lassen sich Verzeichnisse anlegen, Dateien und Verzeichnisse können auch gelöscht oder umbenannt werden. Natürlich kann man sich als User durch die Verzeichnisstruktur bewegen und die entsprechenden Dateien darin auflisten.

FTP benötigt eine *TCP*-Verbindung, setzt also auf *IP*, das Internetprotokoll auf. Der Standardport für den Steuerkanal (*command channel*) einer FTP-Verbindung ist *Port 21*. Über diesen Port sendet das dafür spezialisierte Programm, der FTP-Client seine Befehle, die der Server beantwortet. Über einen weiteren Port, normalerweise TCP-Port 20 oder einen zufällig gewählten Port fließen die Daten.

Grundsätzlich verlangt FTP eine Anmeldung am Server. Allerdings kann diese Anmeldung auch anonym sein, indem der Anmeldename *anonymous* verwendet wird. Ein beliebiges Passwort kann eingegeben werden, wobei im Falle anonymer Verbindungen gerne manchmal noch eine E-Mailadresse verwendet wird. Für öffentlich zugängliche FTP-Server ist ein anonymer Login durchaus sinnvoll. Viele Softwarehersteller distribuieren zum Beispiel Updates über einen FTP-Server.

Im Hosting-Szenario wird man meist auf die Notwendigkeit stoßen, sich authentifizieren zu müssen, damit nur Berechtigte auf das FTP-Repository zugreifen können. Auf Webserver-Ebene kann man unterschiedlichen FTP-Usern unterschiedliche Zugriffsrechte zuweisen.

ZWEI ÜBERTRAGUNGSMODI: EINER FÜR TEXT- UND EINER FÜR BINÄRDATEIEN

FTP kennt verschiedene Übertragungsmodi: Einen für Binärdateien und einen für Textdateien. Der Unterschied ist dann relevant, wenn es um die Übertragung von Textdateien zwischen zwei verschiedenen Systemen geht, die unterschiedliche Codetabellen zum En- bzw. Decodieren von Zeichen verwenden. Wählt man in einem solchen Fall den Binärmodus, kann es passieren, dass die übertragenen Codes anders interpretiert werden und einiger Zeichensalat entsteht. Die Textmodusübertragung verhindert das. Der FTP-Binärmodus überträgt Byte für Byte, während der Textübertragungsmodus eine Umwandlung vornimmt, so dass

in ANSI dargestellte Zeichen (wie in Windows verwendet) richtig in *ASCII* codierte Zeichen (in Linux üblich) überführt werden.

AKTIVER UND PASSIVER MODUS

FTP unterscheidet zwischen einem aktiven Modus und einem passiven Modus. Beim Active FTP baut der FTP-Client über Port 21 eine Verbindung zum FTP-Server auf. Der FTP-Server antwortet mit einem Verbindungsversuch über Port 20 an die IP-Adresse, die er vom FTP-Client mitgeteilt bekommen hat. Das funktioniert, wenn der FTP-Client sich nicht hinter einer Firewall befindet, die die IP-Adressen "übersetzt", was in privaten Netzen oft der Fall ist. Dafür gibt es dann den passive mode, wie man den passiven Modus auch nennt. Dabei wird dem nach der vom Client initiierten Verbindung vom Server über Port 21 eine zufällig gewählte Portadresse mitgeteilt, die der Client verwendet, um über diesen Port, der dann als Datenkanal verwendet wird, eine weitere Verbindung zu öffnen. Port 20 wird beim passiven FTP dann nicht als Datenkanal verwendet.

Logindaten und Nutzdaten werden bei FTP in seiner ursprünglichen Form, die seit 1971 nur wenig verändert worden ist, im Klartext übertragen. Um eine Verschlüsselung zu ermöglichen, kann die Transport Layer Security verwendet werden. Beim so bezeichneten FTP over SSL oder kurz FTPS muss der Host sich authentifizieren. Der verwendete Verschlüsselungsmechanismus ist dabei *TLS*. Der Client legitimiert sich dann mit verschlüsselt übertragenem Benutzernamen und Passwort.

Eine Alternative dafür ist SFTP, also SSH File Transfer Protocol, das nicht auf SSL, sondern auf SSH basiert. SSH steht für Secure Shell und ist die Bezeichnung für ein anderes geschütztes Protokoll, das verschlüsselte Netzwerkverbindungen aufbauen kann.

Als Webdesign-Experte zieht man es vielleicht vor, mittels Shell-Zugriff Änderungen an Dateien direkt auf dem Server vorzunehmen. Mit Secure Shell, kurz SSH, kann man eine authentifizierte und sichere Verbindung zwischen PC und Server herstellen. Als Client verwenden Experten gerne PuTTY oder WinSCP. Damit kann man serverseitig implementierte Befehle ausführen. Das eröffnet mehr Möglichkeiten der Datenmanipulation als dies mit FTP der Fall ist: Eine typische Anwendung wäre das direkte Herunterladen aus Webquellen mit einem einzigen Befehl.

DATENBANKINHALTE SICHERN MIT PHPMYADMIN UND ANDEREN TOOLS

Um eine Webanwendung wie ein CMS (dazu zählen wir WordPress, Joomla, Drupal) nach einem Datenverlust wieder zum Laufen zu bringen, müssen bei einem manuellen Backup wie hier beschrieben die Datenbankinhalte gesichert werden.

Die Daten, die in der MySQL-Datenbank verwaltet werden, liegen nicht auf dem Webspace, also dem Bereich, der für User von Webhostingpaketen per FTP zugänglich ist. Natürlich ist auch die MySQL-Datenbank am Ende eine Datei, allerdings befindet sich diese Datei in einem für FTP nicht zugänglichen Bereich. Neben MySQL sind eine Reihe anderer Datenbanktechnologien verbreitet, wobei MySQL sicher, was die Marktdurchdringung angeht, in der Spitzegruppe liegt. Im Hosting-Umfeld, vor allem, wenn die Hostingprodukte mit Linux- oder linuxartigen Technologien realisiert sind, hat man es zu meist mit MySQL zu tun.

Für gewöhnlich speichern populäre Webanwendungen vor allem Texte und Informationen über Beziehungen (Links, Speicherort für Medien etc.) in einer Datenbank ab. Diese Datenbank wird bei der Installation der Anwendung erzeugt und füllt sich im Laufe der Zeit mit teilweise sehr viel Inhalt. Meist ist die Größe einer Datenbank schon aus praktischen und pragmatischen Gründen begrenzt. Üblich ist, dass eine MySQL Datenbank pro Webhosting-Kunde ein, gelegentlich zwei Gigabyte an Daten umfassen kann.

Je größer die Datenbank, desto schwieriger ist ein Backup.

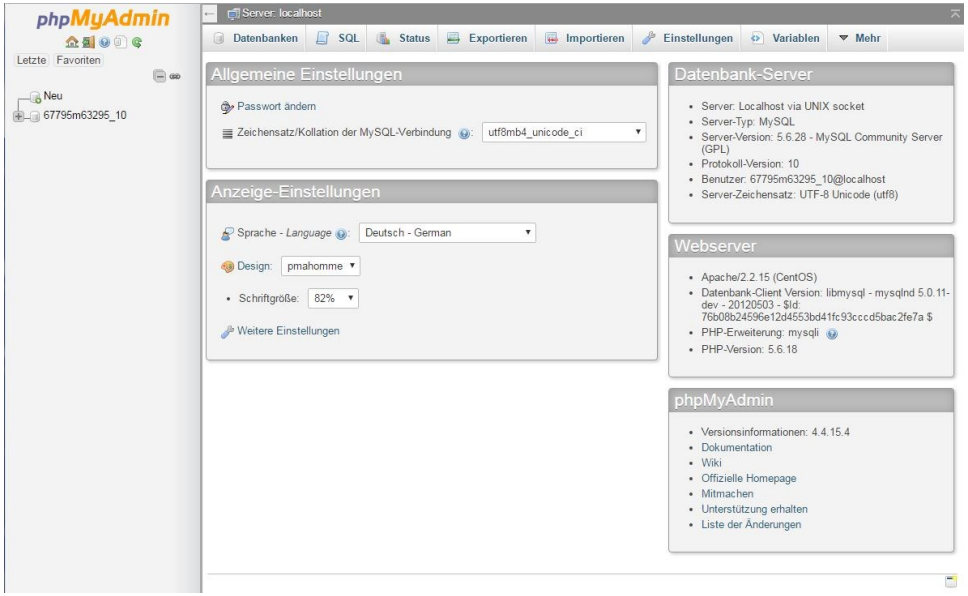
In vielen Fällen reicht für eine Sicherungskopie der Datenbankinhalte das Tool PHPMyAdmin. Dies ist eigentlich dafür gedacht, Datenbankinhalte mittels einer grafischen Benutzeroberfläche, die im normalen Webbrowser gezeigt wird, gezielt zu durchsuchen oder zu verändern oder neue Tabellen hinzuzufügen, bestehende zu löschen oder gezielt zu verändern, verfügt aber auch über Import- und Exportfunktionen, die man sich für Backupzwecke zunutze machen kann.

Da das Tool Datenbankinhalte verändern kann – das heißt auch: vernichten kann -, muss man umsichtig damit umgehen. Es gibt kein „Rückgängig-Machen" und keinen „Papierkorb".

Bei goneo startet man PHPMyAdmin, das bei goneo als „Datenbankadministrationstool" bezeichnet ist, über den entsprechenden Menüpunkt im Kundencenter:

Nach dem Start wird man zur Eingabe des Datenbanknamens und des Passworts aufgefordert, ehe man auf die Datenbestände zugreifen kann. Sollten diese Angaben noch nicht bekannt sein, hilft ein Blick in den Abschnitt „Webserver" > „Datenbank Übersicht".

Das Fenster für das Datenbankadministrationstool ist zweigeteilt: In der schmaleren Spalte links befindet sich die Ansicht der Datenbank mit den beinhalteten Tabellen. Angezeigt wird die Datenbank mit ihrem Namen. Das „+"-Zeichen im Kasten deutet schon darauf hin, dass sich eine Liste der in dieser Datenbank enthaltenen Datenbanktabellen ausklappen lässt. Der Datenbankname wird vom System vergeben (zumindest bei goneo und einigen anderen Hostern ist dies so), die Namen der einzelnen Datenbanktabellen werden durch die Anwendung erzeugt. Diese Namen sollten übrigens nicht verändert werden.



Für einen Export genügt es, den Datenbanknamen durch einen einfachen Mausklick zu markieren.

Auf der PHPMyAdmin-Oberfläche findet man den Menüpunkt „Exportieren" im oberen Teil der größeren rechten Spalte. Mit einem Klick darauf startet man den

Download einer Datei mit dem Namen der Datenbank und Endung sql. Es lassen sich viele Feineinstellungen vornehmen, die für Backupzwecke nicht von Belang sind.

Mit dieser heruntergeladenen Datei haben wir ein Backup (einen sogenannten Dump) der MySQL Datenbank, in der die Webapplikation Inhalte ablegt, erzeugt. Es handelt sich bei der ausgegebenen Datei im Grunde um eine Textdatei. Man kann diese Datei im Prinzip mit einem Texteditor betrachten. Die Inhalte sind in Klarschrift hinterlegt. Es handelt sich dabei aber nicht nur um die reinen Nutzdaten, sondern auch um SQL-Befehle. Man sollte also den Inhalt nicht verändern, da die Gefahr besteht, dass dann diese Datei nicht mehr zurückgesichert werden kann, da die Struktur verletzt worden ist.

Diese heruntergeladene Datei ist nun die Sicherungsdatei für die MySQL-Datenbank und sollte an einen sicheren Ort gespeichert werden. Zusammen mit den Website-Dateien kann man daraus im Notfall wieder eine lauffähige Installation der Webapplikation (Joomla, WordPress, Drupal) erstellen.

DIE GRENZEN DER SICHERUNG MIT PHPMYADMIN

Bei der Verwendung von PHPMyAdmin, dem Datenbankadministrationstool kann es bei sehr großen Datenbanken möglicherweise zu einem Abbruch kommen, wenn man die Funktion „Exportieren" benutzt.

Grund ist dann in aller Regel die serverseitig eingestellte maximale Skriptlaufzeit. Diese lässt sich oft innerhalb bestimmter Grenzen erhöhen. Dies geschieht über die Datei php.ini (oder über eine Einstellung im goneo Kundencenter, die unter „Experten Funktionen" > „PHP Konfiguration" zu finden ist). Der entsprechende Wert lautet „max_execution_time". Normalerweise sollte die Skriptlaufzeit von standardmäßig 30 Sekunden ausreichen, um eine Datenbank mit einem üblichen zu sichern und herunterzuladen, auch wenn sich sehr viele Tabellen in dieser Datenbank befinden. Insbesondere bei Foren oder sehr erweiterten Systemen kann es aber Probleme geben.

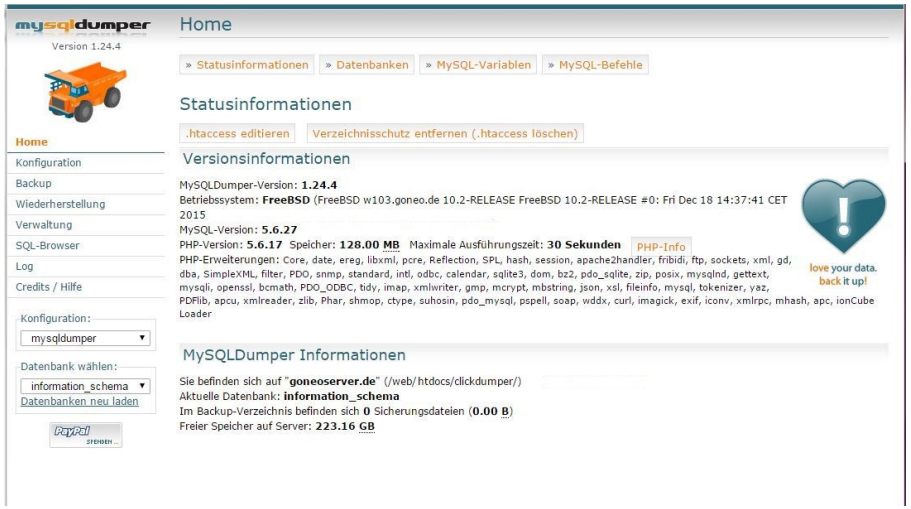
Außerdem muss man auch an das Rücksichern denken: Ist die Datei mit dem Dump zu groß und übersteigt das serverseitig gesetzte Upload-Limit, ist ein Import nicht mehr ohne weiteres möglich. Behelfen könnte man sich mit einer gestückelten Sicherung einer großen Datenbank. Möglicherweise ist dies aber der Moment, andere Sicherungstools einzusetzen.

DATENBANKSICHERUNG MIT MYSQLDUMPER

Als sehr hilfreich hat sich ein kleines Open-Source-Werkzeug namens MySQLDumper erwiesen. Damit lassen sich Datenbanksicherungen schrittweise ausführen, so dass die maximale Skriptlaufzeit nicht überschritten wird und keine Probleme bei Importieren entstehen.

MySQLDumper lässt sich einfach installieren (z.B. bei goneo indem man die Funktion clickStart verwendet, die im goneo Kundencenter zugänglich ist; unter dem gleichnamigen Menüpunkt und dort unter „Verschiedenes" findet man die Anwendung zur sofortigen automatischen Installation). Während des Installationsdialogs legt man die zu bearbeitende bzw. sichernde Datenbank fest.

MySQLDumper bietet allerlei Funktionen für deren Sicherung und Rücksicherung. Das Tool speichert die Datenbankinhalte in einer Datei ab, auf Wunsch verschlüsselt und komprimiert. Die erzeugten Sicherungsdateien können heruntergeladen werden oder auf dem Server verbleiben.

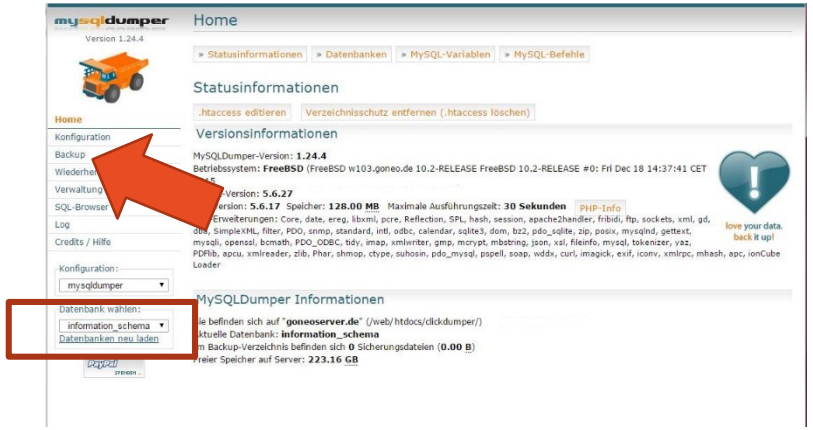


Das Tool mutet recht technisch an und berichtet auf einer Übersichtsseite („Statusinformationen") viele technische Parameter. Man sieht hier die Version des Programms sowie Informationen über das Serverbetriebssystem. Dies wird in den allermeisten Fällen ein linux- beziehungsweise unixartiges Betriebssystem sein, im Falle von goneo FreeBSD oder – je nach Produkt – CENT OS. Man kann hier auch erkennen, welche PHP-Version aktiv ist und welche MySQL-Version der Datenbank zugrunde liegt. Dies kann durchaus relevant sein, wenn nach einem Datenverlust die Webanwendung neu aufgesetzt werden soll und die Datenbankinhalte zurück gespielt werden müssen. Man sollte dann darauf achten, diese Versionen wieder zu verwenden. Eine Abweichung kann es geben, wenn man eine recht alte PHP Version verwendet oder eine Vorgängerversion von MySQL. Letzteres kommt eher vor, wenn man versucht, mittels Datenbankdump von einem Server zum anderen umzuziehen, also eine Migration bewältigen muss.

Zudem listet MySQLDumper die integrierten PHP Module auf.

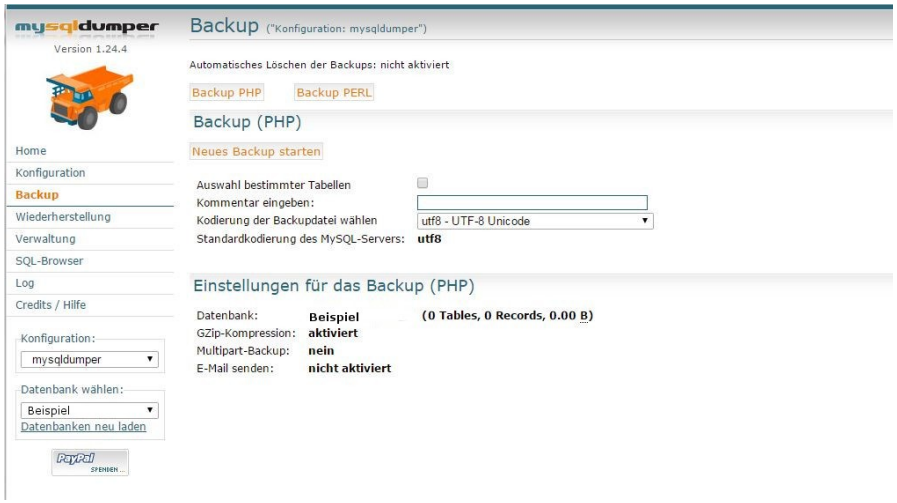
MySQLDumper kann Sicherungen von allen Tabellen in einer Datenbank erstellen, jedoch nicht Sicherungen von mehreren Datenbanken auf einmal.

Man muss also die zu sichernde Datenbank auswählen. Um die Backupfunktion zu nutzen, klickt man zunächst auf den Menüpunkt „Backup" (linke Spalte).



Auf der nun erscheinenden Seite finden sich oben zwei Buttons: „Backup PHP" und „Backup PERL". MySQLDumper kann also das Backupprogramm im PHP- und im

PERL-Code ausführen. Im goneo Kontext nutzen wir die PHP-Variante, da PERL hier konfigurationsbedingt nicht so angesprochen werden kann.



Wichtig ist darauf zu achten, dass man die richtige Datenbank ausgewählt hat und nicht etwa „Information Scheme", welche ebenfalls eventuell im Pulldown-Menu angezeigt wird, aber keine Nutzerdaten enthält.

Bei goneo sind die Datenbanknamen und Datenbankbenutzernamen mit einer Zeichenkette benannt, die aus Ziffern und Buchstaben besteht. Am Ende dieser Zeichenkette befindet sich „_", gefolgt von einer weiteren ein- oder zweistelligen Zahl. Beide Namen, also für die Datenbank und den Datenbankbenutzer sind bei goneo identisch, auf anderen Servern wird dies in der Regel nicht der Fall sein und die Benennungssystematik wird sich unterscheiden. Sowohl Datenbankname als auch Datenbankbenutzername lassen sich nicht bei jedem Anbieter ändern (auch bei goneo nicht). Änderbar ist im goneo-Kundencenter jedoch das Passwort für diese Datenbank.

Für die Produktion eines Datenbankdumps (Backups) und das Wiedereinspielen ist die Benennung aber nicht von Belang.

Im goneo-Kundencenter findet man die Liste der im Hosting-Paket angelegten Datenbanken, deren Namen und Zugangspasswörter, die bei der Anlage des Hosting-Pakets automatisch vergeben wurden, aber änderbar sind. In der Übersichtstabelle muss man auf den kleinen Button mit dem Symbol „A" in der jeweiligen Zeile der Datenbank klicken, um das Passwort sichtbar zu machen.

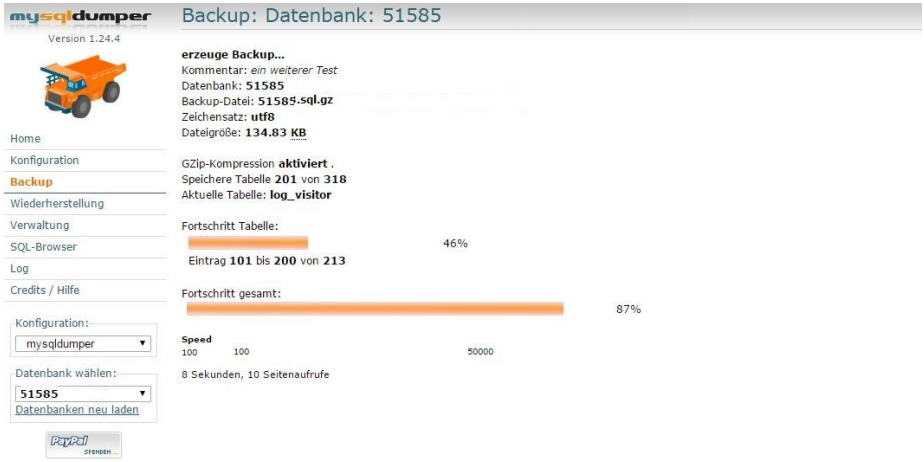
Wer will, kann die Auswahl der zu sichernden Tabellen eingrenzen. In der Standardeinstellung werden alle Tabellen der ausgewählten Datenbank gesichert. Möglicherweise ist es auch sinnvoll, einen Kommentar einzugeben, der mit der Sicherungsdatei verknüpft wird.

In der Grundeinstellung speichert MySQLDumper die Sicherungsdatei auf dem Server komprimiert ab, um Speicherplatz zu sparen. Verwendet wird die GZip-Kompression. Dies lässt sich unter „Konfiguration" > „Allgemein" ausschalten.

Zudem kann man MySQLDumper veranlassen, die Sicherung in mehrere Dateien aufzuteilen. Zu einer Zeit, in der MySQLDumper entstanden ist, war es nicht immer ohne weiteres möglich, vergleichsweise große Dateien zu einem Server hochzuladen oder auch herunterzuladen. Man musste den Download stückeln. Dies hat heute kaum noch Bedeutung.

MySQLDumper kann die Sicherungsdateien auch von Server zu Server übertragen. Dazu ist es notwendig, unter „Konfiguration“ > „FTP“ einen oder mehrere Zugänge anzulegen.

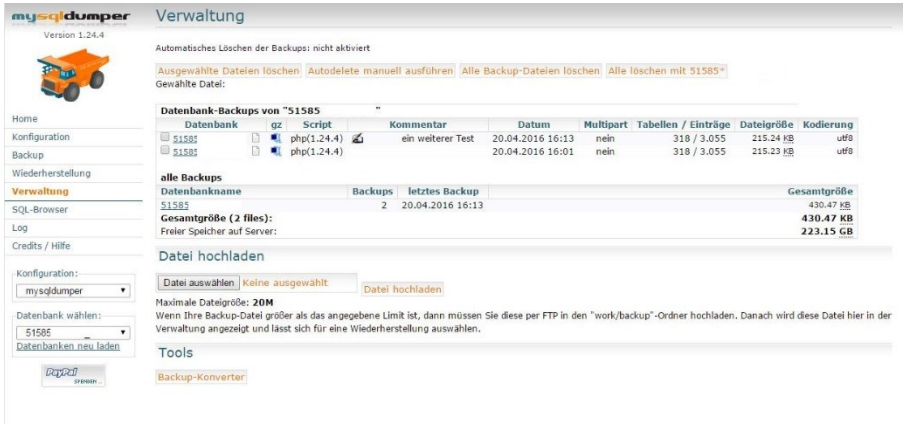
Mit Klick auf „Neues Backup starten“ beginnt der Backupprozess.



Man sollte nun nicht erschrecken, wenn das Browserfenster mit MySQLDumper flackert und sich schnell immer wieder neu aufbaut. MySQLDumper führt das Backup nicht in einem Schritt durch, sondern unterteilt es in viele Einzelschritte. Dies geschieht, um auch große, stark untergliederte Datenbanken sichern zu können. Ein PHP-Skript darf auf vielen Servern nur eine begrenzte Zeit laufen. Wird diese überschritten, bricht der Server die Ausführung ab. Würde also die Sicherung der Datenbank länger als die erlaubte Zeit benötigen, wäre kein Backup möglich. MySQLDumper zeigt den Fortschritt tabellenweise an. Meist geschieht dies aber so schnell, dass die Fensteranzeige nicht mit der Aktualisierung nachkommt.

Bei einer erfolgreichen Sicherung meldet sich MySQLDumper mit einem entsprechenden Status.

Die erstellten Datenbanksicherungen kann man mit dem Menüpunkt „Verwaltung“ abrufen.



Die hier aufgelisteten Sicherungsdateien befinden sich auf dem Server, können aber in der Verwaltungsansicht durch Anklicken des Dateinamens heruntergeladen werden. Dies sollte man auch tun, wenn man eine Sicherheitskopie lokal aufbewahren möchte. Diese Datei kann zu der Sammlung der per FTP heruntergeladenen Webdokumente gestellt werden.

Auf diese Weise ist nun mit MySQLDumper ein Backup der Datenbank erzeugt worden. Ob man dieses Tool verwenden möchte oder die direkte Ausgabe

(„Export“) von PHPMyAdmin (bei goneo: „Datenbankadmintool“) verwendet, ist Geschmacksache, solange die Datenbankgröße überschaubar ist. Der Output der „Export“-Funktion erzeugt unter Umständen eine recht große, unkomprimierte Datei, die aber den Vorteil hat, dass sie mit einem herkömmlichen Texteditor gelesen werden kann. MySQLDumper erzeugt standardmäßig eine gezippte Datei. Grundsätzlich ist MySQLDumper funktionaler, da die Software auch die Verwaltung der gesicherten Datenbanken übernimmt und auch sonst einige komfortable Features bietet. Allerdings muss das Tool eben erst installiert werden.

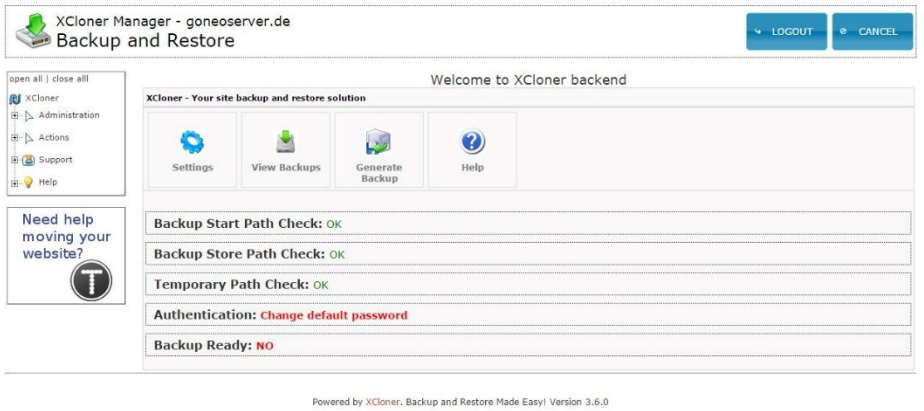
Im Falle einer Rücksicherung muss dann der Menüpunkt „Wiederherstellung“ ausgewählt werden.

ALTERNATIVEN ZU MYSQL DUMPER

Für die Sicherung von MySQL-Datenbankinhalten haben wir MySQLDumper vorgeschlagen, doch natürlich gibt es auch Alternativen.

Bei PhPMyBackupPro (http://www.phpmybackuppro.net/) handelt es sich wie bei MySQLDumper um ein Datenbankbackuptool.

Eine andere interessante Anwendung ist XCloner (http://www.xcloner.com/) Die letzte Version trägt das Datum 2014 und wurde seitdem offensichtlich nicht mehr grundsätzlich erneuert.



Das Tool ist recht einfach zu installieren und setzt PHP mit JSON in der Version 5.3 voraus (Voraussetzung bei goneo gegeben). Mit PHP 5.6 läuft es problemlos. Das letzte Commit auf Github war im November 2016, also kann man davon ausgehen, dass das Projekt noch lebt.

XCloner unterstützt auch Migrationsprozesse, also Umzüge von Server zu Server. Es kann also beim Transferieren von Datenbanken helfen. Man muss (S)FTP und MySQL-Zugangsdaten für den Startserver angeben, sobald das Tool auf dem Webspace installiert ist. Danach lassen sich diverse Einstellungen vornehmen, um einigen Eventualitäten des Servers Rechnung tragen zu können. Insbesondere die Skriptlaufzeit kann bei großen Datenbanken kritisch werden. Um eine Datenbank zu übertragen fordert XCloner auf, drei Dateien herunterzuladen und auf dem Zielserver hochzuladen. In diesen drei Dateien befinden sich die Datenbankinhalte, einige Konfigurationsdaten und eine Minianwendungen, die XCloner auf dem

Zielserver installiert. Unter Umständen kann XCloner diese Dateien auch selbst per (S)FTP übertragen.

Was XCloner aber auch nicht tut, ist, die Webdokumente, PHP-, JS-Skripte und dergleichen zu übertragen. Das muss man mittels (S)FTP selbst tun.

SICHERUNGEN MIT ANWENDUNGSERWEITERUNGEN

Für diverse Anwendungen wie WordPress oder Joomla gibt es Plugins, die Backups und auch Servermigrationen vornehmen können. Für WordPress wird oft das Plugin All-in-one WP Migration Tool empfohlen, das eine komplette Sicherung und einen nahtlosen Umzug verspricht.

Weitere WordPress Plugin, speziell für Backups sind VaultPress, wobei zu beachten ist, dass dieser Dienst nicht kostenlos ist. Es handelt sich um ein Abomodell, bei dem monatlich Kosten anfallen. Mit ähnlichen Modellen arbeiten auch viele der weiteren über 800 Backup-Plugins, die im Pluginverzeichnis bei WordPress aktuell angeboten werden. Bei anderen Modellen gibt es eine kostenlose und eine oftmals „pro" genannte Version mit erweiterten Features.

Kritisch wird es bei solchen Plugins immer bei Versionssprüngen der Anwendung. Meistens dauert es ein wenig bis die Pluginhersteller ihre Software für neue WordPress-Versionen angepasst und getestet haben. Bei Lösungen, die die Sicherungsdateien auf Public Cloud Speicherlösungen wie Dropbox oder Amazon S3 schreiben sollte man Datenschutzaspekte berücksichtigen. Ein weiterer Aspekt bei der Verwendung von Plugins als Backuptool ist, dass das System eben um ein weiteres Plugin aufgebläht wird. Jedes Plugin muss geupdated werden und erfordert Aufmerksamkeit hinsichtlich Sicherheitslücken. Das liegt in der Natur der Sache. Nicht zuletzt können sich zwei Plugins auch gegenseitig ins Gehege kommen. Bei Backupplugins ist die Wahrscheinlichkeit nicht besonders hoch, aber gegeben.

Auch für Joomla gibt es viele Backup-Tools, die sich direkt in das Joomla-Hauptsystem einklinken. Das Akeeba Backup gehört wie auch das EJB Easy Joomla Backup zu den bekanntesten und meistverwendeten für Joomla 3.X. Es kann auch Hilfe bei Webserverumzügen leisten.

Dabei muss man sich vergegenwärtigen, dass man, sollte man solche Erweiterungen einsetzt, sogenannte Third Party Software nutzt. Damit holt man sich zwar mehr Komfort, aber auch mehr Risiko ins Haus: Die Produzenten dieser Erweiterungen könnten ihr Geschäftsmodell umstellen, die Erweiterung kann sich technisch sehr verändern, die Erweiterung speichert Dateien möglicherweise in irgendeinen Cloudspeicher etc. Risiken und Nutzen sind also auch hier abzuwägen.

SICHERUNG VON E-MAILS

Bei goneo befindet sich der Speicherplatz, der den Usern für E-Mails und Anhänge zur Verfügung steht, normalerweise auf einem anderen System. Auch dieses System wird von goneo automatisch gesichert. Dennoch wollen Sie vielleicht selbst Sicherungskopien herstellen. Wichtig ist hierbei zu bedenken, dass die E-Mail-Daten auf dem Server nur solange gespeichert sind wie ein Vertrag mit dem Anbieter besteht.

Auch eine Sicherung der eingegangenen und gesendeten E-Mails ist durchaus notwendig. Dies ist teilweise gesetzlich gefordert. Für Gewerbetreibende gibt es eine Aufbewahrungspflicht, die sich aus den Vorschriften u.a. des Handelsgesetzbuch ergeben. So müssen E-Mails teilweise nach gängiger Auffassung bis zu sieben Jahre lang vorgehalten werden. Eine Archivierung und ein Backup sind dann also gewissermaßen Pflicht. Der Gesetzgeber macht aber keine Vorschriften, wie die E-Mails zu archivieren sind, sagt aber, dass sie zu archivieren sind.

E-Mails sind am einfachsten dadurch sichern, dass mit einem E-Mail-Programm, auch Mailclient genannt, auf die E-Mails zugegriffen wird. Innerhalb der Anwendung können nun die E-Mails, die empfangen oder versendet wurden, heruntergeladen und damit gesichert werden.

Goneo bietet zwei Protokolle an, um auf E-Mails zuzugreifen: Zum einen gibt es das POP3-Protokoll. Damit lädt man beim Zugriff Mails herunter, wobei nach dem Herunterladen diese Mails auf dem Server gelöscht werden. Alternativ dazu existiert das IMAP Protokoll, mit dem Mails sozusagen zwischen Mailserver und Mailclient synchronisiert werden.

Auch für E-Mails sollte man sich eine Sicherungsstrategie zurecht legen. Eine Möglichkeit ist, die Mails von einem Mailkonto in ein anderes zu kopieren, eine andere ist, die Mails auf die lokale Festplatte zu exportieren. Leider gibt es keinen eindeutigen Standard, wie die E-Mails auf einem lokalen Medium abgelegt werden. Jedes Mailprogramm macht das anders.

Vorausgesetzt, man verfügt über zwei E-Mail-Konten, die beide IMAP-fähig sind und genügend Speicherplatz bereitstellen, könnte man ein E-Mailkonto als Archiv oder Sicherungskonto definieren.

Die Konten müssen nicht zwingend beim gleichen Anbieter liegen. In einer Mailsoftware wie Thunderbird richtet man beide Konten parallel ein. Nun kann man Mails von einem Konto zum anderen Konto durch Drag an Drop kopieren (oder auch verschieben, womit man eine Archivfunktion hätte). Die Mails werden von der Software zum Server wieder hochgeladen.

Auf dieser Weise lassen sich auch Mailumzüge von Anbieter zu Anbieter realisieren.

Die Bedrohungslage im Bereich Mailserver ist etwas anders. Angriffe auf Webserver haben das Ziel, den Webserver zu übernehmen. Angriffe gegen E-Mail-Konten richten sich oft gegen die E-Mail-Clients, also Outlook, Thunderbird und dergleichen, die auf den Rechnern der User installiert sind. Meist versuchen die Hacker dort, Zugangsdaten zu E-Mailkonten abzugreifen. Zum Einsatz kommen

dann Tastaturlogger oder andere Schadsoftware, die über Trojaner eingeschleust werden.

Angriffe gegen Mailkonten des Mailservers sind häufig Brute-Force-Attacken. Das heißt, hier versuchen Angreifer durch stumpfes Ausprobieren, Zugangsdaten sozusagen zu erraten. Einfach gestrickte Passwörter machen Hackern das Leben leichter. Daher gelten meist einige Regeln bei der Erstellung von Mailkontopasswörtern. Üblich ist eine Mindestlänge der Zeichenkette und Notwendigkeit, Ziffern, Sonderzeichen sowie Groß- und Kleinbuchstaben zu verwenden.

Mit erbeuteten Zugangsdaten lassen sich Identitäten stehlen. So könnte ein Hacker mit einer gestohlenen Identität im Web Bestellungen auf Rechnung tätigen, diese Bestellungen bestätigen (er hat ja Zugriff auf das Mailkonto und kann einen Bestätigungslink anklicken) und die Ware irgendwohin schicken lassen (an eine Packstation zum Beispiel). Das alles passiert sozusagen im Namen desjenigen, dem die E-Mailadresse eigentlich gehört. Man sollte auf seine E-Mailkonten also gut aufpassen.

In der Wahrnehmung vieler Menschen ist die einzelne E-Mail-Nachricht nicht besonders schützenswert. Das Eindringen von Hackern in den E-Mail-Account bekommt man vielleicht auch erst sehr spät mit, nämlich dann, wenn Geschädigte Rückfragen stellen oder die eigene E-Mailadresse auf Spamlisten landet. Gelegentlich erhalten Geschädigte auch „Bouncemails", also automatisch generierte Hinweise, wonach eine E-Mail abgewiesen wurde, weil der Empfänger nicht erreichbar ist. Das ist ein Hinweis darauf, dass die Mailidentität zum Spamversand missbraucht wird, möglicherweise (und sogar wahrscheinlich) auf einem ganz anderen System. Die muss also nicht bedeuten, dass der Spamversand von einem gehackten Mailkonto ausgeht. Oft wird auch „nur" eine echte E-Mail-Adresse angegeben, um der Spammail zu einer erhöhten Aufmerksamkeit beim Empfänger zu verhelfen.

Eine Hürde stellen die IMAP-Ordner dar, die mit IMAP von Mailclients angelegt werden oder vom User angelegt worden sind. Mit Thunderbird lassen sich die in einem Mailkonto angelegten Ordner samt Inhalt zu einem neuen Mailkonto verschieben. Dies ist in diesem Fall ein Kopiervorgang.

Auch andere Mailprogramme ermöglichen einen Export und auch Import von E-Mails. Outlook von Microsoft speichert Mails in einem eigenen Format in einer Datendatei. Zudem kann Outlook auch ein Archiv exportieren. Verwendet man also Outlook als Mailsoftware, kann man zum Beispiel die entsprechende Daten- oder Archivdatei kopieren und somit sichern.

Dabei ist zu überlegen, ob das Mailarchiv nicht auch mit der obligatorischen Sicherung des PCs oder Notebooks angelegt wird. Somit wäre ein eigenes Mailkontenbackup eventuell verzichtbar. Dennoch erscheint es sinnvoll, auch von den Inhalten der E-Mail-Konten regelmäßig Sicherungen herzustellen.

Da es für bestimmte Personen und Institutionen eine gesetzliche Pflicht gibt, E-Mails als geschäfts- oder steuerrelevante Daten für eine vorgeschriebene Frist aufzubewahren, gibt es auf dem Markt diverse Angebote.

Sicherungswürdig sind auch die gesammelten Kontaktdaten wie sie in den diversen Adressbüchern von Mailclients gesammelt werden. Diese Kontaktsammlungen werden für gewöhnlich nicht auf dem Server abgelegt (es gibt Ausnahmen), so dass die eigentliche Datendatei auf der lokalen Festplatte zu finden ist und mit der Sicherung der lokalen Festplatte kopiert werden sollte.

EIN FAZIT

Für Desktops und Notebooks gibt es vor allem für das Windows von Microsoft viele Tools und Anwendungen, die bei der Erstellung von Sicherheitskopien helfen. Selbst im Betriebssystem sind entsprechende mehr oder weniger komfortable Funktionen eingebaut. Die Sicherungsprinzipien sind die gleichen wie im Falle einer Sicherheitskopie der Website. Man sichert entweder vollständig, teilweise oder in einer festgelegten Variante inkrementell oder differenziell. Auch für die Betriebssysteme von Apple gibt es natürlich Sicherungsprogramme. In vielen Fällen wird auf eine externe oder auch dafür vorgesehene interne Festplatte gesichert. Sicherheitskopien oder Fragmente davon auf einen entfernten Server abzulegen wird offensichtlich aber immer mehr die Regel. Smartphone-Betriebssysteme sind, je nach Hersteller, schon mit Cloud-Speicherplätzen verknüpft, so dass der komplette Datenbestand dahin abgespeichert wird.

Wenn man also Website-Dokumente, Datenbankdumps und E-Mailkopien auf der lokalen Festplatte lädt und die lokale Festplatte ebenso gesichert wird, ist ein manchmal schon ausreichendes Sicherheitsniveau erreicht.

Für den Bereich Websites und Webapplikationen gibt es kein Backuptool, das für alle Szenarien und Anwendungen empfohlen werden könnte. Das ist insoweit verwunderlich als dass der Bedarf an einem universellen Backuptool recht groß sein dürfte. Die meisten Tools beschränken sich darauf, einen Datenbankdump herzustellen, wahrscheinlich da dies als komplexeste Aufgabe gesehen wird.

Im Regelfall wird also die Backupaufgabe immer in zwei Teile zerfallen: 1. Kopiere die Daten, die auf dem Webspace liegen und 2. erstelle eine Kopie der Datenbankinhalte.

Für den ersten Teil kommt hauptsächlich FTP mit einer Anwendung wie Filezilla (Windows, Linux) oder Cyberduck (MacOS) in Frage.

AUS SICHERUNGSDATEIEN WEBSITES WIEDER HERSTELLEN

VORBEREITUNG AUF DEN ERNSTFALL: DIE RÜCKSICHERUNG ÜBEN

Die Wiederherstellung von Daten kann man durchaus auch simulieren, also in einer Art Übung testen, ob das Konzept, das man sich zurecht gelegt hat, auch wirklich funktioniert.

Ein Backup zu erstellen ist die eine Sache, daraus wieder eine lauffähige Webanwendung zu machen, eine andere. Neben der Verfügbarkeit der Backups muss man meist auch die Webanwendung gut genug kennen, um eine nahtlose Wiederherstellung zu ermöglichen.

TESTWEISE RÜCKSICHERUNG AUF EINEM ANDEREN WEBSERVER

In gewissen Grenzen kann man die Backups auf Funktionsfähigkeit testen. So ist es möglich, zu versuchen, auf einem weiteren Webserver, die Daten hochzuladen, wieder zu entpacken und die Inhalte in eine leere, unbenutzte Datenbank zu schreiben. Dazu nutzt man am besten einen Domainnamen, der nicht für die Öffentlichkeit gedacht ist. Dies lässt sich über die Funktion „Subdomain anlegen" bei goneo recht leicht implementieren. Zudem stehen, je nach Tarif beziehungsweise Leistungspaket mehrere Datenbanken zur Verfügung. So kann man den Ernstfall proben und Punkte entdecken, die entgegen früherer Annahmen dann doch noch Probleme bereiten.

Natürlich ist zu berücksichtigen, dass die Webanwendung, sei es nun WordPress oder Joomla oder eine andere Software in den Konfigurationseinstellungen die Verbindung zu der eigentlichen Datenbank vorhält und auch die eigentliche Domain irgendwo gespeichert sein muss.

Wenn sich also der Domainname und die Datenbank ändern (bedingt durch die Testdomain und die Testdatenbank), muss dies für die Rücksicherung beachtet werden. WordPress speichert solche Informationen in der Datei wp_config.php. Ein solcher Versuch ist also nicht ganz ohne Komplikationen, zeigt aber auf, auf welche Dinge man eigentlich achten muss.

WEBANWENDUNG AUS BACKUPS AUF DEM HEIMISCHEN NOTEBOOK ODER DESKTOP PC WIEDERHERSTELLEN

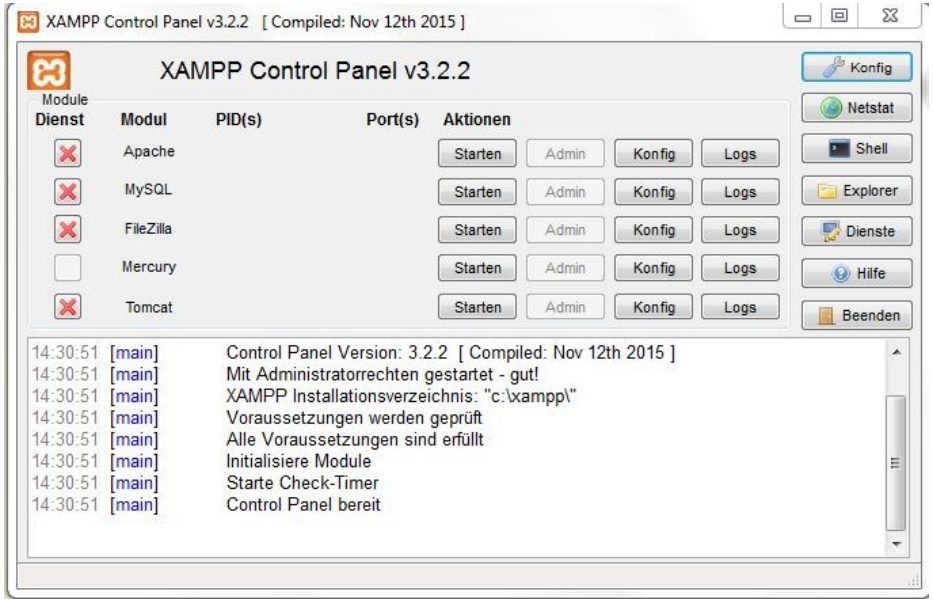
Wem es (verständlicherweise) nur wenig behagt, die Backupdateien auf dem Server oder Webhosting-Paket wieder auszupacken und zurückzusichern, obwohl das System ja läuft („*never touch a running system*") kann sein eigenes Notebook oder den Desktop PC verwenden. Schließlich besteht die akute Gefahr des Überschreibens von Daten.

Die Software, die man installieren kann, um eine ähnliche Umgebung auf dem PC herzustellen, in der sich WordPress und Co wohlfühlen, heißt XAMP. Dieses

Softwarebündel gibt es für Windows, Linux und MacOS fertig zur Installation unter https://www.apachefriends.org/de (kostenlos) und stellt einen Apache-Webserver mit Datenbank und weiteren Komponenten bereit.

Dies wäre eine Möglichkeit, das Backup von Webanwendungen unter Fast-Realbedingungen gefahrlos auszuprobieren. Zudem gewinnt man einiges an Erfahrung, wenn es darum geht, im Ernstfall alles wieder herstellen zu müssen. Eine solche Testumgebung lässt es übrigens auch gefahrfrei zu, zu prüfen, ob eine Anwendung zum Beispiel mit einer neuen PHP-Version zurechtkommt.

Tipp: Es ist ratsam, mit einem Backup zu experimentieren, das im Ernstfall verzichtbar wäre, also unter Umständen mit einer Kopie eines aktuellen Vollbackups.



XAMP bringt ein Control Panel mit, so dass man den Apache Webserver per Klick starten und stoppen kann sowie Datenbanken einrichten kann, ohne das über das Konsolenfenster per Tastatur tun zu müssen. Mit PHPMyAdmin, das freundlicherweise ebenso schon in der lokalen Installation integriert ist, kann man eine Datenbank bequem mit der Weboberfläche anlegen. Man kann sich das Leben etwas einfacher machen, indem man die Datenbank genauso nennt wie auf dem Server, auf dem die produktive Version der Anwendung läuft. Es spricht auch nichts dagegen, lokal den gleichen Datenbankbenutzernamen und das gleiche Passwort zu verwenden. Dann muss man nicht in den Konfigurationseinstellungen so viel ändern, um die Anwendung lokal (also in der auf dem Notebook oder PC installierten Version) zum Laufen zu bringen. Lediglich der Domainname wird

dann noch Problemchen verursachen. Einen Mailserver (in der aktuellen Grundinstallation ist Mercury enthalten) oder Javaserver (Tomcat) wird man für diese Zwecke nicht brauchen.

Um die Sicherungsdateien verwenden zu können, muss man eigentlich „nur" die Dateien für die Webdokumente, die per FTP heruntergeladen wurden, an entsprechender Stelle mit dem Dateimanager einkopieren. Im Browser sollte sich dann die Anwendung aufrufen lassen.

Auch wenn die lokale Installation nicht hundertprozentig sauber läuft, lässt die teilweise erfolgreiche Installation dann doch einigermaßen sichere Rückschlüsse darauf zu, ob das Backup vollständig und zumindest prinzipiell ausreichend ist.

VORGEHEN BEI EINER WIEDERHERSTELLUNG DER ANWENDUNG AUS EINEM BACKUP

Egal, ob man auf dem Ausgangssystem nach einer Havarie die Daten wiederherstellen muss oder ob man ein neues Zielsystem verwendet, das Vorgehen für eine Wiederherstellung ist recht ähnlich: Das Zielsystem wird in einem ersten Schritt vorbereitet (eventuell noch vorhandene Daten werden gelöscht).

Danach werden Anwendungsdaten und Datenbankinhalte zurückgesichert. Erstere via (S)FTP, zweitere mit PHPMyAdmin oder einem Tool wie MySQLDumper. Es bietet sich meistens an, die Datenbankinhalte zuerst zurückzusichern.

Man ist gut beraten, zur Rücksicherung die gleichen Tools zu verwenden, mit denen man die Backups erstellt hat. Das kann bedeuten, dass zunächst diese Tools wieder installiert werden müssen. Hier ist XCloner gegenüber MYSQLDumper etwas im Vorteil, da XCloner eine Minimalinstallation in die Sicherungsdatei packt.

Ob man auf dem Zielsystem alle Dateien zunächst entfernen will, hängt von der Art der Havarie und des Schadens ab. Wenn sicher nur die Datenbank zerstört wurde, müsste man nur die Datenbank wiederherstellen. Analog reicht es nach einem versehentlichen Löschen der Anwendungsdaten oder eines Teils davon, die HTML-, CSS, JavaScript- und PHP-Dateien der Anwendung wieder herzustellen. Was zurückgesichert werden muss, hängt vom Einzelfall ab.

Vorsicht ist geboten, wenn ein Befall mit Viren oder anderer Schadsoftware der Grund für die Notwendigkeit gewesen ist, auf das Backup zurückzugreifen. Dann ist es wohl sicherer, alle Dateien und Datenbankinhalte zu entfernen und vom Backup einzuspielen, auch wenn das länger dauert.

Sollte die Wiederherstellung am gleichen Platz erfolgen, sollten die Zugangsdaten noch unverändert sein. Das heißt, die Konfigurationsdateien müssen nicht verändert werden. Ändert sich die Umgebung, muss man manuell in die Konfigurationseinstellungen eingreifen und diese so ändern, dass die Anwendung auf die Datenbank zugreifen kann.

Leider ist dies in der Praxis nicht immer so einfach. Daher muss man die Anwendung etwas kennen.

WORDPRESS AUS EINEM BACKUP WIEDER ZUM LAUFEN BRINGEN (IN EINER NEUEN UMGEBUNG)

WordPress gehört zu den meistverwendeten Webanwendungen weltweit. Dank seiner technischen Genügsamkeit ist es rund um den Erdball gleichermaßen beliebt, nicht nur bei Bloggern, für die es eigentlich gedacht war. Als quelloffene Software war die Anwendung auch bei Programmierern beliebt, die sehr viele Erweiterungen (Plugins) für nahezu jeden Zweck und Vorlagen (die Vorlagen oder Templates heißen bei WordPress Themes) beigesteuert haben. Heute gibt es ganze Communities und Shops auf WordPress-Basis. Grund genug also, am Beispiel von WordPress zu zeigen, wie aus einem Backup eine wieder lauffähige Anwendung erstellt werden kann.

WordPress speichert den Domainnamen (genauer: die komplette URL) sowohl in der Datei wp-config.php als auch in der MySQL Datenbank. So kann man beide Stellen editieren. Ruft man jedoch WordPress sobald es auf dem neuen Server liegt bei bereits funktionierender Datenbankverbindung auf, versucht WordPress die Pfade zu in den Blogposts eingebetteten Mediendateien entsprechend der Angaben auf der Setting-Seite (die auf die Daten in der MySQL-Datenbank zurückgreift) zu korrigieren. Das führt mit hoher Wahrscheinlichkeit zu nicht gewünschten Ergebnissen, was sich an „Datei-fehlt"-Bildplatzhaltern äußert, wenn man einen Beitrag mit Mediendatei aufruft. Dabei wird offensichtlich zwischen Medien in Beiträgen und Beitragsbildern unterschieden.

Um die Kopie von WordPress sauber zum Laufen zu bekommen, sollte man vorgehen, wie es auf der WordPress-Seite beschrieben ist (https://codex.wordpress.org/Moving_WordPress):

1. Dateien herunterladen
2. Die MySQL Datenbank exportieren
3. Die Kopien der Dateien und die als Sicherheitskopie an einen geschützten Platz ablegen
4. Nun in die bestehende WordPress Seite einloggen und unter "Einstellungen" > "Allgemein" den Domainnamen ändern (also von Beispielsweise http://www.beispiel.de auf http://www.anderes-beispiel.de). Dach Änderungen speichern. Im Normalfall erscheint dann eine 404-Fehlerseite.
5. Nun die Dateien nochmals herunterladen.
6. Nun die Datenbank noch einmal exportieren.
7. Die Datei wp-config.php editieren und die Datenbankverbindungsangaben des neuen Servers verwenden (Datenbankserver, Datenbankname, Datenbankbenutzername und Passwort).
8. Die zuletzt heruntergeladenen Dateien auf dem neuen Speicherplatz hochladen.

9. Die zuletzt gesicherten Datenbankinhalte in die (leere) Datenbank des neuen Servers importieren.

Damit sollte WordPress in der neuen Umgebung lauffähig sein. Natürlich ist nicht auszuschließen, dass einige Plugins sich eventuell nicht so verhalten wie sie sollten. Unter Umständen muss man auch die Schreib- und Leserechte auf dem neuen Server anpassen. Dies sollte mit dem FTP-Programm möglich sein.

ANDERE WEBANWENDUNGEN

Für Backups von Joomla gelten die oben beschriebenen Verfahrensweisen analog: Sollte man nur per FTP Zugriff auf den Server haben, kopiert man die Dateien und macht mit PHPMyAdmin oder einem Tool wie XCloner oder MySQLDumper eine Kopie der Datenbank. Eine Rücksicherung funktioniert dann analog auf umgekehrte Weise.

Geht es darum, auf einem neuen oder anderen Server diese Kopie zum Laufen zu bringen, ist ähnlich wie bei WordPress ein Eingriff eine Konfigurationsdatei erforderlich: Es handelt sich um configuration.php und darin speziell um den Abschnitt, der die Datenbankverbindung definiert. Wenn die Pfadangaben auch nicht mehr übereinstimmen, sollte Joomla dennoch laufen. Extensions können dann aber nicht hinzugefügt werden. Dies ist aber nach entsprechender Anpassung in System > System Information > Directory Permissions wieder möglich. Ansonsten enthält die Seite https://docs.joomla.org/Copying_a_Joomla_website noch weitere Hinweise über Datei- und Verzeichnisrechte, die eventuell angepasst werden müssen.

Für Joomla wird oft Akeeba als Backuptool empfohlen. Akeeba wird beim Versuch, die Joomla-Installation in einer neuen Umgebung wieder zum Laufen zu bringen, um die Eingabe der Datenbankverbindungsparameter bitten.

Es gibt einige externe Tools oder Onlinetools wie „Drop my site" (www.dropmysite.com), die Webseitenbesitzern den Transfer und das Backup einer Webseite erleichtern wollen. Das funktioniert mit Dateien, die per FTP heruntergeladen werden können ganz gut. Die gesicherten Dateien werden irgendwo auf einem Server als Backup gespeichert. Schwierig wird es bei Datenbankverbindungen, die bei vielen Anbietern nicht extern zugänglich sind, sondern nur von der Webapplikation angesprochen werden können. Vor allem im Shared Hosting Bereich ist üblich, dass auf die MySQL Datenbank extern nicht zugegriffen werden kann.

ABSCHLIEßENDE HINWEISE

Backups und Datensicherungen haben nicht das beste Image. Das liegt vielleicht daran, dass man keinen unmittelbaren Nutzen hat und das Sicherheitsgefühl sehr trügerisch ist. Man vertraut sehr gerne darauf, dass morgen alles so gut weiter läuft wie gestern und heute. Statistischen Angaben zufolge sah sich jedoch jedes dritte deutsche Unternehmen mindestens einmal mit einem Datenverlust konfrontiert. Schnell erreichen die Schäden Höhen von mehreren Millionen Euro. Im Privatbereich wird man es eher mit ideellen Werten zu tun haben, die man nur schwer in Geld ausdrücken kann. Was ist ein umfangreiches Bilderarchiv wert? Ohne Frage haben Daten einen gewissen Wert, den man, wenn man nicht gerade vor einem Desaster steht, tendenziell unterschätzt.

Daher einige abschließende Tipps:

- Ganz **wesentlich** ist es, 1.Backups herzustellen und 2.regelmäßig Backups herzustellen.
- Folge der **3-2-1 Regel**
  Es sollte mindestens drei Kopien jeder Datei geben, zwei auf unterschiedlichen Datenträgern und eine an einem anderen sicheren Ort.
- **Plane** Backups
  Es sollte einen Plan für Sicherungsläufe geben, an den man sich auch halt. Kalendererinnerungen (Serientermine) können helfen. Zudem kann man sich eine Tabelle mit entsprechender Planung zurechtlegen. Bewährt hat sich auch ein fester Freitag-Nachmittag-Kaffee-und-Backup-Termin, eventuell mit dem Team, in dem man arbeitet.
- **Teste** Backupmedien regelmäßig
  Wiederverwendete Backupmedien können (und werden früher oder später) Schaden nehmen und ausfallen. Datenträger sollten in Abständen getauscht werden, ehe sie ausfallen.
- **Sichere** deine Backups
  Verschlüsselung ist empfehlenswert. Und achte gut auf den Schlüssel.

Autor: Markus Käkenmeister (@markus2009) für goneo Internet GmbH, Minden
Stand Mai 2016