INFONEWS

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

www.goSecurity.ch
Mit Sicherheit an der richtigen Adresse.

Backup Strategie

Daten und Informationen sind die wichtigsten Elemente, um ein Unternehmen betreiben zu können. Seien dies nun Briefe, Offerten oder gar Verträge, alle diese Dokumente müssen Gesetzeswegen aufbewahrt werden oder aber für den Betrieb verfügbar sein. Neben den Interessen der Firma existieren auch diverse Vorschriften von Behörden. Die Buchhaltung zum Beispiel muss während zehn Jahren in unveränderbarem Zustand archiviert sein. Obwohl Speicher (Harddisk, SAN, NAS, etc.) immer billiger werden, lohnt es sich, ein Backup in traditioneller Weise zu machen. Neben der Systemsicherung sind auch die Daten der Laptops und der Handheld zu sichern.

Falls Sie Anregungen oder Ideen aus Ihrem eigenen IT-Alltag haben, nehmen wir diese gerne auf. Wir freuen uns auf ein Feedback von Ihnen.

Dies ist eine kostenlose Dienstleistung der GO OUT Production GmbH (www.goSecurity.ch/INFONEWS).

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Welche Daten müssen gesichert werden?

Diese Frage global zu beantworten ist nicht möglich. Zu unterschiedlich sind die Unternehmensanforderungen. Daher ist es wichtig, dass vor dem Einsatz eines Backupsystems überlegt werden muss, welche Daten für das Überleben der Firma notwendig sind. Die verschiedenen Abteilungen und Personen müssen für Ihren Bereich angeben, auf welche Daten sie in welcher Zeit wieder zugreifen müssen. Oder was muss wie lange Archiviert werden. Mit diesen Angaben kann anschliessend mit der Planung des Backups begonnen werden. Die IT-Leitung muss ihrerseits die Verfügbarkeitsanforderung an die Systeme, welche durch den Betrieb vorgegeben

wird, mit einbeziehen. z.B. die Komplettsicherung eines Systems, Handheld, entfernbare Speichermedium, wie Memory Sticks, Laptops usw.. Dies erhöht vermutlich den Kapazitätsbedarf um ein vielfaches. Es lohnt sich, diese Punkte genau anzuschauen. Welche Vor- und Nachteile sind damit verbunden? Lohnt sich der Aufwand?

Erstellen Sie sich eine Liste mit allen relevanten Daten und Applikationen. Versuchen Sie die einzelnen Bedürfnisse mit den entsprechenden Verantwortlichen zu erarbeiten. Damit erhalten sie einen ersten Überblick, über die zu erwartenden Anforderungen.

Objekt	Menge (in MB)	Datenschutz ein Thema?	Verfügbarkeit ein Thema?	Archivierung nötig? (Dauer)
Allg. File (auf dem FileServer)	780'000	Ja	Ja	~
Email Server	1'800	-	Ja	-
Email Box	10'000	Ja	Teilweise	1 Jahr
Email Verkehr		Ja	-	1 Jahr
Shop Datenbank	890	-	24 h	6 Monat
ERP Server		-	Ja	-
ERP Daten		Ja	Ja	10 Jahre
Logfile (pro Tag)	130	Ja	-	6 Monate
CNC Daten	400	Ja	Ja	5 Jahr
LDAP Server	1'400	~	Ja	-
LDAP Daten	300	~	Ja	6 Monate
Palm Daten	50	Ja	-	1 Monat
Laptop (Verkäufer)	100	Ja	-	6 Monate
Laptop (Allgemein)	100	~	-	1 Monat

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 Wie soll ein Backup durchgeführt werden?

Die Möglichkeiten, wie man ein Backup durchführt, sind sehr vielfältig, was wiederum die Planung erschwert. Wir möchten in diesem Kapitel die häufigsten Arten des Backups mit Ihren Vor- und Nachteilen kurz beschreiben. Beachten Sie, dass ein RAID, Diskmirroring oder ein zweiter Server nicht so schnell ausser Haus gebracht werden können und die Daten würden z.B. im Brandfall zerstört.

2.1.1 Klassisches Backup auf Tape

Bei dieser Art des Backups ist ein Bandlaufwerk notwendig. Der Markt bietet hier eine Unzahl von Möglichkeiten an. DAT, DLT, LTO, AIT sind typische Bezeichnungen. Was ist aber nun das Richtige? Mit der Planung der zu sichernden Daten hat man einen Hinweis auf die Kapazität, die benötigt wird. Jedes Medium bietet ein unterschiedliches Platzangebot, viele Geräte können die Daten auch noch komprimieren, was den zur Verfügung stehenden Platz erweitert. Unsere Erfahrung zeigt jedoch, dass die Komprimierung nicht das bietet, was sie verspricht. Oft werden die angeschriebenen Werte bei weitem nicht erreicht. Wir raten Ihnen daher, die unkomprimierte Angabe als Planungswert zu verwenden.

Wenn bei der Planung ersichtlich ist, dass ein Band nicht ausreichen wird, kann ein Bandroboter in Betracht gezogen werden. Dabei ist es möglich, mehrere Bänder einzulegen und das Backupsystem verteilt die zu sichernden Daten selbständig.

Ein weiterer, zentraler Wert ist die Schreibgeschwindigkeit. Die zu sichernden Daten müssen in einer bestimmten Zeit auf dem Band sein. Die zu sichernden Daten nehmen immer mehr zu und die Nacht wird nicht länger. Diesem Umstand sollte schon bei der Planung Beachtung geschenkt werden. Die Daten müssen möglichst schnell auf dem Band oder einem Zwischenspeicher liegen.

2.1.2 Backup auf Harddisk, von dort auf das Band

Der Zeitfaktor spielt immer eine grössere Rolle. Sei dies nun in Firmen, die Schichtbetrieb haben und nicht beliebig ein Backup durchführen können, oder wenn der Datenbestand nicht in der verfügbaren Zeit gesichert werden kann. Die billigste und oft auch einfachste Möglichkeit ist es, die Daten auf eine freigegebene Harddisk oder eine SAN-Station zu sichern. Der Schreibzugriff auf diese Datenträger ist um ein x-faches schneller, als auf das Band. Von diesem Zwischenspeicher können die Daten anschliessend in aller Ruhe auf das Band gesichert werden. Eine kostenlose Möglichkeit auf der Windows-Plattform ist das MS Backup, welches in den letzten Jahren stark zugelegt hat und nicht mehr im Schatten von kommerziellen Systemen zu stehen braucht. Gerade für eine Sicherung auf einen Datenträger ist dies eine schnell zu konfigurierende und praktikable Lösung.

2.1.3 Daten brennen

Viele Rechner werden heute mit einem CD- oder gar DVD-Brenner ausgeliefert. Da liegt es natürlich nahe, dieses Medium auch für das Backup zu verwenden. Obwohl auch eine DVD nicht an die Kapazität eines Bandes herankommt, kann sich dies lohnen. Die Rohlinge werden immer billiger, und bieten zudem die gewünschte Unveränderbarkeit der Daten. Wir empfehlen diese Art des Backups jedoch nur für eine tägliche, vollständige

Sicherung. Zudem muss jeden Tag ein neues Medium eingelegt werden. Dies will Personell gut organisiert sein. Beim Hinzufügen von Sessions auf der gleichen DVD kann es oft zu Problemen kommen. Daher raten wir davon ab.

2.1.4 Images

In den letzten Jahren ist eine neue Art der Sicherung entstanden. Das Erstellen eines Images. Dies kann nach dem Starten eines speziellen Betriebssystems (für Serversysteme vermutlich nicht durchführbar) oder im laufenden Betrieb erfolgen. Dabei wird eine 1:1 Kopie der gesamten Platte erstellt. Bei einer Wiederherstellung müssen nur die Datei wiederhergestellt werden, der Rest wird durch Image sichergestellt. Der grosse Nachteil, diese Wiederherstellung läuft nur auf einem identischen HardwareSystem!

3 Wann soll ein Backup durchgeführt werden?

Bevor diese Frage beantwortet wird, zuerst eine kurze Übersicht über die verschiedenen Möglichkeiten, die praktisch jedes Programm, inkl. deren der Betriebssysteme, bietet.

3.1.1 Full-Backup

Beim Fullbackup werden alle angewählten Daten gesichert, unabhängig, wie das Archivbit gesetzt ist. Das Archivbit der gesicherten Daten wird dabei gelöscht.

3.1.2 Differentielles Backup

Bei dieser Art des Backups werden nur die Veränderungen seit dem letzten Full-Backup gesichert (d.h. nur Dateien, bei denen das Archivattribut gesetzt ist). Das Archivbit wird gelöscht.

Vorteile:
Sie brauchen weniger Speicherplatz als bei ausschliesslicher Vollbackup-Sicherung. Für die Wiederherstellung eines Standes benötigen Sie das eine differentielle Backup vom betreffenden Datum und das letzte davor liegende Vollbackup.

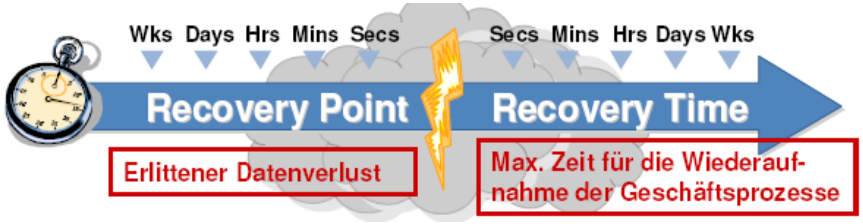
Nachteil:
Eine einmal geänderte Datei wird bis zum nächsten Vollbackup in jedem differentiellen Backup erneut gesichert, auch wenn sie nicht weiter bearbeitet wurde. Dies führt immer noch zu unnötig belegtem Speicherplatz.

3.1.3 Inkremental Backup

Dabei werden alle Veränderungen seit dem letzten Backup gesichert. Das Archivbit wird gelöscht.

Vorteil:
Da jeder Dateistand nur einmal gesichert wird, ist der Speicherbedarf optimal niedrig.

Nachteil:
Für einen kompletten Datenbestand ist das letzte Vollbackup und alle seither erzeugten inkrementellen Backups erforderlich. Um eine Datei wieder zu finden, brauchen Sie entweder ein gutes Verwaltungstool oder die Arbeit wird mühsam und fehleranfällig.



GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Wie oft ein Backup durchgeführt wird, und welche Art dabei verwendet wird, kann nicht global gesagt werden. Alle Arten bieten Vor- und Nachteile. Der grosse Vorteil beim Full-Backup ist sicher, dass alle Daten vorhanden sind. Eine Wiederherstellung eines Systems kann dadurch sehr schnell durchgeführt werden. Nachteilig wirkt sich jedoch der benötigte Speicherplatz aus. Dies ist hingegen der Vorteil des Differential Backups. Der Platzbedarf für jede weitere Sicherung ist bedeutend geringer, als beim Full-Backup. Eine Wiederherstellung kann jedoch sehr aufwändig sein, wenn alle Daten gerettet werden müssen. Dieses Manko wird durch das Inkremental Backup abgefedert. Bei einem Totalausfall muss nur das letzte Fullbackup sowie das letzte Inkremental wieder eingespielt werden. Nachteilig wirkt sich hier allenfalls der höhere Platzbedarf aus.

Bevor Sie mit der Umsetzung beginnen, müssen Sie sich mit dem möglichen Datenverlust und der Verfügbarkeit auseinander setzen. Dabei kommen folgende zwei Begriffe RPO (recovery point objective) und RTO (recovery time objective) zum Einsatz. Mit diesen beiden Begriffen präzisieren Sie die Art und das Intervall der Datensicherung.

Legen Sie die maximale RPO Zeit pro geschäftskritischen Applikation und Daten fest. Erweitern Sie dazu die vorangehend erarbeitete Tabelle inkl. der maximalen Ausfalldauer, dem RPO und dem RTO der einzelnen Objekte.

Zum Beispiel:

Objekt	**Max. Ausfalldauer**	**PRO**	**RTO**
Allg. File (auf dem File-Server)	24 h	4 h	-
Email Server	6 h		
Email Box		1 h	4 h
Email Verkehr	-	-	-
Shop Datenbank			
ERP Server	6 h	2 h	3 h
ERP Daten	6 h	2 h	3 h
Logfile (pro Tag)			
Print Server	4 h	-	5 h
LDAP Server			
LDAP Daten			

Im Fall des Mailservers müsste man sich Gedanken über ein redundantes System machen. Als Alternative könnte man die Mailbox einmal pro Stunde auf eine andere Harddisk auf dem Backupsystem sichern. Ab dieser Harddisk können Sie in Ruhe einmal pro Tag ein Tape erstellen, ohne das die Produktion in irgendeiner Form belastet wird. Damit können Sie die RPO Zeit auf einer Stunde halten und je nach Vorfall die RTO Zeit auf wenigen Minuten.
Im Fall das Print Servers würde man das System und die Druckertreiber einmal pro Änderung, oder noch weniger, einmal pro Monat automatisiert auf ein externes Band sichern.

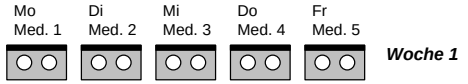
Mit einer guten Vorbereitung, also einem Konzept mit den genauen Anforderungen an die einzelnen Applikationen, haben Sie die Möglichkeit die wichtigsten Systeme dem Bedürfnis entsprechend zu sichern. Wenn Sie die Anforderung kennen, können Sie die Art der Sicherung festlegen. Dabei gibt es diverse Möglichkeiten wie Band, Harddisk, SAN, DVD, ShadowCopy, usw. Denken Sie daran, oft wird eine gemischte Lösung das Optimale zwischen Prozessorbelastung, Datenmenge, Geschwindigkeit und Recovery Zeit sein.

Der Intervall und evtl. den Zeitpunkt der Sicherung können Sie ebenfalls aus der Tabelle ableiten. Beachten Sie, dass Sie mit bilden von Gruppen die Übersicht behalten.

3.1.4 Medienrotationsverfahren

Es gibt viele verschiedene Medienrotationsstrategien, mit denen Sie Ihre Daten schützen respektive aufbewahren können. Der Hauptunterschied zwischen diesen Verfahren liegt in der Anzahl der benötigten Medien und im Zeitraum, nach dem die Medien in das Rotationsschema zurückkehren (Sicherungshorizont).

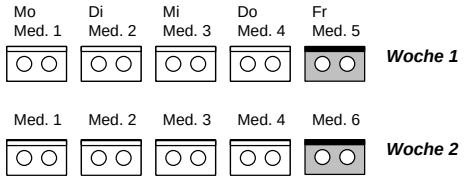
Sicherungsstrategie: Sohn
Anzahl der benötigten Medien: min. 1
Sicherungshorizont: letzte Sicherung
Beim Sohn-Schema wird jeden Tag eine Gesamtsicherung durchgeführt. Obwohl diese Strategie einfach zu verwalten ist, ist das Sichern mit nur einem Medium KEIN effektives Verfahren. Magentische Medien nutzen sich durch häufige Verwendung ab, und Sie können nur die Daten wiederherstellen, die seit der letzten Sicherung gesichert wurden.



Sicherungsstrategie: Vater/Sohn
Anzahl der benötigten Medien: min. 6
Sicherungshorizont: letzte zwei Wochen

Das Vater/Sohn Schema ist eine Kombination aus Gesamtsicherungen und Differential- bzw. Zuwachsicherungen über einen Zeitraum von zwei Wochen.

Bei dieser Strategie werden vier Medien für die Differential- oder Zuwachssicherungen von Montag bis Donnerstag benötigt. Die beiden anderen Medien enthalten Gesamtsicherungen und werden jeden Freitag aus der Rotation entnommen und ausserhalb des Unternehmens aufbewahrt.



Die Vater/Sohn Strategie ist leicht zu verwalten, und Sie können die Daten länger behalten als bei der Sohn-Strategie. Trotzdem ist sie für den in den meisten Netzwerken benötigten Datenschutz nicht ausreichend.

Sicherungsstrategie: Grossvater
Anzahl der benötigten Medien: min. 19
Sicherungshorizont: ein Jahr

Das Grossvater Schema ist eine der am häufigsten verwendeten Medien-rotationsstrategien. Es ist einfach zu

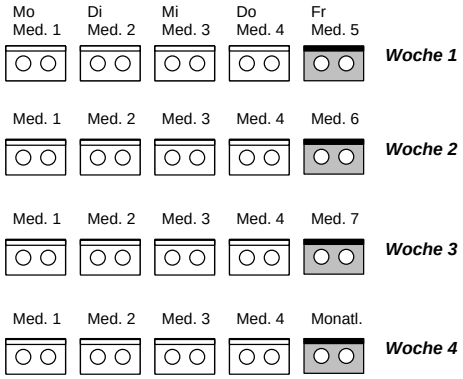
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

verwalten und umfassend genug, um Dateien für die Wiederherstellung wieder zu finden.

Bei dieser Sicherungsstrategie werden vier Medien benötigt, um von Montag bis Donnerstag Differentialsicherungen durchzuführen. Drei weitere Medien werden für Gesamtsicherungen am Freitag verwendet. Die übrigen zwölf Medien sind für monatliche Gesamtsicherung gedacht und werden ausserhalb des Unternehmens aufwahrt.

Die Grossvater-Strategie wird empfohlen, weil das Verhältnis der Anzahl der Medien zur Aufbewahrungszeit der Daten günstig ist (19 Medien / 1 Jahr).



Ausserdem lässt sie sich leicht verändern, wenn mehr Medien eingesetzt werden sollen. So können Sie zum Beispiel an jedem letzten Samstag des Monats eine Gesamtsicherung durchführen und diese dauerhaft archivieren.

3.1.5 Zuständigkeiten, Überwachung und Kontrollblatt

Regeln Sie die Zuständigkeiten für die Durchführung und für die Überwachung. Wenn möglich teilen Sie die beiden Aufgaben auf. Bei der Überwachung gilt es die nicht gesicherten Daten, noch verfügbarer Platz auf dem Sicherungsmedium etc. im Auge zu behalten. Führen Sie ein Kontrollblatt mit der Konfiguration des Backups und eines mit der Kontrolle des Ablaufes.

Datum	Bandname	Protokoll Check	Visum	Ausgetauscht	Visum
	Montag				
	Dienstag				
	Mittwoch				
	Donnerstag				
	Freitag 1				
	Samstag				
	Sonntag				
	Montag				
	Dienstag				
	Mittwoch				
	Donnerstag				
	Freitag 2				
	.....				

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

4 Wie sollen Datenträger gelagert werden?

Ganz klar nicht am gleichen Ort, wo das Backup geschrieben wird! Als Lagerungsmöglichkeit kommen folgende Orte in Frage:

anderes Gebäude, anderer Brandabschnitt: Der Vorteil hier liegt ganz klar in der Verfügbarkeit. Die Bänder (oder andere Medien) sind in der Nähe und können sofort verwendet werden. Die Datenträger gehören zwingend in einen Tresor.

Banksafe: Banken bieten die Möglichkeit, Datenträger in Ihren Safes zu lagern. Hier fallen Gebühren an und bei einem Notfall am Wochenende kann nur in Ausnahmefällen auf die Datenträger zurückgegriffen werden.

Beim IT-Chef oder Geschäftsführer zu Hause: Diese Lösung trifft man in sehr vielen Fällen an. Der Vorteil sind sicher die nicht vorhandenen Kosten, doch sollte beachtet werden, dass bei Ferienabwesenheit dieser Person auf die Datenträger zurückgegriffen werden kann. Auch sollten die Datenträger nicht im Nachttisch verstaut werden, sondern auch hier fachgerecht bzw. vor fremden Zugriffen geschützt aufbewahrt werden.

Achten Sie bei der Beschriftung, dass keine Rückschlüsse auf den Inhalt und Herkunft der Bänder geschlossen werden kann.

5 Wie wird ein Disaster-Recovery getestet?

Bestimmte Daten wiederherstellen wurde bei den meisten Firmen bereits einmal gemacht. Sehr schnell ist eine Datei aus Versehen gelöscht und muss von den Sicherungsbändern zurückgeholt werden. Ob dies auch in einem Notfall funktioniert, kann dabei nicht beantwortet werden. Ein Disaster liegt dann vor, wenn zum Beispiel nicht mehr auf dem üblichen System eine Wiederherstellung durchführbar ist. Daher sollte in regelmässigen Abständen, mindestens nach einer Anpassung des Backupplans, ein Disaster-Recovery durchgeführt werden. Dazu sollte ein neues System so vorbereitet sein, dass ein Bandlaufwerk angeschlossen werden kann. Nun gilt es, alle Daten von den entsprechenden Bändern zurück zu holen. Sollten nur Daten darauf gespeichert sein, ist dies weiter nicht problematisch. Schwieriger wird es, wenn auch das Betriebssystem gesichert wurde. Oft klappt die Wiederherstellung dieser Daten nur noch auf einem baugleichen System. Daher sollte hier zusätzlich ein identisches Ersatz-Gerät bereit stehen oder ein entsprechendes Konzept vorhanden sein.

Disaster-Recovery ist ein eigenes grosses Kapitel, was zu einem spätern Zeitpunkt, in einer anderen INFONEWS Ausgabe behandelt wird.

6 Welche Kontrollen sind durchzuführen?

Mit dem Durchführen des Backups ist es nicht getan. Nach jeder Sicherung muss das Ergebnis kontrolliert werden. Meistens genügt ein Blick in die Logdatei des entsprechenden Programms. Wurden alle Daten gesi-

chert? Sind Störungen aufgetreten (Daten gesperrt, zu wenig Platz auf dem eingelegten Medium u.ä.)? Wie sieht der Zustand des Bandes aus? Muss das Laufwerk wieder gereinigt werden? Welches Band muss als nächstes eingelegt werden? Dies sind Fragen, die jeden Tag beantwortet werden müssen. Die Kontrolle und das Ersetzen eines Mediums sollten schriftlich festgehalten werden.
Wie bereits erwähnt, sollte nach jeder Änderung am Backup ein Disaster-Recovery durchgeführt werden. Wie lange dauert die Wiederherstellung, bis ein geordneter Betrieb garantiert werden kann, ist dabei einer der zentralsten Fragen, die es zu beantworten gilt.

Wenn Sie all diese Punkte in Ihrem Backupkonzept vorsehen und dies entsprechend umsetzen, sind Sie vor einem möglichen Datenverlust gefeit.

Kontrollieren Sie Ihr Konzept und Implementation auf folgende Punkte:

Zeitintervall und Zeitpunkt der Datensicherung
Können Sie zu jedem Zeitpunkt sicherstellen, dass die RPO - und RTO Zeit eingehalten werden kann? z.B.
Worst-Case Montag 06:30
Sonntag 06:00
Sonntag 23:00
Freitag 20:15
Mittwoch 12:05.

Umfang der zu sichernden Daten
Werden alle Daten und Konfiguration so gesichert, dass diese bei einem Teil- oder Disaster-Recovery brauchbar zur Verfügung stehen? Denken Sie dabei auch an die Generationen und der stetigen Veränderungen des Systems.

- *Zuständigkeiten*
  Wer wechselt wann die Bänder, was geschieht bei Ferienabwesenheit oder Krankheitsfall? Wer überprüft die Sicherung, das LogFile und geht möglichen Problemen nach? Wer muss feststellen, wenn Bänder voll sind oder wann diese ausgetauscht werden müssen?

- *Dokumentation*
  Wer ist für die Dokumentation des Backups zuständig? Wird es halbjährlich auf Vollständigkeit überprüft? Werden dabei Änderungen am System mitberücksichtigt?

- *Definition der Mobilengeräte*
  Haben Sie festgelegt, was mit den Daten auf Palm, Handheld, Handy oder Laptop geschieht? Wissen die Benutzer bescheid, wenn Sie die Daten manuell auf den Server kopieren müssen und wer Kontrolliert das in unregelmässigen Abständen?

- *Vertraulichkeit*
  Wo werden die Bänder gelagert und wer hat dabei Zugriff? Was geschieht bei Krankheit oder einer Brandkatastrophe?

Die GO OUT Production GmbH erstellt gemäss Ihren Anforderungen ein Backupkonzept, welches die zu sichernden Daten, die Art der Sicherung (Medium, Anzahl) und die Wiederherstellung sowie Kontrolle beinhaltet. Sprechen Sie mit uns, bevor Sie Ihre Daten verlieren.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21