

TeamDrive Personal Server


Benutzerhandbuch

Letztes Änderungsdatum: 12. September 2013

*Diese Anleitung wurde aktualisiert für TeamDrive Personal Server
Version 1.1.058*

Inhaltsverzeichnis

1	Installation.....	4
1.1	Windows/Mac OS X.....	4
1.2	Linux.....	4
2	Aktualisierung einer bestehenden Installation.....	6
2.1	Windows/Mac OS X.....	6
2.2	Linux.....	8
3	Konfiguration.....	8
3.1	Windows/Mac OS X.....	8
3.2	Linux.....	9
3.3	Einstellungen.....	9
3.3.1	Lizenzschlüssel.....	9
3.3.2	Hostname/IP-Adresse.....	9
3.3.3	Port.....	10
3.3.4	Passwort.....	10
3.3.5	Name des Datenverzeichnisses (Repository).....	11
3.3.6	Space-Namen als Klartext speichern.....	11
3.3.7	Pfad des Datenverzeichnisses (Repository).....	11
3.3.8	Maximale Größe des Datenverzeichnisses (Repository).....	12
3.3.9	Maximale Anzahl an Verbindungen.....	12
3.3.10	Poll-Interval.....	13
3.3.11	Connection-Timeout.....	13
3.3.12	Put-Verify-Timeout.....	13
4	Betrieb des TeamDrive Personal Servers.....	13
4.1	Windows/Mac OS X.....	13
4.1.1	Starten des Servers.....	13
4.1.2	Stoppen des Servers.....	14
4.1.3	Überwachen des Servers.....	14
4.2	Linux.....	14
4.2.1	Starten des Servers.....	14
4.2.2	Stoppen des Servers.....	14
4.2.3	Überwachen des Servers.....	14
5	TeamDrive Client anbinden.....	15
6	Sicherung und Wiederherstellung.....	15
6.1	Sicherung.....	15



6.2	Online-Sicherung	16
6.3	Wiederherstellung	16
6.4	TeamDrive Client Space-Wiederherstellung	17
7	Sicherheit	18
7.1	Verschlüsselung	18
7.2	Antiviren-Software	19
7.3	Hinweise zu Datenschutz und Administration	19
7.4	Besondere Hinweise zu Sekundärdaten/Protokolldaten	20
7.5	Hinweis für Daten von Berufsgeheimnisträgern i.S.d. § 203 StGB	21

1 Installation

1.1 Windows/Mac OS X

- a) Starten Sie die Installation mit einem Doppelklick auf das Installationsprogramm.
- b) Folgen Sie den Installationsanweisungen auf dem Bildschirm.
- c) Schließen Sie die Installation ab.

Hinweis:

Vor der ersten Inbetriebnahme des Servers muss dieser noch konfiguriert werden.

Lesen Sie mehr dazu in Kapitel 3 „[Konfiguration](#)“.

Um TeamDrive Clients mit dem TeamDrive Personal Server zu betreiben, müssen diese ebenfalls noch konfiguriert werden.

Lesen Sie mehr dazu in Kapitel 5 „[TeamDrive Client anbinden](#)“.

1.2 Linux

- a) Entpacken Sie das Installationspaket.

Öffnen Sie hierzu ein Terminalfenster und wechseln Sie in das Verzeichnis, welches das Installationspaket enthält.

- b) Entpacken Sie die Datei „TeamDrivePersonalServerLinux_xxxx.tar.gz“ mit folgendem Befehl: „tar -xvzf TeamDrivePersonalServerLinux_xxxx.tar.gz“. Das xxx entspricht der aktuellen Versionsnummer (in Zahlen).

- c) Wechseln Sie mit dem Befehl „cd tdps“ in das Verzeichnis „tdps“.

In diesem Ordner befinden sich die wesentlichen Komponenten (Dateien/Verzeichnisse) zum Betrieb des TeamDrive Personal Servers:

- tdpsd: Die Server-Anwendung.
- stop-tdps: Datei zum Stoppen des Personal Servers.
- watch-tdps: Zeigt den Server-Status im Konsolenfenster an.
- tdps-md5pwd: Verschlüsselt ihr Passwort per MD5-Algorithmus.
- tdps.config: Hier sind sämtliche Einstellungen Ihres TeamDrive Personal Servers gespeichert. Sie müssen diese noch manuell mit einem Texteditor editieren.


Hinweis:

Wir empfehlen, regelmäßig eine Sicherung der Datei „tdps.config“ anzulegen.

- data/

In diesem Verzeichnis wird standardmäßig das Repository Ihres Servers angelegt.

Alle Daten aus den Spaces aller Nutzer, die an diesem Server angemeldet sind, liegen in diesem Verzeichnis.



Sie können den Speicherort der Daten über die Einstellung „repository-data“ in der Konfigurationsdatei „tdps.config“ ändern.

Hinweis:

Das Repository Ihres Servers sollte auf einem lokalen Volume liegen.

Netzlaufwerke werden nicht unterstützt.

Der Server arbeitet mit File-Locking.

Achtung:

Machen Sie unbedingt regelmäßig eine Sicherung dieses Verzeichnisses, insbesondere vor einer Aktualisierung.

Alle Daten der Nutzer des TeamDrive Personal Servers sind hier gespeichert.

Sollten Sie den Standardpfad nutzen, könnte dieser bei einer Neuinstallation oder einer Aktualisierung überschrieben werden.

d) Verschlüsseln Sie Ihr Passwort wie folgt: „/tdps-md5pwd meinPasswort“, wobei „meinPasswort“ das von Ihnen gewählte Passwort darstellt.

Dieses Passwort wird für die weitere Konfiguration des Servers benötigt.

Achtung:

Der TeamDrive Personal Server darf nicht als Benutzer „root“ ausgeführt werden.

Wir empfehlen hierfür einen eigenen Benutzer anzulegen.

Hinweis:

Vor der ersten Inbetriebnahme des Servers muss dieser noch konfiguriert werden.

Lesen Sie dazu mehr in Kapitel 3 „[Konfiguration](#)“.

Um TeamDrive Clients mit dem TeamDrive Personal Server zu betreiben, müssen diese ebenfalls noch konfiguriert werden.

Lesen Sie dazu mehr in Kapitel 5 „[TeamDrive Client anbinden](#)“.

2 Aktualisierung einer bestehenden Installation

Hinweis:

Wir empfehlen, vor einer Aktualisierung eine vollständige Sicherung Ihrer bestehenden Daten durchzuführen.

Lesen Sie mehr dazu in Kapitel 6 „Sicherung und Wiederherstellung“.

Überprüfen Sie außerdem auf unserer Website, ob eine aktualisierte Version dieser Dokumentation existiert und beachten Sie dann diese.

2.1 Windows/Mac OS X

Um eine Aktualisierung des TeamDrive Personal Servers von der Version 1.0.047 oder früher durchzuführen, führen Sie bitte folgende Schritte aus:

Windows:

- Stoppen Sie den TeamDrive Personal Server.
- Verschieben Sie die Konfigurationsdatei „tdps.config“ und das gesamte „data“-Verzeichnis (Repository) Ihrer bisherigen Installation des TeamDrive Personal Servers an einen Ort außerhalb des Installationsverzeichnisses des TeamDrive Personal Servers.
- Deinstallieren Sie den bisherigen TeamDrive Personal Server.
- Unter Windows 8 können Sie den TeamDrive Personal Server über den Menüpunkt „Programm deinstallieren“ in der Systemsteuerung entfernen.

In allen anderen Windows-Versionen kann der TeamDrive Personal Server durch den entsprechenden Startmenüeintrag deinstalliert werden.

Beantworten Sie die Frage, ob die Space-Daten entfernt werden sollen mit „Nein“.

- Installieren Sie nun die neue Version des TeamDrive Personal Servers entweder in das vorgeschlagene Standardverzeichnis oder in ein leeres Verzeichnis und starten Sie anschließend den Konfigurationsdialog.
- Klicken Sie im Abschnitt „Konfiguration“ auf die Schaltfläche „...“ und wählen Sie die zuvor gesicherte Konfigurationsdatei „tdps.config“ der vorherigen Installation aus.
- Klicken Sie nun auf „Konfigurations-Datei“, um die ausgewählte Konfigurationsdatei zu editieren.

Wählen Sie im erscheinenden Dialog mit einem Klick auf die Schaltfläche „...“ das zuvor gesicherte „data“ Verzeichnis (Repository) der vorherigen Installation als Repository-Pfad mit den Space-Daten des TeamDrive Personal Servers aus.

- Schließen Sie die Konfiguration mit einem Klick auf „Speichern“ ab.
- Der TeamDrive Personal Server wird nun automatisch gestartet und kann beispielsweise als Dienst eingerichtet werden.

Andernfalls kann der TeamDrive Personal Server durch Klick auf „Server starten“ manuell gestartet werden.

Mac OS X:

- Stoppen und schließen Sie den TeamDrive Personal Server über die entsprechende Oberfläche.
- Deinstallieren Sie die bisherige Installation des TeamDrive Personal Servers, indem Sie im Finder im Ordner „Programme“ die Anwendung „TeamDrivePersonalServer“ in den Papierkorb verschieben.
- Installieren Sie nun die neue Version des TeamDrive Personal Servers und starten Sie anschließend den Konfigurationsdialog.
- Klicken Sie im Abschnitt „Konfiguration“ auf die Schaltfläche „...“ und wählen Sie Konfigurationsdatei „tdps.config“ der vorherigen Installation aus.

Standardmäßig ist diese unter dem folgenden Pfad zu finden: „/Users/<Benutzername>/Library/Application Support/TeamDrivePersonalServer/tdps.config“.

Da das Verzeichnis „Library“ standardmäßig im Finder nicht angezeigt wird, gehen Sie bitte wie folgt vor, um die Datei auswählen zu können:

- Wählen Sie im Öffnen-Dialog zunächst links Ihr Benutzerverzeichnis aus.
- Drücken Sie anschließend die Tastenkombination [Cmd] + [Shift] + [G], um den Dialog „Gehe zu“ zu öffnen.
- Geben Sie dort „Library“ ein und bestätigen Sie Ihre Eingabe durch Klick auf „Öffnen“.
- Wechseln Sie nun in die Unterordner „Application Support“ → „TeamDrivePersonalServer“ und wählen Sie dort die Konfigurationsdatei „tdps.config“ aus.
- Klicken Sie nun auf „Konfigurations-Datei“, um die ausgewählte Konfigurationsdatei zu editieren.

Stellen Sie im erscheinenden Dialog sicher, dass die Option Repository-Pfad auf das „data“-Verzeichnis der vorherigen Installation des TeamDrive Personal Servers verweist.

Standardmäßig ist dieser Pfad „/Users/<Benutzername>/Library/Application Support/TeamDrivePersonalServer/data“.

Der Pfad kann andernfalls mit einem Klick auf die Schaltfläche „...“ und der obigen Beschreibung angepasst werden.

- Schließen Sie die Konfiguration mit einem Klick auf „Speichern“ ab.
- Der TeamDrive Personal Server wird nun automatisch gestartet und kann beispielsweise als Hintergrundprozess eingerichtet werden.

Andernfalls kann der TeamDrive Personal Server durch Klick auf „Server starten“ manuell gestartet werden.

Für die Aktualisierung des TeamDrive Personal Servers ab Version 1.0.048 müssen lediglich die folgenden Schritte durchgeführt werden:

- a) Stoppen Sie den TeamDrive Personal Server.
Informationen hierzu finden Sie im Kapitel [4.1.2 „Stoppen des Servers“](#).
- b) Führen Sie das Setup der neuen Version aus und folgen Sie den Anweisungen des Installationsprogramms.

2.2 Linux

Achtung:

Sichern Sie zunächst die Konfigurationsdatei „tdps.config“ und Ihr Datenverzeichnis (Repository).

Bei der Aktualisierung können ältere Dateien leicht überschrieben werden.

- a) Stoppen Sie den TeamDrive Personal Server.
- b) Installieren Sie die neue Version unbedingt in ein leeres Verzeichnis.
- c) Kopieren Sie ihr existierendes Datenverzeichnis (Repository) sowie die bisher verwendete Konfigurationsdatei „tdps.config“ der alten Version in das neue Installationsverzeichnis oder passen Sie die Konfiguration des Servers entsprechend an.

3 Konfiguration

3.1 Windows/Mac OS X

Wie bereits in Abschnitt 2 erläutert, werden sämtliche Konfigurationseinstellungen für den Server in einer Datei mit dem Namen „tdps.config“ gespeichert.

Standardmäßig wird diese Datei unter folgendem Verzeichnis gespeichert:

Windows XP: „C:\Dokumente und Einstellungen\<>Benutzername>\Anwendungsdaten\TeamDrive Personal Server“

Windows Vista/7/8: “C:\Users\<>Benutzername>\AppData\Roaming\TeamDrive Personal Server\”

Mac OS X: „/Users/<Benutzername>/TeamDrive Personal Server/“

Linux: Im Hauptverzeichnis des TeamDrive Personal Servers

Hinweis:

Wir empfehlen, regelmäßig eine Sicherung dieser Datei anzulegen.

Starten Sie die Management-Anwendung des TeamDrive Personal Servers.

Im Abschnitt Konfiguration haben Sie die Möglichkeit eine bereits vorhandene Konfigurationsdatei auszuwählen.

Mit der Schaltfläche „Konfiguration ändern/anzeigen“ bzw. dem Menüpunkt „Server konfigurieren...“ können Sie die ausgewählte Konfigurationsdatei bequem editieren.

Hinweis:

Wir empfehlen die Konfiguration ausschließlich über die Management-Anwendung des TeamDrive Personal Servers zu editieren und die Datei nicht manuell mit einem Texteditor zu editieren.

3.2 Linux

Stoppen Sie den TeamDrive Personal Server bevor Sie Änderungen an der Konfiguration vornehmen.

Editieren Sie die Datei „tdps.config“.

Sie befindet sich standardmäßig im Hauptverzeichnis des TeamDrive Personal Servers.

3.3 Einstellungen

Hinweis: Für den Aufbau und Betrieb eines Testservers; wird lediglich die Angabe eines Hostnamens bzw. einer IP-Adresse, sowie ein Server-Passwort benötigt.

Die meisten Einstellungen können unverändert mit Ihren Standardwerten verwendet werden.

Die wichtigsten Einstellungen werden im Folgenden erläutert. Am Ende jeder Option, steht die entsprechende Standardangabe aus der Konfigurationsdatei.

3.3.1 Lizenzschlüssel

Hier wird Ihr Lizenzschlüssel eingetragen.

Sie bekommen diesen, wenn Sie einen Personal Server erworben haben, von uns mitgeteilt.

Vorkonfiguriert ist ein Demoschlüssel für 10 GB Server-Speicherplatz, der unbegrenzt gültig ist.

```
license-key=TMDR-010G-5AD1-97CF-0000-0769
```

3.3.2 Hostname/IP-Adresse

Geben Sie hier die Adresse (Hostname oder IP-Adresse) ein, unter der Ihr Server von außen erreichbar ist.

Hinweis: Geben Sie die Adresse ohne „http://“ ein.

Hinweis:

Bei einer lokalen Installation (Server und Client befinden sich auf dem gleichen System) kann „127.0.0.1“ bzw. „localhost“ als Adresse verwendet werden.

Soll der Client auf einem anderen Rechner laufen, tragen Sie hier bitte die IP-Adresse des Servers ein.

Die IP-Adresse des Servers lässt sich wie folgt herausfinden:

– Unter Windows: Öffnen Sie die Eingabeaufforderung und geben Sie in das Fenster der Eingabeaufforderung den Befehl „ipconfig /all“ ein.

– Unter Linux/Mac OS X: Öffnen Sie ein „Terminal“-Fenster und geben Sie „ifconfig“ ein.

Soll der Server auch über das Internet erreichbar sein (von Clients, die nicht im lokalen Netzwerk sind) und ist ein Router vor den Server geschaltet, muss hier die nach außen sichtbare IP-Adresse des Routers eingetragen werden. Im Router selbst muss dann zusätzlich eine entsprechende Weiterleitung an den gewählten Port eingerichtet werden. Weiter Informationen hierzu finden Sie im Kapitel [3.3.3 „Port“](#).

Bedenken Sie außerdem, dass Ihr Internet Service Provider (ISP) Ihnen unter Umständen bei jeder Verbindung eine andere IP-Adresse zuweist.

Um unter diesen Umständen eine für den Client feste Adresse zu erzeugen, können Sie einen externen Dienst wie zum Beispiel Dyn DNS (<http://dyn.com/dns/>) nutzen.

In diesem Fall muss hier der bei DynDNS registrierte Hostname eingetragen werden, beispielsweise „teamdrive-Server.dyndns.net“.

```
server-host=192.168.30.157
```

3.3.3 Port

Der Port, über welchen man sich mit dem Server verbinden kann.

Hinweis: Der Port muss gegebenenfalls in der Firewall freigegeben werden.

```
server-port=37655
```

3.3.4 Passwort

Unter Windows/Mac OS X geben Sie Ihr Passwort in der Management-Anwendung des TeamDrive Personal Servers als Klartext ein.

Es wird automatisch mittels MD5-Algorithmus verschlüsselt in der Konfigurationsdatei „tdps.config“ gespeichert.

Unter Linux muss das mit dem MD5-Algorithmus verschlüsselte Passwort manuell in die Konfigurationsdatei eingetragen werden.

Sie können dazu den mitgelieferten MD5-Generator benutzen.

Siehe hierzu auch Kapitel [1.2 „Linux“](#).

Hier als Beispiel „meinPasswort“:

```
server-password=f14a298bc87fff2cd757f71054fdd94d
```

3.3.5 Name des Datenverzeichnisses (Repository)

Der Name des Datenverzeichnisses ist die erste Pfadkomponente der URL zum Zugriff auf einen Space.

Zum Beispiel: `http://myhost:37655/repo1/...`

Erlaubte Zeichen sind: [a-z], [A-Z], [0-9], [], [-].

```
repository-name=repo1
```

3.3.6 Space-Namen als Klartext speichern

Diese Einstellung kann aktiviert (,yes') oder deaktiviert (,no') werden.

Ist diese Einstellung aktiviert, werden alle Space-Namen als Klartext in der Datei „space-db“ abgelegt.

Aus Datenschutzgründen empfehlen wir, die Standardeinstellung (,no') beizubehalten.

```
store-space-titles=no
```

3.3.7 Pfad des Datenverzeichnisses (Repository)

Hier wird das Repository des Servers abgelegt.

In diesem Verzeichnis liegen alle Daten aus den Spaces der Nutzer, die an diesem Server angemeldet sind.

Zum nachträglichen Verschieben des Datenverzeichnisses beenden Sie den Server, sofern dieser ausgeführt wird, und verschieben Sie das existierende Datenverzeichnis an den gewünschten Speicherort.

Anschließend legen Sie diesen dann als neuen Pfad fest.

Hinweis: Achten Sie darauf, dass das Repository auf einem lokalen Volume liegt.

Netzlaufwerke werden nicht unterstützt.

Der Server arbeitet mit File-Locking.

Unter Windows empfehlen wir die Nutzung eines lokalen NTFS-Volumes.

Achtung:

Machen Sie unbedingt regelmäßig eine Sicherung dieses Verzeichnisses, insbesondere vor einer Aktualisierung.

Alle Daten der Nutzer des Servers sind hier gespeichert.

Sollten Sie den Standardpfad nutzen, könnte dieser bei einer Neuinstallation oder einer Aktualisierung überschrieben werden.

repository-data=

3.3.8 Maximale Größe des Datenverzeichnisses (Repository)

Die minimale Größe für ein Repository ist 10 MB. Sollten Sie eine Lizenz mit limitiertem Speicherplatz verwenden, darf dieser Wert die maximale Speicherplatzgröße nicht überschreiten, da sonst der Server nicht startet.

Die maximale Größe für das Repository muss als Zahl, gefolgt von einem der folgenden Einheitenkürzel MB, GB oder TB, in der Konfigurationsdatei angegeben werden.

Die folgenden Einstellungen sind nur für erfahrene Nutzer und Administratoren bestimmt.

Generell empfehlen wir die bereits voreingestellten Werte zu verwenden.

repository-size=10GB

3.3.9 Maximale Anzahl an Verbindungen

Dieser Wert legt die maximale Anzahl gleichzeitig offener Verbindungen zum TeamDrive Personal Server fest.

Wird dieser Wert überschritten muss ein Client auf eine freie Verbindung warten.

maximum-connections=20

3.3.10 Poll-Interval

Dieser in Sekunden angegebene Wert bestimmt, wie oft aktive Clients den Server auf Änderungen prüfen.

```
poll-interval=60
```

3.3.11 Connection-Timeout

Wenn innerhalb der angegebenen Zeit keine Daten auf einer Verbindung empfangen werden, wird angenommen, dass die Verbindung geschlossen wurde.

Die Angabe erfolgt in Millisekunden.

```
connection-timeout=120000
```

3.3.12 Put-Verify-Timeout

Nachdem eine Datei vollständig hochgeladen wurde, erfolgt ein MD5-Check um die Daten auf der Festplatte zu überprüfen.

Wenn dieser Vorgang zu lange dauert, schickt der Server einen HTTP Status-Code 100 und setzt seine Arbeit nach Ablauf der hier angegebenen Zeit fort.

Die Angabe erfolgt in Millisekunden.

```
put-verify-timeout=100000
```

4 Betrieb des TeamDrive Personal Servers

4.1 Windows/Mac OS X

Hinweis: Wir empfehlen für die Steuerung des TeamDrive Personal Servers ausschließlich die Management-Anwendung des TeamDrive Personal Servers zu verwenden.

4.1.1 Starten des Servers

Um den Server zu starten, verwenden Sie die Schaltfläche „Server Starten“.

Der Betriebsstatus des Servers wird in der Zeile „Server Status“ angezeigt. Rot bedeutet Server ist gestoppt, grün bedeutet Server ist gestartet.

Der Server kann als Dienst unter Windows bzw. als Hintergrundprozess unter Mac OS X betrieben werden.

Hierbei wird der Server automatisch gestartet.

4.1.2 Stoppen des Servers

Um den Server zu stoppen, verwenden Sie die Schaltfläche „Server Stoppen“.

Der Betriebsstatus des Servers wird in der Zeile „Server Status“ angezeigt. Rot bedeutet Server ist gestoppt, grün bedeutet Server ist gestartet.

4.1.3 Überwachen des Servers

Unter Windows können Sie je nach Konfiguration in die Windows Dienste-Ansicht bzw. den Taskmanager wechseln, unter Mac OS X in die Aktivitätsanzeige wechseln und prüfen, ob der Server läuft.

Benutzen Sie hierzu die Schaltfläche „Informationen zum Server-Prozess anzeigen“.

Sollte der Server nicht starten, kann die Log-Datei "tdpsd.log" Aufschluss darüber geben, warum der Server nicht startet.

Benutzen Sie hierzu die Schaltfläche "Log-Datei anzeigen" oder die entsprechende Menüoption.

4.2 Linux

Achtung: Der TeamDrive Personal Server darf nicht als Benutzer „root“ ausgeführt werden.

Wir empfehlen zur Ausführung einen eigenen Benutzer anzulegen.

4.2.1 Starten des Servers

Starten Sie den Server mit dem Befehl „./tdpsd“

4.2.2 Stoppen des Servers

Stoppen Sie den Server mit dem Befehl „./stop-tdps“.

4.2.3 Überwachen des Servers

Starten Sie die Überwachung des Servers mit dem Befehl „./watch-tdps“.

Der aktuelle Status wird dann in der Konsole angezeigt.

Außerdem wird der Serverstatus jederzeit in der Log-Datei „tdpsd.log“ protokolliert.

5 TeamDrive Client anbinden

- a) Starten Sie den TeamDrive Client.
- b) Gehen Sie auf „Extras“ → „Einstellungen...“ und wählen Sie den Tab „Hostserver“ aus.
- c) Wählen Sie rechts unten „Personal Server hinzufügen...“ aus.
- d) Tragen Sie die notwendigen Informationen für Ihren TeamDrive Personal Server ein und klicken Sie auf „OK“. Bitte beachten Sie, dass standardmäßig die Option „Zum Standard machen“ aktiviert ist.
- e) Schließen Sie die TeamDrive Client „Einstellungen“ wieder.
- f) Ihr TeamDrive Client kann nun mit Ihrem TeamDrive Personal Server benutzt werden.
- g) Sie können nun wie gewohnt neue Spaces auf dem neuen TeamDrive Personal Server erstellen, indem Sie Ihren TeamDrive Personal Server bei Erstellung aus der Serverliste auswählen.

6 Sicherung und Wiederherstellung

Alles was Sie generell zur vollständigen Wiederherstellung eines TeamDrive Personal Servers brauchen, sind das Datenverzeichnis/Repository (data) und die Konfigurationsdatei „tdps.config“.

Daher ist es wichtig diese beiden Komponenten zu sichern.

Wir empfehlen auch, Ihre Daten zu sichern, bevor Sie eine Aktualisierung des Servers durchführen.

Die Daten befinden sich in dem in der Konfiguration als Datenverzeichnis (Repository) angegebenen Pfad.

Der Administrator ist verantwortlich für die Sicherheit der Space-Daten, die auf dem TeamDrive Personal Server gespeichert werden.

Im Folgenden beschreiben wir Verfahren zur Durchführung von Sicherung und Wiederherstellung für das Datenverzeichnis (Repository).

6.1 Sicherung

Die einfachste Möglichkeit, eine Sicherung zu erstellen, ist, den TeamDrive Personal Server herunterzufahren und eine vollständige Kopie des Datenverzeichnisses (durch den Konfigurationsparameter repository-data festgelegt) anzulegen.

Darüber hinaus ist es empfehlenswert, die Konfigurationsdatei „tdps.config“ sowie die Datei „mime.types“ zu sichern, sofern Sie diese Datei geändert haben.

Natürlich können zur Sicherung statt einer vollständigen manuellen Kopie externe Programme wie „rsync“ verwendet werden, um eine bestehende Sicherung zu aktualisieren.

6.2 Online-Sicherung

Wenn Ihre Anforderungen an die Verfügbarkeit es nicht erlauben den Server herunterzufahren, können Sie eine Online-Sicherung auf folgendem Weg durchführen:

- Der folgende Vorgang muss für jeden einzelnen Space (Ordner mit fortlaufender Nummer) im Datenverzeichnis (Repository) durchgeführt werden:
 - Erstellen Sie eine Sicherung der Log-Dateien im „protolog“-Unterverzeichnis im jeweiligen Space-Ordner gemacht werden:
 - Setzen Sie ein exklusives Lock auf die Datei „last.log“, sofern diese existiert (hierfür benötigen Sie Software, die nicht im Lieferumfang enthalten ist).
 - Durchsuchen Sie das Verzeichnis und bestimmen Sie die Log-Datei mit der höchsten Nummer.
 - Sichern Sie die Datei „last.log“.
 - Heben Sie den exklusiven Lock auf die Datei „last.log“ auf (hierfür benötigen Sie Software, die nicht im Lieferumfang enthalten ist).
 - Sichern Sie alle nummerierten Log-Dateien, die eine Nummer kleiner/gleich der von Ihnen bestimmten höchsten Nummer aus dem vorigen Schritt haben.
 - Sichern Sie alle Dateien im Unterverzeichnis von „data“.
- Sichern Sie alle weiteren Dateien im Datenverzeichnis (Repository).

6.3 Wiederherstellung

Eine Wiederherstellung der Sicherung kann nur offline durchgeführt werden.

Selbst wenn nur ein Teil des Datenbestandes wiederhergestellt wird, wird der Server das Wiederherstellungsverfahren für das gesamte Datenverzeichnis durchführen.

Dies ist kein Problem, weil die Clients erkennen können, dass sich ein Space nach der Wiederherstellung nicht verändert hat und die Synchronisation in diesem Space normal fortsetzen.

Führen Sie das Verfahren zur Wiederherstellung des Datenverzeichnisses (Repository) wie folgt durch:

- Beenden Sie den Server.
- Ersetzen Sie das Datenverzeichnis durch das entsprechende Verzeichnis der Sicherung.
- Wie oben beschrieben können Sie auch selektiv einzelne Space-Verzeichnisse (Ordner mit fortlaufender Nummerierung im Datenverzeichnis) wiederherstellen.
- Starten Sie den Server mit dem Programmargument „--restored“. Der Server wird alle Spaces des Datenverzeichnisses wiederherstellen bevor Verbindungen der Clients angenommen werden.

Als Alternative zum Start mit dem Programmargument „--restored“ kann eine Datei mit dem Namen „restored“ im Datenverzeichnis vor dem Start des Servers angelegt werden.

Den Pfad zum Datenverzeichnis (Repository) finden Sie in der Datei „tdps.config“.

Wenn der Server bei der Wiederherstellung angehalten wird, wird der Vorgang automatisch beim nächsten Start fortgesetzt.

Die Datei „restore-state“ enthält alle relevanten Informationen zum aktuellen Wiederherstellungsvorgang.

Sollten Sie während des laufenden Wiederherstellungsvorgangs diesen abbrechen und von neuem starten wollen, beispielsweise weil Sie feststellen, dass Sie eine falsche Sicherung wiederherstellen, entfernen Sie die Datei „restore-state“ und starten den Server mit dem „-restored“ Programmargument wie oben beschrieben erneut.

Während der Wiederherstellung durchsucht der Server jeden Space und ermittelt den aktuellen Log-Offset.

Informationen hierzu werden in der Datei „r-state“ im Space-Verzeichnis hinterlegt.

Des Weiteren wird die globale Restore-ID inkrementiert.

Diese Restore-ID entspricht dem Zeitpunkt der Wiederherstellung dargestellt als Sekunden seit dem 01.01.2010.

6.4 TeamDrive Client Space-Wiederherstellung

Die Wiederherstellung der Spaces im Client erfolgt automatisch, falls dies nötig ist.

Die Client-Software kontrolliert den Zustand der Wiederherstellung eines Spaces, wenn die lokale Restore-ID eines Spaces im Client ungleich der globalen Restore-ID auf dem Server ist.

Wenn der Log-Offset im Client über dem Log-Offset des Servers (nach Abschluss der Wiederherstellung) liegt, beginnt der Client lokal mit der Wiederherstellung des entsprechenden Spaces.

Der Client stellt einen Space durch Zurücksetzen des Spaces auf den entsprechenden Synchronisationsstand des Spaces zum Zeitpunkt der Wiederherstellung her (wie auf dem Server vorhanden).

Bevor dieser Vorgang angestoßen wird, wird eine Sicherungskopie des lokalen Datenbestandes (Dateisystem) des Space erstellt.

Der Benutzer selbst ist in der Verantwortung zu überprüfen, ob lokale Änderungen zwischen der wiederhergestellten Sicherung des Spaces und der Sicherungskopie des lokalen Datenbestandes (Dateisystem) bestehen.

Der Benutzer sollte dann entsprechende Änderungen am Datenbestand des Spaces manuell abgleichen und aktualisieren, beispielsweise durch überschreiben der entsprechenden Dateien mit den geänderten Dateien der Sicherungskopie.

Hierfür ist unter Umständen eine Absprache bzw. Koordination mit anderen Space-Mitgliedern erforderlich um mehrfache Abgleicharbeiten zu vermeiden.

7 Sicherheit

Der jeweilige Client-PC und Server sollte hinreichend vor dem unberechtigten Zugriff Dritter geschützt werden.

Hinweis:

Hierzu empfehlen wir die entsprechende Literatur des Bundesamtes für Sicherheit und Informationstechnologie (BSI) (<https://www.bsi.bund.de/>), insbesondere verweisen wir auf das Grundschutzhandbuch des BSI.

7.1 Verschlüsselung

Verschlüsselter Datenaustausch während des gesamten Datenflusses ist das grundlegende Merkmal von TeamDrive.

Der verschlüsselte Datenaustausch unterteilt sich in drei Schritte:

- a) Wird ein Mitglied (Benutzer eines Client-PCs) in einen Space eingeladen, ruft die TeamDrive-Software den Public Key (öffentlichen Schlüssel) vom Registrierungsserver ab.
- b) Für den Zugriff auf einen (gemeinsamen) Space wird ein „Datenschlüssel“ (256 Bit-AES-Schlüssel) lokal erzeugt, der mit dem Public Key des eingeladenen Mitglieds verschlüsselt und über einen eigenen Kommunikationsweg dem TeamDrive-Anwender übermittelt wird.
- c) Mit dem Datenschlüssel werden die Daten des Spaces verschlüsselt, sobald Sie den Client-PC verlassen.

In verschlüsselter Form werden die Daten auf einem Server zwischengespeichert.

Die Verschlüsselung gewährleistet, dass die Daten des Spaces nur von dessen Mitgliedern abgerufen werden können.

Auf dem Server liegen nur verschlüsselte Daten.

Indem jedes Mitglied einen Datenschlüssel zugeteilt bekommen hat, ist es gleichzeitig autorisiert und wird Daten aus dem Space erhalten.

Diese Daten werden durch den Daten-Schlüssel automatisch entschlüsselt und können eingesehen bzw. bearbeitet werden.

7.2 Antiviren-Software

Die TeamDrive-Daten werden von der lokalen Antiviren-Software überwacht, u.a. indem der Virenschanner die entsprechende Datei beim Zugriff prüft.

Alle Spaces im lokalen Dateisystem sollten standardmäßig von Ihrer aktuellen Antiviren-Software überwacht werden.

Hinweis:

Wir empfehlen grundsätzlich die Nutzung einer lokalen Antiviren-Software auf jedem Client, weil jeder TeamDrive-Nutzer sehr schnell eine Vielzahl von Spaces mit unterschiedlichen Teams nutzen kann.

Selbstschutz ist die sicherste Methode.

7.3 Hinweise zu Datenschutz und Administration

Mit seinen Standardeinstellungen gewährleistet TeamDrive die Einhaltung der Datenschutzvorschriften von Unternehmen und Behörden.

Um eine optimale Einhaltung der datenschutzrechtlichen Vorschriften auch weiterhin zu ermöglichen, sollten die nachfolgenden Hinweise bei der Installation und Verwendung des Produktes beachtet werden:

Der jeweilige Client-PC und Server sollte hinreichend vor dem unberechtigten Zugriff Dritter geschützt werden.

In der Standardeinstellung des TeamDrive Personal Servers werden Space-Namen nicht als Klartext auf dem Server gespeichert.

Aus Datenschutzgründen empfehlen wir alle Standardeinstellungen beizubehalten. Weitere Informationen hierzu finden Sie im Kapitel [3.3.6 „Space-Namen als Klartext speichern“](#).

Sonstigen betrieblichen Datenschutzvorschriften finden auch beim Einsatz von TeamDrive Anwendung.

Hinsichtlich der Erstellung von Verzeichnissen und der ggf. erforderlichen Vorabkontrolle bestehen keine Besonderheiten beim Einsatz des Produktes.

Für den Fall, dass das Produkt nicht unter Verwendung eines eigenen internen TeamDrive Personal Server zum Einsatz kommt (im lokalen Netzwerk), sind im Verhältnis zum Provider des Servers, auf dem der TeamDrive Personal Server installiert wurde, die Voraussetzungen der Auftragsdatenverarbeitung zu beachten.

Auch hier gelten keine Besonderheiten im Vergleich zu anderen IT-Produkten, die einen externen Datenspeicher nutzen.

Der Auftraggeber muss den Auftragnehmer sorgfältig auswählen und schriftliche Weisungen erteilen.

In der Regel ist ein gesonderter Auftragsdatenverarbeitungsvertrag zu schließen.

Weitere Informationen zur Auftragsdatenverarbeitung mit entsprechenden Mustern finden Sie z. B. beim Virtuellen Datenschutzbüro (<http://www.datenschutz.de/>). Bei weiteren Fragen sind wir auch gerne behilflich und können ggf. Kontakte vermitteln.

Dieses Produkt enthält Programmbibliotheken des OpenSSL Projektes zur Verwendung des OpenSSL Toolkits (<http://www.openssl.org/>).

7.4 Besondere Hinweise zu Sekundärdaten/Protokolldaten

Personenbezogene Daten, welche in einem Space als Datei gespeichert wurden, können durch einen Administrator samt aller Dateiinhalte endgültig gelöscht werden. Der Dateiname der Datei verbleibt in der Space-Log-Datei, bis auch der Space mit allen Primär- und Sekundär-Daten gelöscht wird.

Jeder Benutzer, der einen Space erzeugt, ist automatisch Administrator und Besitzer dieses Spaces. Wenn dieser Benutzer seinen Space auf dem Server löscht, werden auch alle seine Daten in diesem Spaces inklusive der Log-Datei dem gesamten Inhalt gelöscht (alle Primär- und Sekundär-daten werden gelöscht).

Verlässt ein Mitglied einen Space, bleiben Informationen über diese Mitgliedschaft, den Beitritt, das Verlassen und welche Dateien bearbeitet wurden in der Log-Datei erhalten. Die Log-Datei wird erst mit dem endgültigem löschen des Spaces vom Server gelöscht. Besteht ein z.B. ausscheidender Mitarbeiter in einem Unternehmen auf vollständige Löschung all seiner Daten, muss der Space selbst vollständig gelöscht werden. Sollen die sich darin befindlichen Daten (Primär-Daten von anderen Usern) weiter benutzt werden, müssen sie vorher gesichert werden und in einen neu erstellten Space verschoben werden.

7.5 Hinweis für Daten von Berufsheimnisträgern i.S.d. § 203 StGB

TeamDrive ist generell zur Speicherung und zum Teilen von Daten und Informationen, die einem Berufsgeheimnis i.S.d. § 203 StGB unterliegen, geeignet. Die verwendeten Verschlüsselungsverfahren und -technologien schützen vor einem unbefugten Zugriff durch Dritte.

Ein unbefugter Zugriff i.S.d. § 203 StGB kann in der Regel nur dann erfolgen, wenn ein menschliches Fehlverhalten vorgekommen ist und z.B. falsche Berechtigungen und Freigaben auf einen Space vergeben wurden.

Wir raten Ihnen in Verbindung mit dem Einsatz von TeamDrive als Berufsheimnisträger dazu, unseren zusätzlichen Passwortschutz zu verwenden. Durch den zusätzlichen Passwortschutz muss vor dem Versenden einer Einladung ein Passwort eingegeben werden. Dieses Passwort muss dem Empfänger auf einem unabhängigen, separaten Weg mitgeteilt werden. Der Empfänger muss dann beim Annehmen der Einladung das Passwort eingeben. Sie sollten dabei ein hinreichend langes und komplexes Passwort verwenden, um den höchstmöglichen Schutz für Ihre Daten zu gewährleisten.