Was ist FTP: Profi-Erklärung für Online-Experten

Category: Online-Marketing
geschrieben von Tobias Hager | 9. Februar 2026



Was ist FTP: Profi-Erklärung für Online-

Experten

FTP klingt wie ein Relikt aus der Steinzeit des Internets – und genau deshalb wird es ständig unterschätzt. Dabei ist FTP nach wie vor das Rückgrat vieler Webprozesse, und wer im Online-Marketing, Webhosting oder in der technischen SEO wirklich mitreden will, sollte FTP nicht nur kennen, sondern beherrschen. In diesem Artikel zerlegen wir FTP in all seine Einzelteile – technisch, kritisch und ohne Bullshit. Bereit für ein Pro-Level-Deep-Dive in eines der ältesten, aber immer noch relevanten Internetprotokolle? Dann schnall dich an.

- Was FTP wirklich ist – und warum es mehr als nur "Dateiübertragung" bedeutet
- Wie FTP technisch funktioniert – inklusive Client-Server-Kommunikation und Ports
- Warum FTP im modernen Webhosting immer noch gebraucht wird
- FTP vs. SFTP vs. FTPS – was sind die Unterschiede und was bedeutet das für die Sicherheit?
- Typische FTP-Anwendungen im Online-Marketing und technischen SEO
- Best Practices für FTP-Zugänge, Sicherheit und Automatisierung
- Die größten Fehler beim Einsatz von FTP – und wie man sie vermeidet
- FTP-Clients, Tools und Automatisierung – was Profis wirklich nutzen

Was ist FTP? Eine technische Einführung für echte Profis

FTP steht für File Transfer Protocol. Klingt trocken, ist aber die Grundlage für einen Großteil der Dateiübertragungen zwischen lokalen Rechnern und Servern im Internet. FTP ist ein sogenanntes Application Layer Protocol, das auf der TCP/IP-Protokollfamilie basiert. Es wurde bereits in den 1970ern definiert – ja, richtig gelesen: vor dem World Wide Web. Und trotzdem lebt es weiter, weil es eine konkrete Aufgabe extrem gut erfüllt: Dateien effizient übertragen.

Anders als HTTP, das für Webseiten gedacht ist, geht es bei FTP nicht um Inhalte im Browser, sondern um die direkte Manipulation von Dateien und Verzeichnissen auf entfernten Systemen. FTP erlaubt es, Dateien hochzuladen (Upload), herunterzuladen (Download), umzubenennen, zu löschen oder zu verschieben. Dabei kommuniziert ein FTP-Client (zum Beispiel FileZilla oder WinSCP) mit einem FTP-Server über eine definierte Portstruktur – typischerweise Port 21 für Steuerbefehle (Control Connection) und dynamische Ports für die eigentlichen Datenübertragungen (Data Connection).

Gerade im Webhosting ist FTP nach wie vor Standard. Wenn du WordPress-Installationen manuell verwaltest, Themes oder Plugins direkt auf den Server schiebst oder Backups herunterziehst, dann bist du auf FTP angewiesen. Klar, viele Hoster bieten heute Web-Interfaces – aber ernsthafte Arbeit erledigt

man nicht über Klick-Klick-Oberflächen, sondern über Protokolle. Und FTP ist das Protokoll der Wahl, wenn du Zugriff auf das Dateisystem brauchst.

Der große Vorteil von FTP: Es ist verdammt schnell. Und es funktioniert fast überall – unabhängig vom Betriebssystem. Der große Nachteil: Es ist (in der Basisversion) unsicher. Aber dazu später mehr.

Wie funktioniert FTP technisch? Ports, Modi und Sessions erklärt

FTP basiert auf einem klassischen Client-Server-Modell. Der Client initiiert eine Verbindung zum Server, authentifiziert sich mit Benutzername und Passwort und kann anschließend über eine Steuerverbindung Befehle an den Server senden. Das Besondere: FTP nutzt zwei Verbindungen gleichzeitig – eine für Steuerbefehle (Control Channel) und eine für die Datenübertragung (Data Channel).

Hier kommt die erste technische Krux: Der Control Channel läuft über Port 21 (standardmäßig unverschlüsselt), der Data Channel hingegen nutzt dynamische Ports. Je nach Modus (Active oder Passive) sieht die Kommunikation unterschiedlich aus:

- Active Mode: Der Client öffnet einen zufälligen Port und teilt dem Server mit, dass er dort auf die Datenverbindung wartet. Der Server baut dann eine Verbindung zu diesem Port auf.
- Passive Mode: Der Server öffnet einen Port und teilt dem Client mit, wo er sich verbinden soll. Der Client initiiert dann die Verbindung. Dieser Modus ist heute Standard, insbesondere wegen Firewalls und NATs.

FTP überträgt Daten im Klartext – sowohl die Steuerbefehle als auch die Zugangsdaten. Deshalb ist das Protokoll ohne zusätzliche Absicherung ein Sicherheitsrisiko sondergleichen. Aber genau hier kommt die Evolution ins Spiel: FTPS und SFTP.

Was viele verwechseln: SFTP ist kein “sicheres FTP” im Sinne von FTP mit SSL. SFTP basiert auf SSH (Secure Shell) und ist ein komplett anderes Protokoll, das nur ähnlich heißt. FTPS hingegen ist tatsächlich FTP über SSL/TLS – also die verschlüsselte Variante des klassischen FTP. Beide Varianten haben ihre Daseinsberechtigung, aber sie funktionieren vollständig unterschiedlich. Wer denkt, er könne einfach “SFTP” in einem FTP-Client aktivieren, hat das Konzept nicht verstanden.

FTP im Online-Marketing und

Webhosting – warum es immer noch gebraucht wird

Im Zeitalter von APIs, REST-Schnittstellen und CI/CD-Pipelines könnte man denken, dass FTP ein Anachronismus ist. Aber genau das Gegenteil ist der Fall. In der Praxis wird FTP täglich eingesetzt – und zwar in den kritischsten Bereichen digitaler Infrastruktur.

Wenn du eine WordPress-Website betreibst und ein Plugin zerschießt dir das Frontend, kannst du dich entweder wochenlang mit Caching, Recovery und Login-Problemen herumschlagen – oder du loggst dich per FTP ein, löscht das Plugin-Verzeichnis, und der Spuk ist vorbei. Kein anderer Zugang bietet dir diese Direktheit.

Auch bei der Migration von Websites ist FTP unverzichtbar. Du brauchst vollen Zugriff auf alle Dateien, kannst .htaccess-Dateien editieren, Backup-ZIPs ziehen oder die wp-config.php ändern. Ohne FTP bist du darauf angewiesen, dass dein Webhoster ein brauchbares Interface bietet – und das ist oft nicht der Fall.

Im technischen SEO ist FTP ein Insider-Werkzeug. Wenn du Server-Antworten analysieren, Redirect-Ketten manuell prüfen oder Logfiles auslesen willst, brauchst du oft Zugriff auf Dateien, die nicht über HTTP erreichbar sind. Hier ist FTP dein Werkzeug der Wahl – vorausgesetzt, der Server ist entsprechend konfiguriert.

Und auch beim Thema Sicherheit spielt FTP eine Rolle – ironischerweise. Denn oft ist ein falsch konfigurierter FTP-Zugang das Einfallstor für Angreifer. Wer FTP nutzt, muss wissen, was er tut – oder er öffnet digitalen Einbrechern Tür und Tor.

Sicherheit bei FTP: Warum Standard-FTP gefährlich ist – und wie du es richtig machst

FTP überträgt alles im Klartext – inklusive Benutzername und Passwort. Das bedeutet, dass jeder, der in der Lage ist, den Netzwerkverkehr abzuhören (z. B. in einem öffentlichen WLAN), deine Zugangsdaten mitlesen kann. Für ein Protokoll, das direkten Zugriff auf Dateisysteme erlaubt, ist das ein Super-GAU.

Deshalb gilt: Standard-FTP ist tot. Punkt. Wer heute noch unverschlüsseltes FTP anbietet, handelt grob fahrlässig. Die einzige akzeptable Form ist FTPS oder SFTP – und selbst da gibt es Unterschiede. Während FTPS auf SSL/TLS basiert und mit FTP-Clients wie FileZilla kompatibel ist, benötigt SFTP einen

SSH-Zugang. Das bedeutet: Du kannst dich mit denselben Zugangsdaten wie beim SSH-Login verbinden – aber eben nur, wenn der Server das auch unterstützt.

Für maximale Sicherheit gelten folgende Best Practices:

- Immer verschlüsselte Verbindungen nutzen (FTPS oder SFTP)
- Starke Passwörter oder – besser – Public-Key-Authentifizierung verwenden
- FTP-Zugänge zeitlich begrenzen und nur bei Bedarf aktivieren
- Nur den Zugriff auf notwendige Verzeichnisse erlauben (Chroot)
- Zugriffe protokollieren und regelmäßig auswerten (FTP-Logs)

Und noch ein Profi-Tipp: Wenn du regelmäßig mit FTP arbeitest, nutze keine Browser-Plugins oder Drittanbieter-Webinterfaces. Diese sind oft veraltet, unsicher und anfällig für Exploits. Setze auf professionelle Clients, die FTPS und SFTP nativ unterstützen und dir die volle Kontrolle geben.

FTP-Tools, Automatisierung und Fehlervermeidung für Fortgeschrittene

Wer FTP ernsthaft nutzt, sollte sich von Klick-und-schieb-Interfaces verabschieden. Profis arbeiten mit Tools wie:

- FileZilla Pro: Unterstützt FTP, FTPS, SFTP und sogar Cloud-Services wie AWS S3
- WinSCP: Ideal für automatisierte FTP-Prozesse unter Windows, inkl. Skripting
- Cyberduck: Für Mac-User mit Support für FTP, SFTP, WebDAV und Cloud
- lftp: Kommandozeilentool für Linux mit extrem mächtigen Funktionen

Automatisierung ist das nächste Level. Mit lftp oder WinSCP-Skripten kannst du regelmäßige Backups, Uploads oder Deployments fahren – ganz ohne manuelles Zutun. In CI/CD-Prozessen lassen sich FTP-Deployments über GitHub Actions oder Jenkins steuern, sofern der Server keine SSH-Deploys akzeptiert.

Aber Vorsicht: Automatisierung ist nur dann sicher, wenn du mit Key-basierten Authentifizierungen arbeitest und die Skripte nicht im Klartext in deinen Repos rumliegen. Wer Passwörter in Shell-Skripten speichert, hat das Thema Security nicht verstanden.

Typische Fehler beim FTP-Einsatz:

- Unverschlüsselte Verbindungen (Standard-FTP)
- Globale Lese-/Schreibrechte auf dem Server (CHMOD 777 lässt grüßen)
- Zugangsdaten in Klartext-Dateien speichern
- Veraltete Clients oder Plugins nutzen
- Keine Logs oder Zugriffskontrollen implementieren

FTP ist mächtig – aber auch gefährlich. Wer damit arbeitet, muss wissen, was

er tut. Es ist wie ein chirurgisches Werkzeug: In den falschen Händen wird es zur Waffe.

Fazit: FTP ist alt – aber alles andere als tot

FTP ist kein Relikt, sondern ein Werkzeug. Und wie jedes Werkzeug kann es entweder meisterhaft oder katastrophal eingesetzt werden. Wer im Online-Marketing, Hosting oder SEO wirklich ernst genommen werden will, kommt an FTP nicht vorbei. Es ist der direkte Draht zum Server, zur Infrastruktur – zum Kern deiner digitalen Präsenz.

Aber FTP ist nichts für Amateure. Es erfordert technisches Verständnis, Sicherheitsbewusstsein und die Bereitschaft, sich mit Protokollen, Ports und Clients auseinanderzusetzen. Wer das tut, bekommt ein Werkzeug an die Hand, das schneller, direkter und zuverlässiger ist als jede Web-Oberfläche. Wer es ignoriert, bleibt im Sandkasten der Digitalindustrie. Willkommen in der Profi-Liga. Willkommen bei FTP.