



FTAPI® WHITE PAPER

Sicherer Dateitransfer für Ihr Unternehmen – aber richtig!

Was Sie beachten sollten, um eine sichere und effektive Dateitransferlösung in Ihrem Unternehmen zu etablieren.

Impressum

FTAPI[®] Software UG
(haftungsbeschränkt)
Heißstraße 89
80797 München

<http://www.ftapi.com>
<http://facebook.ftapi.com>
<http://twitter.com/ftapi>

© 2011 – FTAPI Software UG (haftungsbeschränkt)
Irrtümer und technische Änderungen vorbehalten.

1. Hintergrund	4
2. Grundsätzliche Sicherheitsfaktoren	5
2.1 Weiche vs. harte Verschlüsselung	6
2.2 Verschlüsselung der Dateien	7
2.3 Verschlüsselung der Passwörter	8
2.4 Datenintegrität	9
2.5 Qualifizierte Zustellung mit Empfangsbestätigung	9
2.6 Revisions sichere Protokollierung	10
3. Smart Transfer – Intelligente Übertragung	11
3.1 Unterbrechungstoleranz	11
3.2 Automatische Fehlerkorrektur	11
3.3 Automatische Komprimierung und Dekomprimierung	12
3.4 Redundanzvermeidung	13
4. Einfache Bedienung	13
5. Flexibilität und Erweiterbarkeit	14

1. Hintergrund

Geschäftliche Dokumente in den Händen des Wettbewerbs, manipulierte Konstruktionsdaten oder nicht freigegebene Informationen im Internet. Die Liste der Schreckensszenarien ließe sich noch weiter fortführen und die möglichen Auswirkungen können gravierend sein. Trotzdem bleibt das Thema Informationssicherheit häufig nur ein Grundrauschen in den Unternehmen, bis neue Meldungen oder gar ein internes Datenleck für die nötige Aufmerksamkeit sorgen. Häufig ist es dann aber bereits zu spät.

Deutsche Unternehmen investieren Milliarden in IT-Infrastrukturen, um unbefugte Zugriffe auf Firmen- und Kundendaten zu verhindern. Doch im Dickicht der IT-Sicherheit wird in vielen Unternehmen ein wesentlicher Risikofaktor unterschätzt oder schlichtweg übersehen: die Dateiübertragung.

Wesentlich ist, was mit den Dateien passiert, nachdem sie den Versender-PC verlassen haben. Eine zuverlässige und beruhigende Antwort auf diese Frage bieten jedoch nur wenige der gängigen Systeme, die für geschäftlichen Dateitransfer verwendet werden.

So werden selbst die physischen Transportmöglichkeiten für Dateien - wie USB-Sticks und andere Speichermedien - trotz des offensichtlichen Risikos noch in vielen Unternehmen genutzt. Doch auch die klassische E-Mail sowie die, vor allem für größere Dateien gern genutzten Online-Dienstleister und FTP-Systeme scheiden für eine sichere Übertragung geschäftlicher Dateien aus. In allen Fällen werden die Dateien auf einem über das Internet erreichbaren Server unverschlüsselt abgelegt, ohne jegliche Kontrollmöglichkeit über deren Verbleib. Darüber hinaus erfüllen sie oftmals nicht einmal die minimalsten Sicherheits-Anforderungen.

Doch fehlende Sicherheitsstandards sind nicht die einzigen Probleme, die vielen CIOs Kopfzerbrechen bereiten, wenn es darum geht, eine optimale File Transfer Lösung für das Unternehmen auszuwählen. Hinzu kommen Aspekte wie z.B. Unterbrechungstoleranz, Geschwindigkeitsoptimierung, Kostensenkung und nicht zuletzt die einfache Bedienbarkeit der Lösung durch alle Beteiligten.

Dieses Whitepaper soll Ihnen als komprimierter Leitfaden für die Auswahl einer geeigneten Secure File Transfer Lösung dienen.

2. Grundsätzliche Sicherheitsfaktoren

Unternehmen, die geschäftliche Dateien mit Kunden und Partnern austauschen, sollten sich mindestens an folgenden wesentlichen Sicherheitsfaktoren orientieren:

- **Verschlüsselte Übertragung** - Die Dateien sind während der Übertragung geschützt („secure in motion“).
- **Verschlüsselte Ablage** – In den meisten Fällen werden Dateien zur Übertragung auf einen Server zwischengespeichert, von wo sie dann weitergeleitet werden oder für den Empfänger zum Download bereit stehen. Diese Phase der Zwischenablage beansprucht in der Regel den größten Zeitanteil des Transfers. Daher ist gerade hier eine durchgehende Verschlüsselung der Dateien unerlässlich („secure at rest“).
- **Geeigneter Speicherort** – Neben der Verschlüsselung der Dateien ist auch der Ort, an dem die Dateien gespeichert werden, relevant. So kann u.a. verhindert werden, dass dort zwischengelagerte Dateien von Dritten missbraucht oder gelöscht werden. Auch rechtlichen Problemen kann durch die geeignete Wahl des Serverstandorts entgegnet werden. Aus diesem Grund sollte in vielen Fällen eine „in-house“ Installation im eigenen Rechenzentrum oder zumindest in einer Private Cloud einer fremd gehosteten Variante in der Public Cloud vorgezogen werden.
- **Manipulationssicherheit** – Ein sicheres System stellt die Integrität der zugestellten Dateien sicher, indem es Manipulationsversuche erkennt und veränderte Dateien als solche kennzeichnet.
- **Compliance & Nachweisbarkeit** – Ein sicheres System gewährleistet lückenlose Transparenz und Kontrolle der gesamten Transaktionen. Es muss revisionssicher nachvollziehbar sein, wann im Unternehmen welche Dateien von den einzelnen Mitarbeitern empfangen bzw. versendet wurden. Nur so kann im Zweifelsfall auch ein zuverlässiger Nachweis für die erfolgte Zustellung erbracht werden bzw. der Verantwortliche ausfindig gemacht werden.
- **Empfänger-Verifizierung** – Es muss sichergestellt sein, dass nur der berechnete Empfänger die Dateien herunterladen kann.

Neben den genannten technischen Sicherheitsfaktoren gibt es eine weitere entscheidende Voraussetzung für die praktische Sicherheit eines Systems zum Dateiaustausch mit Partnern und Kunden: Dessen Akzeptanz bei allen Mitarbeitern. Ist die Verwendung der Lösung komplex oder zeitaufwändig, besteht eher das Risiko, dass Mitarbeiter auf Kosten der Sicherheit auf andere Versandmethoden zurückgreifen und damit alle Sicherheitsregeln außer Kraft setzen.

Aus diesem Grund ist es unbedingt erforderlich, dass ein sicheres System nicht nur die genannten minimalen Sicherheitsanforderungen erfüllt, sondern zusätzlich auch einfach zu bedienen ist. Ein System kann nur dann seine Sicherheit voll ausspielen, wenn es auch von allen Anwendern akzeptiert und eingesetzt wird.

Mit FTAPI[®] SecuTransfer können große Dateien so einfach wie per E-Mail versendet werden. Und dies unter Berücksichtigung aller genannten Sicherheitsanforderungen.

2.1 Weiche vs. harte Verschlüsselung

Wenn bei gängigen Systemen behauptet wird, dass die Übertragung verschlüsselt erfolgt und damit ein sicherer Transfer gewährleistet wird, ist dies nur die halbe Wahrheit. Viele dieser Systeme verwenden nämlich lediglich eine sogenannte *weiche Verschlüsselung*, was bedeutet, dass nur der Übertragungskanal verschlüsselt ist. Die Dateien selbst werden hingegen unverschlüsselt auf einem Server zwischengespeichert, der durch das Internet erreichbar ist, und bleiben dort für mehrere Stunden oder sogar Tage im Klartext liegen. Zwar werben einige Anbieter zusätzlich damit, die Dateien in einem weiteren Schritt auf dem Server zu verschlüsseln. Allerdings wird hierdurch die Sicherheit nur unwesentlich erhöht, da trotzdem immer ein Bruch der Verschlüsselung bestehen bleibt. Für eine durchgehende Sicherheitsarchitektur ist dies nicht akzeptabel. Hier ist eine sogenannte *harte Ende-zu-Ende-Verschlüsselung* unabdingbar, bei der die Dateien durchgehend vom Sender bis zum Empfänger verschlüsselt bleiben.

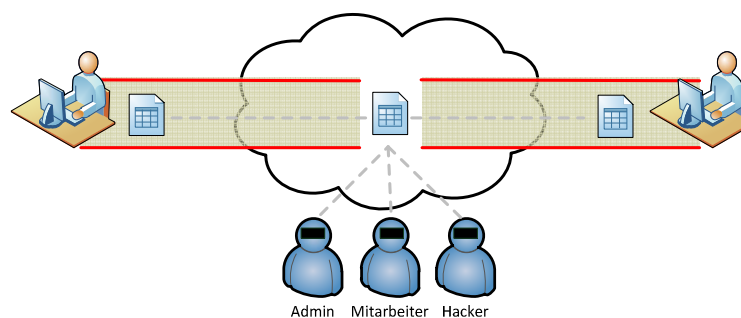


Abbildung 1: Bei der **weichen Verschlüsselung** werden nur die Übertragungskanäle verschlüsselt. Dadurch entsteht eine Sicherheitslücke bei der Zwischenspeicherung der Datei. An dieser Stelle können nicht-loyale Administratoren und Mitarbeiter, sowie Hacker die Dateien verhältnismäßig einfach abgreifen.

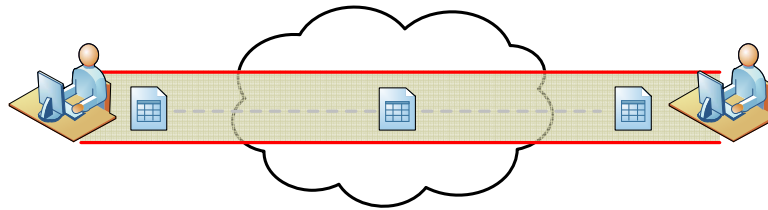


Abbildung 2: Bei der **harten Verschlüsselung** (Ende-zu-Ende-Verschlüsselung) bleibt die Datei durchgehend verschlüsselt, bis sie den Empfänger erreicht hat. Ein Abgreifen und Entschlüsseln der Dateien ist nahezu unmöglich.

Der Grund, weshalb die meisten Systeme nur eine weiche Verschlüsselung anbieten, liegt unter anderem darin, dass diese im Vergleich zur harten deutlich einfacher zu implementieren ist. Eine harte Verschlüsselung benötigt ein kompliziertes Schlüsselmanagement, welches in den meisten Fällen mit erheblichem Aufwand auch für den Anwender verbunden ist.

Werden Sie misstrauisch, wenn ein Anbieter eine durchgehende Verschlüsselung verspricht und für den Upload bzw. Download von Dateien aber lediglich einen Web-Browser voraussetzt. Hier werden in der Regel die Dateien im Klartext auf dem Server abgespeichert oder es besteht zumindest ein gefährlicher Bruch der Verschlüsselungskette auf Serverseite. Dies kann nicht als echte Ende-zu-Ende-Verschlüsselung bezeichnet werden, da dies technisch mit einem Web-Browser ohne jegliche Plugins (z.B. Java) oder zusätzliche Software nicht möglich ist.

FTAPI[®] SecuTransfer bietet ad-hoc eine harte Ende-zu-Ende-Verschlüsselung aller Dateien, ohne manuelle Schlüsselverwaltung für Versender und Empfänger. Ein üblicher Web-Browser mit einer installierten Java-Runtime reicht aus. Java ist auf 97% aller Desktopsysteme bereits vorinstalliert.

2.2 Verschlüsselung der Dateien

Die zugrundeliegende Verschlüsselungstechnologie einer Secure File Transfer Lösung ist wesentlich für die Einhaltung entsprechender Sicherheitsstandards. Viele Verschlüsselungstechniken, die derzeit immer noch produktiv eingesetzt werden, sind hoffnungslos veraltet und bieten so gut wie keinen Schutz mehr. Da nützt es wenig, wenn ein Anbieter behauptet, dass er die Dateien verschlüsselt, wenn diese Verschlüsselung mit nur wenig Aufwand geknackt werden kann.

Grundsätzlich kann gesagt werden, dass dem symmetrischen Verfahren AES stets der Vorzug vor DES gegeben werden sollte. AES wird z.B. in den USA für die Verschlüsselung von staatlichen Dokumenten mit der höchsten Geheimhaltungsstufe verwendet. Dabei bietet AES-256 mit einer

Schlüssellänge von 256 Bits den größtmöglichen Schutz. Aber auch AES-128 kann immer noch als verhältnismäßig sicher betrachtet werden. Hinzu kommt, dass eine harte Verschlüsselung stets einer weichen Verschlüsselung vorgezogen werden sollte, da nur diese den bestmöglichen Schutz bietet.

Achten Sie darauf, dass ein Secure File Transfer System die Dateien durchgehend - also bereits auf Versenderseite - mit mindestens AES-128 verschlüsselt und diese erst auf Empfängerseite wieder entschlüsselt werden können.

FTAPI[®] SecuTransfer verschlüsselt Ihre Dateien bereits auf Versenderseite unter Verwendung von AES-256.

2.3 Verschlüsselung der Passwörter

Neben der Verschlüsselung der Dateien ist es auch wichtig, dass die Passwörter für den Login verschlüsselt übertragen und abgelegt werden.

Um die Passwörter während der Übertragung zum Server zu schützen, ist eine SSL/TLS-Verbindung mit mindestens einer Stärke von RSA-1024 empfohlen. Einen deutlich besseren Schutz bietet eine RSA-2048 Verschlüsselung. Dies kann z.B. durch die Verwendung von HTTPS erreicht werden.

Passwörter sollten niemals im Klartext auf dem Server abgelegt werden, sondern zuvor immer mit einem Einweg-Verschlüsselungsverfahren, auch Hashing-Verfahren genannt, verschlüsselt sein. Einmal auf diese Art verschlüsselte Passwörter können nicht mehr entschlüsselt werden und sind damit auch für das technische Personal, welches Zugriff auf die Passwort-Datenbank hat, nicht verwendbar. Wichtig hierbei ist jedoch, dass ein ausreichend gutes Hashing-Verfahren verwendet wird. Als extrem unsicher gelten die weit verbreiteten Verfahren MD5 und SHA-1, da es mit verhältnismäßig geringem Aufwand möglich ist, damit verschlüsselte Passwörter zu reproduzieren bzw. auf andere Weise zu knacken. Empfohlen werden hingegen Hashing-Verfahren der SHA-2-Familie, wobei SHA-512 hier das derzeitig sicherste Verfahren darstellt.

Um die Passwort-Hashes resistent gegenüber Dictionary- und Brute-Force-Attacken zu machen, ist es unbedingt notwendig, dass ein Secure File Transfer System diese zusätzlich mit Salt- und Key-Stretching-Verfahren bearbeitet. Kommen dann noch Passwort-Policies zum Einsatz, wie z.B. dass ein Passwort eine bestimmte Mindestlänge und Kombination von Zeichenarten besitzen muss, so kann die Ablage der Passwörter als sicher bezeichnet werden.

Der Anmelde-Vorgang sollte z.B. mit HTTPS und mindestens RSA-1024 abgesichert sein. Die Passwörter hierfür müssen mit mindestens SHA-256 verschlüsselt sein und mit einem Salt-, Key-Stretching- und Passwort-Policy-Verfahren gesichert auf Serverseite abgelegt werden.

FTAPI[®] SecuTransfer verschlüsselt alle Passwörter grundsätzlich mit SHA-512 und wendet vor dem Speichern zusätzlich Salting und Key-Stretching an. Administratoren können zudem beliebige Passwort-Policies festlegen.

Der Login erfolgt über HTTPS, wobei die Verschlüsselungsstärke selbst durch das Zertifikat bestimmt werden kann - in der Regel RSA-2048.

2.4 Datenintegrität

Immer wenn eine Datei übermittelt wird, sollte überprüft werden, ob diese Datei während des Transports verändert wurde. Mit anderen Worten: Es gilt sicher zu stellen, dass der Inhalt der Datei nicht mutwillig abgeändert wurde. Dies erfolgt, indem die Datenintegrität sichergestellt wird. Dadurch wird sofort erkannt, falls z.B. Vertragsinhalte, Preislisten oder Marketing-Assets während der Übertragung durch Dritte manipuliert wurden.

Ein gutes Secure File Transfer System stellt in jedem Fall sicher, dass Manipulationsversuche an den übermittelten Dateien unmittelbar erkannt werden. Dies geschieht durch Einsatz entsprechender Maßnahmen zur Sicherstellung der Datenintegrität.

FTAPI[®] SecuTransfer überprüft schon während der Übertragung die Integrität der übermittelten Bestandteile einer Datei - vollständig transparent für alle Anwender.

2.5 Qualifizierte Zustellung mit Empfangsbestätigung

Um sicher zu stellen, dass eine Datei genau an diejenige Person zugestellt wird, für die sie bestimmt ist, ist eine qualifizierte Zustellung unabdingbar. Dabei wird die Datei mit dem öffentlichen Schlüssel des Empfängers verschlüsselt, so dass nur dieser die Datei wieder entschlüsseln kann.

Der Empfänger wiederum kann durch ein qualifiziertes Zertifikat eine qualifizierte Empfangsbestätigung für den Versender ausstellen, welche - je nach Qualifikation - sogar eine Beweiskraft vor Gericht besitzt.

Neben der qualifizierten Empfangsbestätigung ist in manchen Fällen auch eine einfache Empfangsbestätigung ausreichend.

Ein professionelles File Transfer System stellt Möglichkeiten zur Verfügung, um qualifizierte Zustellungen und Empfangsbestätigungen durchführen zu können.

FTAPI[®] SecuTransfer bietet standardmäßig eine solche Empfangsbestätigung, wodurch der qualifizierte Empfänger keinerlei zusätzliche Maßnahmen einleiten muss. Der Versender hat die Sicherheit, dass der Empfänger die Datei erst dann öffnen kann, nachdem der Empfang quittiert wurde.

2.6 Revisionssichere Protokollierung

Ein weiterer wichtiger Aspekt der Sicherheit ist die Rückverfolgbarkeit der Transaktionen. Es sollte nachvollziehbar sein, wer welche Aktionen zu welchem Zeitpunkt im System durchgeführt hat. Hierzu zählen unter anderem der Versand und Empfang von bestimmten Dateien aber auch die Änderung von Benutzer- oder Einstellungsdaten. Damit wird gewährleistet, dass Verantwortliche gefunden und Sicherheitslecks schnellstmöglich erkannt und geschlossen werden können.

Die Ablage dieser Protokolle sollte revisionssicher erfolgen. Hierzu zählt unter anderem, dass diese wieder auffindbar, nachvollziehbar, unveränderbar und fälschungssicher archiviert werden.

Durch die revisionssichere Protokollierung können Verantwortliche gefunden und Sicherheitslecks schnellstmöglich erkannt und geschlossen werden.

FTAPI[®] SecuTransfer loggt feingranular ausnahmslos alle Aktionen jedes Benutzers und speichert diese unter Berücksichtigung von Datenschutzaspekten revisionssicher ab.

3. Smart Transfer – Intelligente Übertragung

Unter Smart Transfer werden alle Funktionen zusammengefasst, welche die Übertragung von Dateien beschleunigen oder stabiler machen. Je größer eine zu übermittelnde Datei ist, desto wichtiger werden diese Smart Transfer Funktionen, die nachfolgend näher betrachtet werden.

3.1 Unterbrechungstoleranz

Die *Unterbrechungstoleranz* stellt sicher, dass bei Verbindungsabbrüchen während des Transfers die Übertragung an der letzten Stelle fortgesetzt werden kann und nicht von Vorne begonnen werden muss. Weder E-Mail noch One-Click-Hoster können eine solche Funktion für den Versand bzw. HTML-Upload aufgrund technischer Beschränkungen anbieten. Auch Standard-FTP enthält keine solche Funktion. Somit kann es beispielsweise passieren, dass ein seit mehreren Stunden andauernder Upload aufgrund eines Verbindungsabbruches komplett von Vorne begonnen werden muss.

Ein optimales File Transfer System stellt jederzeit sicher, dass Übertragungen nach einem Verbindungsabbruch an der letzten Stelle wieder fortgesetzt werden können.

FTAPI[®] SecuTransfer erkennt Verbindungsabbrüche automatisch und erlaubt das Fortsetzen der Übertragung am Unterbrechungspunkt.

3.2 Automatische Fehlerkorrektur

Die *Fehlerkorrektur* geht im Vergleich zur Unterbrechungstoleranz noch einen Schritt weiter und stellt bereits während der Übertragung sicher, dass diejenigen Bestandteile einer Datei, die bereits übermittelt wurden, auch vollständig und fehlerfrei sind. Falls nicht, werden diese automatisch - soweit möglich - korrigiert. Damit ist am Ende sichergestellt, dass die gesamte Datei fehlerfrei übermittelt wurde. Die Fehlerkorrektur vermeidet so beispielsweise, dass sich eine vermeintlich fehlerfrei übertragene Datei später doch nicht öffnen lässt, da sie während der Übertragung beschädigt wurde.

Nur die wenigsten der gängigen Transfer-Systeme unterstützen eine automatische Fehlerkorrektur. Hier ist der Empfänger selbst dafür verantwortlich festzustellen, ob er eine Datei fehlerfrei empfangen hat, z.B. mit entsprechenden Software-Tools. Im Fehlerfall muss die gesamte Übertragung erneut vom Versender beantragt werden.

Ein gutes File Transfer System versucht durch geeignete Fehlerkorrekturmaßnahmen Übertragungsfehler selbständig zu korrigieren, um zu vermeiden, dass eine Übertragung von Neuem begonnen werden muss.

FTAPI[®] SecuTransfer besitzt einen innovativen Fehlerkorrektur-Mechanismus, bei dem bereits während der Übertragung Fehler erkannt und repariert werden, ohne manuelles Zutun der Anwender.

3.3 Automatische Komprimierung und Dekomprimierung

Bei größeren Dateimengen bietet es sich an, diese vor deren Übertragung zu komprimieren, um deren Größe und damit die Übertragungszeit teils erheblich zu reduzieren. Abhängig vom jeweiligen Dateiformat lässt sich hierdurch die Übertragungszeit um bis zu 60% verkürzen. Auch der benötigte Speicherplatz für die Zwischenspeicherung auf einem Datenträger wird dadurch erheblich reduziert.

Dieser Vorgang sollte automatisch im Hintergrund erfolgen, so dass auf Seiten des Versenders die Dateien automatisch komprimiert werden und auf Empfängerseite wieder eine Dekomprimierung durchgeführt wird. Für die Anwender selbst sollte dieses Vorgehen vollkommen transparent sein. Sie profitieren direkt von der verkürzten Übertragungsgeschwindigkeit ohne manuell mit Komprimierungssoftware hantieren zu müssen.

Gängige Transfer-Systeme beinhalten in der Regel keine solche automatische (De-)Komprimierungsfunktion. Insofern müssen Versender wie auch Empfänger zusätzliche Software installieren oder eine längere Übertragungszeit in Kauf nehmen.

File Transfer Systeme, die über eine automatische (De-)Komprimierung verfügen, können erheblich dazu beitragen, Transferzeit, Speicherplatz und damit Kosten einzusparen.

FTAPI[®] SecuTransfer kann Dateien optional vor deren Übertragung komprimieren und auf Empfängerseite wieder dekomprimieren. Vollständig transparent und ohne Mehraufwand für Versender und Empfänger.

3.4 Redundanzvermeidung

In Unternehmen kommt es nicht selten vor, dass ein und dieselben Dateien durch unterschiedliche Personen mehrmals versendet werden. Mit jedem Vorgang werden sowohl das Netzwerk als auch die Speicherkapazität belastet.

Intelligente File Transfer Systeme erkennen, wenn eine Datei zuvor bereits übermittelt wurde und machen dadurch den erneuten Upload überflüssig. Im Idealfall erfolgt dies vollständig im Hintergrund. Der Benutzer merkt lediglich, dass die Übertragung schneller als sonst abgeschlossen ist.

Noch einen Schritt weiter gehen Systeme, die erkennen, wenn sich zu übermittelnde Dateien nur in geringen Teilen von zuvor bereits transferierten unterscheiden. In diesem Fall wird nur noch das Delta – also nur die tatsächliche inhaltliche Veränderung - übertragen.

Durch Redundanzvermeidung können erhebliche zeitliche wie auch technische Ressourceneinsparungen erreicht werden.

FTAPI[®] SecuTransfer erkennt bereits auf dem Server befindliche Datei-Segmente und übermittelt diese nicht erneut. So werden „Dateiduplikate“ auf dem Server vermieden.

4. Einfache Bedienung

Wie bereits zu Beginn erwähnt, kann ein Secure File Transfer System seine Sicherheit nur dann vollständig ausspielen, wenn es von allen Beteiligten akzeptiert und eingesetzt wird. Ein wichtiger Schlüssel hierfür ist, dass das System so einfach wie möglich in Betrieb genommen und bedient werden kann und zwar unabhängig von der Größe der zu übermittelnden Datei. Umständliche Systeme werden von den Beteiligten oftmals zugunsten von einfacheren aber unsichereren Systemen umgangen. Unternehmensrichtlinien helfen hier in der Regel wenig.

Einfach zu bedienende Systeme erhöhen die Akzeptanz bei den Anwendern und vermeiden, dass diese auf andere, unsichere Systeme zurückgreifen.

FTAPI[®] SecuTransfer kann beliebig große Dateien so einfach wie E-Mails übermitteln. Ein Web-Browser genügt (optional mit installiertem Java). Versender und Empfänger werden per E-Mail über den aktuellen Status von Übertragungen benachrichtigt oder können diese über die Web-UI in Echtzeit mit verfolgen.

5. Flexibilität und Erweiterbarkeit

Monolithische Systeme, die nur schwer an Unternehmensprozesse anpassbar sind, sollten gemieden werden. Wünschenswert sind hingegen Systeme, die einfach administriert und erweiterbar sind und sich an die jeweiligen Gegebenheiten in der Unternehmens-IT anpassen lassen.

Durch Skripts bzw. APIs werden Möglichkeiten der Automatisierung und Remotesteuerung geboten, die vor allem für eine Optimierung von Prozessen von großer Bedeutung sein können.

Maßnahmen zur Skalierbarkeit erlauben, dass ein File Transfer System mit dem Unternehmen wachsen und auch größere Anfragemengen bewältigen kann.

Professionelle File Transfer Systeme sollten sich optimal in die eigene IT-Landschaft integrieren lassen und mit den Bedürfnissen des Unternehmens wachsen können.

FTAPI[®] SecutTransfer basiert auf einer äußerst flexiblen und skalierbaren Architektur, die auf nahezu allen Betriebssystemen lauffähig ist. Die REST API sowie das Command Line Interface ermöglichen eine Anbindung externer Systeme, unabhängig von einer speziellen Programmiersprache. Serverseitige Event-Skripte erlauben zudem eine Automatisierung von serverseitigen Abläufen.



Kontakt

Die **FTAPI Software UG** mit Sitz in München ist Spezialist für die sichere Distribution und Speicherung von Dateien.

Das Unternehmen bietet mit der Software **FTAPI® Secure File Transfer** eine innovative Lösung für den professionellen, überbetrieblichen Versand von Dateien beliebiger Größe.

FTAPI® Software UG
(haftungsbeschränkt)
Heßstraße 89
80797 München

Tel.: +49 (0)89 1265 3105
info@ftapi.com
<http://www.ftapi.com>