

# Sicheres Data-Streaming mit Attachmate FileXpress

## Gute Gründe gegen herkömmliche Store-and-Forward-Konzepte

Niemand wird bestreiten, dass ein sicherer Transfer geschäftlicher Daten unverzichtbar ist. Was aber geschieht am Ende der Leitung, also in dem unsicheren Zeitfenster, in dem die Daten darauf warten, abgeholt zu werden?

Die meisten internetgestützten Übertragungslösungen nutzen ein zentrales Repository, das mitten in der DMZ angesiedelt ist und dazu dient, ein- und ausgehende Dateien zwischen zu speichern. In solchen Repositories liegen die Dateien häufig Stunden oder Tage ungeschützt, bevor sie von Geschäftspartnern oder Kunden abgeholt werden. Ohne konstantes Backup und geeignete Sicherheitsmaßnahmen unterliegen diese Repositories zahllosen Sicherheitsrisiken.

Diese Sicherheitsrisiken entfallen beim sicheren Data-Streaming, weil hier die Daten unmittelbar und ohne Zwischenspeicherung an Backend-Server weitergereicht werden. Der vorliegende Fachbeitrag setzt sich mit den Problemen herkömmlicher Store-and-Forward-Konzepte auseinander und erläutert, wie sicheres Data-Streaming mit Attachmate® FileXpress® dazu beiträgt, die Probleme zu überwinden.

### Das Store-and-Forward-Konzept und damit verbundene Probleme

Die meisten traditionellen File-Transfer-Lösungen (inkl. FTP) arbeiten mit Repositories oder nach dem Store-and-Forward-Prinzip. Wer eine Store-and-Forward-Lösung einsetzt oder einzusetzen gedenkt, sollte im eigenen Interesse folgende Fragen beantworten können:

1. Wie ist sichergestellt, dass das Repository nicht durch interne oder externe Nutzer kompromittiert wird, Administratoren eingeschlossen?
2. Welcher zusätzliche Overhead entsteht bei großen Dateien dadurch, dass die Dateien zweimal gelesen und geschrieben werden müssen, nämlich zunächst im Repository und dann beim Adressaten?
3. Wie werden Daten zwischen Repository und Backend-System übertragen? Welches Protokoll wird benutzt? Muss das Backend-System alle Übertragungen veranlassen oder kann das Repository die Daten direkt an das Backend-System senden? Falls das Backend-System die Daten aus dem Repository entnehmen muss, wie oft muss es dazu das Repository abfragen? Wird ein externer Scheduler für diese Aufgaben benötigt?

4. Welche Backup-Verfahren sind für das Repository notwendig?
5. Was geschieht, wenn das Repository offline ist, sei es unplanmäßig oder zwecks Wartung? Gibt es Automatismen, um auf ein gespiegeltes System umzustellen, oder muss die gesamte Übertragung ausgesetzt werden?
6. Wie erfolgt die Verwaltung der Dateien im Repository? (Eine unbefristete Speicherung ist keine Option.) Ist das System so konfigurierbar, dass die Dateien automatisch entfernt werden, oder müssen bestimmte Wartungsschritte regelmäßig durchgeführt werden?
7. Wie viel Platz wird aktuell für das Repository benötigt? Wie lässt sich dieser Platz in Zukunft erweitern? Gibt es hierfür Prozesse? Wie steht es mit den Kosten?
8. Zwei getrennte Ereignisse sorgen dafür, dass Daten zur Zieladresse gelangen: (1) Die Datei wird in das Repository geschrieben; (2) Die Datei wird an das vorgesehene Ziel übertragen (bei ausgehenden Dateien an das Remote-System, bei eingehenden Dateien an den Backend-Server). Wie erfolgt das Logging dieser Ereignisse? Können beide Enden der Transaktion abgebildet werden, um einen vollständigen Blick auf die Transaktion zu erhalten?
9. Wie werden Versionskontrolle und Datenintegrität gehandhabt? Können Dateien problemlos aktualisiert werden, die schon in das Repository eingestellt worden sind, oder muss ein zweiter Satz Dateien eingestellt werden? Ist sichergestellt, dass die Anwender die neueste Version erkennen können?

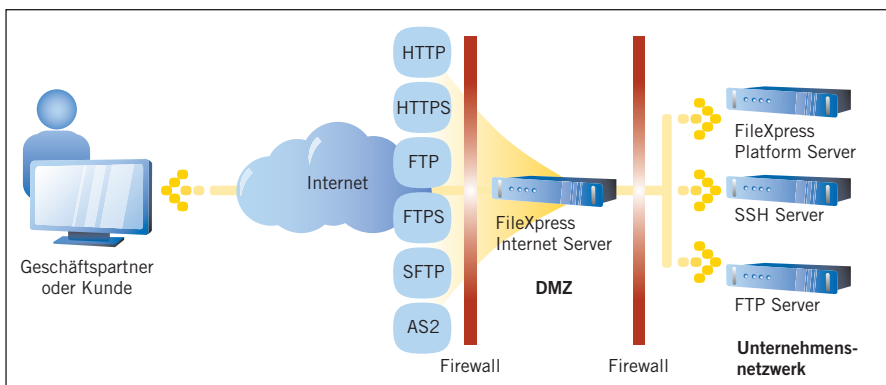
Unter dem Strich gilt, dass es bei einer Store-and-Forward-Lösung kostspielig und aufwendig ist, Risiken und Ineffizienzen auszuschließen. Gut, dass es hierzu eine überzeugende Alternative gibt: Data-Streaming.

### Sicheres Data-Streaming als Alternative

Beim sicheren Data-Streaming entfällt die Notwendigkeit, Daten in einem zentralen Repository abzulegen. Stattdessen bleiben die Ausgangsdaten so lange auf dem Backend-System (wo sie auch erstellt worden sind), bis sie vom Geschäftspartner

oder Kunden abgeholt werden. Die eingehenden Daten werden direkt an das Backend-System übertragen, wo sie gemäß den Geschäftsregeln weiterverarbeitet werden.

Attachmate FileXpress beinhaltet eine ganze Reihe von Managed-File-Transfer-Lösungen und dient zur sicheren Übertragung von Dateien beliebiger Größe auf allen gängigen Plattformen zu allen Standorten. FileXpress Internet Server ist in der DMZ zu Hause. Dieser Server übernimmt die sichere Verwaltung der von Kunden aufgebauten Verbindungen, nutzt dabei verschiedene Protokolle und baut anschließend neue, separate Verbindungen zu den internen Backend-Servern auf. Die Backend-Server unterstützen entweder SFTP-, FTPS- oder FTP-Dienste. Alternativ kann auch FileXpress Platform Server (eine weitere Lösung aus der FileXpress-Familie) genutzt werden.



FileXpress Internet Server übernimmt die sichere Verwaltung der von Kunden aufgebauten Verbindungen und erstellt dann neue, separate Verbindungen zu(m) internen Backend-Server(n).

FileXpress bietet dank sicherem Data-Streaming folgende Vorteile:

- Höhere Sicherheit**  
 Dringt ein Hacker in ein Repository ein, besteht die Gefahr, dass er Zugang zu allen übertragenen Daten hat. FileXpress Internet Server beseitigt diese ernste Schwachstelle. Die Lösung stellt einen sicheren Proxy bereit, der jede direkte Verbindung nach außen zu den Backend-Systemen verhindert und jede Konfiguration oder Netzwerktopologie im Inneren verbirgt.
- Durchgängiger Prozess**  
 FileXpress Internet Server nutzt kein zentrales Repository, weshalb es sich erübrigt, eine Datei zunächst in das Repository zu schreiben und dann in eine andere Umgebung zu übertragen.
- Automatische Weiterverarbeitung**  
 FileXpress kann in der DMZ und auf dem Backend-System implementiert sein, um dort Daten anhand von Geschäftsregeln weiterverarbeiten zu können, die vom Administrator vorgegeben werden (beispielsweise in Abhängigkeit vom sendenden Benutzer oder Datentyp). Beispielsweise könnte eine Weiterverarbeitung so konfiguriert sein, dass eine hochgeladene Datei nach Daten durchsucht wird, die dann zur Aktualisierung einer Datenbank herangezogen werden.
- Einfache Speicherverwaltung**  
 Mit FileXpress sind Unternehmen in der Lage, die Backup- und Recovery-Funktionen zu nutzen, die bereits auf ihren Backend-Systemen implementiert sind. Es ist nicht nötig, neue Backup- oder Recovery-Systeme zu entwickeln, wie dies beispielsweise für Lösungen der Fall ist, die mit zentralen Repositories arbeiten.

So erhöht FileXpress die Sicherheit und senkt die Kosten, weil es nicht mehr nötig ist, sensible Informationen in der DMZ zu speichern. Gleichzeitig wird die Effizienz im File-Transfer-Workflow verbessert.

### Besonders hohe Sicherheit beim File-Transfer

Dank sicherem Data-Streaming bleiben Übertragungen mit FileXpress von Anfang bis Ende geschützt. Die mehrschichtige Architektur der Lösung trägt mit folgender Funktionalität zu einer noch größeren Sicherheit bei:

- Reverse mit Protokollumschaltung im Datenstrom**  
 FileXpress beinhaltet einen Reverse-Proxy, der als sicherer Makler zwischen Fileservern und externen Clients dient, die darauf zugreifen versuchen. Der Proxy nutzt eine neue Verbindung mit einem völlig anderen Protokoll als die ursprüngliche Verbindung, beendet dabei die Verbindungen in der DMZ und baut neue Verbindungen zum Backend-Server auf. Auf diese Weise wird die Außenwelt sehr wirksam vom Unternehmensnetz getrennt.
- Starke Authentifizierung**  
 FileXpress ergänzt den vorhandenen Sicherheits-Framework mit einer robusten Zugangskontrollschicht. Diese Schicht räumt Benutzern bestimmte Rechte für das Übertragen oder Senden von Daten ein. Dank Integration von LDAP und Microsoft Active Directory versetzt FileXpress Unternehmen in die Lage, ihre vorhandenen Verzeichnissysteme zu nutzen.
- System Obfuscation**  
 FileXpress nutzt die sogenannte „system obfuscation“, ein Sicherheitsverfahren, mit dem Konfigurationsdetails des Backend-Systems „verschleiert“ werden, um sogenannte „socially engineered“-Angriffe abzuwehren. FileXpress lässt sich auch so einrichten, dass Dateien und Verzeichnisse für eine Reihe von Backend-Systemen freigegeben werden. In diesem Szenario stellt

FileXpress den Endanwendern nur eine logische Sicht bereit, egal wie diese auf den FileXpress Internet Server zugreifen. Über einen File-Transfer-Client, eine Befehlszeile oder einen Webbrowser sind nur die Dateien, nicht aber die Backend-Systeme sichtbar.

FileXpress erschließt Partnern und Kunden so Zugang zu den benötigten Dateien, während gleichzeitig sichergestellt ist, dass keine Details über die internen Systeme, auf denen diese Dateien gespeichert sind, bekannt werden.

### **Bessere Leistung. Niedrigere Kosten. Wirksamere Kontrollen.**

Sicheres Data-Streaming bietet überzeugende Vorteile gegenüber herkömmlichen Store-and-Forward-Konzepten. Durch Wegfall der in vielen Internet-File-Transfer-Lösungen üblichen zentralen Repositories sind Unternehmen in der Lage, erhebliche Leistungssteigerungen zu erzielen, ihre Gesamtkosten zu senken, wirksamere Kontrolle ihrer Datenverarbeitung zu implementieren und gleichzeitig die allgemeine Sicherheit zu verbessern.

### Die FileXpress-Produktreihe

Attachmate FileXpress ist eine strategische Lösung für die sichere Übertragung von Dateien innerhalb und außerhalb von Unternehmen. Die FileXpress-Produktreihe umfasst folgende Lösungen:

- **FileXpress Platform Server** ist eine leistungsstarke File-Transfer-Engine. Sie sorgt auf allen gängigen Plattformen für die sichere Zustellung beliebig großer Dateien.
- **FileXpress Internet Server** ist ein Portal für sämtliche Internet-Dateien. Die Lösung gewährleistet die sichere Interaktion mit Partnern und Kunden weltweit.
- **FileXpress Command Center** ist ein digitales Dashboard für alle File-Transfer-Aktivitäten. Übertragungsereignisse lassen sich von einer zentralen Stelle ausführen, verfolgen, protokollieren, prüfen und unterstützen.
- **FileXpress FileShot** ist die passende Lösung für Dateiübertragungen zwischen allen Benutzern. Nahtlos in Microsoft Outlook integriert können hiermit Dateien jeder Größe versendet und volle Postfächer vermieden werden. Ebenso können alle Übertragungen nachvollzogen und archiviert werden.

### Über Attachmate

Attachmate ist ein führender Hersteller von Softwarelösungen für Terminalemulation, Applikationsintegration, Managed File Transfer und Enterprise Fraud Management. Weltweit setzen mehr als 65.000 Kunden auf unsere Technologien, um ihre IT-Anlagen auf neuartige Weise optimal zu nutzen. [www.attachmate.de](http://www.attachmate.de)



**Hauptsitz**  
1500 Dexter Avenue North  
Seattle, Washington 98109  
TEL +1 206 217 7500  
FAX +1 206 217 7515

**Europäische Zentrale**  
Niederlande  
TEL +31 172 50 55 55  
FAX +31 172 50 55 51

**Österreich**  
TEL +43 1 595 4335 0  
FAX +43 1 595 4335 11  
[www.attachmate.at](http://www.attachmate.at)  
[info-at@attachmate.com](mailto:info-at@attachmate.com)

**Schweiz**  
TEL +41 43 399 2090  
FAX +41 43 399 2099  
[www.attachmate.ch](http://www.attachmate.ch)  
[InfoCH@attachmate.com](mailto:InfoCH@attachmate.com)

**Deutschland**  
TEL +49 89 99 351 0  
FAX +49 89 99 351 111  
TEL +49 2102 4965 0  
FAX +49 2102 4965 65  
[www.attachmate.de](http://www.attachmate.de)  
[info-de@attachmate.com](mailto:info-de@attachmate.com)

Weitere Niederlassungen von Attachmate finden Sie unter [www.attachmate.de](http://www.attachmate.de).