

## VERWALTETER DATEITRANSFER UND PCI DATA SECURITY STANDARD

*„Der PCI Security Standard Council ist ein offenes, globales Forum für die fortgesetzte Entwicklung, Verbesserung, Speicherung, Verbreitung und Implementierung von Sicherheitsstandards zum Schutz von Kontoinformationen. Ziel des PCI Security Standards Council ist die Optimierung der Sicherheit von Zahlungskontodaten durch Förderung der allgemeinen Anwendung der PCI-Sicherheitsstandards. Die Organisation wurde von American Express, Discover Financial Services, JCB, MasterCard Worldwide und Visa International gegründet.“*

[www.pcisecuritystandards.org/index.htm](http://www.pcisecuritystandards.org/index.htm)

Ipswitch ist Sponsor von:



Der Payment Card Industry Data Security Standard (PCI DSS) dient der Verwendung durch Händler, Finanzbearbeiter, Point-of-Sale-Verkäufer und Banken, Kreditgenossenschaften und anderen Finanzinstituten, die Daten von Kreditkarteninhabern übertragen, verarbeiten und/oder speichern. Dieses Dokument soll diesen Unternehmen folgende Aspekte verdeutlichen:

(1) Anwendung der Standards auf Produkte und Lösungen für die verwaltete Datenübertragung (Managed File Transfer, MFT) im Allgemeinen und (2) den Beitrag der MOVEit MFT-Softwareprodukte von Ipswitch, diese Standards einzuhalten und dies zu demonstrieren. Dieses Dokument beginnt mit einem Überblick über PCI DSS, den MOVEit Central-Client und die MOVEit DMZ-Serverprodukte und beschreibt dann ausführlich die einzelnen Datensicherheitsstandards (DSS) im Zusammenhang mit MFT und erklärt, welchen Beitrag die Funktionen der MOVEit-Produkte zur Einhaltung von Bestimmungen leisten.

### PCI DATA SECURITY STANDARD V.1.2 – WICHTIGE DATEN

PCIDSS Version 1.2 ist der von den Kreditkartenorganisationen für alle Unternehmen, die Informationen von Karteninhabern verarbeiten, speichern oder übertragen, eingeführte globale Datensicherheitsstandard. Es wurden keine wesentlichen Änderungen im Vergleich zur Version 1.1 vorgenommen, sondern vielmehr zahlreiche Erklärungen und Erläuterungen hinzugefügt. Die ursprünglichen sechs Abschnitte und zwölf Hauptanforderungen bleiben unverändert. PCI DSS 1.2 trat am 1. Oktober 2008 in Kraft, und die Gültigkeit von PCI DSS 1.1 endete am 31. Dezember 2008.

Der in sechs Abschnitte gegliederte PCI DSS v.1.2 enthält die folgenden zwölf Anforderungen für die Sicherheit vertraulicher Daten.<sup>1</sup>

**Aufbau und Verwaltung eines sicheren Netzwerks**

Anforderung 1: Installation und Verwaltung einer Firewallkonfiguration zum Schutz von Karteninhaberdaten

Anforderung 2: Keine Verwendung der Standardwerte des Herstellers für Systemkennwörter und andere Sicherheitsparameter

**Schutz von Karteninhaberdaten**

Anforderung 3: Schutz von gespeicherten Karteninhaberdaten

Anforderung 4: Verschlüsselte Übertragung von Karteninhaberdaten über offene, öffentliche Netzwerke

**Verwaltung eines Programms zur Bewältigung von Sicherheitsrisiken**

Anforderung 5: Einsatz und regelmäßige Aktualisierung von Virenschutzsoftware oder -programmen

Anforderung 6: Entwicklung und Verwaltung sicherer Systeme und Anwendungen

**Implementierung umfassender Zugriffskontrollmaßnahmen**

Anforderung 7: Beschränkung des Zugriffs auf Karteninhaberdaten auf die geschäftlich erforderlichen Daten

Anforderung 8: Zuweisung einer eindeutigen Benutzerkennung für jede Person mit Computerzugang

Anforderung 9: Beschränkung des physischen Zugriffs auf Karteninhaberdaten

**Regelmäßiges Überwachen und Testen von Netzwerken**

Anforderung 10: Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten

Anforderung 11: Regelmäßiges Testen von Sicherheitssystemen und -prozessen

**Verwaltung einer Richtlinie zur Informationssicherheit**

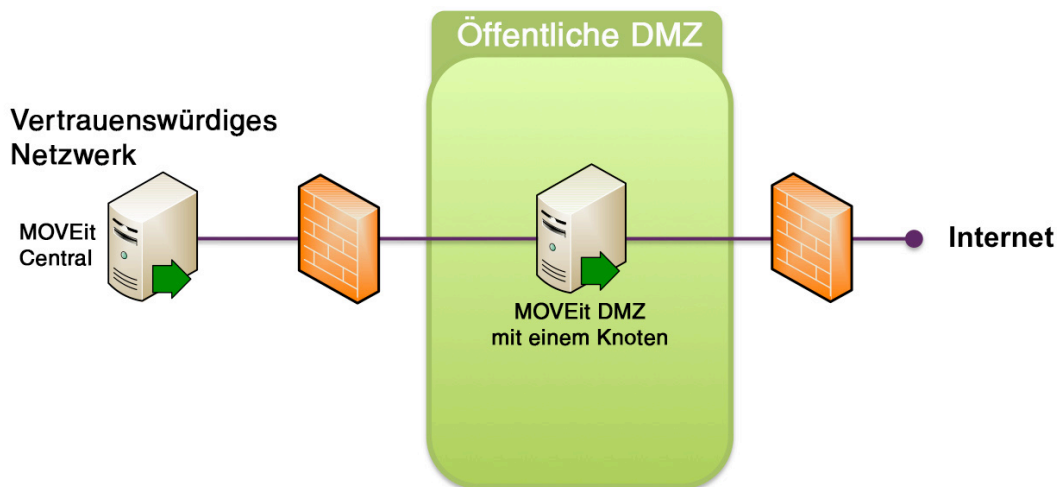
Anforderung 12: Verwaltung einer Richtlinie zur Informationssicherheit für Mitarbeiter und Auftragnehmer

<sup>1</sup> Quelle: PCI Data Security Standard Version 1.2 unter [https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download\\_agreement.html](https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html)

**MOVEIT CENTRAL: WORKFLOW-ENGINE FÜR VERWALTETE DATENTRANSFERS**

MOVEit DMZ und MOVEit Central sind Windows-basierte MFT-Lösungen auf Unternehmensebene, die – je nachdem, ob Datenübertragungsserver- und/oder Workflow-Automatisierungsfunktionen benötigt werden – gemeinsam oder auf Standalone-Basis eingesetzt werden können. Während einige MFT-Anbieter diese Funktionen in einem einzigen Produkt kombinieren, bietet Ipswitch sie aus Sicherheits- und Kostengründen separat als MOVEit DMZ und MOVEit Central an. Bei gemeinsamer Verwendung bietet diese Kombination ganz besondere Vorteile.

Die MOVEit Central Workflow-Engine und Prozessverarbeitungslösung für die Dateiübertragung ist ein leistungsstarkes Tool, mit dem IT-Mitarbeiter die Übertragung und Verarbeitung von Dateien auf geplanter, ereignisgesteuerter oder On-Demand-Basis automatisieren können. Central ist eine Allround-Lösung zur Übertragung großer Mengen von Dateien jeder Größe zwischen fast jedem internen oder externen System, einschließlich MOVEit DMZ-Servern. Normalerweise wird MOVEit Central im internen, vertrauenswürdigen Netzwerk eines Unternehmens implementiert.



Implementierung eines einzelnen MOVEit Central

Mit MOVEit Central werden Dateien anhand von einfach erstellbaren Aufgaben verschoben. Dazu ist kein Skripting oder Programmieren erforderlich. Aufgaben können die integrierten AS1-, AS2-, AS3-, FTP-, FTPS/TLS-, HTTPS-, SFTP/SCP2- und SMTP/POP3-Clients von Central sowie die Funktion zum Kopieren in das lokale Dateisystem und/oder freigegebene Netzwerkordner nutzen.

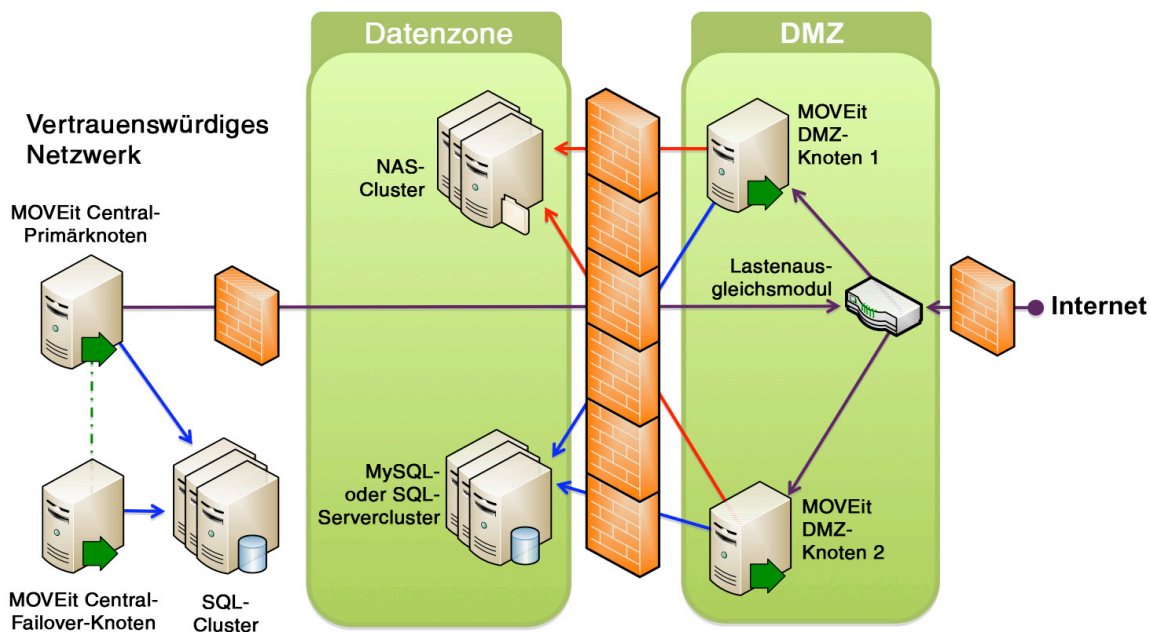
Außerdem lassen sich Dateien automatisch mithilfe verschiedener integrierter Funktionen wie OpenPGP- und SMIME-Verschlüsselung, beispielhafter und benutzerdefinierter VBS-Skripts und durch Ausführung von Drittanbieter-Anwendungen verarbeiten.

MOVEit Central umfasst auch verschiedene weitere Funktionen: eine API-Schnittstelle zur Steuerung von Aufgaben durch Drittanbieter-Programme (z. B. Enterprise-Job- oder Workflow-Scheduler) unter Verwendung der MOVEit Central API COM-Komponente und/oder Java-Klasse, sowie die Möglichkeit der Implementierung auf Hochverfügbarkeitsbasis für automatisches, unbeaufsichtigtes Failover von einem Produktionssystem zu einer kontinuierlich aktualisierten, betriebsbereiten Kopie von MOVEit Central.

### MOVEIT DMZ: VERWALTETER DATEITRANSFER-SERVER

MOVEit DMZ ist ein sicherheitsverstärktes „Portal“ für verwalteten Dateitransfer, über das Anwendungen und Endbenutzer Dateien sicher über Webbrowser und verschiedene Secure FTP-Clients von MOVEit und Drittanbietern übertragen können, die eine der folgenden SSL- oder SSH2-Verschlüsselungsmethoden unterstützen: (AS1), AS2, AS3, FTPS, HTTPS, SCP2, SFTP oder TLS. Diese Funktion und sein einzigartiges FIPS-140-2-validiertes, AES-verschlüsseltes Datenspeichersystem sorgen dafür, dass Daten mit MOVEit DMZ ohne PGP automatisch und durchgehend verschlüsselt übertragen und gespeichert werden können.

MOVEit DMZ befindet sich in der Regel in einer sogenannten DMZ: einem durch die Umkreisfirewall(s) eines Unternehmens geschützten Netzwerksegment. Auf diese Weise ist ein sicherer Zugriff auf MOVEit DMZ vom lokalen internen Netzwerk und vom Internet aus möglich.



MOVEit Central-Multi-Tier-Bereitstellung und DMZ-Webfarm

Anders als einige andere MFT-Produkte handelt es sich bei MOVEit DMZ ausschließlich um einen Server. Dieser kann keine Verbindung zu anderen Systemen herstellen. Wie durch die Pfeile unten gezeigt, müssen alle Verbindungen zu einem MOVEit DMZ durch geeignete Clients, Anwendungen, APIs oder Dienste eingeleitet werden. Daher muss die Firewall vom DMZ-Segment in das interne Netzwerk nicht geöffnet werden.

DMZ-basierte MFT-Produkte, die Dateien in das interne Netzwerk verschieben, und solche, die DMZ-basierte Proxys für die sichere Datenübertragung verwenden, benötigen normalerweise mindestens einen offenen Port vom DMZ in das interne Netzwerk.

MOVEit DMZ umfasst außerdem verschiedene weitere Funktionen: eine API-Schnittstelle für sicheren, programmatischen Remote-Zugriff auf die Dienste für Datei- und Nachrichtentransfers, sichere Datenspeicherung und Benutzerdatenbanken über die MOVEit DMZ API COM-Komponente und/oder Java-Klasse; Benutzeroberflächen in französischer und englischer Sprache; und die Möglichkeit der Implementierung auf Hochverfügbarkeitsbasis für Skalierbarkeit und automatisches, unbeaufsichtigtes Failover in einer Umgebung mit mehreren Produktionsservern und Lastenausgleich.

Anders als einige andere MFT-Produkte handelt es sich bei MOVEit DMZ ausschließlich um einen Server. Dieser kann keine Verbindung zu anderen Systemen herstellen. Wie durch die Pfeile unten gezeigt, müssen alle Verbindungen zu einem MOVEit DMZ durch einen geeigneten Client eingeleitet werden. Daher muss die Firewall von dem DMZ-Segment in das interne Netzwerk nicht geöffnet werden.

DMZ-basierte MFT-Produkte, die Dateien in das interne Netzwerk verschieben, und solche, die DMZ-basierte Proxys für die sichere Datenübertragung verwenden, benötigen normalerweise mindestens einen offenen Port vom DMZ in das interne Netzwerk.

MOVEit DMZ umfasst außerdem verschiedene weitere Funktionen: eine API-Schnittstelle für sicheren, programmatischen Remote-Zugriff auf die Dienste für Datei- und Nachrichtentransfers, sichere Datenspeicherung und Benutzerdatenbanken über die MOVEit DMZ API COM-Komponente und/oder Java-Klasse; Benutzeroberflächen in französischer und englischer Sprache; und die Möglichkeit der Implementierung auf Hochverfügbarkeitsbasis für Skalierbarkeit und automatisches, unbeaufsichtigtes Failover in einer Umgebung mit mehreren Produktionsservern und Lastenausgleich.

## PCI DSS: AUFBAU UND VERWALTUNG EINES SICHEREN NETZWERKS

### 1: INSTALLATION UND VERWALTUNG EINER FIREWALLKONFIGURATION ZUM SCHUTZ VON KARTENINHABERDATEN.

Das MOVEit-System für verwalteten Dateitransfer wurde zur Verwendung mit dem in der PCI DSS-Anforderung 1 beschriebenen mehrschichtigen Netzwerk entwickelt, das häufig über mehrere Firewalls verfügt. Der MOVEit DMZ-Server für sicheren Dateitransfer wurde für den Einsatz in einem firewallgeschützten DMZ-Netzwerksegment entwickelt, in dem es teilweise über das Internet erreichbar ist. Der vorgesehene Einsatzort des MOVEit Central MFT-Clients ist ein internes, vertrauenswürdigen Netzwerk, von dem aus er durch eine Firewall Verbindungen zum MOVEit DMZ-Server herstellen kann.

Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**1.1.5:** Diese beziehen sich auf bestimmte Protokolle, die bei Verwendung der Standards zulässig sind. MOVEit DMZ und MOVEit Central können alle erforderlichen Dateiübertragungsfunktionen mit den Protokollen HTTP/S (SSL) und SFTP (SSH2) durchführen, die beide gemäß Abschnitt 1.1.6 ausdrücklich zulässig sind. Hinweis: Wenn MOVEit FTP verwendet, wird es verschlüsselt, bevor es mithilfe eines der folgenden Verschlüsselungsstandards übertragen wird: AS3, FTP/S (SSL), PGP oder SMIME.

### 2: KEINE VERWENDUNG DER STANDARDWERTE DES HERSTELLERS FÜR SYSTEMKENNWÖRTER UND ANDERE SICHERHEITSPARAMETER.

Aus Sicherheitsgründen umfassen der MOVEit Central-Client und der MOVEit DMZ-Server keine werkseitig eingestellten Standardwerte für Systemkennwörter oder andere Sicherheitsparameter. Während der Einrichtung und Konfiguration der MOVEit-Installationspakete und der Software muss der installierende Benutzer/Administrator eigene Benutzernamen und Passwörter festlegen. Hinweis: Der MOVEit DMZ-Server kann eindeutige, zufällig erzeugte Passwörter vorschlagen und bietet Administratoren auch die Möglichkeit, sichere Passwörter für alle Konten zu erzwingen.

Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**2.2.1:** Gemäß diesem Abschnitt darf auf jedem Server nur eine Primärfunktion implementiert werden. Die MOVEit-Produkte unterstützen diese Anforderung, indem alle „Dateisammlungsdienste“ auf dem Server positioniert werden, auf dem sich MOVEit DMZ befindet, während alle Dienste, die Dateiübertragungen initiieren, auf dem Server mit MOVEit Central ausgeführt werden. Darüber hinaus kann MOVEit DMZ in einer Schichtenarchitektur in einem segmentierten Netzwerk bereitgestellt und die Primärfunktionen dabei auf mehrere Server verteilt werden. So kann die MOVEit DMZ-Hauptanwendung auf einem Server installiert werden, das verschlüsselte Dateisystem auf einem zweiten und die Datenbank auf einem dritten.

**2.2.2, 2.2.3 UND 2.2.4:** Dieser Abschnitt behandelt die Sperrung oder Sicherheitsverstärkung von Serverplattformen. Die CISSP- und SANS-zertifizierten Techniker von Ipswitch haben ein Dienstprogramm namens SecurityAuxiliary entwickelt, das im Bundle mit der MOVEit DMZ- und MOVEit Central-Software geliefert wird. Es führt zahlreiche

gängige Maßnahmen zur Sicherheitsverstärkung für die Hostplattform durch, auf der die MOVEit-Software installiert ist. Außerdem verfügt MOVEit über ein eigenes „SecAux-Tool“, das mehr als hundert zusätzliche Windows-Einstellungen automatisch sperrt (z. B.: Berechtigung zur Verwendung des Befehlszeilendienstprogramms, basierend auf den Betriebseinstellungen). Obwohl MOVEit DMZ nicht direkt von dem zugrunde liegenden Windows-Betriebssystem abhängt, versucht es, dieses zu schützen. In den Installationsanweisungen für MOVEit DMZ wird beispielsweise die Verwendung automatisierter Sicherheitstools für das Betriebssystem empfohlen. Dazu gehören unter anderem:

- URLScan
- IIS-Sperrprogramm
- Windows-Sicherheitsrichtlinien
- IPSec
- Automatische Aktualisierung von Windows

**2.3:** Gemäß diesem Abschnitt muss jeder Verwaltungszugriff, der nicht über die Konsole erfolgt, verschlüsselt sein. Der Verwaltungszugriff auf MOVEit DMZ erfolgt über einen Webbrowser und unter Verwendung der HTTPS-Verschlüsselung. Der Verwaltungszugriff auf MOVEit Central erfolgt über ein Windows-Programm und SSL.

## PCI DSS: SCHUTZ VON KARTENINHABERDATEN

### 3: SCHUTZ GESPEICHERTER KARTENINHABERDATEN.

MOVEit Central und MOVEit DMZ bieten mit Defense-in-Depth einen im Vergleich zu anderen Dateiübertragungsprodukten einzigartigen Vorteil bei der Sicherung gespeicherter Karteninhaberdaten.

Die MOVEit-Produkte wurden von Beginn an mit einer eigenen integrierten Benutzerautorisierung, Zugriffskontrolle und starken Kryptografie ausgestattet. Auf diese Weise kann die MOVEit-Software genau steuern, wer sich anmelden kann und was angemeldete Benutzer im Hinblick auf Befehle, Dateien, Ordner, Protokolle und andere Benutzer sehen und durchführen können.

Zudem wurden beide MOVEit-Produkte mit einem eigenen Datenspeichersystem ausgestattet, das unsere Kryptografiesoftware MOVEit Crypto nutzt. MOVEit Crypto wurde durch das US-amerikanische National Institute of Standards and Testing (NIST) und das kanadische Communications Security Establishment (CSE) FIPS 140-2-validiert. Es handelt sich hierbei um eines der ersten kryptografischen Softwaremodule, das die FIPS 140-2-Validierung erhalten hat (Zertifikatnr. 310, erteilt im März 2003 an Standard Networks, heute Teil von Ipswitch). MOVEit Crypto unterstützt die 256-Bit-AES-Verschlüsselung (von der MOVEit-Software zum sicheren Speichern von Daten verwendet) und den Hash-Algorithmus SHA1 (verwendet zum Schutz von Passwörtern und Verschlüsselungsschlüsseln sowie zur Durchführung von Dateintegritätsprüfungen).

Dank dieser integrierten Authentifizierungs-, Zugriffskontroll- und Kryptografiesysteme hängt die Sicherheit der MOVEit-Produkte und der darauf gespeicherten Daten nicht von der Sicherheit des zugrunde liegenden Betriebssystems ab. Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**3.1:** Löschen von Daten. MOVEit Central und MOVEit DMZ können alte Dateien und Ordner planmäßig, automatisch und sicher unter Berücksichtigung der SP 800-88-Löschregelungen des NIST so löschen, dass sie sich nicht wiederherstellen lassen.

**3.2:** Archivieren von Authentifizierungsdaten. Wenn für den Zugriff auf ein Remote-System Passwörter oder andere Anmeldedaten benötigt werden, speichert MOVEit Central diese anhand einer starken, umkehrbaren Verschlüsselung. Wenn Passwörter zur lokalen Authentifizierung erforderlich sind, verwenden MOVEit DMZ und MOVEit Central nicht umkehrbare starke Hashfunktionen. MOVEit DMZ lässt sich außerdem optional an eine oder mehrere externe Authentifizierungsquellen wie LDAP-Server anbinden, sodass vollständig auf eine lokale Authentifizierung verzichtet werden kann. Ferner unterstützt MOVEit DMZ starke Passwortregeln und Richtlinien zur Verwendung vorheriger Passwörter.

**3.4:** Schutz gespeicherter Daten. In diesem Abschnitt wird festgelegt, dass gespeicherte Kreditkartennummern (Primary Account Number, PAN) durch starke Verschlüsselung geschützt werden müssen. Die meisten MFT-Systeme sind nicht in der Lage, gespeicherte Daten selbst zu verschlüsseln. Der MOVEit DMZ-Server und der MOVEit Central-Client umfassen hingegen beide starke systemeigene und betriebssystem-unabhängige Verschlüsselungsfunktionen. Alle von einem MOVEit DMZ-Server empfangenen Daten werden verschlüsselt, bevor sie mit der starken, integrierten und FIPS 140-2-validierten 256-Bit-AES-Verschlüsselung gesichert werden. Standardmäßig kann der MFT-Client von MOVEit Central bearbeitete Dateien mittels PGP-, SMIME- und/oder AS2-Kryptografie verschlüsseln.

**3.5 UND 3.6:** Speichern kryptografischer Schlüssel. In diesem Abschnitt werden sehr technische Aspekte der Schlüsselspeicherung behandelt, die den Rahmen dieses Whitepapers sprengen würden. Wenden Sie sich für weitere Informationen daher bitte an den MOVEit-Support von Ipswitch. Beachten Sie jedoch, dass die MOVEit-Software alle PCI DSS-Anforderungen für die Speicherung von Schlüsseln erfüllt.

#### **4: VERSCHLÜSSELTE ÜBERTRAGUNG VON KARTENINHABERDATEN ÜBER OFFENE, ÖFFENTLICHE NETZWERKE.**

Die MFT-Produkte von MOVEit unterstützen zahlreiche verschlüsselte Übertragungsmethoden, die für den Austausch von Karteninhaberdaten über öffentliche Netzwerke, einschließlich dem Internet, und für VPN-Implementierungen verwendet werden können.

Der MOVEit Central-Client kann Übertragungen über Secure FTP über SSL (FTPS) und Secure FTP über SSH2 (SFTP und SCP2) sowie sichere Dateiübertragungen über die Protokolle HTTP (HTTPS), AS1, AS2 und AS3 durchführen. Darüber hinaus kombiniert Central die PGP- oder S/MIME-Verschlüsselung auf Dateiebene mit dem unverschlüsselten Transfer von Protokollen wie FTP oder Windows SMB, um eine verschlüsselte Datenübertragung in Legacy-Systeme oder bei Migration zu ermöglichen.

Der MOVEit DMZ-Server unterstützt Übertragungen über Secure FTP über SSL (FTPS), Secure FTP über SSH2 (SFTP und SCP2) sowie sichere Dateiübertragungen über die Protokolle HTTP (HTTPS), AS2 und AS3.

#### **PCI DSS: VERWALTUNG EINES PROGRAMMS ZUR BEWÄLTIGUNG VON SICHERHEITSRISIKEN**

**5:** Bei Installation auf einer Plattform mit McAfee-, Symantec- oder Trend-AV-Software liefert der MOVEit Central-Client integrierten Virenschutz und Prüffunktionen. Sobald eine dieser Anwendungen einen Virus entdeckt, führt MOVEit Central automatisch die folgenden Schritte durch:

**Anhalten** der Übertragung

**Löschen** der Datei in dem System, von dem MOVEit Central sie heruntergeladen hat oder

**Speichern** der Eigenschaften der Datei, damit diese nie wieder übertragen wird

**Protokollieren** der Namen der Datei, des Virus und der Anti-Virus-Software, des Datums und der Uhrzeit, zu der die Infektion erkannt wurde, und der von MOVEit Central durchgeführten Maßnahmen

**Warnung** relevanter Personen per E-Mail

Zusätzlich bieten sowohl der MOVEit Central-Client als auch der MOVEit DMZ-Server gesicherte, FIPS 140-2-verifizierte Prüfprotokolle. Auf diese Weise werden die internen Prüfdatenbanken durch eine Reihe kryptografischer Hashfunktionen geschützt, die es erschweren oder sogar unmöglich machen, Prüfaufzeichnungen unerkannt hinzuzufügen, zu löschen oder zu bearbeiten.

#### **6: ENTWICKLUNG UND VERWALTUNG SICHERER SYSTEME UND ANWENDUNGEN.**

Die Anforderungen in diesem Abschnitt sind entweder bereits in den MOVEit-Produkten implementiert oder werden bei der Bereitstellung der MOVEit-Software in der Dokumentation empfohlen. In der folgenden Liste aller Anforderungen aus dem entwicklerzentrierten Abschnitt 6.5 werden einige Vorkehrungen veranschaulicht, die durch die MOVEit-Software getroffen werden.

**6.5: ENTWICKLUNG SICHERER WEBANWENDUNGEN.** Dieser Abschnitt besagt, dass die Entwicklung von Webanwendungen auf sicheren Kodierungsrichtlinien beruht (ähnlich denen des Open Web Application Security Project) und die Überprüfung benutzerdefinierter Anwendungscodes zur Identifizierung von Kodierungsschwachstellen sowie die Vermeidung häufiger Kodierungsschwachstellen bei der Softwareentwicklung umfassen sollte. Dazu gehören unter anderem:

6.5.1: Cross-Site Scripting (XSS)

6.5.2: Injection-Schwachstellen, insbesondere SQL-Injections. Zu berücksichtigen sind außerdem LDAP- und XPath-Injections und andere Injection-Schwachstellen.

6.5.3: Ausführung nicht vertrauenswürdiger Dateien

6.5.4: Unsichere direkte Objektverweise

6.5.5: Cross-Site Request Forgery (CSRF)

6.5.6: Datenverlust und unangemessene Fehlerbehandlung

6.5.7: Fehlerhaftes Authentifizierungs- und Sitzungsmanagement

6.5.8: Unsichere kryptografische Speicherung

6.5.9: Unsichere Kommunikation

6.5.10: Nicht beschränkter URL-Zugriff

**6.6:** Für alle öffentlich zugänglichen Webanwendungen muss eine der folgenden Maßnahmen getroffen werden: 1) Überprüfung der Anwendungen durch manuelle oder automatisierte Tools oder Methoden zur Beurteilung von Schwachstellen oder 2) Installation einer Firewall auf Anwendungsebene vor den öffentlich zugänglichen Webanwendungen

Während der Entwicklung verwendet Ipswitch WebInspect, die beliebte Software zur Sicherheitsbewertung von Webapplikationen von Hewlett Packard, und verschiedene sogenannte Fuzzing-Anwendungen zum Testen mit zufälligen Daten, um Sicherheitsprobleme zu identifizieren, bevor sie in der Praxis auftreten. Diese Tools, Dutzende automatische und halbautomatische Anwendungen in unserer Testsuite für die Qualitätssicherung sowie unzählige manuelle Tests sorgen dafür, dass alle Versionen unserer Produkte den PCI-Sicherheitsanforderungen mehr als gerecht werden.

Um die Sicherheit der MOVEit-Produkte stets aufrecht zu erhalten, veröffentlicht der Ipswitch-Support auf der MOVEit-Support-Website regelmäßig Sicherheitsupdates (verwaltet durch die Verwendung von MOVEit Central und MOVEit DMZ). Sicherheitswarnungen und aktuelle Informationen zu Testergebnissen bezüglich Sicherheitspatches für Betriebssysteme werden über die sicheren Nachrichtenfunktionen des unternehmenseigenen MOVEit DMZ-Servers von Ipswitch an die Lizenznehmer gesendet.

Der Zugriff auf die Supportsite erfolgt über eine sichere, SSL-verschlüsselte Verbindung, und für die Anmeldung auf der Site ist eine Authentifizierung und Autorisierung erforderlich. MOVEit-Lizenznehmer sind berechtigt, Patches und Upgrades im Rahmen der erforderlichen jährlichen Softwarewartung kostenlos zu implementieren.

## PCI DSS: IMPLEMENTIERUNG UMFASSENDE ZUGRIFFSKONTROLLMASSNAHMEN

### 7: BESCHRÄNKUNG DES ZUGRIFFS AUF KARTENINHABERDATEN AUF DIE GESCHÄFTLICH ERFORDERLICHEN DATEN.

Mit den MOVEit-Produkten können Ordnerberechtigungen, Protokoll-Zugriffsbeschränkungen, IP-Adressbeschränkungen und andere beschränkte Rechte individuell zugewiesen werden. Für alle diese Elemente gilt normalerweise die Regel „kein Zugriff ohne Berechtigung“. Die MOVEit-Software erlaubt außerdem die Übertragung von Rechten, sodass Administratoren nicht die Kontrolle über das gesamte MOVEit-System besitzen müssen, sondern nur über einen Teil von Ordnern, Übertragungsaufgaben oder eine Reihe von Benutzern.

### 8: ZUWEISUNG EINER EINDEUTIGEN BENUTZERKENNUNG FÜR JEDE PERSON MIT COMPUTERZUGANG.

Die MOVEit-Produkte unterstützen die Zuweisung einer eindeutigen Benutzerkennung für jede Person mit Computerzugang. Dies geschieht am besten durch Erteilung spezieller Zugriffsrechte für eine einzelne Ressource (Ordner, Übertragungsaufgabe usw.) für mehrere Benutzer. So können beispielsweise zwei Benutzer Lesezugriff und ein dritter Schreibzugriff auf einen Ordner haben. Diese spezifische Rechtevergabe für überlappende Ressourcen sorgt dafür, dass sich Benutzer eher mit eigenen Benutzernamen anmelden, anstatt ein leistungsstärkeres gemeinsames Konto zu verwenden.

Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**8.2: ZUSÄTZLICHE ANMELDEINFORMATIONEN ZUR AUTHENTIFIZIERUNG ÜBER BENUTZERNAME UND PASSWORT HINAUS.** Der MOVEit Central-Client und der MOVEit DMZ-Server unterstützen folgende zusätzliche Authentifizierungsmethoden:

**Client-Schlüssel.** Verwendung mit Secure FTP über SSH2 (SFTP und SCP2) und mit PGP-Verschlüsselung.

**Client-Zertifikate.** Verwendung mit Secure FTP über SSL (FTPS) und HTTPS, AS1, AS2 und AS3 sowie mit S/MIME-Verschlüsselung.

**8.3: ZWEI-FAKTOR-AUTHENTIFIZIERUNG.** Während der Schwerpunkt in diesem Abschnitt stärker auf dem Netzwerkzugriff als auf der Dateiübertragung liegt, sind sowohl der MOVEit Central-Client als auch der MOVEit DMZ-Server in der Lage, Zwei- (und sogar Drei-) Faktor-Authentifizierung auf alle Verwaltungs- und Dateiübertragungsschnittstellen anzuwenden.

**8.4: SCHUTZ VON ANMELDEINFORMATIONEN.** Die MOVEit-Produkte schützen gespeicherte Passwörter und Schlüssel (siehe Abschnitte 3.2, 3.5 und 3.6). Zudem setzen beide Produkte ihre Funktionen zur sicheren Übertragung mittels SSL- und SSH2-Verschlüsselung ein, um Anmeldeinformationen auch während der Übertragung zu schützen.

**8.5: PASSWÖRTER UND BENUTZERREGELN.** Dank ihrer konfigurierbaren Passwort- und Benutzerrichtlinien erfüllen der MOVEit Central-Client und der MOVEit DMZ-Server alle in diesem Abschnitt beschriebenen Regelungen.

- 8.5.1: Kontrolliertes Hinzufügen, Löschen und Verändern von Benutzerkennungen, Anmeldedaten und anderen Identifizierungselementen.
- 8.5.2: Verifizierung der Benutzeridentität vor dem Zurücksetzen von Passwörtern.
- 8.5.3: Festlegen des ersten Passworts jedes Benutzers auf einen eindeutigen Wert und sofortiges Ändern nach der ersten Verwendung.
- 8.5.4: Sofortiges Widerrufen der Zugriffsrechte ausscheidender Benutzer.
- 8.5.5: Entfernen/Deaktivieren inaktiver Benutzerkonten mindestens alle 90 Tage.
- 8.5.6: Aktivieren von durch Lieferanten zur Fernwartung verwendeten Konten nur während des erforderlichen Zeitraums.
- 8.5.7: Melden von Passwortverfahren und -richtlinien an alle Benutzer, die Zugang zu Karteninhaberdaten haben.
- 8.5.8: Kein Verwenden von Gruppen-, gemeinsamen oder generischen Konten und Passwörtern.
- 8.5.9: Ändern von Benutzerkennwörtern mindestens alle 90 Tage.
- 8.5.10: Passwortlänge von mindestens sieben Zeichen.
- 8.5.11: Verwenden von Passwörtern mit numerischen und alphabetischen Zeichen.
- 8.5.12: Neue Passwörter dürfen nicht mit einem der letzten vier vom jeweiligen Benutzer verwendeten Passwörtern übereinstimmen.
- 8.5.13: Beschränkung wiederholter Zugriffsversuche durch Sperren von Benutzerkennungen nach höchstens sechs Versuchen.
- 8.5.14: Festlegen der Sperrdauer auf mindestens 30 Minuten oder bis der Administrator die Benutzerkennung reaktiviert.
- 8.5.15: Erforderliche erneute Passworteingabe durch Benutzer zur Reaktivierung des Terminals, wenn eine Sitzung länger als 15 Minuten lang inaktiv war.
- 8.5.16: Authentifizieren des gesamten Zugriffs auf jegliche Datenbanken mit Karteninhaberinformationen. Dies umfasst den Zugriff durch Anwendungen, Administratoren und alle anderen Benutzer.

## 9: BESCHRÄNKUNG DES PHYSISCHEN ZUGRIFFS AUF KARTENINHABERDATEN.

Die MOVEit-Produkte können Unternehmen auch bei der Erfüllung einiger physischer Sicherheitsanforderungen helfen. Wenn es beispielsweise einem Eindringling gelingt, physischen Zugriff auf einen MOVEit DMZ-Server zu erhalten, kann er keine der gespeicherten Karteninhaberdaten lesen, da jede Datei mit einem eigenen Schlüssel gesichert ist, der wiederum individuell durch 256-Bit-AES verschlüsselt ist.

**9.5: EXTERNE BACKUPS.** Der MOVEit Central-Client und der MOVEit DMZ-Server können eine große Anzahl von Dateien jeder Größe problemlos, sicher und zuverlässig automatisch übertragen, verarbeiten und speichern. Auf diese Weise können sie einige bandbasierte physische Backups ersetzen.

**9.7.2: ÜBERTRAGUNGSZUVERLÄSSIGKEIT.** Wenn bandbasierte Backups durch MOVEit-Produkte ersetzt werden, müssen die in diesem Abschnitt beschriebenen Anforderungen nicht erfüllt werden.

**9.10: LÖSCHEN VON MEDIEN.** Zwar können die MOVEit-Produkte nicht zur physischen Zerstörung von Medien verwendet werden, doch sowohl der MOVEit Central-Client als auch der MOVEit DMZ-Server ermöglichen die Löschung von Daten nach NIST 800-88.

## PCI DSS: REGELMÄSSIGES ÜBERWACHEN UND TESTEN VON NETZWERKEN

### 10: VERFOLGUNG UND ÜBERWACHUNG ALLER ZUGRIFFE AUF NETZWERKRESSOURCEN UND KARTENINHABERDATEN.

MOVEit bietet umfassendere Prüfprotokollfunktionen als die meisten anderen MFT-Produkte. Viele Konkurrenzprodukte erstellen lediglich textbasierte Protokolle, die kaum mehr Informationen als den Zeitpunkt von Anmeldungen und Dateiübertragungen enthalten. Bei diesen Protokollen ergeben sich häufig folgende Probleme:

**Sicherheit von Protokolldaten.** Textbasierte MFT-Protokolle werden häufig im Klartext auf Festplatte geschrieben und können daher problemlos mit einem Desktop-Editor überschrieben werden, um nicht autorisierte Vorgänge zu verbergen. MOVEit Central und MOVEit DMZ schreiben ihre Prüfberichte auf eine integrierte, kommerziell lizenzierte Datenbank. Der Zugriff auf die MOVEit-Datenbanken ist nur mit Autorisierung und Authentifizierung möglich. Für einen optimierten Schutz vor Manipulationen beinhalten die MOVEit-Produkte eine Reihe kryptografischer Hashfunktionen, die anzeigen, ob die Aufzeichnungen in Datenbanken verändert wurden oder nicht.

**Administrative Protokolldaten.** Textbasierte MFT-Protokolle enthalten häufig keine Informationen über administrative Vorgänge wie das Hinzufügen von Benutzern, die Änderung von Ordnerberechtigungen und andere wichtige Sicherheitsmodifikationen. Dadurch ist es schwierig – wenn nicht gar unmöglich –, nicht autorisierte administrative Änderungen zu identifizieren. Die MOVEit-Produkte zeichnen alle administrativen Vorgänge ausführlich in der sicheren Datenbank auf.

**Benutzerfreundlichkeit.** Textbasierte MFT-Protokolle müssen häufig durch sogenannte Protokollparser von Drittanbietern verarbeitet werden, um aussagekräftige Informationen zu liefern. Die MOVEit-Produkte hingegen bieten Ad-hoc-Ansichten der Prüfergebnisse. Zusätzlich umfassen sie integrierte und benutzerdefinierbare Berichte, mit denen Administratoren ihre MOVEit-Produkte schnell und einfach verfolgen und überwachen können, ohne einen Protokollparser zu verwenden.

Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**10.1-10.3: BENUTZERINFORMATIONEN.** In diesen drei Abschnitten wird beschrieben, wie bestimmte Aktionen mit bestimmten Benutzern verknüpft werden können, welche Aktionen geprüft werden sollten und welche Informationen die Aufzeichnungen enthalten sollten. Der MOVEit DMZ-Server unterstützt das in Abschnitt 10.1 beschriebene Konzept „ein Benutzerkonto pro Person“ (siehe auch 8) und erfüllt die Regelungen zum Inhalt und Umfang von Protokollen der Abschnitte 10.2 und 10.3.

**10.4: ZEITSYNCHRONISIERUNG.** Zeitsynchronisierung. Die MOVEit-Produkte unterstützen die Zeitsynchronisierung zwischen Computern und sind mit Dienstprogrammen und Dokumentationsfunktionen zur Durchführung dieses Vorgangs mittels Standard-Zeitprotokoll ausgestattet.

**10.5: SCHUTZ VON PRÜFDATEN.** Dieser Abschnitt umfasst die folgenden MFT-relevanten Unterabschnitte:

**10.5.1: ZUGRIFFSBESCHRÄNKUNG.** Dieser Abschnitt behandelt die Bereitstellung von beschränktem Zugriff auf Prüfaufzeichnungen. Anders als MFT-Produkte, die textbasierte Prüfprotokolle verwenden, zeichnen MOVEit Central und MOVEit DMZ Prüfdaten in der integrierten, kommerziell lizenzierten Datenbank mit Zugriffssteuerung auf. Diese bietet Schutz vor Benutzern, die sich unautorisierten Zugriff auf oder Kontrolle über das zugrunde liegende Betriebssystem verschafft haben. Da der Zugriff auf die MOVEit-Prüfaufzeichnungen kontrolliert wird, können Benutzer nur die Ereignisse sehen, die sich auf ihr Unternehmen und/oder die Gruppen, Benutzer, Ordner und Übertragungsaufgaben beziehen, die sie kontrollieren.

**10.5.2: MANIPULATIONSSCHUTZ.** In diesem Abschnitt geht es um die Erfordernis, Prüfaufzeichnungen vor nicht autorisierter Veränderung zu schützen. Dazu kontrollieren die MOVEit-Produkte den Datenzugriff (siehe Abschnitt 10.5.1) mithilfe einer Reihe kryptografischer Hashfunktionen zur Überprüfung der Dateiintegrität, um festzustellen, ob die Daten verändert wurden, und bei Identifizierung einer Manipulation eine Warnmeldung auszugeben.

**10.5.3: DUPLIZIERUNG VON AUFZEICHNUNGEN.** In diesem Abschnitt wird die umgehende Duplizierung von Prüfaufzeichnungen empfohlen – entweder auf einem zentralisierten Server oder auf „schwer zu verändernden Medien“ (z. B. ausgedruckte Unterlagen). MOVEit Central und MOVEit DMZ bieten eine Beschreibung, wie Prüfaufzeichnungen entweder an einen zentralisierten Server gesendet (über SysLog oder SNMP) oder in die Drucker-Warteschlange gereicht werden können.

**10.5.5: INTEGRITÄTSÜBERWACHUNG.** In diesem Abschnitt wird die Verwendung von Software zur Überwachung der Dateiintegrität und Identifizierung von Modifikationen gefordert, um Änderungen der Prüfaufzeichnungen zu beobachten. Wie in Abschnitt 10.5.2 beschrieben, führen die MOVEit-Produkte eine automatische Überprüfung der Dateiintegrität durch und geben bei Problemen Warnmeldungen aus.

**10.6: ÜBERPRÜFUNG VON AUFZEICHNUNGEN.** In diesem Abschnitt wird die regelmäßige Überprüfung der Prüfaufzeichnungen gefordert und die Automatisierung dieser Vorgänge empfohlen. MOVEit Central und MOVEit DMZ sind in der Lage, Ad-hoc-Ansichten der Prüfdaten anzuzeigen und mehr als 90 vordefinierte Berichte über Dateiübertragungen, sichere Nachrichten, Benutzerstatus, Systemleistung, Speicherstatus und Sicherheit zu erzeugen. Berichte können auf geplanter oder auf On-Demand-Basis ausgeführt und in den Formaten CSV, HTML oder XML erstellt werden. Da sie in die zentralisierte Überwachung integriert werden können, unterstützen die MOVEit-Produkte automatisierte Überprüfungen (siehe Abschnitt 10.5.3). Darüber hinaus lassen sich mit beiden Produkten benutzerdefinierte Berichte erstellen, die Information an spezielle Systeme zur Identifizierung bestimmter Unregelmäßigkeiten senden.

**10.7: ARCHIVIEREN/LÖSCHEN VON AUFZEICHNUNGEN.** Die Protokolle der MOVEit-Produkte werden nach einem konfigurierbaren Zeitraum automatisch bereinigt. Auch die automatische Archivierung bereinigter Protokolle in einem archivierungsfreundlichen Format zur langfristigen Speicherung ist möglich.

#### **11: REGELMÄSSIGES TESTEN VON SICHERHEITSSYSTEMEN UND – PROZESSEN.**

Wie in Abschnitt 6 beschrieben, rät Ipswitch Besitzern von MOVEit Central- und MOVEit DMZ-Lizenzen, ihre MOVEit-Test- und Produktionssysteme regelmäßig zu untersuchen und zu scannen. Die MOVEit-Produkte können auch mit entsprechend konfigurierter Drittanbieter-Software zur Erkennung von Änderungen an Anwendungsdateien ausgeführt werden (siehe Abschnitt 11.5).

### **PCI DSS: VERWALTUNG EINER RICHTLINIE ZUR INFORMATIONSSICHERHEIT**

#### **12: VERWALTUNG EINER RICHTLINIE ZUR INFORMATIONSSICHERHEIT.**

In der Produktdokumentation zu MOVEit Central und MOVEit DMZ werden Zusammenstellungen von Konfigurationsoptionen, insbesondere von Sicherheitsoptionen, als „Richtlinien“ bezeichnet. Dieser Begriff wurde bewusst gewählt. Die MOVEit-Richtlinien sollen Lizenznehmern helfen, ihre Software so zu konfigurieren, dass ihre Unternehmensrichtlinien durchgesetzt werden. Die folgenden Abschnitte dieser Anforderung gelten für MFT-Produkte.

**12.2 UND 12.5.5: TÄGLICHE ABLÄUFE.** In diesem Abschnitt werden täglich durchgeführte Sicherheitsvorgänge einschließlich der Verwaltung von Benutzerkonten und der Überprüfung von Protokollen behandelt. Die MOVEit-Produkte sind mit einer wartungsorientierten Verwaltungsoberfläche ausgestattet, über die hunderte von Übertragungsaufgaben (MOVEit Central-Client) und tausende von Benutzern (MOVEit DMZ-Server) verwaltet werden können. Kontextsensitive Optionen wie „Show audit logs for selected user“ (Prüfprotokolle für ausgewählte Benutzer anzeigen) und Nachschlagefelder helfen ebenso bei der täglichen Sicherheitsverwaltung der MOVEit-Produkte wie die automatische Erzeugung und Bereitstellung vorkonfigurierter und benutzerdefinierter Sicherheitsberichte.

**12.5.2: ÜBERWACHUNG UND ANALYSE VON WARNMELDUNGEN.** Die MOVEit Central- und MOVEit DMZ-Produkte nehmen Einträge in Ereignisprotokolle vor, die an zentrale Überwachungssysteme wie SysLog oder SNMP gesendet werden können.

**12.5.4: ÜBERTRAGUNG DER BENUTZERVERWALTUNG.** Mit MOVEit Central können Administratoren die Kontrolle über bestimmte Übertragungsaufgaben an festgelegte Personen übertragen, und die Administratoren von MOVEit DMZ können die Kontrolle über Benutzergruppen und deren Ordner an bestimmte „Gruppenadministratoren“ übertragen.

**12.10: PCI DSS-COMPLIANCE VON PARTNERUNTERNEHMEN.** In diesem Abschnitt geht es um die Erfordernis der PCI DSS-Compliance von Geschäftspartnern, mit denen ihr Unternehmen Karteninhaberinformationen austauscht. Viele Finanzinstitute und -bearbeiter verwenden MOVEit-Produkte – darunter auch 20 Prozent der Organisationen im Vorstand und Beirat des PCI-Rats.

#### **FAZIT**

Die MOVEit-Produkte bieten eine umfassende Reihe von Sicherheits- und Betriebsfunktionen, mit denen Unternehmen für die Einhaltung des Datensicherheitsstandards PCI und insbesondere für die Sicherheit in den entscheidenden Bereiche Speicherung, Übertragung, Zugriffskontrolle und Prüfaufzeichnungen im Zusammenhang mit Karteninhaberdaten sorgen und dies demonstrieren können. Dies ist einer der Gründe, warum so viele Finanzbearbeiter und Banken, Kreditgenossenschaften und andere Finanzinstitute in Nordamerika und Europa MOVEit-Produkte verwenden.

Informationen zu Anfragen für eine Live-Demonstration von MOVEit, eine Bewertung vor Ort oder ein Preisangebot erhalten Sie telefonisch beim MOVEit-Vertriebsteam von Ipswitch oder im Internet unter [www.lpswitchFT.com](http://www.lpswitchFT.com).



File Transfer Division von Ipswitch kontaktieren