MOVEIT: SECURE BY DESIGN

VON JONATHAN LAMPE, CISSP

Der Datenübertragungsserver MOVEit DMZ, die Workflow-Engine MOVEit Central, die MOVEit-Clients und die FIPS 140-2-validierten MOVEit Kryptographie-Softwareprodukte von Ipswitch File Transfer wurden von Grund auf für die sichere, durchgehend verschlüsselte Übertragung und Speicherung vertraulicher Dateien, Nachrichten und Webpostings mittels zahlreicher gängiger öffentlicher Standards und Protokolle entwickelt. Es handelt sich weder um FTP-Produkte mit nachträglich hinzugefügten Sicherheitsfunktionen, noch um herstellerspezifische Dateiübertragungsprogramme, die anschließend um Unterstützung für offene Standards erweitert wurden.

Dank des modularen Designs und dem Schwerpunkt auf HTTPS-basierter Kommunikation können die MOVEit-Produkte in hoch sicheren Umkreisnetzwerken eingesetzt werden, ohne auf „Passthrough-Proxys“, proprietäre VPNs, umständliche Firewallregeln oder andere Methoden mit nicht standardisierten Netzwerkidentitäten zugreifen zu müssen. Zusammengenommen stellen die MOVEit-Produkte eine Lösung zur sicheren Übertragung, Verarbeitung und Speicherung von Daten auf Unternehmensebene dar.

In diesem Dokument wird anhand einer Reihe von allgemein anerkannten Best Practices für die Sicherheit gezeigt, dass die MOVEit-Produkte von Grund auf sicher gestaltet wurden. Diese bewährten Verfahren stammen aus dem Bericht „Engineering Principles for Information Technology Security“ des US National Institute of Standards and Technology (NIST) vom Juni 2004.

Das NIST entwickelt Standards und Richtlinien zur Gewährleistung der Informationssicherheit für US-amerikanische Regierungsbehörden. In diesem Rahmen hat es eine Reihe von Standards geschaffen, die als FIPS (Federal Information Processing Standards) bekannt sind. Kryptische Module werden durch den Standard FIPS 140 unterstützt, dessen neueste und strengste Version FIPS 140-2 ist. Gemeinsam mit dem Communications Security Establishment der kanadischen Regierung verwaltet das NIST das Cryptographic Module Validation Program (CMVP) zur Überprüfung von Produkten auf FIPS-Konformität.

Im Bericht „Engineering Principles“ des NIST werden Kryptographie, Softwareaspekte und Netzwerkdesign behandelt. Dabei liegt der Schwerpunkt auf dem Aufbau eines umfassenden Abwehrsystems durch Verwendung von „Sicherheitsprinzipien auf Systemebene“ bei „Design, Entwicklung und Betrieb“ von IT-Systemen.

Die Sonderveröffentlichung 800 27A des NIST, „Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A“, finden Sie im Internet unter: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf

„BEHANDLUNG VON SICHERHEIT ALS INTEGRALER BESTANDTEIL DES GESAMTEN SYSTEMDESIGNS“

Bei der Entwicklung der MOVEit-Produkte standen wir dem Internet, den Betriebssystemen und den zugehörigen Programmen, die unsere Produkte verwenden sollten, geradezu paranoid gegenüber.

Daher haben wir eine Defense-in-Depth-Architektur eingeführt. Im Folgenden finden Sie einige Beispiele, die in unserer MOVEit DMZ-Software für sichere Datenübertragung und Speicherserver realisiert wurden.

- Die Sicherheit der mit MOVEit DMZ verarbeiteten Dateien hängt nicht von der – nicht immer optimalen – Sicherheit des zugrunde liegenden Betriebssystems ab.
- Da MOVEit DMZ aufgrund seines Designs nicht in der Lage ist, Dateien zu verschieben, kann es im Fall einer Manipulation auch keine Malware in vertrauenswürdige Netzwerke übertragen.
- Durch Autorisierung mit minimalen Berechtigungsvorgaben („Least Privilege“) kann genau kontrolliert werden, über welche Rechte ein Benutzer verfügt.
- Die virtuelle Benutzerschnittstelle von MOVEit DMZ trägt zur Implementierung der minimalen Berechtigungsvorgaben bei, indem sie eine genaue administrative Kontrolle darüber bietet, was Benutzer sehen können und was ihnen verborgen bleibt. Dazu gehören Befehlsoptionen, Dateien, Ordner, Protokolle und Benutzerinformationen.
- MOVEit DMZ bedient sich einer anderen Benennungskonvention für Dateien und Ordner/Verzeichnisse als das zugrunde liegende Betriebssystem – ein weiterer Vorteil der virtuellen Schnittstelle.
- Für die Übertragung und Speicherung wird ausschließlich die FIPS 140-2-validierte Verschlüsselung verwendet.
- Da alle vom MOVEit DMZ empfangenen Dateien mit der integrierten AES-Verschlüsselung gespeichert werden, können sie nicht von nicht vertrauenswürdigen Dritten gelesen oder ausgeführt werden.

Diese und andere Beispiele werden weiter unten in diesem Dokument ausführlich beschrieben.

Der MOVEit DMZ-Server stellt einen sicheren Austauschpunkt dar, auf den sowohl Webbrowser als auch sichere Datenübertragungs-Clients von MOVEit und Drittanbietern Dateien, Nachrichten und Webpostings hochladen, herunterladen und speichern können. Er wird auf einem sicherheitsverstärkten Windows 2003- oder 2008-Server in einem DMZ-Segment hinter einer Firewall ausgeführt. Das Produkt unterstützt HTTPS-, FTPS- und SFTP-basierte verschlüsselte Datentransfers und umfasst eine integrierte, FIPS 140-2-validierte Kryptographie für die einzigartige AES-verschlüsselte Datenspeicherung bei 256 Bit. Dank dieser Funktionen können Daten mit MOVEit DMZ ohne zusätzliche Verschlüsselungsprogramme von Drittanbietern sicher und durchgehend verschlüsselt übertragen werden.

„SICHERSTELLUNG, DASS ENTWICKLER IN DER ERSTELLUNG SICHERER SOFTWARE GESCHULT SIND“

Viele unserer MOVEit-Entwickler und Supportmitarbeiter besitzen eine oder mehrere aktuelle Sicherheitszertifikate von dem angesehenen SANS-Institut (SysAdmin, Audit, Network, Security) oder (ISC)². SANS (www.sans.org) bietet Schulungen und Zertifizierungen zur Informationssicherheit auf globaler Basis und leitet das „Internet-Frühwarnsystem“ Internet Storm Center. (ISC)² erteilt CISSP-Zertifikate.

Darüber hinaus werden die MOVEit-Produkte von Entwicklern in den USA entwickelt und gewartet, die über eine umfassende Ausbildung und langjährige Erfahrung in den Bereichen Sicherheit und Technik verfügen. Die meisten von ihnen haben ein mindestens vierjähriges Studium in Engineering oder Computerwissenschaft absolviert und können auf durchschnittlich zehn Jahre postakademischer Erfahrung in der Entwicklung zurückblicken.

Darüber hinaus sind alle Entwickler und Supportmitarbeiter von Ipswitch File Transfer Mitarbeiter des Unternehmens. Keiner von ihnen arbeitet im Ausland oder als Vertragsarbeiter. Wir fertigen unsere Produkte in Eigenarbeit und stellen den Support selbst bereit.

„ANNAHME, DASS EXTERNE SYSTEME UNSICHER SIND“

Da MOVEit DMZ von Beginn an für die Ausführung auf Windows-Servern entwickelt wurde, hängt seine Sicherheit nicht vom zugrunde liegenden Betriebssystem ab.

Daher haben wir eine eigene FIPS 140-2 validierte Kryptographie-Plattform, eine eigene Dateiübertragungslösung und einen sicheren Einstellungsspeicher entwickelt. Um Angriffen auf das Betriebssystem standzuhalten, werden Daten mit MOVEit DMZ nicht ungeschützt auf der Festplatte oder im Speicher abgelegt, sondern stets umfassend verschlüsselt.

MOVEit Central führt automatisierte geplante und ereignisgesteuerte Dateitransferaufgaben aus, die sich ganz einfach einrichten lassen. Mit diesen werden Dateien von Quellsystemen abgerufen, durch Prozesse verarbeitet und in Zielsysteme verschoben. In der Regel befindet sich MOVEit Central innerhalb eines vertrauenswürdigen Netzwerks und dient zum Verschieben von Dateien zwischen MOVEit DMZ und lokalen Systemen sowie zwischen diesen und Remote-Systemen. Dies geschieht mittels der verschlüsselten Übertragungsprotokolle HTTPS, FTPS, SFTP und S/MIME, der Übertragungsprotokolle FTP und SMTP/POP3 sowie der Standards AS1, AS2 und AS3, und durch Kopieren der Daten auf vernetzte und lokale Dateisysteme. Optional kann MOVEit Central Dateidaten

verarbeiten, Befehlszeilenprogramme auslösen und Programme mit COM-Schnittstellen und in VBScript, Perl und anderen Sprachen verfassten, übersetzten Skripts (mit Interpreter) ausführen. MOVEit Central wird als Dienst unter Windows XP, 2003, Vista oder 2008 ausgeführt.

„VERWENDUNG VON GRENZMECHANISMEN, UM COMPUTERSYSTEME UND INFRASTRUKTUREN ZU TRENNEN“

Die folgende Abbildung zeigt ein gängiges Netzwerkdesign mit einer solchen Aufteilung.

- Externe Benutzer dürfen keine Verbindung über das Internet zu Systemen in einem der vertrauenswürdigen internen Netzwerke herstellen.
- Interne Benutzer dürfen keine Verbindung aus den vertrauenswürdigen Netzwerken zu Systemen im Internet herstellen (es sei denn, dies geschieht über einen Webproxy-Server).

Bei diesem Ansatz wird für die Übertragung einer Datei über das Internet ein interner Client benötigt, der die Datei auf einen Server im lokalen DMZ-Segment verschiebt, und ein weiterer Client (mit Berechtigung zur Verbindung mit dem Internet), der die Datei vom Server abruft und auf einen Remote-Server verschiebt. Von dort kann er anschließend in das vertrauenswürdige Remote-Netzwerk heruntergeladen werden.

Mithilfe der MOVEit-Produkte kann dies wie folgt geschehen:

- Ein Client (WS_FTP Professional, MOVEit Central, MOVEit DMZ API, MOVEit Freely Webbrowser mit MOVEit Wizard) verschiebt die Datei auf geplanter, ereignisgesteuerter oder Ad-hoc-Basis über eine HTTPS-, FTPS-, SFTP-, AS1-, AS2- oder AS3-verschlüsselte Verbindung auf den MOVEit DMZ-Server im lokalen DMZ-Segment.
- Bei Eintreffen der Datei auf dem MOVEit DMZ wird der automatische geplante oder ereignisgesteuerte Download durch einen MOVEit Central-Client im lokalen DMZ-Segment ausgelöst. Daraufhin wird die Datei über SFTP, FTPS, HTTPS, AS1, AS2 oder AS3 auf den Remote-Server verschoben.
- Mit MOVEit DMZ und MOVEit Central können auch E-Mails mit Informationen über den endgültigen Übertragungsstatus an den Absender, Empfänger und/oder Administrator gesendet werden.

„SCHUTZ VON INFORMATIONEN WÄHREND DER VERARBEITUNG, BEI DER ÜBERTRAGUNG UND IM SPEICHER“

Bei den meisten Produkten zur sicheren Datenübertragung geht es fast ausschließlich um den Schutz der Daten während der Übertragung. Dateien sind jedoch in der Regel selbst im Vergleich zur Übermittlung über das Internet viel angreifbarer, wenn sie auf einem öffentlich zugänglichen Server zur sicheren Dateiübertragung gespeichert sind.

Im Allgemeinen werden Dateien beim Verschlüsseln und Senden von einem sicheren Übertragungsclient an einen sicheren Dateiübertragungsserver von diesem empfangen, entschlüsselt und gespeichert. Wenn die Datei zum Zeitpunkt der Verschlüsselung für die Übertragung nicht verschlüsselt war, wird sie auch auf dem Server unverschlüsselt gespeichert. Entsprechend kann sie von jedem gelesen werden, der Zugriff auf den Server hat.

Mit dem MOVEit DMZ-Datenübertragungsserver wird diese Schwachstelle beseitigt, indem jede empfangene Datei vor dem Schreiben auf die Festplatte automatisch erneut verschlüsselt wird. Gleichzeitig kann bei diesem Ansatz meist auf die Verwendung von PGP und anderen Verschlüsselungsprogrammen von Drittanbietern und damit auch auf die mühsame Verteilung derartiger Programme und die Verwaltung der Schlüssel verzichtet werden.

Zum Schutz von Dateien während der Übertragung verwenden der MOVEit DMZ-Server und die Windows-basierten MOVEit-Clients FIPS 140-2-validierte SSL-Verschlüsselungsbibliotheken von Microsoft.

Gespeicherte Dateien werden vom MOVEit DMZ-Server durch 256-Bit AES-Verschlüsselung und die SHA-1-Bibliotheken in seinem integrierten, FIPS 140-2-validierten Kryptographiemodul MOVEit Crypto gesichert.

Während der Verarbeitung von Dateien zwischen der Verschlüsselung für den Transfer und die Speicherung verwendet MOVEit DMZ schließlich die kleinst möglichen Puffer, sodass sich im Speicher keine größeren Mengen ungeschützter vertraulicher Daten befinden.

Damit auch verschlüsselte Dateien nicht länger als unbedingt nötig auf der Festplatte verbleiben, werden sie mit kryptographisch sicheren Zufallsdaten überschrieben, wenn sie aus dem verschlüsselten Dateispeicher MOVEit DMZ und dem Arbeitsspeicher von MOVEit Central gelöscht werden. Diese Art der Datenlöschung ist NIST 800-88-konform und erfüllt die PCI-Anforderungen 9.10.2: „Die Daten von Karteninhabern auf elektronischen Medien müssen so gelöscht werden, dass sie nicht rekonstruiert werden können.“

Den Schutz der Konfigurationsinformationen übernimmt das in die MOVEit Central-Workflow-Engine integrierte Modul MOVEit Crypto.

„SCHUTZ VOR ALLEN MÖGLICHEN ANGRIFFSKLASSEN UND IMPLEMENTIERUNG MINIMALER BERECHTIGUNGSVORGABEN"

Die MOVEit-Systeme wurden entwickelt, um Web-, FTP- und SSH-Angriffe durch Benutzer aus dem Internet sowie Netzwerkangriffe durch interne Benutzer und nicht autorisierte Administratoren von der lokalen Konsole zu verhindern. Daher spielt nicht nur die sorgfältige Datenbereinigung, sondern auch das Prinzip der minimalen Berechtigungsvorgaben (Least Privilege) eine entscheidende Rolle beim Schutz der MOVEit DMZ-Server vor Angriffen aus dem Internet.

Dies bedeutet, dass Benutzer ausschließlich die Berechtigungen erhalten, die zur Durchführung einer bestimmten Aufgabe unbedingt erforderlich sind. Auf Betriebssystemebene wird dieses Prinzip durch die Sicherheitsrichtlinien des Betriebssystems und NTFS-Berechtigungen umgesetzt. Die minimalen Berechtigungsvorgaben werden auf Anwendungsebene durch ein strenges System aus Benutzer- und Gruppenberechtigungen gesteuert. Zur einfacheren Verwaltung sind diese in Sicherheitsprofile organisiert. Die folgenden Beispiele sind nur einige von zahlreichen Möglichkeiten, wie MOVEit-Produkte das Prinzip der minimalen Berechtigungsvorgaben implementieren können.

- Standardmäßig kann nur der Administrator den MOVEit DMZ-Datenübertragungsserver und die MOVEit Central Workflow-Engine konfigurieren und über die Konsole auf sie zugreifen, der sie installiert hat. Der Fernzugriff muss gesondert aktiviert werden.
- Ebenso können MOVEit DMZ-Benutzer standardmäßig nicht auf bestimmte Basisordner zugreifen. Die zusätzlichen Zugriffsrechte müssen durch einen MOVEit DMZ-Administrator erteilt werden, und Einzelheiten zu dieser Änderung werden automatisch in das Protokoll eingetragen.
- Neue MOVEit Central-Betreibergruppen sind standardmäßig nicht befugt, Aufgaben zu bearbeiten oder ausführen. Diese Berechtigungen müssen gesondert erteilt werden.

Der Upload-/Download-Assistent von MOVEit ist eine Kombination aus kostenlosen ActiveX- und Java-Steuerelementen, mit denen Webbrowser wie Internet Explorer von Microsoft, Firefox oder Safari um eine Reihe nützlicher Funktionen erweitert werden. Dazu gehört eine bedienerfreundliche grafische Benutzeroberfläche (GUI), über die mehrere Dateien ausgewählt und übertragen werden können, und die Möglichkeit, browserinterne Beschränkungen bezüglich Dateigrößen und Timeouts zu umgehen. Darüber hinaus unterstützt der MOVEit Wizard die Integritätsprüfung von Dateien mittels SHA-1 (ein integraler Bestandteil der Nicht-Ablehnung von Dateien), die automatische Dateikomprimierung und die automatische Wiederaufnahme unterbrochener Dateiübertragungen.

„FÜR OPTIMALE MOBILITÄT UND INTEROPERABILITÄT SOLLTE SICHERHEIT WENN MÖGLICH AUF OFFENEN STANDARDS BASIEREN"

Die folgenden Beispiele zeigen, dass die MOVEit-Produkte von Beginn an auf Basis offener Standards entwickelt wurden.

- MOVEit Kryptographie verwendet die Verschlüsselungsstandards AES, SHA-1 AS1/AS2/AS3, SSH und SSL.
- Die MOVEit-Dateiübertragungsdienste basieren auf den Industriestandards HTTP über SSL (HTTPS), FTP über SSL (FTPS) und SSH (SFTP), die in RFC-Dokumenten international definiert sind.
- Sowohl MOVEit DMZ als auch MOVEit Central unterstützen X.509-Zertifikate.
- Die externen Authentifizierungsfunktionen von MOVEit DMZ basieren auf den Protokollen Standard LDAP, Secure LDAP und RADIUS Server.
- MOVEit Central unterstützt die Ver- und Entschlüsselung von E-Mails durch S/MIME und PGP.

„FLEXIBLES SICHERHEITSDESIGN FÜR KOMPATIBILITÄT MIT NEUEN TECHNOLOGIEN, EINSCHLIESSLICH EINES SICHEREN UND LOGISCHEN VERFAHRENS FÜR TECHNOLOGIE-UPGRADES"

- Dank der konsequenten Verfolgung des Quellcode-Änderungsmanagements sind Sicherheitspatches bei (nur selten auftretenden) neuen Problemen in kürzester Zeit verfügbar.
- MOVEit-Installationen und -Upgrades werden über die gleichen MOVEit-Installationsdateien verwaltet. In der Regel nehmen MOVEit-Softwareupgrades weniger als fünf Minuten in Anspruch.

MOVEit EZ ist ein Client zur sicheren Dateiübertragung, der das firewall-freundliche HTTPS verwendet, um Dateien auf geplanter, automatischer Basis mit einem MOVE DMZ-Server auszutauschen. MOVEit EZ kann entweder im Vordergrund in der Taskleiste oder als Dienst unter Windows ausgeführt werden. Dateien können mit MOVEit EZ mittels SHA-1 auf ihre Integrität überprüft werden – ein integraler Bestandteil der Nicht-Ablehnung von Dateien. Weitere Funktionen sind die automatische Dateikomprimierung und die automatische Wiederaufnahme unterbrochener Dateiübertragungen.

„ANSTREBEN EINES BENUTZERFREUNDLICHEN BETRIEBS“

Der sichere Austausch von Daten mit MOVEit DMZ-Servern über verschlüsselte Verbindungen erfolgt anhand verschiedener sicherer SSL- und SSH-basierten FTP-Clients von MOVEit und Drittanbietern, sowie über die Webbrowser Internet Explorer, Firefox, Opera und Safari (mit oder ohne Java- und ActiveX-basierte Dateiübertragungsassistenten von MOVEit). Diese bieten GUI- und Befehlszeilenlösungen für manuelle und automatische/geplante Übertragungen in nahezu jeder Computerumgebung.

Neben der verschlüsselten Übertragung zeichnen sich alle MOVEit-Clients bei Einsatz mit MOVEit DMZ-Servern durch folgende automatische Funktionen aus:

- SHA-1-Integritätsprüfung von Dateien (im Rahmen der Nicht-Ablehnung von Dateien).
- Dateikomprimierung (zur schnelleren Übertragung).
- Wiederaufnahme unterbrochener Übertragungen (spart Zeit beim Senden großer Dateien).

Sowohl der MOVEit DMZ-Server als auch der MOVEit Central-Client verfügen über interaktive und programmatische Verwaltungsschnittstellen. Diese ermöglichen die Konfiguration und Überwachung in Echtzeit. Zwar kann der Zugriff auf diese Schnittstellen auch per Fernzugriff erfolgen; dies ist jedoch nur über eine SSL-verschlüsselte Verbindung und mit entsprechender Authentifizierung und Autorisierung möglich.

MOVEit DMZ, MOVEit Central und die anderen MOVEit-Clients geben Lizenznehmern die betriebliche Flexibilität, die sie für den sicheren Austausch vertraulicher Daten benötigen. Dies gilt vor allem für folgende Situationen:

- Die Lizenznehmer sind nicht in der Lage, ihren Geschäftspartnern Netzwerkstandards vorzuschreiben, und
- Die Partner verwenden eines der zahlreichen gängigen offenen Übertragungsprotokolle und von MOVEit DMZ und MOVEit Central unterstützte Clients.

Der MOVEit API Java-Client verwendet die XML API-Schnittstelle des MOVE DMZ-Servers zur Bereitstellung eines sicheren, firewall-freundlichen und programmatischen Zugriffs auf HTTPS-Basis für die Erstellung, Verwaltung, Übertragung und Löschung von Dateien, Ordnern, Benutzern und Berechtigungen. MOVEit API Java wird auf Mainframes, Solaris, Linux und anderen Systemen verwendet. Es verfügt über eine kostenlose, vorkompilierte FTP-Client-Befehlszeilenschnittstelle und kann so durch JCL oder Unix/Linux-Shellskripte sowie durch lokale Betriebssystem-Scheduler wie Cron gesteuert werden. MOVEit API Java ermöglicht die automatische Integritätsprüfung von Dateien mit SHA-1, die Komprimierung von Dateien und die Wiederaufnahme unterbrochener Dateiübertragungen.

„IMPLEMENTIERUNG MEHRSCHICHTIGER SICHERHEIT“

MOVEit-Systeme werden idealerweise in modernen, mehrschichtigen Sicherheitsumgebungen eingesetzt. Die Verwendung mehrerer Firewalls, Netzwerksegmente und Proxyserver wird vorausgesetzt und empfohlen.

MOVEit enthält eine Installationsvorlage für ein sicherheitsverstärktes Betriebssystem. Doch anstatt sich auf die Sicherheit des zugrunde liegenden Betriebssystems zu verlassen, vertraut MOVEit beim Schutz von Dateien und Einstellungen vor unautorisiertem Zugriff auf ein eigenes Berechtigungssystem und FIPS 140-2-validierte Kryptographie.

Das heißt: Auch wenn sich ein Hacker Administratorrechte für Windows verschafft, kann er die Benutzerpasswörter von MOVEit DMZ nicht zurücksetzen, weil die MOVEit DMZ-Anwenderbasis ein eigenes, separates System besitzt. Selbst wenn er durch einen Pufferüberlauf oder auf eine andere Weise Zugang zu der MOVEit DMZ-Anwendung erhält, benötigt der Eindringling immer noch die richtigen Schlüssel, um auch auf die MOVEit DMZ-Daten zugreifen zu können. Und da jede Datei auf den MOVEit DMZ-Servern mit einem eigenen, ebenfalls verschlüsselten Schlüssel gesichert ist und Windows-Benutzer keine Pauschalberechtigungen erhalten, ist dies nicht einfach.

Darüber hinaus verschleiert das virtuelle Dateisystem von MOVEit DMZ die Identität der zugrunde liegenden Dateistruktur. Beispiele hierfür sind der Ersatz von Datei- und Ordnernamen durch zufällige IDs.

„ENTWICKLUNG UND IMPLEMENTIERUNG VON PRÜFMECHANISMEN ZUR ERKENNUNG VON UNBEFUGTEM ZUGRIFF UND ZUR VERBESSERTEN UNTERSUCHUNG VON STÖRFÄLLEN“

Der MOVEit DMZ-Server und der MOVEit Central-Client zeichnen Vorgänge wie Dateiübertragungen, Benutzer- und Ordnerverwaltung, Änderungen von Einstellungen, Anmeldungen und sichere Nachrichten aktiv auf. Bei auffälligen Ereignissen wie der Sperrung eines Benutzers nach zu häufiger Eingabe eines falschen Passworts können E-Mail-Benachrichtigungen an autorisierte Benutzer versendet werden.

Anstatt Protokolleinträge in langen Textdateien zu vermerken, werden die Prüfaufzeichnungen von MOVEit DMZ und MOVEit Central in einer einfach zugänglichen, gesicherten ODBC-Datenbank gespeichert.

Sowohl MOVEit DMZ als auch MOVEit Central sind mit einer Online-Screeningfunktion für Prüfaufzeichnungen ausgestattet. Offline-Prüfberichte lassen sich problemlos mit einer beliebigen Anzahl von Planungstools, einschließlich MOVEit Central, erstellen. Zur permanenten Speicherung außerhalb des Servers können Prüfaufzeichnungen auch archiviert werden.

Über die XML API-Schnittstelle des MOVE DMZ-Servers stellt der MOVEit API Windows-Client sicheren, programmatischen Zugriff auf HTTPS-Basis für die Erstellung, Verwaltung, Übertragung und Löschung von Dateien, Ordnern, Benutzern und Berechtigungen bereit. MOVEit API Windows ist eine COM-Komponente und offene Spezifikation, die für die Verwendung durch Windows-Entwickler konzipiert wurde. Es verfügt über eine kostenlose, vorkompilierte FTP-Client-Befehlszeilenschnittstelle und kann so durch Skripts und Batchdateien sowie durch geplante Aufgaben von Windows gesteuert werden. MOVEit API Windows ermöglicht die automatische Integritätsüberprüfung von Dateien mit SHA-1, die Komprimierung von Dateien und die Wiederaufnahme unterbrochener Dateiübertragungen.

„IDENTIFIZIERUNG UND VERHINDERUNG HÄUFIGER FEHLER UND SCHWACHSTELLEN“

Die meisten Schwachstellen von Software mit Internetverbindung entstehen durch die unangemessene Handhabung von Eingaben. Dazu gehören beispielsweise die in vielen C++-Programmen auftretenden Pufferüberläufe und die „SQL Smash“-Probleme vieler Datenbankanwendungen. Um diese zu vermeiden, bereinigt MOVEit DMZ eingehende Informationen und formatiert sie so, dass sie sicher zwischen den verschiedenen MOVEit-Komponenten übertragen werden können.

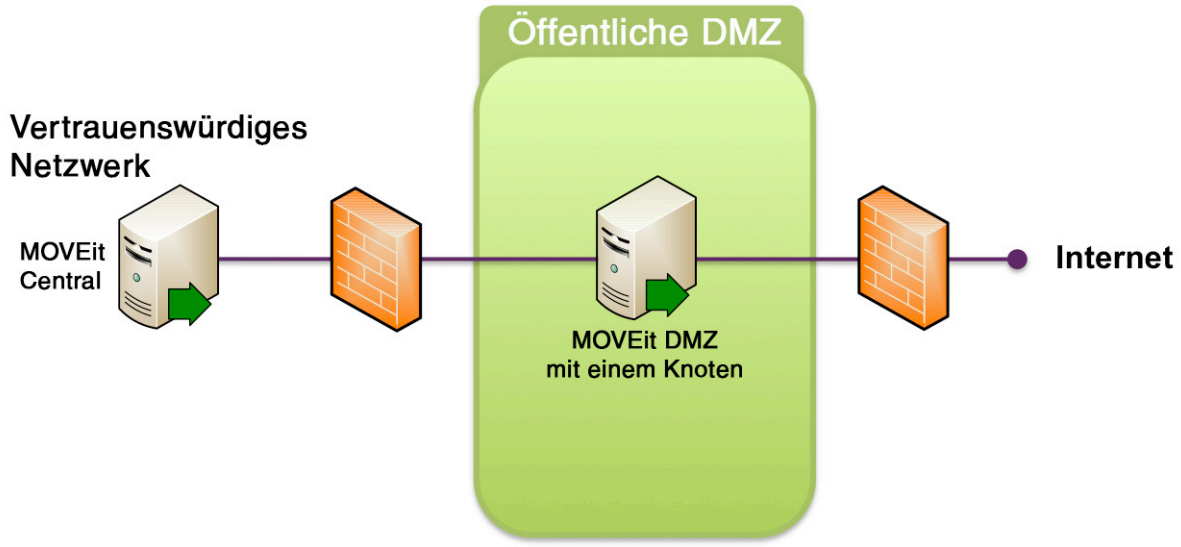
Um Angriffe auf die MOVEit-Produkte zusätzlich zu erschweren, werden keine sensiblen Informationen wie Versionsnummern oder interne Codes bekannt gegeben. So können unautorisierte Benutzer über die FTPS- (SSL) und SFTP- (SSH) Schnittstellen beispielsweise nicht auf den Produktnamen und die Versionsnummer von MOVEit DMZ zugreifen, und das Gerät kann so konfiguriert werden, dass auch Benutzer seiner Webschnittstelle keinen Zugang zu diesen Informationen haben. So können Eindringlinge nur schwer herausfinden, was sie angreifen – und welches die beste Vorgehensweise dafür ist.

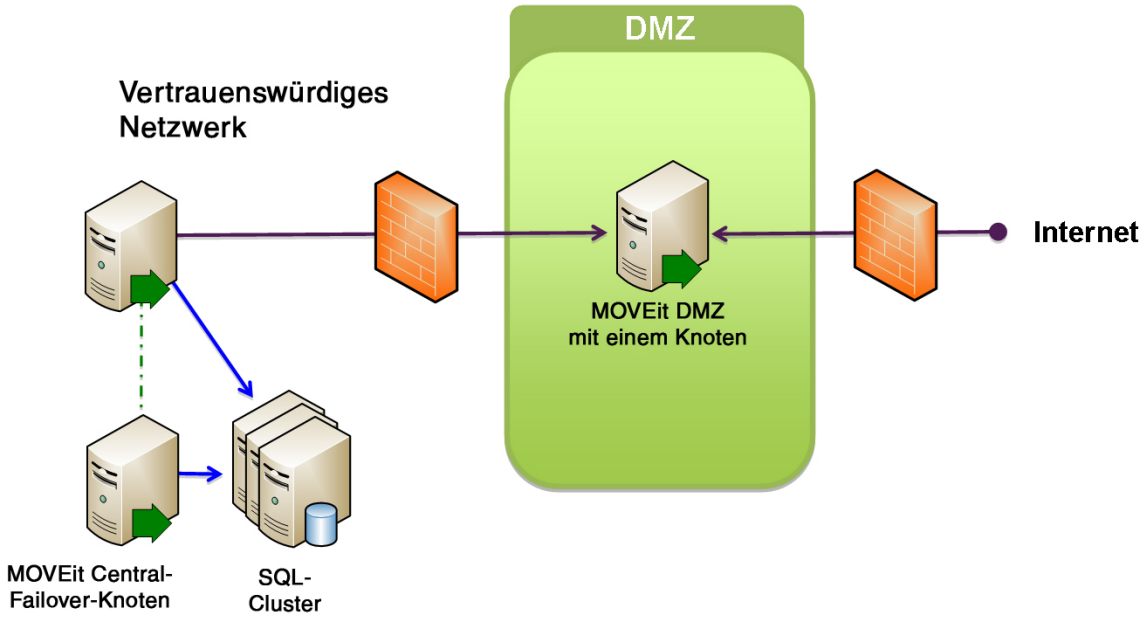
Obwohl MOVEit DMZ nicht direkt von dem zugrunde liegenden Windows-Betriebssystem abhängt, versucht es, dieses zu schützen. In den Installationsanweisungen für MOVEit DMZ wird beispielsweise die Verwendung automatisierter Sicherheitstools für das Betriebssystem empfohlen. Dazu gehören unter anderem:

- URLScan
- IIS Lockdown Tool
- Windows-Sicherheitsrichtlinien
- IPSec
- Automatische Aktualisierung von Windows

Die MOVEit DMZ-Dokumentation enthält Beispielkonfigurationen für die meisten dieser Tools. Außerdem verfügt das Produkt 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).

MOVEit Freely ist ein kostenloser Windows-Befehlszeilenclient, der Dateien über FTP und FTP über SSL (FTPS) mit Servern wie MOVEit DMZ austauschen kann, die diese Methoden unterstützen. MOVEit Freely Windows ermöglicht die Integritätsprüfung von Dateien mit SHA-1, die Komprimierung von Dateien und die automatische Wiederaufnahme unterbrochener Dateiübertragungen.





Weitere Informationen erhalten Sie bei der File Transfer Division von Ipswitch unter www.IpswitchFT.com.

IPSWITCH File Transfer
Simple. Secure. Managed.

File Transfer Division von Ipswitch kontaktieren