IPSWITCH

IPSWITCH Secure File Transfer

WS_FTP Secure File Transfer Backgrounder

Zusammenfassung

Der Transfer von Dateien ist Bestandteil des geschäftlichen Informationsaustausches. Allein schon aufgrund des gestiegenen Informationstransfers wird daher der Bedarf an einem vollständig abgesicherten Umgang mit den Daten immer dringender. Hinzu kommen die steigenden Anforderungen und das damit einhergehende Risiko auf Grund restriktiver gesetzlicher Vorgaben. Auch sie verlangen nach einer gesicherten und unverfälschten Übertragung von Informationen und Dateien. Um den dabei steigenden komplexeren Anforderungen zu begegnen, muss die Sicherheit als geschäftliche Grundlage fixiert und die Anwendung der Sicherheitsfunktionen auf der Applikationsebene implementiert werden. Die proaktive Einhaltung der Compliance-Forderungen reduziert die Kosten und erhöht die Wettbewerbsfähigkeit, in dem die Einhaltung der Regeln als elementare Anforderung festgeschrieben wird.

Sicherheitsanforderungen und Compliance

Informationen zur richtigen Zeit an die richtigen Mitarbeiter und Geschäftspartner zu bringen, wird für die Unternehmen immer wichtiger. Ein Weg, um den Informationsaustausch sicherzustellen, ist der direkte Transfer von Dateien zu den gewünschten Adressaten. Hierbei muss allerdings darauf geachtet werden, dass sowohl die Dateien als auch die Empfänger zweifelsfrei die Richtigen und Gewünschten, also authentisch sind.

Nicht zuletzt wegen gesetzlicher Vorgaben und derer zwingender Einhaltung, der Compliance, erhalten die Aspekte

- Vertraulichkeit und Nichtmanipulation (Integrität) der Informationen,
- Nachvollziehbarkeit der Aktionen und Abläufe,
- Authentizität der Absender, Empfänger und Informationen sowie
- Zuverlässigkeit und Verfügbarkeit des Systems einen wichtigen Stellenwert.

In den USA und Europa gibt es eine ganze Reihe von gesetzlichen Vorgaben, wie

- Health Information Portability
- Accountability Act (HIPAA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- BASEL II
- GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen)
- Bundesdatenschutzgesetz
- KontaG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- Signaturgesetz

Eine grundlegende Voraussetzung bei all den Verfahren ist die Sicherheit und Nachvollziehbarkeit oder Revisionssicherheit von geschäftlichen Abläufen. Dies kann z.B. bedeuten, dass nachgewiesen werden muss, wer wann die Möglichkeit zur Einsicht oder dem Verändern von Daten hatte. Überträgt man diese Anforderungen auf die IT-Belange, und hierbei insbesondere auf den Transfer von Dateien, so ist es nicht mehr damit getan, die Daten einfach zu übertragen; vielmehr muss der gesamte Vorgang nachvollziehbar und revisionssicher sein. Um dem zu begegnen, wird ein gesicherter Filetransfer notwendig, hierbei spricht man vom Secure File Transfer.

Historie des File Transfer Protokolls (FTP)

Einer der wichtigsten Standards zur Datenübermittlung, das File Transfer Protokoll (FTP), kann auf eine lange Tradition zurückblicken. Das Kommunikationsprotokoll basiert auf den Konzepten einer allgemein gängigen Kommunikation zwischen Computersystemen. Die Wurzeln reichen bis in das Jahr 1970 zurück. Die Technologie basiert auf den Forschungen die seinerzeit im MIT, dem Massachusetts Institute of Technology, vorgenommen wurden.

Eine weitere Rolle im Zusammenhang mit der Entwicklung des Standards spielt die Internet Engineering Task Force (IETF), eine Organisation, die sich mit der technischen Weiterentwicklung des Internets befasst. FTP verwendet nach dieser Definition zwei Kanäle, die auch als Ports bezeichnet werden: Je ein Kanal zum Senden und einer zum Empfangen der Daten.

Die ursprüngliche Definition des Protokolls sah kaum Sicherheitsvorkehrungen vor. Das Internet existierte noch nicht in der heutigen Form mit all seinen Bedrohungen, so wie wir es heute kennen. Mit der Verbreitung des Internets jedoch entstanden neue Gefahren, denen das bestehende Protokoll nicht gewachsen ist. So kennt FTP beispielsweise keine Vorkehrungen für eine gesicherte Benutzer-Authentifizierung. Stattdessen wird sowohl der Benutzername als auch das Passwort als ungeschützter Textstring übertragen und kann folglich durch Netzwerk-Analysatoren oder andere Angriffswerkzeuge ausgespäht werden. Noch gravierender ist die Tatsache, dass FTP keinerlei Vorkehrung zur verschlüsselten Übertragung von Dateien beinhaltet.

Werden Daten über öffentliche Leitungen unverschlüsselt übertragen, so können sie von potenziellen Angreifern mitgelesen werden. Beim „Man-in-the-middle“-Angriff beispielsweise positioniert sich der Angreifer zwischen dem Sender und Empfänger der Daten und greift diese durch geeignete Sniffing-Tools ab. Die heute auf dem FTP-Verfahren basierenden Kommunikationsverbindungen haben weder eine Vorkehrung zur Codierung der Daten noch bieten sie weiteren Schutz wie zum Beispiel eine Überwachung des gesamten Datentransfers.

FTP im Vergleich zu Email, Instant Messaging und Web-Download

Neben FTP können Dateien auch über Email, Instant Messaging (IM) oder Web-Download übertragen werden. Allerdings zeigen sich bei diesem Verfahren Restriktionen, die einem professionellem Einsatz im Unternehmen entgegen stehen.

Durch die einfache, angenehme und unkomplizierte Bedienung ist das Email-System zu einem wichtigen Pfeiler in Unternehmen geworden. Der Versand großer Datenmengen passiert meist als Email-Anhang. Um jedoch das Mailsystem nicht mit zu großen Datenaufkommen zu belasten, begrenzen manche Firmen die Größe der Anhänge auf einen Maximalwert. Dadurch werden größere Dateien nicht mehr korrekt zugestellt. Aufgrund der Zunahme von Spam und Viren werden außerdem Email-Anhänge verstärkt geprüft und auch aussortiert. Weitere Probleme liegen in einer schlechten Ausnutzung der zur Verfügung stehenden Ressourcen und einer umständlichen Verwaltung der transferierten Daten.

Die Grundfunktion des Instant Messagings (IM) ist der Austausch von Textnachrichten. Viele dieser Werkzeuge erlauben darüber hinaus auch den Versand von Dateien aus der Instant Messaging-Sitzung heraus. Probleme des IM für den Versand von Dateien liegen in der fehlenden Benutzer-Authentifizierung, dem fehlenden Schutz vor einer Manipulation der Daten beim Transfer und auch dem Datendiebstahl. Hinzu kommt eine fehlende oder umständliche Nachvollziehbarkeit der durchgeführten Aktion.

Auf vielen Webseiten gibt es heute Downloadbereiche vor allem für Dokumente (meist im PDF-Format), Software oder Multimedia-Dateien. Der Zugriff des Benutzers erfolgt über den Browser. Die Dateiübertragung kann über https verschlüsselt erfolgen. Problematisch ist die Benutzer- und Zugriffsrechteverwaltung, das Handling zum Einstellen neuer Dateien und die Automatisierung von Abläufen.

Secure Filetransfer

Unter Berücksichtigung der aktuellen Anforderungen an einen professionellen Informationsaustausch können die existierenden Verfahren, wie der herkömmliche FTP-Dateitransfer, Email, Instant Messaging und Web-Download, die Anforderungen nicht erfüllen. Die Dateien und Mailanhänge liegen verstreut auf den Speichermedien, ihre mehrfache Übertragung kostet Zeit und Ressourcen und Informationen über die Aktualität der parallel gespeicherten Dokumente gibt es nicht. Eine gemeinsame Verwaltung der Dokumente, die über die verschiedenen Kanäle wie Mailsystem oder Instant Messaging ausgetauscht werden, ist ebenfalls nicht vorhanden. Ganz zu schweigen von den Anforderungen an Vertrauensschutz, Datensicherheit, Zugriffsschutz oder Effizienz im gesamten Informationstransfer.

Ein robustes Werkzeug für den Dateitransfer muss daher ein Bündel an geeigneten Sicherheitskonzepten beinhalten, die alle Phasen der Informationshaltung und -übertragung umfassen: vor dem Transfer, beim Transfer selbst und auch die nachfolgenden Aktionen. Denn nur dann ist das Vertrauen in einen gesicherten Umgang mit den Daten zu gewährleisten.

Eine Möglichkeit, diesen Schutz zu erzielen, ist, die Daten generell zu verschlüsseln. Zwei gängige Verfahren, um die Übertragung der Daten abzusichern, sind die Protokolle von Secure Sockets Layer (SSL) und Secure Shell (SSH). Zur Sicherung der Daten auf dem Medium kann OpenPGP herangezogen werden. Viele Experten empfehlen für eine optimale Sicherheit und um die gesamte Kette abzusichern, die Kombination aus SSL oder SSH zusammen mit OpenPGP. Erst in der Kombination der beiden Verfahren erfolgt eine Sicherung der Daten auf dem Speichermedium als auch der gesicherte Transfer zum Zielsystem einer Übertragung.

WS_FTP und SSL (Secure Sockets Layer)

Das SSL-Protokoll, das ursprünglich von Netscape entwickelt wurde, ist heute ein weit verbreitetes Verfahren, um im Internet zwischen Webserver und Browser Sicherheitsanforderungen wie Authentisierung und Vertraulichkeit zu gewährleisten. SSL unterstützt die Verwendung von PKI-Zertifikaten zur gegenseitigen Zertifizierung von Server und Client. Die Nutzdaten werden über symmetrische Schlüssel ver- und entschlüsselt, die jeweils für eine Übertragungs-Session dynamisch erzeugt werden (Hybrid-Verfahren).

SSL erlaubt, in Kombination mit FTP, eine verschlüsselte Datenübertragung über Standard FTP-Verbindungen. Man nennt diese Verfahren FTPS oder „Secure FTP über SSL“.

WS_FTP und SSH (Secure Shell)

Secure Shell (SSH) stellt ein weitverbreitetes Protokoll zur sicheren Übertragung von Daten zwischen Computern dar, und wird auch für gesicherte FTP-Verbindungen herangezogen. Hierfür werden die Begriffe SFTP oder "SSH File Transfer Protocol" verwendet. SFTP verwendet SSH2 (Secure Shell 2) als Verschlüsselungs-Protokoll. Dabei wird, um einen sicheren Dateitransfer zu erreichen, eine FTP-Verbindung emuliert.

SSH wird heute von den meisten Computern unterstützt. Da SSH nur einen einzigen Port für den Upload und Download von Dateien benötigt, sind keine komplizierten Firewall-Eingriffe erforderlich. Durch die integrierte Datenkomprimierung bei der Übertragung sorgt SFTP für eine schonende Nutzung der Netzwerkbandbreiten.

WS_FTP und OpenPGP (Pretty Good Privacy)

SSL und SSH verschlüsseln die Daten bei der Übertragung. OpenPGP hingegen wird verwendet, um die einzelnen Dateien im Speichersystem zu verschlüsseln. Um Daten zu verschlüsseln, benötigt der Absender den öffentlichen Schlüssel des Empfängers. Da diese Verschlüsselung ausschließlich mit dem privaten Schlüssel des Empfängers wieder entschlüsselt werden kann, ist sichergestellt, dass die Daten nicht in falsche Hände geraten. Umgekehrt werden Dateien mit dem privaten Schlüssel des Absenders signiert. Der Empfänger überprüft dann die Signatur mit dem öffentlichen Schlüssel des Absenders.

Symmetrische und Asymmetrische Verschlüsselungsverfahren

Bei symmetrischen Verschlüsselungsverfahren wird derselbe Schlüssel für den Verschlüsselung- und den Entschlüsselungsvorgang verwendet. Dies bedeutet, dass der Sender und der Empfänger der verschlüsselten Nachricht über denselben Schlüssel verfügen muss. Symmetrische Verschlüsselungsverfahren sind sehr leistungsfähig haben aber das grundsätzliche Risiko, dass der Schlüssel mehrfach vorkommt.

Mitte der 70er Jahre hatten die Forscher Whitfield Diffie und Martin Hellman eine grundlegend neue Idee. Sie entwickelten die ersten asymmetrischen Kryptoverfahren, auch Public-Key-Verfahren genannt. Jeder Teilnehmer (das kann eine Person oder auch ein Rechner oder ein Terminal sein) bekommt ein Schlüsselpaar zugeordnet, das aus dem öffentlichen Schlüssel (Public Key) und dem privaten Schlüssel (Private Key) besteht. Der Public Key eines Teilnehmers wird allen potenziellen Kommunikationsteilnehmern bekannt gemacht. Der Private Key hingegen wird geheim gehalten und ist ausschließlich im Besitz des Teilnehmers. Zwischen den beiden Schlüsseln besteht eine mathematische Beziehung. Jedoch ist es mit an Sicherheit grenzender Wahrscheinlichkeit nicht möglich, den privaten Schlüssel aus dem Wissen des öffentlichen Schlüssels zu berechnen. Im Gegensatz zu symmetrischen Verfahren ist kein vertraulicher Austausch eines Secret Key mehr notwendig.

Bei der Verschlüsselung dient der öffentliche Schlüssel zur Verschlüsselung von Nachrichten an den diesem Schlüssel zugeordneten Teilnehmer. Nur mit dem zum Public Key gehörenden Private Key des Teilnehmers kann die Nachricht entschlüsselt werden.

Ein weiteres Sicherheitsziel, das durch asymmetrische Verfahren verwirklicht wird, ist die Authentifizierung und Signatur. Ein Teilnehmer kann sich durch Verwendung des privaten Schlüssels gegenüber anderen (z.B. einem IT-System) authentisieren, d.h. nachweisen, dass er wirklich der ist, für den er sich ausgibt, und den Inhalt signieren (digital unterschreiben).

Wichtige Standards in Zusammenhang mit asymmetrischen Verschlüsselungsverfahren sind X.509 und PGP. Bei X.509 wird die Zuordnung eines asymmetrischen Schlüsselpaares zu einer Person oder einem IT-Objekt, wie einen Webserver, von einer vertrauenswürdigen Instanz zertifiziert. Die Zertifikate sind von dieser Zertizierungsinstanz, auch Certificate Agency oder Trust Center genannt, digital signiert.

Pretty Good Privacy (PGP), ursprünglich von Phil Zimmermann 1981 entwickelt, kennt keine Zertifizierungsinstanz. Der Teilnehmer entscheidet selbst, welchem öffentlichen Schlüssel er vertraut und übernimmt die Rolle der Zertifizierungsinstanz (CA), indem er selbst im Vertrauensfall den öffentlichen Schlüssel eines anderen signiert. OpenPGP ist eine Variante, die auf PGP 5.x zurückgeht und 1998 im Open Source Umfeld entstanden ist.

Asymmetrische Verschlüsselungen sind aufwendiger durchzuführen als symmetrische. Deshalb verwendet man häufig sogenannte Hybridverfahren. Das asymmetrische Verfahren wird zur gegenseitigen Authentisierung und zur verschlüsselten Übertragung eines symmetrischen Schlüssels verwendet, der jeweils dynamisch für eine Übertragungs-Session erzeugt wird. Mit diesem Schlüssel werden die Nutzdaten verschlüsselt und entschlüsselt. Der Vorteil eines Hybridverfahren liegt darin, dass die in der Regel schnelleren symmetrischen Verfahren zur Ver- und Entschlüsselung der Nutzdaten verwendet werden können, während die asymmetrische Kryptographie eine sichere Verteilung des verwendeten Schlüssels ermöglicht. OpenPGP gehört zu den hybriden Verfahren.

WS_FTP und SHA (Secure Hash Algorithmen)

Durch integrierte Datei-Integritäts-Prüfungen (File Integrity Checking) wird sichergestellt, dass die Übertragung korrekt vorgenommen wurde und die Dateien auf dem Weg vom Sender zum Empfänger nicht verändert wurden. SHA stellt somit sicher, dass die gesendete Datei mit der empfangenen exakt übereinstimmt. Die dazu verwendeten Prüfverfahren sind die Secure Hash Algorithmen wie etwa SHA-1, SHA-256 und sogar SHA-512.

WS_FTP und Audits

Über ein leistungsfähiges Logging-Tool werden alle Client-/ Servertransaktionen inklusive der Administratoreingriffe festgehalten. Die Weitergabe der Daten zur Auswertung ist über die Syslog Standardschnittstelle sowie über Exportfunktionen möglich. Damit lassen sich problemlos Audits zur Compliance-Überprüfung durchführen.

WS_FTP und Berechtigungsmanagement

Über ein differenziertes Berechtigungsmanagement erfolgt ein fein granulierter Zugriff auf Dateien, Ordner-Gruppen, Speichervolumen, Dateianzahl und Bandbreitengebrauch. Die Übernahme von Benutzerdaten aus dem Active Directory wird unterstützt. Eine sichere Benutzerauthentisierung wird durch Passworte mit Komplexitätsvorgabe sowie durch ein vorgegebenes Verfallsdatum erreicht.

WS_FTP und Hochverfügbarkeit

Durch das gesamte Instrumentarium, wie Hardware- und Softwareredundanz, Clustering, automatische Wiederholungen und Loadbalancing können hochverfügbare FTP-Infrastrukturen realisiert werden, die sich für unternehmenskritsche Anwendungen einsetzen lassen. Durch eine Automatisierung von Abläufen unter Verwendung von Regeln und Triggern ist eine Integration in übergreifende Geschäftsprozesse möglich.

IPSWITCH
10 Maguire Road
Lexington, MA 02421
(781) 676-5700

Zekeringstraat 17
1014 BM Amsterdam
The Netherlands

IPSWITCH