Anwendungszenarien WS_FTP Server 6

Der WS_FTP Server mit SSH von Ipswitch macht FTP zu einer IT-Infrastruktur Komponente, die mit geringen Kosten neue, auch unternehmenskritische Einsatzgebiete erschließt. Die Anforderungen nach Sicherheit und Compliance sowie Integration und Prozessunterstützung werden erfüllt.

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.

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 1970 am MIT, dem Massachusetts Institute of Technology, entwickelt wurden. Eine Weiterentwicklung des Standards erfolgte dann durch die Internet Engineering Task Force (IETF).

Mit der starken Verbreitung des Internets in den vergangenen Jahren entstanden neue Gefahren, denen das bestehende Protokoll nicht gewachsen war. Die ursprüngliche Definition des Protokolls sah kaum Sicherheitsvorkehrungen vor. Auch war FTP nicht darauf ausgelegt, Abläufe zu automatisieren und Geschäftsprozesse zu unterstützen.

Mit dem WS_FTP Server 6 mit SSH von Ipswitch werden die Anforderungen nach Sicherheit und Compliance sowie Integration und Prozessunterstützung erfüllt. Damit werden neue Einsatzgebiete erschlossen. FTP / SSH wird zu einer wichtigen Komponente heutiger und künftiger IT-Infrastrukturen und -Architekturen.

Anforderungen von Unternehmen an Integration und Prozessunterstützung

Die IT-Systemlandschaften in den meisten Unternehmen sind heterogen gewachsen. Für unterschiedliche Anwendungen, wie etwa Enterprise Resource Planning (ERP) im kaufmännischen Bereich, Customer Relationship Management (CRM) in Marketing und Vertrieb sowie Supply Chain Management (SCM) und Management Executive Systems (MES) in Logistik und Fertigung sind unterschiedliche Systeme im Einsatz. Die IT-Infrastrukturen sind darauf ausgerichtet die Geschäftsprozesse eines Unternehmens durchgängig und effizient zu unterstützen. Darüber hinaus besteht die Anforderung die eigenen Prozesse mit denen von Kunden und Lieferanten zu übergreifenden Prozessen zu verbinden. Vor diesem Hintergrund ist Integration heute eine Herausforderung für die IT. Auch muss die IT immer schneller und flexibler auf veränderte Markt- und organisatorische Anforderungen der Anwender reagieren. Dies erfordert entsprechende Infrastrukturen und Architekturen.

Service orientierte Architekturen (SOA) bieten heute Lösungen für umfangreiche Integrationsanforderungen. SOA ist ein Architekturansatz, der sich an den Geschäftsprozessen orientiert. Software Services (Anwendungsfunktionen) werden einzelnen Prozessschritten zugeordnet. Damit wird die IT näher an die Betriebswirtschaft herangebracht und bietet den Unternehmen die Möglichkeit, sich flexibel an die sich schnell verändernden Anforderungen anzupassen.

Das herkömmliche FTP ist weit von solchen Integrationslösungen entfernt. Mit FTP wird eine Punkt-zu-Punkt Daten-Integration zwischen unterschiedlichen Systemen ermöglicht. Die Benutzer laden über den FTP-Client Dateien vom FTP-Server auf ihre Systemumgebung herunter oder übertragen Dateien zum Server, damit andere diese Dateien in ihre jeweilige Systemumgebungen downloaden. In dieser Funktion ersetzt FTP auf komfortable Weise den manuellen Austausch von Datenträgern.

WS_FTP Server 6 ermöglicht die Automatisierung von Abläufen.

Im Zusammenspiel von WS_FTP Server und WS_FTP Client können durch Definition von Regeln und das Setzen von Triggern Abläufe auch über mehrere Schritte, ohne dass ein Benutzer eingreifen muss, automatisiert werden. Der automatisierte entkoppelte Datenaustausch mit FTP Server 6 mit SSH in Verbindung mit XML als Dateiformat ermöglicht die Lösung von durchaus anspruchsvollen Integrationsaufgaben. Über das WS_FTP Berechtigungsmanagement kann der Zugriff auf Dateien und Ressourcen differenziert gesteuert werden. Bei Auftreten von Fehlern wird an den Administrator automatisch eine entsprechende Mitteilung abgesetzt.

Verbindet man diese Funktionalitäten mit den Verschlüsselungsverfahren SSH und PGP, nutzt PGP auch zur Signatur von Dateien und stellt damit deren Authentizität sicher, und betreibt dieses System auf einem hochverfügbaren Server, dann kommt die Mächtigkeit des WS_FTP Server 6 in einer unternehmensweiten IT-Infrastruktur/ Architektur zum Ausdruck.

Der WS_FTP Server 6 lässt sich auch in eine umfassendere Service orientierte Architektur (SOA) integrieren. Der Zugriff auf den Server (Up- und Download) wird dabei als ein Service definiert, der in eine Kette von Services eingebunden ist, über die ein Geschäftsprozess definiert ist.

Konkreter Einsatz: WS_FTP Server 6 unterstützt die Bestellabwicklung bei ALSO, dem führenden Distributor und Logistikdienstleister für die Branchen IT, Unterhaltungselektronik und Telekommunikation in der Schweiz.

Der Bestellabwicklungsprozess bei ALSO sieht vor, dass der Händler seine Aufträge online am Web-Portal erfasst, die Aufträge zur Abwicklung in das Warenwirtschaftsystem von ALSO übertragen werden, und der Händler nach Prüfung der Warenverfügbarkeit im Minutenzeitfenster seine Auftragsbestätigung mit Liefertermin zurück erhält.

Der WS_FTP Server, der zur Unterstützung dieses Prozesses zum Einsatz kommt, wird vom Internet Service Provider (ISP) gehostet. Das Warenwirtschaftssystem und der FTP-Client werden von der ALSO–IT Organisation betrieben. Loggt sich ein Fachhändler in das Portal ein, ruft das Warenwirtschaftssystem den FTP-Client auf, der den Bestellablauf über den WS_FTP Server beim ISP triggert. Um einen sicheren Datentransfer herzustellen, wird dabei eine FTP-Verbindung emuliert. Da SSH nur einen Port für Up- und Download von Daten benötigt, sind keine besonderen Firewall-Eingriffe erforderlich.

Anforderungen von Unternehmen an Sicherheit und Compliance

Die Compliance, und damit die Sicherstellung der Konformität zu den vielfältigen gesetzlichen Regelungen, betrieblichen Vorgaben und Anforderungen seitens der Kunden, wird für die Unternehmen zu einer immer wichtigeren Aufgabe.

Beispiele für gesetzliche Vorgaben sind:

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

Wichtige Standards und Regelwerke auf dem Gebiet der Information Security sind:

- ISO 17799
  (Anleitung für die Praxis des Managements für Informationssicherheit)

- ISO 27001
  (Basis für die Auditierung und Zertifizierung von Information Management Systemen)
- IT-Grundschutzhandbuch und
- ITIL (Information Technology Infrastructure Library)

Für alle diese Regelungen grundlegend ist die Forderung nach 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. Hohe Anforderungen werden in diesem Zusammenhang auch an

- die Vertraulichkeit und Nichtmanipulation (Integrität) von Informationen,
- die Sicherstellung der Authentizität von Absendern und Empfängern von Informationen sowie
- die Zuverlässigkeit und Verfügbarkeit der eingesetzten Hard- und Software gestellt.

Der herkömmliche FTP-Standard kennt 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.

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.

WS_FTP Server 6 erfüllt all diese Anforderungen nach Compliance und Security durch Verwendung von leistungsfähigen Verfahren, wie SSL, SSH, SHA und OpenPGP.

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

Mit Hilfe eines leistungsfähigen Logging-Tools 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.

Durch das gesamte Instrumentarium, wie Hardware- und Softwareredundanz, Clustering, automatische Wiederholungen und Loadbalancing können hochverfügbare FTP-Infrastrukturen realisiert werden, die sich für unternehmenskritische Anwendungen einsetzen lassen.

Hintergrundinformationen zu den eingesetzten Verfahren und Standards: SSL (Secure Sockets Layer), SSH (Secure Shell), SHA (Secure Hash Algorithmen) und PGP (Pretty Good Privacy)

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“.

Secure Shell (SSH) stellt ein weit verbreitetes 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.

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. Die dazu verwendeten Prüfverfahren sind die Secure Hash Algorithmen, wie etwa SHA-1, SHA-256 und SHA-512. Diese stellen sicher, dass die gesendete Datei mit der empfangenen exakt übereinstimmt.

SSL und SSH verschlüsseln die Daten bei der Übertragung. OpenPGP hingegen wird verwendet, um die einzelnen Dateien im Speichersystem zu verschlüsseln. OpenPGP ist eine Variante von PGP (Pretty Good Privacy), die im Open Source Umfeld entstanden ist. 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. PGP benötigt keine Zertifizierungsinstanz. Die Erzeugung des Schlüsselpaars (privat und öffentlich) erfolgt durch den WS_FTP Client auf Veranlassung des Benutzers. Dieser entscheidet auch selbst darüber, welchem öffentlichen Schlüssel eines anderen Benutzers er vertraut.