

Managed File Transfer bietet bei großen Datentransfers den besten Schutz

Datenübertragung – ein unterschätztes Sicherheitsrisiko

Virenschutz, Spam, Hacker-Angriffe – diese Begriffe fallen, wenn das Thema IT-Sicherheit in Firmen zur Sprache kommt. Ein Aspekt wird hierbei vor allem in großen Unternehmen sträflich vernachlässigt: die sichere Übertragung von Daten.

Egal, ob interner File Transfer, die Kommunikation mit Geschäftspartnern oder versendete Kundeninformationen – dieser Bereich der IT-Sicherheit gewinnt stetig an Bedeutung. Die Tatsache, dass der überwiegende Teil der heute transferierten Daten sowohl von geschäftskritischer als auch sensibler Natur ist, wird jedoch von den meisten Unternehmen unterschätzt. Dabei steigt die Zahl vertraulicher Informationen wie Kreditkarten- oder Sozialversicherungsnummern weiter an. Auch für Energieversorger können Nachlässigkeiten bei der Datenübertragung schnell zu einem unangenehmen Problem werden.

Drei Maßnahmen für mehr Sicherheit

Für große Unternehmen sind vor allem drei Punkte im Zusammenhang mit File Transfer von besonderer Bedeutung: die sichere Übertragung von Daten, die Einhaltung von Compliance-Vorschriften und das Sicherstellen des erfolgreichen File Transfers. Mit der Abdeckung dieser Punkte lassen sich die größten Sicherheitsrisiken minimieren. Das geeignete Mittel hierfür ist die Implementierung eines Managed-File-Transfer-Produkts, das in die automatisierten IT-Prozesse eingebunden wird.

Viele Unternehmen setzen heute das gängige File Transfer Protocol (FTP) ein. Der scheinbare Vorteil: Es ist eine kostenlose Möglichkeit, Daten zu transferie-

ren. Dieses Argument verliert jedoch schnell an Zugkraft, wenn man betrachtet, welche teils immensen hohen Wartungs- und Managementkosten dieses Verfahren mit sich bringt. Zudem ist FTP ein extrem unsicheres Verfahren, um Daten von A nach B zu schicken.

Wichtig bei der sicheren Übertragung von Daten hingegen ist, dass die gängigen Managed-File-Transfer-Lösungen die Kommunikation zwischen Sender und Empfänger per SSL- oder SSH-Verschlüsselung schützt. Zudem sollte das Produkt über eine Daten-Authentifizierung verfügen. Diese stellt sicher, dass die Daten ihr Ziel so erreichen, wie sie abgeschickt wurden.

Ein weiterer Punkt: Die Kommunikation über mehrere unterschiedliche Plattformen hinweg ermöglicht auch immer einen Zugriff von außen auf die übertragenen Informationen. Daher ist es für Unternehmen wichtig, die Übertragungswege sicher zu verschlüsseln und darauf zu achten, möglichst wenige solcher Nahtstellen zwischen den einzelnen Welten zu haben.

Unerlaubte Zugriffe von Mitarbeitern stellen ein sehr großes Sicherheitsrisiko dar: Auf physikalischen Datenträgern wie USB-Sticks oder selbstgebrannten CD-ROMs lassen sich vertrauliche Unternehmensdaten entwenden. Aber auch offene Übertragungswege wie FTP bieten ein Einfallstor für solchen Missbrauch.

Einhaltung von Compliance-Vorschriften

Nutzt ein Unternehmen eine heterogene IT-Umgebung, benötigt es eine Strategie für den Austausch von Daten. Denn die Compliance-Richtlinien zur Einhaltung von gesetzlichen Vorgaben steigen stetig an. Ebenfalls ist nicht jedem bekannt, dass beim Bruch der Compliance-Regeln Verantwortliche und Ge-

schäftsführer persönlich haften können.

Nationale und internationale Gesetze wie der Sarbanes-Oxley Act (SOX) oder die 8. EU-Richtlinie sehen die Sicherheit von Daten als oberste Priorität an. Unternehmen müssen vorweisen können, welche Maßnahmen sie ergreifen, um Datenverluste zu vermeiden. Hierfür braucht ein Unternehmen einen vollständigen Einblick in die Datentransfer-Prozesse. Nur so kann es fehlerhafte oder unvollständige Übertragungen nachvollziehen. FTP scheidet bei solchen Vorgaben aus.

Sicherstellen des erfolgreichen File Transfers

Managed File Transfer erfüllt auch eine weitere Seite der IT-Sicherheit: Für ein Unternehmen ist es essentiell, dass die Übertragung von Daten auch tatsächlich erfolgreich abgeschlossen ist. Wenn Daten verloren gehen, bedeutet dies nicht nur einen Verlust von möglicherweise sensiblen Informationen. Es entstehen gleichzeitig Zusatzkosten durch Zeitverlust, erhöhten Personalaufwand oder finanzielle Einbußen, etwa durch Abrechnungsverzögerungen.

Wichtig ist auch die Nachverfolgung von Fehlern im Betrieb. Ein Managed-File-Transfer-Produkt sollte in der Lage sein, den Verantwortlichen einen durchgängigen Überblick über die gesamte IT-Infrastruktur zu geben. Dadurch lassen sich Abläufe steuern und überwachen und eine Fehlerdiagnose betreiben.

Unternehmen, vor allem solche mit vielen Datentransfers, sollten überprüfen, auf welche Weise sie ihre Dateien verschicken. Die Gefahren und Anforderungen nehmen immer mehr zu. Ein Umstieg auf neue, sichere Lösungen ist daher für einen risikominimierten Datentransfer alternativlos.

Christoph Maier, Stonebranch GmbH, Hannover
www.stonebranch.com