

# Wasserdichter Datenaustausch

Industriespionage hat Hochkonjunktur. Wissensvorsprung ist gerade jetzt ein bedeutender Wettbewerbsvorteil. So steht der Datentransfer großer und mittelständischer Unternehmen immer stärker im Fokus ausländischer Nachrichtendienste.

TEXT: Jochen Werner FOTOS: Sterling Commerce

Der Kalte Krieg ist ausgekämpft – stattdessen erleben wir einen globalen Wirtschaftskrieg. Das umkämpfte Gut sind Daten: So feilen zum Beispiel in vielen großen wie auch mittelständischen Unternehmen Entwicklerteams an unterschiedlichsten Standorten an einem neuen Produkt oder einer bahnbrechenden Erfindung. Dabei tauschen sie Daten digital mit teilweise hohen Volumina oder hoher Sensibilität aus, etwa CAD-Dateien zu technischen Details oder Informationen zu Unternehmens- und Marktstrategien. Und das häufig ohne oder mit unzureichender Verschlüsselung und weiteren Sicherheitsvorkehrungen wie Authentisierung und dem Einsatz einer sicheren Übertragungssoftware.

Unkontrollierte und unkoordinierte Datenübertragung von sensiblen Informationen per E-Mail und File Transfer Protocol (FTP) gehört somit zur Tagesordnung und wird leichte Beute für Datendiebe. Laut Verfassungsschutzbericht 2008 sind zunehmend deutsche Unternehmen und Regierungsstellen Ziel von Wirtschaftsspionage. Nach Ansicht der Verfassungsschützer ist Deutschland wegen seiner wichtigen Rolle in der EU und der NATO sowie als Standort zahlreicher Unternehmen mit Spitzentechnologie für fremde Nachrichtendienste interessant. Der finanzielle Schaden durch Wirtschaftsspionage für die deutsche Volkswirtschaft lässt sich nicht genau beziffern, beträgt nach Schätzungen der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) aber jährlich mindestens 20 Milliarden Euro. Das Gefährdungspotenzial beziffert die ASW mit 50 Milliarden Euro.

## Zeit zu handeln

Nachrichten dieser Art sollten Unternehmen, die sensible und wertvolle Daten auf ihren Systemen gespeichert haben und mit Zweigstellen und Partnern austauschen,

wachrütteln. Doch sind die mit Datenverlusten verbundenen Umsatzeinbußen und eventuelle Vertrags- oder Konventionalstrafen nicht das Ende der Fahnenstange. Datenverluste schaden auch dem Image und der Glaubwürdigkeit derjenigen Unternehmen, die ihre Daten – darunter zum Teil auch sensible Kundendaten – schlampig absichern, was Fälle bei der Deutschen Telekom (17 Millionen Kundendaten von T-Mobile gestohlen) oder der Berliner Landesbank (Zehntausende Kundendaten bei Berliner Landesbank ausgespäht) belegen. Höchste Zeit, sich die Gefahr digitaler Angriffe ins Bewusstsein zu rufen und die eigenen Sicherheitsstrategien und -maßnahmen auf den neuesten Stand zu bringen.

Sicherheits-Projekte scheitern aber häufig an den damit verbundenen Kosten. Dieser allgemeingültige Trend wird derzeit noch verstärkt, denn in der aktuellen Wirtschaftskrise fahren nach einer internationalen Befragung der Wirtschaftsprüfungsgesellschaft Deloitte immer mehr Unternehmen ihre Budgets für IT-Sicherheit zurück. Die große Mehrheit der befragten Firmen scheinen die Risiken durch veraltete oder nicht existente Sicherheitstechnologien zu unterschätzen. So befürchten die Experten, dass die Unternehmen an der falschen Stelle sparen und in Zukunft durch wachsende Bedrohungen aus dem Internet Probleme bekommen könnten. Ein Grund für mehr anstatt weniger Investitionen. Betrachtet man die möglichen Folgekosten von Datenverlusten und dem damit verbundenen möglichen Datenmissbrauch, so liefern sinnvoll eingesetzte Security-Komponenten einen klaren Return-on-Investment (RoI) – das überzeugendste Argument für deren Anschaffung. Denn nur wenn entsprechende Sicherheitstechnologien im Hintergrund arbeiten, kann die IT ihr volles, gewinnbringendes Potenzial entfalten.



Deutsche Unternehmen werden immer häufiger Opfer von Industriespionage



Geldwert: Sterling Managed File Transfer ermöglicht Unternehmen einen sicheren Datentransfer

## Datenflut bringt Probleme mit sich

Der Austausch von Daten nimmt kontinuierlich zu und läuft in und zwischen Unternehmen nahezu permanent ab – sei es bei Datenbankaktualisierungen, Systemupdates von unterschiedlichen Zweigstellen oder beim Austausch mit Geschäftspartnern. Unternehmen setzen bei der Dateiübertragung jedoch häufig unsichere Verfahren ein, die sich nicht steuern lassen und allen möglichen Kommunikationsproblemen unterliegen können. Häufig basieren diese Verfahren auf FTP, das ohne spezielle Erweiterungen nur sehr wenig Sicherheit bietet und leicht abgefangen werden kann.

## Zeigt her eure Daten

So beinhalten Standard-FTP-Spezifikationen zum Beispiel keine Strong Authentication mit verschlüsselten Passwörtern und Sicherheits-Tokens. Werden die Login-Daten in Klartext übertragen, können sie leicht abgefangen und dann für den nicht autorisierten Zugang verwendet werden. Schlimmer noch: Weder die zu übermittelnden Daten noch die Verbindung sind verschlüsselt. Dadurch wird ein Man-in-the-Middle-Angriff möglich, und damit ein Ausspionieren der Daten während der Übertragung oder auf dem Server – eine große Bedrohung für die Datensicherheit und Chance für Hackerangriffe. Für die meisten Datenübertragungen ist Standard-FTP einfach nicht genug, da es große Mängel bei Sicherheit, Verwaltung, Monitoring und Prozesskontrolle gibt. Es gibt zwar zahlreiche Anbieter von Sicherheitserweiterungen für FTP und sicheren Alternativen

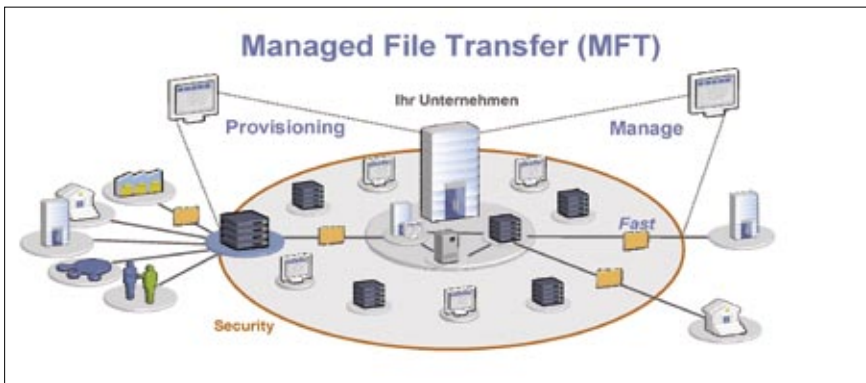
zu FTP. Beispiele hierfür sind Secure FTP (SFTP), FTP over the Secure Shell (SSH) und Secure Sockets Layer over Transport Layer Security (SSL/TLS). Doch können diese Erweiterungen, die mehr Sicherheit und Zuverlässigkeit bringen, zu Lasten der Effizienz, Kompatibilität und Flexibilität gehen.

## Den Datendieben ein Schnippchen schlagen

Es gibt bereits einige Unternehmen, die sich über die Sensibilität und Wichtigkeit der Daten, die sie untereinander austauschen, durchaus im Klaren sind. Sie haben Pionierarbeit geleistet, wenn es darum geht, die Defizite von FTP auszumerzen und effektivere Sicherheitstechnologien zu implementieren. Mittlerweile zeichnet sich ein Trend zum Einsatz so genannter Managed-File-Transfer-(MFT)-Produkte ab.

Darunter versteht man den kontrollierten, sicheren und planbaren Dateitransport von einem Ort zu einem anderen. Diese Lösungen punkten durch Sicherheit, Prognose-Funktionalität und effektives Datenmanagement innerhalb und außerhalb der Unternehmen. Ausgestattet mit zusätzlichen Verschlüsselungsdiensten lassen sich Datenpakete bereits während der Übertragung sichern. Zudem reduziert sich der manuelle Eingriff – meist das schwächste Glied innerhalb der gesamten Sicherheitskette – auf ein Minimum. Dass MFT eine sehr verlässliche und sichere Art der Datenübertragung ist, zeigt folgendes Beispiel: Bisher gab es noch keinen unautorisierten Zugriff auf das proprietäre und sichere Connect-Direct-Protokoll, das Sterling Commerce bei seiner Managed-File-Transfer-Lösung einsetzt.

Ein Plus an Sicherheit beim Managed-File-Transfer bieten von einigen Anbietern bereitgestellte Proxy-Lösungen. >



**Mindestens 20 Milliarden Euro jährlich verlieren deutsche Unternehmen durch Wirtschaftsspionage und deren Folgen**

Diese arbeiten in der DMZ (Demilitarized Zone – entmilitarisierte Zone) zwischen Firewalls und trennen das Internet von den Unternehmensressourcen. Der Dateitransfer aus dem öffentlichen Internet in das Unternehmen wird abgesichert, indem strikte Kontrollen, zum Beispiel Autorisierung von Handelspartnern, Multi-Faktor-Authentisierung und Sitzungsunterbrechung implementiert werden, bevor die Daten in die Sicherheitszone des Unternehmens gelangen können.

### Ganzheitliche Sicherheitsstrategien sind gefragt

Doch alle Anstrengungen bei der Realisierung eines sicheren Datenaustauschs bringen nichts, wenn keine übergeordnete Sicherheitsstrategie existiert und andere „Baustellen“ vernachlässigt werden. So werden in vielen Unternehmen noch immer die verschiedenen Aspekte der IT-Sicherheit voneinander getrennt betrachtet. Auf der einen Seite die strategische Ausprägung in Form von Sicherheitskonzepten und Richtlinien und auf der anderen Seite – davon losgelöst – die technischen Sicherheitsmaßnahmen wie Firewalls, Verschlüsselungssysteme oder Virenschutz. Unternehmen müssen zur Schaffung maximaler IT-Sicherheit darauf achten, dass Sicherheitskonzepte und Sicherheitsmaßnahmen nicht als Insellösungen betrachtet werden. Sie sind vielmehr im Gesamtkontext zu betrachten. Nur so kann ein lückenloser Schutz und ein einheitliches Sicherheitsniveau für alle zu schützenden Komponenten gewährleistet werden. Denn wie gut die IT-Sicherheit eines Unternehmens ist, bestimmt das schwächste Glied in der Security-Kette.

Neben der reinen Technik spielt der Mitarbeiter eine große Rolle, der in den Sicherheitsprozess einbezogen werden muss. Mitarbeiter müssen dahingehend geschult werden, wann ein Sicherheitsverstoß vorliegt und welches Verhalten hierbei angebracht ist. Darüber hinaus müssen die eingesetzten Instrumente kontinuierlich getestet und kontrolliert werden, denn mit ständigen Änderungen des eigenen Geschäftsumfeldes entstehen neue Bedrohungen und treten weitere Schwachstellen zu Tage. Hinzu kommt: Da die ei-

genen Unternehmensgrenzen zunehmend verschwimmen und Memory Sticks oder iPods weit verbreiteten Einsatz finden, spielt die Perimeter-Sicherheit – die Sicherheit an den Nahtstellen, die das Unternehmensnetz mit der Öffentlichkeit verbinden – eine große Rolle bei jeder Sicherheitsstrategie. Weit verbreitet ist beispielsweise die Praxis, vertrauliche Daten auf USB-Laufwerke zu kopieren, um mobil und flexibel mit den kopierten Daten weiterarbeiten zu können – Verbote hin oder her! In Zukunft könnte es für Unternehmen sogar noch schwieriger werden, IT-Sicherheitsmaßnahmen effektiv durchzusetzen, denn mit der zunehmenden Nutzung mobiler Technologien steigt auch das Risiko, dass vertrauliche Daten in falsche Hände geraten – sei es durch gezielten Diebstahl oder Verlust der Datenspeicher durch Schusseligkeit der Mitarbeiter.

### Zusammenfassung

Fest steht: Das eigene Sicherheitskonzept muss sowohl mit den aktuellen und kommenden Risiken, den notwendigen Abwehr-Technologie als auch mit dem Einsatz im Tagesgeschäft wachsen. Die Sicherheit bei der Datenübertragung besitzt bei einer Gesamtbetrachtung einen hohen Stellenwert, sind mit ihr doch häufig weitreichende Konsequenzen verbunden. Wenn also die Controlling-Abteilung oder die Geschäftsführung die Kosten für die Sicherheitstechnologien unter die Lupe nimmt, sollte stets bedacht werden, dass Sicherheit einen wichtigen Beitrag zur Produktivität und Wettbewerbsfähigkeit leistet und letztendlich einen klaren Return-on-Investment mit sich bringt. □

### Quellen

- [1] Verfassungsschutzbericht 2008 (Vorabfassung), Bundesministerium des Innern, Mai 2009
- [2] Berthold Stoppelkamp, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW), Interview in Mitteldeutschen Zeitung, 19.05.2009
- [3] Welt: „17 Millionen Kundendaten von T-Mobile gestohlen“, 04. Oktober 2008 <http://www.welt.de/wirtschaft/article2528875/17-Millionen-Kundendaten-von-T-Mobile-gestohlen.html>
- [4] Spiegel: „Zehntausende Kundendaten bei Berliner Landesbank ausgespäht“, 12.12.2008 <http://www.spiegel.de/wirtschaft/0,1518,596200,00.html>
- [5] „Losing Ground – 2009 TMT Global Security Survey“, Deloitte, Mai 2009

> MORE@CLICK SIK10078