



## Mehr Sicherheit für Mitarbeiterdaten

Personalabteilungen stecken in einem Dilemma: Auf der einen Seite müssen sie sicherstellen, dass die Daten von Mitarbeitern keinem Unbefugten in die Hände fallen. Auf der anderen Seite sollen auch andere Abteilungen oder externe Dienstleister auf solche Informationen zugreifen können. Die Human Resources-Abteilung von Fujitsu Technology Solutions fand eine Lösung: Sie setzt den elektronischen Datentresor ein.

**B**erichte über den fahrlässigen Umgang von Unternehmen und Behörden mit Mitarbeiterdaten häufen sich. So kamen dem britischen National Health Service im September vergangenen Jahres mehrere CD-ROMs mit den persönlichen Daten von insgesamt rund 18 000 Mitarbeitern abhanden. Vermutlich gingen die Datenträger beim Versand per Post verloren. Im Jahr 2006 verschwand dagegen eine CD-ROM mit den Stammdaten von 8000 Beschäftigten der IT-Sicherheitsfirma McAfee. In diesem Fall war ein Mitarbeiter der Wirtschaftsprüfungsgesellschaft Deloitte für den Verlust verantwortlich, die für McAfee tätig war.

„Der Schutz personenbezogener Daten hat für uns oberste Priorität“, sagt Hartmut Semmler, Senior Director und Head of HR Payroll and Expert Services bei Fujitsu Technology Solutions (FTS). Das Unternehmen zählt zu den größten Anbietern von IT-Lösungen in Europa. FTS, das am 1. April 2009 aus Fujitsu Siemens Com-

puters hervorging, unterhält in Deutschland 14 Standorte. „Zwischen der Zentrale und den Niederlassungen werden häufig Personalunterlagen, Arbeitsverträge und andere vertrauliche Dokumente ausgetauscht“, erläutert Semmler. „Das muss auf eine Weise geschehen, die schnell, zuverlässig und vor allem sicher ist.“ In diesen Kommunikationsprozess sind auch Externe mit einbezogen. „Wir arbeiten eng mit Partnerfirmen und Dienstleistern zusammen“, sagt Hartmut Semmler, „außerdem mit diversen Betriebsprüfern, Auditoren, Aktuarien und Wirtschaftsprüfern beim Jahresabschluss.“ All diese Personengruppen benötigen regelmäßig Zugang zu vertraulichen Unterlagen von FTS.

### Unsicherheit bei CD-ROM- und E-Mail-Versand

Der Transport der sensiblen Daten erfolgte Jahre lang auf eine Weise, die in vielen Unternehmen üblich ist: Entweder wurden Dokumente auf CD-ROMs

gebrannt und von einem Kurier zu den Empfängern transportiert oder die Mitarbeiter der HR-Abteilung hängten die Dateien mit einfacher Dokumentenverschlüsselung an eine unverschlüsselte E-Mail an und verschickten sie an die entsprechenden Adressaten. Fängt ein Hacker eine solche Nachricht ab, könnte er mit wenig Aufwand Zugang zu vertraulichen Informationen erhalten.

Teilweise wurden Dokumente auch mittels Fax übermittelt – ein umständliches, zeitraubendes und gleichermaßen wenig sicheres Verfahren. „Auch der hohe Zeitaufwand war ein Manko“, sagt Semmler. Ein weiterer Nachteil: In komplexen Projekten war eine saubere Versionsführung der Dokumente, die von vielen Personen an unterschiedlichen Standorten bearbeitet wurden, nicht gewährleistet, sprich wer wann welche Änderungen an einer Datei vorgenommen hatte, konnte nicht nachvollzogen werden. Dieses war unter anderem beim Austausch bei Vertragsverhandlungen äußerst hinderlich.

## „Zwischen der Zentrale und den Niederlassungen werden häufig Personalunterlagen, Arbeitsverträge und andere vertrauliche Dokumente ausgetauscht. Das muss auf eine Weise geschehen, die schnell, zuverlässig und vor allem sicher ist.“

Hartmut Semmler, Senior Director und Head of HR Payroll and Expert Services bei Fujitsu Technology Solutions (FTS).

### Der virtuelle Dokumententresor

Bei der Suche nach einer Alternative wurde FTS bei der Brainloop AG fündig. Die Münchner Firma bietet mit „Secure Dataroom“ einen elektronischen Dokumententresor an. Er wird mithilfe einer Software auf abgesicherten Rechnern angelegt, wobei nicht einmal die Systemadministratoren die Dokumente entschlüsseln können. Im Secure Dataroom lassen sich alle Arten von Daten aufbewahren, ähnlich wie Papierdokumente in einem Safe. Bevor ein Anwender Zugang zu den Informationen erhält, muss er sich ausweisen: mit seiner E-Mail-Adresse und einem Passwort. Alternativ dazu kann der registrierte Anwender auf eine Smartcard oder ein Hardware-Token zurückgreifen, also ein Gerät, das Einmal-Passwörter erzeugt.

Die IT-Abteilung von Fujitsu Technology Solutions installierte vor rund drei Jahren eine Testversion des elektronischen Datentresors. Einige Monate später gab FTS die Lösung dann für den Regelbetrieb frei. Derzeit haben etwa 70 Mitarbeiter von FTS und davon 25 aus der Zentralabteilung Personal sowie einige Partnerunternehmen Zugriff auf die Sicherheitstechnik. „Von diesen 25 Mitarbeitern sind etwa 50 Prozent Externe“, sagt HR-Leiter Hartmut Semmler. Über den Dokumententresor werden überwiegend personenbezogene Daten zwischen der Zentralabteilung Personal und externen Firmen ausgetauscht. „In einem Verzeichnis im Secure Dataroom legt beispielsweise ein Dienstleister die erstellten Kontoauszüge zur Altersversorgung ab“, erläutert Semmler.

Fujitsu Technology Solutions setzt den virtuellen Datenraum außerdem dazu ein, um Informationen mit externen Prü-

fern auszutauschen, etwa dann, wenn der Geschäftsjahresabschluss ansteht. Auch personenbezogene Unterlagen für den Wirtschaftsprüfer werden über den Dokumententresor bereitgestellt.

### Rechtmanagement integriert

Ein Grund, weshalb sich FTS für die Lösung von Brainloop entschied, ist der hohe Sicherheitsstandard bei jedem Bearbeitungsschritt. So verwendet der Brainloop Secure Dataroom eine starke Verschlüsselung. Dabei kommt das Verfahren AES (Advanced Encryption Standard) zum Einsatz – die derzeit beste Verschlüsselungstechnik auf dem Markt. Ebenso wichtig ist für Fujitsu Technology Solutions das integrierte Rechtmanagement von Secure Dataroom. Es regelt, welche Person oder Personengruppe wann mit welchen Daten oder Dokumenten tun darf: lesen, editieren, ausdrucken, kopieren oder weitergeben. Die HR-Abteilung von FTS kann beispielsweise festlegen, dass Externe bestimmte Unterlagen nur lesen dürfen, während die Mitarbeiter der Personalabteilung umfassende Bearbeitungsrechte erhalten. „Dank der Versionskontrolle ist jederzeit nachvollziehbar, welche Änderungen an Unterlagen vorgenommen werden“, sagt Hartmut Semmler. „Das erleichtert und beschleunigt in übergreifenden Projekten die Zusammenarbeit mit Kollegen an anderen Standorten oder mit Personaldienstleistern und externen Prüfern.“ Zudem ist ein asynchrones Bearbeiten von Dokumenten möglich.

### Dokumente im Web-Browser anzeigen

Ein Pluspunkt des sicheren Datenraums ist die einfache Bedienung. Dokumente im elektronischen Dokumententresor

können im Web-Browser „Internet Explorer“ oder mit dem „Windows-Explorer“ angezeigt werden. Im letzteren Fall können Mitarbeiter Dokumente in den Secure Dataroom einstellen, indem sie die entsprechenden Dateien in das Explorer-Fenster verschieben. „Das beschleunigt das Kopieren von Massen-Dateien wie etwa der Kontoauszüge der Altersversorgung von allen Mitarbeitern und das nachfolgende Bearbeiten der Dokumente erheblich“, sagt Semmler.

Derzeit testet Fujitsu Technology Solutions eine weitere Funktion des Datenraums: den einmaligen Austausch von Dokumenten mit Externen, die nicht als Nutzer des Secure Dataroom registriert sind. Mithilfe dieser »Abholfunktion« kann ein externer Mitarbeiter einmalig Unterlagen aus dem Datenraum herunterladen, die für ihn zuvor unter Angabe seiner E-Mail-Adresse freigegeben wurden. Um das Herunterladen zu starten, erhält er nach der Anwahl der Datenraum-Webseite automatisch via E-Mail eine PIN, mit der er anschließend innerhalb eines kurzen Zeitraums die Möglichkeit hat, die für ihn hinterlegten Dokumente aus dem Datenraum herunterzuladen.

Insgesamt ist der Leiter der HR Payroll & Expert Services von FTS mit der Brainloop-Lösung zufrieden: „Mit dem elektronischen Datentresor haben wir eine Möglichkeit gefunden, die den Austausch von personenbezogenen Daten und anderen vertraulichen Dokumenten deutlich vereinfacht und beschleunigt.“

Bernd Reder, freier Journalist, München