

Kommunikations-Sicherheit

Sichere Datenräume verbessern Kollaboration zwischen Unternehmen

Methoden für sichere Datenbearbeitung und Datentransfer

16.10.2009 | Autor: Wilfried Platten

Die interne und externe Zusammenarbeit ist für viele Unternehmen ein geschäftskritischer Faktor, wie auch die Datensicherheit. Das Wegsperrern von Dokumenten in einem Stahlschrank ist keine Lösung, mit solchen Daten muss produktiv gearbeitet werden. Gerade bei Projektarbeit, die über die Unternehmensgrenzen hinaus geht, ist es notwendig, dass Teammitglieder in einem sicheren, aber einfach zu bedienenden Umfeld Informationen und Dokumente austauschen und gemeinsam bearbeiten können.



Zusammenarbeit in und zwischen Unternehmen erfordert oft den Austausch vertraulicher Daten. Will man nicht zur Kette am Koffer greifen sind sichere Datenräume eine brauchbare Alternative.

Die Zahl der Projekte, die von mehreren Unternehmenseinheiten oder von verschiedenen Standorten aus bearbeitet werden, steigt. Und es sind gerade die großen, umfangreichen und anspruchsvollen Projekte, die hier eine Vorreiterrolle einnehmen. Mitarbeiter verschiedenster Standorte, Partner, Zulieferer, Kunden oder externe Berater arbeiten eng in den Projekten zusammen, obwohl sie in den unterschiedlichen Organisationen, Ländern, Zeitzonen und technischen Umgebungen angesiedelt sind.

Einerseits muss jedem Beteiligten die optimale Arbeitsumgebung ermöglicht werden, um die Ergebnisse des Projekts nicht zu gefährden, andererseits muss gewährleistet sein, dass selbst bei einer großen, inhomogenen Gruppe keine vertraulichen Informationen in falsche Hände geraten. Wie schnell es geschehen kann, dass Dokumente etwa per **E-Mail** an falsche Adressaten gesendet werden, zeigt das Beispiel des Pharmaunternehmens Eli Lilly. Hochvertrauliche Prozessunterlagen wurden von der beauftragten Anwaltskanzlei nicht wie beabsichtigt intern weitergeleitet, sondern an einen Journalisten der New York Times. Die versehentliche Auswahl der falschen E-Mail-Adresse in Outlook hatte fatale Folgen, denn mit der Publizierung dieser geheimen Daten wurde der Prozess verloren, ebenso wie Millionen von Dollar.

Es läßt sich nicht verhindern dass wichtige Daten das Unternehmen verlassen

Dieser Vorfall zeigt exemplarisch die Dimensionen der Sicherheitsproblematik beim Umgang mit sensiblen, unternehmenskritischen Dokumenten. Sie lässt sich nicht mit dem Wegsperrern von Dokumenten auf beliebigen Datenträgern in einem Stahlschrank erledigen. Mit diesen Dokumenten wird produktiv gearbeitet, sie sind unverzichtbarer Teil der Wertschöpfungskette. Die moderne Arbeitsteilung lässt zudem die Grenzen zwischen „innen“ und „außen“ immer mehr verschwimmen.

Deshalb müssen auch externe Experten, wie Anwälte, Berater, Behörden oder Lieferanten, zunehmend in den Dokumenten-Workflow integriert werden. Die betriebliche Praxis zeigt, dass es gerade die wichtigen, unternehmenskritischen Informationen sind, die die Grenzen des eigenen Unternehmens verlassen müssen, darunter zum Beispiel Produktentwicklungsdaten und Fondsinformationen. Aber auch vertrauliche Spezifikationen

Unternehmen, Anwälten und Gesetzgebern ausgetauscht, ebenso wie Kundeninformationen oft zwischen Stammhaus und Distributoren oder personenbezogene Daten zwischen Personalabteilung und Personal-Dienstleistern ausgetauscht werden.

Unternehmen stehen damit in einem typischen Zielkonflikt zwischen der Sicherheit und Integrität der unternehmenskritischen Daten und deren schneller, reibungsloser Distribution an alle, die innerhalb und außerhalb der Firma dafür autorisiert sind. Von der Lösung dieser widersprüchlichen Anforderungen hängt oft genug die Wettbewerbsfähigkeit eines Unternehmens ab. Denn je sicherer und effektiver die **Bereitstellung** und Bearbeitung von Dokumenten gelöst wird, desto schlagkräftiger kann das Unternehmen agieren beziehungsweise reagieren.

Anders formuliert bedeutet das: Sämtliche Sicherheitsmaßnahmen wie Zugriffskontrolle, Berechtigungen oder Verschlüsselungen müssen für die gemeinsame Dokumentenbearbeitung innerhalb und außerhalb der **Firewall** organisiert und garantiert werden.

Seite 2: Personenbezogene Daten erfordern Sicherheit bei Datenhaltung und Datentransfer

Personenbezogene Daten erfordern Sicherheit bei Datenhaltung und Datentransfer

Wie schützt man sensible Daten effektiv vor fremden Zugriffen oder Fehlhandlungen und macht sie dabei doch zugänglich für alle beteiligten Parteien? Diese Frage stellten sich die Verantwortlichen bei Fujitsu auch. Ihre Lösung ist der virtuelle Datenraum von Brainloop. So können Fujitsu-Mitarbeiter jetzt Daten schnell und sicher austauschen. „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.“ sagt Hartmut Semmler, Senior Director und Head of HR Payroll and Expert Services bei Fujitsu Technology Solutions (FTS)

Schnell, jedoch enorm unsicher, ist das Versenden vertraulicher Dokumente per **E-Mail-Anhang**. Ein E-Mail-Anhang kann von leidlich technisch versierten Interessierten gelesen werden wie eine Postkarte. Viele E-Mail-Systeme lassen Anhänge zudem nur bis zu einer bestimmten Größe zu. Noch immer wird von vielen Unternehmen die umständliche Methode genutzt, Dokumente in Papierform oder auf CD per Kurier zu versenden.

Doch die Gefahrenpotentiale dieses Distributionsweges sollten seit den Skandalen der letzten Zeit hinlänglich ins allgemeine Bewusstsein gerückt sein – ganz abgesehen davon, dass der Service eines Kuriers nicht nur teuer ist, sondern im Vergleich zu modernen Kommunikationswegen auch extrem langsam! Inhouse-Portale oder unternehmensweite Dokumenten-Management-Systeme sind nur hinter der Firmen- **Firewall** zu betreten und schließen so externe Spezialisten und Projektmitglieder aus. Auch **Passwort**-geschützte **FTP-Server** sind nicht ganz unkompliziert. Sie sind zwar relativ schnell und einfach aufgesetzt. Doch die Rechteverwaltung ist arbeitsaufwendig und der Mangel an integrierten Arbeitsabläufen, die eine reibungslose Zusammenarbeit gewährleisten, ist ein großes Handicap.

Fortschrittliche Unternehmen bedienen sich heute effektiverer, schnellerer und sichererer Methoden. Durch die Entwicklungen im Bereich der IT sind wir heute in der Lage, neue Wege für diese Herausforderungen zu gehen. Bei der Analyse und Bewertung geeigneter Lösungsansätze für diesen Problembereich gilt es, vorab eine technologische Entwicklung ins Kalkül zu ziehen. Dieser Trend wird in Zukunft noch viel stärker die Art und Weise bestimmen, wie Daten und Dokumente bearbeitet, verteilt und gespeichert werden: hin zu **SaaS-Anwendungen (Software as a Service)**, auch **Cloud Computing** genannt.

Nach dem von Großrechnern geprägten Server Based Computing (SBC) und den ausufernden Client-Server-Architekturen mit ihren viel zu funktionsreichen Arbeitsplatz-PCs stehen wir aktuell mitten in einem Paradigmenwechsel, dem nächsten Schritt in der Evolution der IT-Strukturen. Aus Sicht des Anwenders wird nur noch ein Thin Client mit einem Browser, eine Internetverbindung, sowie die Passwort-gesicherte Zugangsberechtigung benötigt. Aus Sicht des Unternehmens liegen die Anwendungen, die Daten und die Dokumente in einem gesicherten Raum. Und dies entweder innerhalb des eigenen Unternehmens oder bei externen IT-Dienstleistern (SaaS, siehe oben). Diese Art zu Arbeiten wird so selbstverständlich werden wie die Nutzung einer Suchmaschine. Es wird genauso einfach und schnell sein und bietet zusätzlich maximale Sicherheit für die Informationen.

Seite 3: Sichere und effiziente Kommunikation

Sichere und effiziente Kommunikation

Auf Basis dieser Technologie ist es möglich geworden, neue Ansätze zur sicheren und effizienten Zusammenarbeit beim Umgang mit sensiblen Dokumenten zu verwirklichen. Sei es nun für die interne Gremienkommunikation oder die externe Kommunikation mit Dienstleistern und Partnern. Der Königsweg dorthin heißt „sicherer Datenraum“. Das bedeutet, sämtliche für einen definierten Personenkreis oder für ein bestimmtes Projekt notwendigen Dokumente liegen mehrfach gesichert in einem abgeschlossenen, von einem externen Dienstleister zur Verfügung gestellten „digitalen Tresor“, der ausschließlich von den Berechtigten benutzt werden darf. Für alle anderen ist dieser Datenraum nicht existent, da dieser ohne Zugangsberechtigung gar nicht angezeigt wird. Der Zugriff erfolgt ganz einfach über einen Browser und Login mit einem EinmalPasswort. Es wird keinerlei zusätzliche Software benötigt.

Willkommene Entlastung

Durch sichere Datenräume werden die internen IT-Abteilungen gleich mehrfach entlastet. Es wird so die interne Ressourcenbindung verringert, die IT-Mitarbeiter können sich intensiver um andere Aufgaben kümmern. Gelangen vertrauliche Informationen nach „außen“, stehen die Mitarbeiter der internen IT-Abteilung aufgrund der ihnen durch die privilegierten Administratorenrechte gegebenen Zugangsmöglichkeiten häufig automatisch unter Anfangsverdacht. Mit einem Secure Dataroom sind sie davon befreit, da die Daten in einem externen Data Center liegen, zu dem sie keinerlei Zugang haben.

Alle aufgeführten Aspekte überzeugen – besonders in Kombination mit der Möglichkeit, den Datenraum zu mieten. Immer mehr Unternehmen vertrauen ihre sensiblen Dokumente einem hochsicheren virtuellen Datenraum an.

Finanzdaten bei der Deutschen Telekom sicher im Griff

Die Deutsche Telekom ist zwar nicht unbedingt für rundum-Datensicherheit bekannt, aber meist betrifft das die extern bei Callcentern gehaltenen Kundendaten. Für interne Finanzdaten wie beispielsweise im Bereich Merger and Acquisitions (M&A) nutzt die Deutsche Telekom den Brainloop Datenraum. Er wird sowohl als Kollaborations-Plattform zur Verteilung und Sammlung der Informationen für das Projektteam eingesetzt, als auch als Dealroom, in dem der Verkäufer die Due Diligence durchführt. Der effizientere Prozessablauf und der drastisch reduzierte logistische Aufwand haben die Deutsche Telekom so überzeugt, dass sie seit 2003 den Brainloop Secure Dataroom selbst vermarktet. „Innerhalb der Due-Diligence-Phase verringert sich der logistische Aufwand für Verkäufer und Käufer durch die Verwendung eines virtuellen Datenraums um ein Vielfaches.“, beschreibt Bernd Adler, Senior Expert Projectmanager, Servicezentrale Mergers & Acquisitions, Deutsche Telekom AG den Nutzen des Dienstes.

Redakteur: Peter Schmitz

Die Beiträge auf dieser Website sind urheberrechtlich geschützt. Bei Fragen zu den Nutzungsrechten wenden Sie sich bitte an manuela.maurer@vogel.de oder Tel.: 0931-418-2888.

Dieses PDF wurde Ihnen bereitgestellt von <http://www.searchsecurity.de>