



# DOK magazin

Technologien, Strategien & Services für das digitale Dokument

„Die Zukunft des Dokuments“ Intuitiver Umgang mit Dokumenten  
**E-Invoicing** Umstellung auf elektronisches Rechnungsmanagement kommt voran  
**SaaS** Sicherheit auf Zeit im ausgelagerten Dokumenten-Tresor

## Information Lifecycle – Lebenszyklus der Informationen Special: Lösungen mit Microsoft SharePoint



# Sicherheit auf Zeit im ausgelagerten Dokumenten-Tresor

Patentanmeldungen, Compliance, Corporate Governance, Enterprise-Rights-Management, Dokumenten-Management, Verschlüsselung, SaaS, Business Cases

Unternehmen und Behörden müssen sicherstellen, dass vertrauliche Informationen jeder Art, egal ob E-Mails, Finanzdaten oder Produktionsunterlagen, nicht in fremde Hände gelangen. Das gilt für den gesamten Lebenszyklus von Dokumenten: vom Erstellen über das Bearbeiten und Weiterleiten wie mit E-Mail bis hin zur Archivierung. Doch das ist leichter gesagt als getan. Ein Beispiel ist der Automobilhersteller Audi. Fotos von Prototypen des Modells A1, das erst 2009 auf den Markt kommen soll, gelangten im Herbst vergangenen Jahres vorzeitig ins Internet – eine Panne, die vermutlich auf das Konto der Presseabteilung des Konzerns geht. Für eine Maschinenbaufirma in Nordrhein-Westfalen hätte ein Informationsleck wiederum, wie die Consulting-Firma Add-Yet berichtet, beinahe weitaus gravierendere Folgen gehabt. Als das Unternehmen beim Patentamt Unterlagen über eine neuartige Technologie einreichte, stellte sich heraus, dass ein Konkurrent aus Fernost kurze Zeit zuvor ein Patent für dasselbe Verfahren beantragt hatte. Die Fachleute des deutschen Maschinenbauers fest, dass es sich um exakt dieselben Unterlagen handelte, die sie selbst eingereicht hatten. Der Mitbewerber beziehungsweise beauftragte „Fachleute“ hatten sich offenbar in die Kommunikationskette zwischen dem westfälischen Hersteller und dessen Patentanwalt eingeklinkt und die Dateien entwendet.

## Geschäftsführung und IT-Leiter haften für Fehler

Solche Pannen beeinträchtigen nicht nur das Image eines Unternehmens, sondern können in hohem Maße geschäftsschädigend sein. Das ist vor allem dann der Fall, wenn interne Daten in die Hände der Konkurrenz gelangen. Wie hoch die dadurch entstandenen Schäden sind, darüber geben Firmen nur ungern Auskunft. Um dem leichtfertigen Umgang mit sensiblen Informationen einen Riegel vorzuschieben, wurden Compliance-Regeln entwickelt. Zu den bekanntesten zählt der 2002 in den USA erlassene „Sarbanes-Oxley Act“ (SOX), der auch für ausländische Firmen gilt, die in den Ver-

[www.brainloop.com](http://www.brainloop.com)

**Bernd Reder** ist freier Journalist in München. Der gelernte Kommunikationswissenschaftler arbeitet als Autor und Berater für Unternehmen.

einigten Staaten tätig sind. Wichtige Vorschriften hierzulande sind das „Gesetz zur Unternehmensintegrität und Modernisierung des Anfechtungsrechts“ (UMAG), das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ (KonTraG) und die „Mindestanforderungen an das Risikomanagement“ in den Kreditvergaberichtlinien von Basel II. Bei Verstößen sieht die EU-Richtlinie Geldstrafen in empfindlicher Höhe vor, ebenso Freiheitsstrafen bei besonders eklatanten Vergehen. In diesen Regelwerken wird dem Management des Unternehmens die Pflicht zur lückenlosen Dokumentation wichtiger Informationsflüsse auferlegt sowie zum aktiven Risikomanagement, insbesondere von Risiken, die aus dem unsachgemäßen Umgang mit vertraulichen Informationen entstehen. Das Fehlen von Prozessen und Werkzeugen für die Dokumentation und den Schutz der Information kann im Extremfall als grobe Fahrlässigkeit ausgelegt werden. In diesen Fällen kann das Management persönlich für entstandene Schäden haften.

## Compliance belastet IT-Abteilungen

Für die Unternehmensleitung und die IT-Abteilung ist es alles andere als einfach, die Compliance-Regeln in die Praxis umzusetzen und den Schutz vertraulicher Dokumente sicherzustellen. Nach einer Untersuchung der Consulting-Firma Exagon überblicken nur sechs Prozent der deutschen IT-Leiter vollständig die für ihr Unternehmen geltenden Compliance-Vorschriften. Gut 16 Prozent sind mit dem Thema in ausreichendem Maße vertraut, 55 Prozent haben dagegen nur begrenzte Kenntnisse der Vorgaben und 23 Prozent so gut wie keine. Nach Angaben der Beratungsgesellschaft Steria Mummert Consulting geben über die Hälfte der IT-Verantwortlichen in deutschen Unternehmen an, dass der Arbeitsaufwand ihrer Abteilungen durch die Einführung von Compliance-Vorschriften deutlich gestiegen ist. Mehr als drei Viertel gehen davon aus, dass die Vorgaben höhere Investitionen in die IT-Technik erforderlich machen.

## Fernzugriff auf Dokumente muss geschützt werden

Corporate Governance verlangt zum einen, dass jederzeit nachvollziehbar ist, wer wann Zugang zu vertraulichen Dokumenten hat und diese bearbeitet. Zum anderen muss der lückenlose Schutz vertraulicher Dokumente auch dann sichergestellt sein, wenn externe Mitarbeiter darauf zugreifen. Zudem müssen die Mitarbeiter des Unternehmens die Möglichkeit haben, Dokumente „remote“ einzusehen und zu bearbeiten – im Büro, unterwegs oder zu Hause. Wichtig ist der durchgängige Schutz der Informationen entlang der gesamten Kette, vom Erstellen der Dokumente bis hin zum „Endpunkt“, beispielsweise das Notebook eines Managers. Der Schutz darf nicht an der Firmengrenze haltmachen, wenn vertrauliche Informationen systematisch mit firmenfremden Personen wie Beratern, Investmentbankern oder Wirtschaftsprüfern erstellt und ausgetauscht werden.

# Einfach unermüdlich.



fi-5900C  
PRODUKTIONSSCANNER



### Was zeichnet einen guten Partner aus?

Man kann sich auf ihn verlassen. Mit Fujitsu als Partner sind Sie in besten Händen, Sie können sich auf uns und jedes unserer Produkte verlassen. Als Markt- und Technologieführer mit jahrzehntelanger Erfahrung sorgen wir dafür, dass Fujitsu Scanner immer auf dem neuesten Stand der Technik sind. Fujitsu hat den idealen Scanner für genau Ihre Anforderungen.

### Was erwarten Sie von einem idealen Produktionsscanner?

Produktivität, Vielseitigkeit, Zuverlässigkeit und Benutzerfreundlichkeit. Dann ist der fi-5900C der Scanner Ihrer Wahl. Er verarbeitet unterschiedlichste Papierqualitäten zuverlässig und optimiert dank integriertem Kofax VRS 4.1 Professional Schnittstellenmodul zeitgleich die gescannten Bilddaten. Aufgrund der einzigartigen Kombination dieser und vieler weiterer Funktionen verändert der fi-5900C die Welt des Produktionsscannens.

Weitere Informationen unter  
<http://emea.fujitsu.com/scanners>

\* Infosource Scanner Market Report Spring 2007

 **ASSURANCE  
PROGRAMME**

**FUJITSU**

THE POSSIBILITIES ARE INFINITE

Alle Namen, Herstellernamen, Marken- und Produktbezeichnungen unterliegen besonderen Schutzrechten und sind Herstellerzeichen und/oder eingetragene Marken der jeweiligen Inhaber. Alle Angaben unverbindlich. Änderungen an den technischen Daten ohne vorherige Ankündigung vorbehalten.

### Standard-Ansätze: Datenverschlüsselung und Rechteverwaltung

Um den Schutz vertraulicher Dokumente zu gewährleisten, haben Unternehmen die Wahl zwischen zwei Optionen: Sie stellen aus verschiedenen Produkten und Technologien quasi eine „handgestrickte“ Lösung zusammen, oder sie greifen auf ein Komplettpaket zurück. Zunächst zur ersten Variante. Nicht selten implementieren die IT-Abteilungen von Firmen und Behörden nur rudimentäre Mechanismen, um sensible Daten zu schützen: Geschäftsunterlagen werden oft unverschlüsselt auf einem speziellen Netzwerk-Laufwerk auf einem Server abgelegt. Der IT-Admin regelt den Zugriff, indem er Benutzergruppen die entsprechenden Rechte zuteilt. Die Nachteile dieses Ansatzes: Die Daten sind gegen Angriffe von außen und innen, sprich durch eigene Mitarbeiter, nur schlecht geschützt. Ein weiterer Schwachpunkt ist der IT-Admin selbst, denn er hat dank seines privilegierten Status jederzeit Zugang zu den Informationen.

Einen besseren Schutz bieten Dokumenten-Management-Systeme (DMS), die um eine Verschlüsselungsfunktion erweitert wurden. Gleiches gilt für Enterprise-Rights-Management-Lösungen wie etwa die „Rights Management Services“ (RMS) von Microsoft. Beide Ansätze sehen eine Verschlüsselung der Dokumente vor. Der Vorteil von DMS-Lösungen besteht darin, dass sie mit einem einzigen Daten-Repository auskommen, was die Verwaltung der Daten vereinfacht. Bei Enterprise-Rights-Management-Lösungen wird eine Client/Server-Architektur implementiert. Auf den Clients muss eine spezielle Software installiert werden, die für die Authentifizierung der Benutzer und das Ver- und Entschlüsseln der Daten zuständig ist. Beide Ansätze bieten eine durchgängige Verschlüsselung von Informationen. Solche Lösungen sind jedoch vor allem für Endanwender nicht einfach zu handhaben und können typischerweise für externe Personen außerhalb der Firewall überhaupt nicht eingesetzt werden. Ein weiterer Nachteil: Auch auf diesen beiden Wegen können sich IT-Mitarbeiter Zugang zu den Daten verschaffen.

### Schwachpunkt: Dokumente über E-Mail verschicken

Das Risiko steigt vor allem dann, wenn unternehmenskritische Informationen das Firmennetz verlassen. Viele Unternehmen übermitteln nach wie vor kritische Geschäftsunterlagen unverschlüsselt als E-Mails. Der Grund dafür ist, dass die Einführung einer Verschlüsselungstechnik aufwendig ist, die IT-Abteilung muss auf den Clients eine Verschlüsselungssoftware installieren. Hinzu kommt ein System für die zentrale Verwaltung der Keys, das typischerweise nur unternehmensinterne Teilnehmer bedienen kann. Nicht zu unterschätzen ist außerdem das Risiko, E-Mails versehentlich an den falschen Adressaten zu schicken. Eine einmal abgeschickte Mail lässt sich so gut wie nie wieder „einfangen“, da hilft auch kein noch so detaillierter Disclaimer.

Selbst vor dem Versand verschlüsselte Nachrichten und Dokumente sind ein Sicherheitsrisiko: Hacker können die E-Mails abfangen und dekodieren. Auch das Verschlüsseln der Festplatten oder Flash-Speicherkarten von Notebooks hilft nur begrenzt. In mehreren Fällen, so das Bayerische Landesamt für Verfassungsschutz, wurden Geschäftsreisende bei der Einreise nach China und in die USA aufgefordert, die Geschäftsunterlagen zu dekodieren, die auf verschlüsselten Festplatten-Partitionen auf ihren Notebooks lagerten. Bei Weigerung wurde das Gerät beschlagnahmt oder zerstört.

### Secure Dataroom als Plattform für den „End-to-End“-Schutz von Informationen

Unternehmen, die sicher sein wollen, benötigen eine Plattform, die eine effiziente, jederzeit nachvollziehbare und sichere Kommunikation erlaubt. Und für den Anwender einfach zu bedienen ist. Das schließt das sichere Bearbeiten und Verteilen von Dokumenten mit ein, auch über die Grenzen des Unternehmens hinweg. Eine dieser Lösungen ist der Secure Dataroom der Brainloop AG, ein elektronischer Daten- und Dokumententresor, der mithilfe einer speziellen Software auf abgesicherten Rechnern angelegt wird. Dort lassen sich alle Arten von sensiblen Daten ablegen, ähnlich wie Papierdokumente in einem Safe. Bevor ein Anwender Zugang zu den Daten erhält, muss er sich mithilfe von zwei Verfahren ausweisen: mit einem Passwort und einem Token (Einmal-Passwort). Dieses wird beispielsweise via SMS auf das Handy des Users übermittelt. Alternativ dazu kann der Anwender auf eine Smartcard oder ein Hardware-Token zurückgreifen.

### Granulare Zugriffsrechte

Neben einer Verschlüsselung der Dokumente, am besten mit dem AES-Verfahren (Advanced Encryption Standard) und 256-Bit-Schlüsseln, ist ein flexibles Rechtemanagement (ERM, Enterprise Rights Management) notwendig. Ein Beispiel: Zwei Unternehmen prüfen, ob sie eine Kooperation eingehen sollen. Im Rahmen der Verhandlungen erhalten Mitarbeiter beider Firmen Einsicht in interne Dokumente des potenziellen Partners. Wenn die Gespräche scheitern, muss sichergestellt sein, dass diese Daten dem Mitbewerber nicht länger zugänglich sind. Secure Dataroom versieht Dokumente mit zeitlich begrenzten Zugriffsrechten, etwa „Nur lesen“. Um zu verhindern, dass geschützte Dokumente auf einen Rechner heruntergeladen und gespeichert werden, sind Document-Viewer-Funktionen vorhanden, mit denen autorisierte Personen die Informationen einsehen, jedoch nicht lokal speichern können. Selbst das Erstellen von Screenshots lässt sich verhindern, indem der Server Dokumente in Form von kachelförmigen Teilbildern übermittelt. Die Zugriffsregeln („Policies“) sind zentral auf dem Server gespeichert.

## Wasserzeichen legen Quellen offen

Ein klassisches Problem beim Umgang mit vertraulichen elektronischen Dokumenten wird mit „digitalen Wasserzeichen“ gelöst: die Suche nach Informationslecks. Dokumente erhalten automatisch bei jedem Zugriff eine Kennzeichnung, die unter anderem den Namen des Nutzers enthält. Damit ist die psychologische Hürde deutlich höher, vertrauliche Informationen weiterzugeben, denn es ist jederzeit nachvollziehbar, von wem die Daten stammen. Während Anbieter wie Oracle, Documentum und Adobe beim Rights-Management auf herstellereigene Client/Server-Software setzen, setzt Secure Dataroom auf das Rights-Management-System RMS (Rights Management Services) von Microsoft. Es arbeitet mit Windows Server 2003 und dessen Nachfolger Windows Server 2008. Außerdem lässt sich das digitale Rechtemanagement von Microsoft Office 2003 oder 2007 verwenden. Der Anwender kann Excel-, Word- oder Powerpoint-Dokumente ansehen, ausdrucken oder bearbeiten und anschließend auf den Server zurückspielen – die Dokumente sind auch während der Arbeit verschlüsselt und für nicht autorisierte Personen unzugänglich.

## Sicherheit als Software as a Service

Software as a Service gilt als Trend, der Outsourcing und fokussierte Abbildung von Geschäftsprozessen vereint, damit sich die Anwender auf ihre Kernprozesse konzentrieren können. Damit einher gehen die Vorteile, die aus Anwendersicht jede SaaS-Lösung kennzeichnen: kein Aufbau einer eigenen Infrastruktur und von internen Skills, ständig aktualisierte Software, automatische Backups, Compliance-konform (Stichwort Disaster Recovery) und anderes mehr. Zudem sind solche Lösungen automatisch klar zu kalkulieren, was bei einer Inhouse-Umsetzung meist nicht der Fall ist. Und: SaaS-Dienstleister können Skaleneffekte aufbauen, von denen die Anwender wiederum in Form von niedrigeren Betriebskosten profitieren. Natürlich wird sich nicht jeder Prozess, jede Arbeit mit Software als Service auslagern lassen. Doch je klarer der Business Case, der Prozess selbst abgebildet wird, wie etwa unter anderem im Bereich E-Billing oder Posteingang, wo mehr und mehr SaaS-Anwendungen und -Plattformen entstehen, desto klarer werden die Vorteile von Software as a Service erkennbar. ■



## Eingemacht für die Ewigkeit?

Bevor es bei Ihren wertvollen Kulturgütern und Dokumenten ans Eingemachte geht, reden Sie mit uns. Wir sind seit 1961 am Markt und bieten Ihnen komplette Digital- und Analogsysteme für die Scan- und Mikrofilmtechnologie auf höchstem Niveau.

**Zeutschel, die Zukunft der Vergangenheit.**

Zeutschel GmbH · Heerweg 2 · 72070 Tübingen  
Tel.: (07071)9706-0 · Fax: (07071)970644  
info@zeutschel.de · [www.zeutschel.de](http://www.zeutschel.de)

www.kraas-  
fachmann.com



**ZEUTSCHEL**