




## Lückenlose Sicherheit beim Umgang mit vertraulichen Dokumenten

---

 [http://www.documanager.de/magazin/artikel\\_2297\\_lueckenlose\\_sicherheit\\_vertraulichen.html](http://www.documanager.de/magazin/artikel_2297_lueckenlose_sicherheit_vertraulichen.html)

Bestimmte **Aktivitäten eines Unternehmens verlangen "Vertraulichkeit auf Zeit"**, für Aufsichtsräte oder externe Berater, für Partner, Investoren oder staatliche Regulierungsbehörden. Hier wird ein Weg gesucht, der schnell, sicher und eben "auf Zeit" eine vertrauliche, abgeschirmte Kommunikation gewährleistet, für die die üblichen Berechtigungs- und Sicherheitsmechanismen der Unternehmens-IT nicht ausgelegt sind. Typische Bereiche sind Finanzen, Rechtsabteilung, M&A, Einkauf und Personalabteilung.

### Unternehmen arbeiten im Extranet

Vieles, was unter den Megathemen Web bzw. Enterprise 2.0, Wissensmanagement oder Collaboration diskutiert wird, bezieht sich im Grunde auf irgendeine Spielart eines Extranets. Entsprechend hat die Dynamik, die Unternehmen heute in der **Ausrichtung ihrer IT-Systeme** erfahren, "**Extranet-Charakter**", ob durch verteilte Arbeitsgruppen, Datenübernahme aus Fremdsystemen oder Kundenorientierung. Wer wann was sehen und bearbeiten darf, ist eine im eigentlichen Wortsinn geschäftskritische Überlegung, umgesetzt durch Rollenbeschreibungen, Berechtigungssysteme, Verschlüsselung und Sicherung von Daten.

Die für die Geschäftsprozesse notwendigen digitalen Dokumente können nicht alle hinter der Firewall des Unternehmens gehalten werden, sondern müssen auf sichere Art unter den berechtigten Personen zirkulieren. Sicherheitsmaßnahmen wie die Verschlüsselung der Dokumente während es Datentransports und auf den verschiedenen Speichermedien sowie unternehmensweites Digital Rights Management (DRM) sind lediglich Teilkomponenten eines umfassend konzipierten **Document Compliance Management (DCM)**. DCM-Lösungen stellen den korrekten Umgang mit Dokumenten, die aus unternehmerischen oder gesetzlichen Gründen besonders geschützt werden müssen, sicher.

### Hochsicherheitstrakt für vertrauliche digitale Dokumente

DCM-Systeme benötigen auf der Basis einer bestimmten IT-Infrastruktur eine Art "digitalen Hochsicherheitstrakt" für Dokumente, der von der Geschäftsführungsebene problemlos über einen Web-Browser genutzt werden kann. Idealerweise ist ein **DCM-System als Software-as-a-Service-Lösung** konzipiert: mit keinerlei Aufbau von lokaler Infrastruktur verbunden und von jedem Arbeitsplatz über das Internet erreichbar. Das System ist so abgeschirmt, dass niemand, insbesondere auch nicht das IT-Personal des Unternehmens oder der externe Serverbetreiber Einblick in die Daten hat.

### Digitale Infrastrukturen

Die Arbeitsabläufe bei Behörden und Unternehmen sind weitgehend durch digitale Infrastrukturen geprägt und das digitale Dokument hat in vielen Bereichen das Papierdokument abgelöst. Dokumenten-Management- und Enterprise-Content-Management-Systeme beeinflussen maßgeblich die Art und Weise der Abläufe und der Bearbeitung. Bei diesen digitalen Abläufen und Kooperationen muss zu jedem Zeitpunkt und an jeder Stelle des Prozesses sichergestellt sein, dass vertrauliche Dokumente nur für berechtigte Personen einzusehen, zu versenden, zu kopieren oder zu verändern sind. Eine **Document-Compliance-Management-Lösung muss vertrauliche Dokumente vor und hinter der Firewall schützen**, und zwar lückenlos, über den gesamten Lebenszyklus hinweg.

Es werden dabei alle überhaupt denkbaren Zugriffsberechtigten und ihre Berechtigungen gespeichert, verwaltet von einem nicht-technischen Administrator, jemandem, der mit den tatsächlichen Sicherheitsanforderungen und Geschäftsfällen vertraut ist, üblicherweise der Leiter des jeweiligen Projekts, das im Datenraum durchgeführt wird. Durch die zeitnahe Aktivierung oder Zuteilung der Berechtigungen durch den Administrator der DCM-Lösung können Unternehmen schnell und vor allem sicher auf wechselnde

Anforderungen reagieren. Das reicht bis hinunter auf eine nachträgliche Zugriffssperre für ein Dokument auf einem Arbeitsplatzrechner.

Das **Spektrum der technischen Infrastruktur** der DCM-Lösung umfasst die durchgängige **Verschlüsselung**, die den gesamten Lebenszyklus abdeckt, eine starke **Authentifizierungskomponente** mit Passwort und Einmal-SMS-PIN sowie eine stringente Transportsicherung, digitale Wasserzeichen, Read-Only Modus und eine rigorose **Schlüsselverwaltung**. Diese sorgt dafür, dass das System vom Rechenzentrumspersonal zwar bedient werden kann, der Zugriff auf die Inhalte jedoch konsequent ausgeschlossen wird.

## Compliance als Prozess

Compliance wird von Experten als umfassender Prozess gesehen, weniger als Teilkomponente im Geschäftsalltag. Genau so sollten die IT-Strukturen ausgelegt sein. Eine Delegation von Teilkomponenten an das IT-Personal oder eine Sicherheit, die sich nur auf Teilbereiche erstreckt, erfüllt letztlich nicht die gesetzlichen Vorgaben zum aktiven Risikomanagement. Auch die Systeme für das **Enterprise Rights Management (ERM)** gewährleisten im Sinne von Compliance **keine Sicherheit**, sondern sind nur in Teilbereichen sicher. Konsequenterweise sollte die gehostet werden, um sensible Dokumente und das geistige Eigentum einer Firma zu schützen.

*Dieser Beitrag erschien im Fachmagazin DOK, Ausgabe 3-09 September 09.*

*Erschienen: 12/2009*

*Autor: Nicole Dietrich*



Nicole Dietrich ist Senior Marketing Director bei der Brainloop AG. Die Brainloop AG mit Firmensitz in München und Boston ist Anbieter von Document-Compliance-Management-Lösungen für den hochsicheren Umgang mit vertraulichen Dokumenten.

DOK

**DOK.**