

Lückenlose Sicherheit beim Umgang mit vertraulichen digitalen Dokumenten

Document Compliance Management

Zentrale geschäftliche Aktivitäten, bei denen es um viel Geld und manchmal um die Existenz eines Unternehmens geht, beziehen in aller Regel viele Personen ein, die nicht oder nicht direkt dem Unternehmen angehören. Das können Aufsichtsräte oder externe Berater sein, Partner, die an einem Joint Venture interessiert sind, und immer öfter staatliche Regulierungsbehörden. Die für diese Geschäftsprozesse relevanten digitalen Dokumente können nicht hinter den Firewall-Systemen des Unternehmens gehalten werden, sondern müssen auf sichere Art unter den berechtigten Personen zirkulieren können. Viele bekannte Sicherheitsmaßnahmen wie Verschlüsselung während des Datentransports und auf den verschiedenen Speichermedien sowie unternehmensweite Digital-Rights-Management-Systeme sind lediglich Teilkomponenten eines umfassenden und ganzheitlich konzipierten Document Compliance Management (DCM), das für die heutige Unternehmensdynamik mit ihrem ausgeprägten „Extranet-Charakter“ ausgelegt ist.

DCM-Systeme benötigen auf der Basis einer speziellen IT-Infrastruktur eine Art digitalen Hochsicherheitstrakt, in dem allen Zugangsberechtigten vertrauliche Dokumente gemäß ihrem jeweiligen Rechtsstatus zugänglich sind. Dieser Hochsicherheitstrakt für Dokumente muss problemlos über einen Web-Browser durch Endanwender zum Beispiel aus der Vorstands- oder Geschäftsführungsebene bedient werden können. Idealerweise ist ein DCM-System als Software-as-a-Service-Lösung realisiert. Es ist von jedem Arbeitsplatz aus erreichbar und arbeitet ohne das Aufspielen von Client-Software. Die Schlüsselverwaltung ist so organisiert, dass niemand, insbesondere auch nicht das IT-Personal des Unternehmens, Einblick und Zugriff hat. Die Verwaltung eines Generalschlüssels für das Notfallmanagement ist auf mehrere Personen, von denen jede nur einen Teil dieses Schlüssels besitzt, aufgeteilt.

Die Problemstellung

Die Arbeitsabläufe bei Behörden und Unternehmen sind heute schon weitgehend durch digitale Infrastrukturen geprägt. Nachrichten und Dokumente sind auf digitalen Speichermedien abgelegt und werden über digitale Netze ausgetauscht. Digitale Dokumente haben Papierdokumente in vielen Bereichen abgelöst. Durch Dokumenten- und Content-Management-systeme lassen sich die digitalen Akten in vielfältiger Weise auswerten und mit anderen Dokumenten abgleichen und verknüpfen. Durch digitales Dokumentenmanagement und dessen Einbindung in die

geschäftlichen Workflows werden indes nicht nur die Verarbeitungsmöglichkeiten erweitert, sondern vor allem auch die Entscheidungsprozesse erheblich beschleunigt. Ganz gleich, ob es sich um die Vorbereitung von Firmenkäufen, um Abstimmungsprozesse im Vorfeld von Hauptversammlungen oder um den Schutz geistigen Eigentums, zum Beispiel von vertraulichen Konstruktionsdaten für Maschinen oder von Rezepturen und Testergebnissen für Pharmaka, handelt: Die betreffenden Infor-

mationen müssen in Sekundenschnelle zwischen den beteiligten Personen ausgetauscht oder auch gemeinsam bearbeitet werden können. Bei diesen digitalen Abläufen und Kooperationen muss zu jedem Zeitpunkt und an jeder Stelle des Prozesses sichergestellt sein, dass die Dokumente nur für jeweils berechnete Personen einsehbar, versendbar, kopierbar oder veränderbar sind. Angesichts der Brisanz der Dokumente dürfen diese für Unbefugte – und das sind in diesem Fall auch die eigenen IT-Systemadministratoren – in unverschlüsselter Form nicht zugänglich sein. Solche Systeme müssen vertrauliche Dokumente von ihrer Entstehung bis zur Archivierung oder Löschung begleiten, ohne dass innerhalb dieses „Lebenszyklus“ auch nur die geringste Lücke in den Sicherheitsmaßnahmen auftritt. Ebenso ist lückenlos zu dokumentieren, wer wann diese Dokumente eingesehen, verschickt oder verändert hat. Ein solcher Anforderungskatalog für den durchgängigen Schutz vertraulicher Dokumente und für die komplette und unveränderbare Dokumentation aller Zwischenstände und Zugriffe wird zunehmend unter dem Be-

Die Eckpunkte eines Document-Compliance-Management-Systems

- Gerade die brisantesten und wertvollsten Daten und Dokumente lassen sich heute nicht mehr hinter einer Firewall halten, wenn nicht die Schlagkraft eines Unternehmens gestört werden soll. Der Raum, in dem heute Dokumente vor unbefugter Einsichtnahme und Änderung geschützt werden müssen, ist das Extranet. Diese Tatsache ist maßgebend für die Architektur von DCM-Lösungen.
- Es ist deshalb konsequent, den DCM-Server außerhalb des eigenen Unternehmens in einer Art Hochsicherheitstrakt unterzubringen.
- Die Nutzer des DCM-Systems dürfen nicht mit IT-Infrastrukturproblemen behelligt werden, sondern sollen das DCM-System als browserbasierte, leicht bedienbare Anwendung erleben.
- Die gesamte Anwendung muss nicht nur absolut angriffssicher gestaltet sein, sondern auch jeden Schritt der Protagonisten lückenlos aufzeichnen, um so allen „Compliance-Forderungen“ interner Revisoren und des Gesetzgebers genügen zu können.
- Eine starke Authentifizierung ist unabdingbar für alle, die mit dem DCM-System arbeiten. Durch Einmal-Passwörter, bei denen das Mobiltelefon als Token benutzt wird, lässt sich die Authentifizierung innerhalb des gesamten Extranets flexibel, kostengünstig und hochsicher gestalten.

griff Document Compliance Management (DCM) diskutiert. Gemeint ist der korrekte Umgang mit Dokumenten, die aus unternehmerischen oder gesetzlichen Gründen besonders geschützt werden müssen.

Ganzheitliche Kontrolle über den gesamten Lebenszyklus eines Dokuments

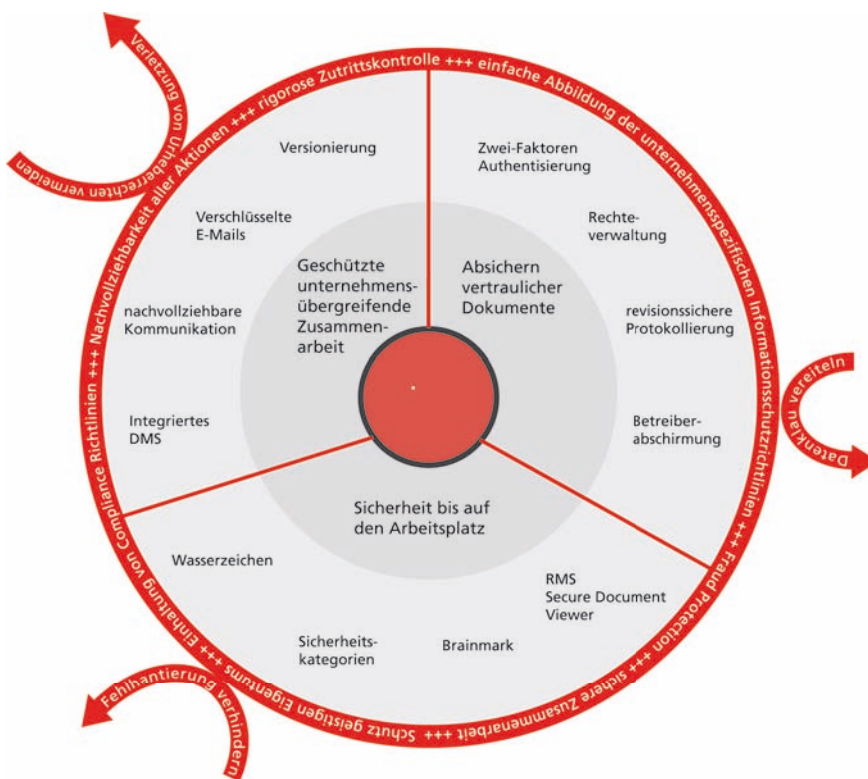
Eine „Document Compliance Management“-Lösung muss also vertrauliche Dokumente sicher schützen, ganz gleich ob sie sich innerhalb oder außerhalb der Unternehmens-Firewall-Systeme befinden. Der Schutz der Dokumente gegen unbeberechtigtes Lesen oder gegen Verfälschungen darf keine Lücken aufweisen. Bei unvollständigen Lösungen ist z. B. ein Dokument, wenn es erst einmal auf den Client geladen worden ist, in keiner Weise mehr zu schützen. Eine wirkliche DCM-Lösung hat den gesamten Lebenszyklus eines Dokuments im Blick und im Griff. Auf einem gesicherten Server sind alle überhaupt möglichen Zugriffsberechtigten und ihre jeweiligen Rechte gespeichert. Diese Festlegungen sind allerdings nicht statisch,

sondern werden ständig angepasst und durch einen nichttechnischen Administrator, beispielsweise den Projektleiter, umgesetzt. Wenn beispielsweise bei einem Firmenverkauf, an dem sich mehrere Bieter beteiligen, ein Bieter ausscheidet, dann werden dessen bisherige Zugriffsrechte sofort durch das System gelöscht. DCM-Lösungen behalten immer die Kontrolle über ein Dokument, vom ersten Anlegen des Dokuments bis zu dessen Löschung.

DCM-System als SaaS-Architektur

Die Verwaltung der Zugriffe auf die vertraulichen Dokumente wird in einem DCM-System von Nicht-IT-Personen durchgeführt, weil nur sie mit den tatsächlichen Geschäftsanforderungen vertraut sind. Dabei ist es ratsam, bestimmte Änderungen und Maßnahmen an ein Mehraugen- beziehungsweise Funktionstrennungsprinzip zu binden. Die IT-technische Infrastruktur, also zum Beispiel die Datenbank, in der die Authentifizierungsdaten verwaltet werden, ist für diese Administratoren nicht sichtbar und natürlich auch nicht beeinflussbar. Für die technischen Administratoren sind diese

Komponenten wie eine „Black Box“, die sie mit ihren Standardtechniken verwalten, ohne in die Innereien schauen zu können. Die Administration der IT-Infrastruktur für ein DCM-System kann und sollte überdies in verschiedene Zuständigkeits-Ebenen aufgeteilt werden. Aus dem Gesagten ergibt sich, dass für ein DCM-System eine browserbasierte Mietlösung (Software-as-a-Service, SaaS) ideal ist. Es wird dabei keine Client-Software benötigt und die IT-Infrastruktur wird von Spezialisten quasi unsichtbar, aber effizient bereitgestellt und gepflegt. Das Document Compliance Management stellt sich insofern für die Nutzer in der Vorstandsetage oder in der Konstruktionsabteilung als eine Anwendung dar, die so wie ein normales Office-Programm zu bedienen ist. Unter dieser leicht zu bedienenden Oberfläche befindet sich die IT-technische Infrastruktur. Das Spektrum reicht hier von durchgängiger Verschlüsselung, die den gesamten Lebenszyklus abdeckt, und einer starken Authentifizierungs-Komponente über eine stringente Transportsicherung, unter anderem für E-Mail oder Dokumenten-Kennzeichnungsverfahren wie digitale Wasserzeichen, bis hin zu einer rigorosen Schlüsselverwaltung auf der Basis von digitalen Zertifikaten, die dafür sorgt, dass das System vom Rechenzentrumspersonal bedient werden kann, der Zugriff auf die Inhalte aber konsequent ausgeschlossen wird.



Das Document-Compliance-Management-Konzept von brainloop: Ähnlich wie bei der Flugsicherung nimmt dieser Sicherheitsansatz das „Reisen der Dokumente“ zum Ausgangspunkt. Reiseroute und die „zusteigenden Personen“ werden den Anforderungen entsprechend gesichert und dokumentiert, Quelle: brainloop.

Autorin



Nicole Dietrich
Senior Marketing Director,
brainloop AG