Sicher vernetzt kooperieren – Brainloop Document Compliance Management

Schnell und grenzenlos soll die Kooperation zwischen Unternehmen heute sein. Nicht selten bleibt dabei jedoch die Datensicherheit auf der Strecke. Die meisten Lösungen für dieses Problem decken allerdings nur Teilaspekte ab und sorgen vor allem nicht für Sicherheit über den gesamten Lebenszyklus eines Dokuments hinweg. Gesucht also: Ein Document Compliance Management, das regelkonform und unkompliziert die barrierefreie Zusammenarbeit intern und über Unternehmensgrenzen hinweg so sicher macht, dass jeder Mitarbeiter den Kopf frei hat für seine eigentlichen Aufgaben.

Die Entdeckung der Außenwelt

Früher waren die Grenzen von Unternehmen wie ein Burgwall, hinter dem alle vertraulichen Dokumente sicher und geschützt waren. Dafür war es umständlich und zeitraubend, Dokumente mit Externen auszutauschen und gemeinsam an ihnen zu arbeiten. Unternehmen waren genau umrissene Organisationen, mit klaren Grenzen und abgeschotteten internen Prozessen. Alle Daten blieben meist im Unternehmen, waren sicher und geschützt. Im Zeitalter von Digitalisierung und Globalisierung sind diese Grenzen jedoch immer durchlässiger und offener geworden; in vielen Fällen kann gar nicht mehr klar angegeben werden, wo „innen" aufhört und „außen" beginnt: Ein externer Rechtsberater, der bei einem Merger berät, wird oft schon als Teil des Unternehmens angesehen. Oder der Patentanwalt: Wie viel weiß er über geheime Forschungen des Unternehmens? Und wie steht es mit einer unternehmensübergreifenden Partnerschaft bei der Entwicklung eines neuen Produkts? Ja, schon der Aufsichtsrat einer Aktiengesellschaft greift letztlich von außen auf interne Dokumente zu. Aber auch bei ganz alltäglicher Zusammenarbeit zwischen Unternehmen, etwa in der Kommunikation mit Investoren, bei Forschungsprojekten oder beim Austausch von Verträgen werden die einst festen Grenzen von Unternehmen zunehmend durchlässig.

Nicht nur die Formen der Zusammenarbeit zwischen Unternehmen oder Partnern werden immer vielfältiger, auch die Geschwindigkeit und Mobilität dieser Kooperationen steigt ständig an: So schnell wie möglich, von jedem Ort zu jedem anderen werden Daten, Dokumente, Themen, Inhalte ausgetauscht. Der elektronische Austausch vertraulicher Dokumente wird zunehmend wichtiger.

Der Preis, den viele Unternehmen heute für Schnelligkeit und grenzüberschreitende Kooperation bezahlen, ist, dass die Datensicherheit auf der Strecke bleibt und geistiges Eigentum oder vertrauliche Unternehmensdaten verloren gehen können.

Beispiele, in denen vertrauliche Dokumente ausgetauscht werden

- Gremienkommunikation: Aufsichtsrat, Verwaltungsrat u.a.
- Kommunikation im Vorstand
- Finanzberichterstattung, Erstellung der Berichte, Kommunikation mit Wirtschaftsprüfern u.a.
- Vertragsverhandlungen & Vertragsmanagement
- Verkauf von Firmenanteilen, Portfolios, Outlicensing
- Interne und externe Audits
- Personenbezogene Daten in der Personalabteilung (z.B. Bewerbermanagement)
- Forschung und Entwicklung – Schutz geistigen Eigentums
- Asset Management (Immobilien effektiv verwalten & veräußern)

Ausweitung der Sicherheitszone

Nun will natürlich niemand zurückkehren zu den nur scheinbar guten alten Zeiten, in denen wichtige Dokumente höchst sicher in Stahlschränken aufbewahrt, aber quälend langsam in Aktenkoffern übergeben wurden. Das wäre auch gar nicht mehr möglich: Wer heute nicht im Hochgeschwindigkeitstakt der firmenübergreifenden Zusammenarbeit mithalten kann, ist bald den Herausforderungen des Marktes nicht mehr gewachsen. Das Mittelalter mit seinen sicheren Burgen und dicken Steinwällen ist längst vorbei – wir leben im Zeitalter der offenen und schnellen Kooperation über alle Grenzen hinweg.
Doch wie kann man die neue Art der Zusammenarbeit leben und trotzdem nicht in offene oder versteckte Sicherheitsfallen geraten? Bisher hinkt in vielen Fällen die Sicherheit den technischen Möglichkeiten des Datenaustausches und der unternehmensübergreifenden Zusammenarbeit hinterher. Gefordert ist eine Lösung, mit der unterschiedliche Partner Dokumente sicher und nachvollziehbar austauschen können, und zwar sowohl innerhalb des geschützten Firmennetzwerks als auch außerhalb der Firewall des Unternehmens. Natürlich müsste dieses grenzüberschreitende Netz leicht bedienbar sein und eine einfache und intuitive Benutzeroberfläche haben, damit die Anwender es sofort akzeptieren. Die Einführung einer solchen Lösung sollte sehr schnell ablaufen und dürfte keine langen und komplizierten Prozesse erfordern. Ebenso sollten keine Installationen auf den Rechnern der externen Partner notwendig sein, da dies die Nutzung verzögern würde. Bei all dem muss immer sichergestellt sein, dass die Compliance - und die Sicherheitsrichtlinien des Unternehmens eingehalten werden. Und zu guter Letzt: Sie sollte die Budgets nicht überlasten.
Gefragt ist daher eine Lösung, die nicht nur einer Abteilung, einer Gruppe von Stakeholdern nützt, sondern allen im Unternehmen, die mit sicherheitssensiblen Dokumenten über Grenzen hinweg kommunizieren. Idealerweise sollte auch nur die tatsächliche Nutzung abgerechnet werden.

Eine Menge Anforderungen! Wäre so eine Lösung denkbar?

Auf der Suche nach der verlorenen Datensicherheit

In aller Regel sind an einer derartigen Lösung verschiedene Personen in unterschiedlichen Funktionen im Unternehmen interessiert: Zunächst die **Anwender,** also diejenigen Mitarbeiter, die z.B. in der Finanz- oder Forschungsabteilung, im Vorstands- oder Personalbüro über Firmengrenzen hinweg kooperieren müssen.

Dann der **Compliance-Verantwortliche**, der dafür zuständig ist, dass alle Prozesse den Regeln und Richtlinien des Unternehmens und des Gesetzes entsprechen.
Und schließlich natürlich der **Sicherheitsbeauftragte**, für den die Datensicherheit an erster Stelle steht.
Jeder der drei hat eine andere Perspektive und andere Bedürfnisse, die ein Document Compliance Management erfüllen muss: Die **Anwender** möchten einfach ihre Dokumente austauschen, der **Compliance-Verantwortliche** möchte gewährleisten, dass Richtlinien eingehalten werden, der **Sicherheitsbeauftragte** muss sicherstellen, dass Daten nicht in falsche Hände geraten.

Macht man sich im Markt auf die Suche, stößt man sehr bald auf Technologien, die Teilaspekte der oben genannten Herausforderungen adressieren. Oft wenden sich solche Kollaborationsanwendungen hauptsächlich an den Endanwender, Regeln und Sicherheit auf Unternehmensebene werden dabei eher als zweitrangig behandelt.

Eine andere Möglichkeit, den Schutz von Dokumenten sicherzustellen, ist die Konzentration auf Verschlüsselungstechnologien, bei denen Festplatten, E-Mails, und Dokumente verschlüsselt werden. Leider wird dabei das Schlüsselmanagement sehr schnell komplex und unhandlich; deshalb finden solche Lösungen meist nicht die Akzeptanz der Anwender. Auch aus Sicht der Compliance- und Sicherheitsverantwortlichen sind diese Verschlüsselungstechnologien nicht zufriedenstellend, da die Dokumente nach der Übermittlung an Externe nicht mehr ausreichend geschützt sind.

Auch bei klassischen Insellösungen, stellen sich schon bald die Nachteile heraus: Man benötigt dann für jeden Anwendungsfall eine eigene Software, und es wird fast unmöglich, eine einheitliche Compliance-Richtlinie zum Umgang mit sensiblen Dokumenten für das ganze Unternehmen zu etablieren. Sowohl die Sicherheitskategorien für die Dokumente als auch die Berechtigungskonzepte für die Abteilungen und Projektteams müssen dann von einer zentralen Stelle immer wieder neu eingerichtet werden. Außerdem wird es schnell teuer, wenn für jeden Anwendungsfall eine eigene Software und ein gesonderter Implementierungsprozess aufgesetzt werden muss. Für das Unternehmen als Ganzes ist also nur ein Konzept sinnvoll, das möglichst viele Bedürfnisse im ganzen Unternehmen mit einer einzigen Lösung abdeckt.

Ein weiterer Ansatz wäre es, innerhalb eines Unternehmens bestehende Portallösungen um Enterprise-Rights-Management-Systeme zu ergänzen. Diese Vorgehensweise hat jedoch mehrere gravierende Nachteile: Zum einen bleibt bei ihnen das Schlüsselmanagement in den Händen der IT-Administratoren, die so die Dokumente mitlesen können. Ein wirklich sicheres System muss dagegen so ausgelegt sein, dass weder die eigene IT-Abteilung noch der Lösungsanbieter Zugriff auf die Daten haben. Nur so bleiben die Dokumente und Daten wirklich bei dem Personenkreis, für den sie gedacht sind. Und zum anderen sind zur Implementierung eines Enterprise-Rights-Management-Systems umfangreiche Installationen sowohl auf den Servern im Rechenzentrum als auch auf den Geräten der Endbenutzer notwendig. Dies ist normalerweise nur im firmeneigenen Intranet möglich; die Kommunikation mit externen Partnern bleibt erheblich erschwert. Wichtige Eigenschaften, wie etwa über Wasserzeichen personalisierte Dokumente oder die Nachvollziehbarkeit der verschiedenen

Fassungen sind nur schwer oder gar nicht zu implementieren. Insgesamt gesehen decken auch diese Systeme lediglich Teilaspekte eines vollwertigen Document Compliance Managements ab.

Im Herzen der Sicherheit – konsequenter Schutz vertraulicher Dokumente

Mit dem Brainloop Document Compliance Management werden vertrauliche Dokumente zu jedem Zeitpunkt der Bearbeitung und über den gesamten Lebenszyklus konsequent geschützt – sogar nach der Auslieferung an den Arbeitsplatz oder das iPad eines Benutzers. Kernstück der Brainloop-Lösung ist die umfassende Sicherheitsarchitektur. Sie gewährleistet, dass Dokumente nicht nur verschlüsselt abgelegt und übertragen werden, sondern auch nur für Berechtigte zugreifbar sind. Auch Brainloop bzw. die Mitarbeiter des Rechenzentrums haben keinen Zugriff auf die Dokumente. Durch die zentrale Vorgabe von Sicherheitseinstellungen für den Umgang mit den einzelnen Dokumentenschutzklassen (Wer erhält Zugriff? In welchem Format werden die Dokumente bereitgestellt? usw.), können Richtlinien eines Unternehmens für den Dokumentenschutz automatisiert in der Organisation implementiert werden und die Mitarbeiter bei der Umsetzung unterstützt werden. Das Berechtigungssystem steuert dabei, welche Benutzergruppen ein Dokument sehen, verändern, drucken oder weiterleiten dürfen. Darüber kann auch vorgegeben werden, ob ein Empfänger ein Dokument im Originalformat erhält oder nur in einem geschützten Brainmark-Format, das zusätzlich mit einem personalisierten Wasserzeichen belegt werden kann.

Die Bereitstellung persönlicher verschlüsselter Kopien der Dokumente gewährleistet, dass der Benutzer die Dokumente zwar in seiner gewohnten PC-Umgebung lesen oder bearbeiten kann, sie aber auch weiterhin geschützt sind und nicht an andere Benutzer weitergeleitet werden können. Zusätzlich kann eine Nutzungsdauer festgelegt werden, nach deren Ablauf die Dokumente automatisch verfallen.

Für die Festlegung seiner individuell benötigten Sicherheitseinstellungen benötigt der Anwender kein spezielles IT-Know-How, auch der Austausch von Schlüsseln ist nicht erforderlich. Gleichzeitig können Compliance- und Sicherheitsverantwortliche über das Reporting und den revisionssicheren Audit-Trail jederzeit die Umsetzung der Sicherheitsrichtlinien prüfen, ohne dass sie dafür Zugriff auf die Dokumente benötigen.

Häufig steht man noch vor ganz anderen Herausforderungen, zum Beispiel wenn innovative Endgeräte auf den Markt kommen. Seit Tablet-Computer wie z.B. das iPad ihren Siegeszug angetreten haben, möchten Führungskräfte und Vorstandsmitglieder alle Dokumente immer und überall auf den neuen mobilen Endgeräten lesen können. Ein Document Compliance Management, das wirklich sicher ist, muss auch Lösungen für diese Endgeräte bereithalten und schnell auf technische Innovationen reagieren können. Sonst besteht jederzeit die Gefahr neuer, gravierender Sicherheitslücken.

Eine Menge Fragen also, auf die man bei der Suche nach einer sicheren Möglichkeit, über Unternehmensgrenzen hinweg zusammenzuarbeiten, stößt. Muss also hundertprozentige Datensicherheit in einer Welt der Geschwindigkeit und der Globalisierung eine Utopie bleiben?

Der Name der Sicherheit

Nein, muss sie nicht. Denn Brainloop hat sich all diesen Herausforderungen gestellt und eine Antwort gefunden: Brainloop Document Compliance Management, eine „Best of Suite"-Lösung, die, einmal im Unternehmen eingeführt, alle Anwendungsfälle abdeckt und von allen Abteilungen genutzt werden kann.

Dabei kann man klein anfangen, mit einem konkreten Fall, und dann nach und nach auch anderen Abteilungen die Vorteile des Brainloop Document Compliance Management zugänglich machen. Eine Vorgehensweise, die auch vom Budget her skalierbar bleibt: nach dem Prinzip „pay as you go" muss nur bezahlt werden, was auch genutzt wird.

Das Document Compliance Management von Brainloop berücksichtigt die Perspektiven aller Stakeholder im Unternehmen, die mit sicheren Dokumenten zu tun haben:

Für den **Anwender** ist die Brainloop-Lösung eine leicht über den Browser zu bedienende Anwendung, für die er weder neue Software installieren noch den Umgang mit ihr mühselig lernen muss. Er hat von überall her, wann immer er will Zugriff auf vertrauliche Dokumente und kann mit externen und internen Partnern problemlos zusammenarbeiten, ohne sich Sorgen um die Sicherheit machen zu müssen. Das breite Funktionsspektrum der Brainloop-Lösung unterstützt ihn in der täglichen Arbeit und verbessert seine Effizienz.

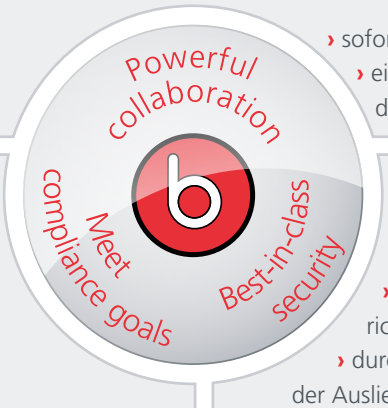
Der **Compliance-Verantwortliche** findet alle seine Anforderungen ebenfalls von Anfang an ins System implementiert. Denn Brainloop hilft ihm, sicher zu stellen, dass alle Abläufe den Regeln und Richtlinien des Unternehmens und den gesetzlichen Vorgaben entsprechen. Und durch eine lückenlose Protokollierung aller Aktivitäten kann er auch einer zukünftigen Revision ruhig entgegensehen.

Der **Sicherheitsbeauftragte** schließlich weiß, dass durch die Brainloop-spezifische Sicherheitsarchitektur keine Dokumente versehentlich in den falschen Händen landen können. Jedes Dokument ist in seinem ganzen Lebenszyklus abgesichert, sowohl auf den eigenen Servern wie auf denen der Partner, bis hin zum Desktop der einzelnen Anwender – die im Übrigen das System durch die unkomplizierte Bedienbarkeit sehr schnell und gerne akzeptieren.

Brainloop Document Compliance Management bietet:

Für Anwender

› sichere Zusammenarbeit mit Kollegen und externen Partnern
› weltweiten Zugriff via Internet – 24/7
› sofortige Verfügbarkeit ohne Installation am Arbeitsplatz
› einfache, intuitive Bedienung ohne Training – und dadurch eine hohe Anwenderakzeptanz



Für Compliance – Verantwortliche

› professionelles Dokumentenmanagement (z.B. durch Versionierung)
› Automatische Umsetzung von Unternehmensrichtlinien
› revisionssichere Nachvollziehbarkeit aller Vorgänge
› SaaS-Plattform in Deutschland, die die Anforderungen des deutschen Datenschutzes erfüllt
› die Verfügbarkeit weiterer SaaS-Plattformen (u.a. in Luxemburg, der Schweiz und den USA)

Für Sicherheitsbeauftragte

› die automatisierte Umsetzung von Sicherheitsrichtlinien
› durchgehenden Schutz der Dokumente – auch nach der Auslieferung an den Arbeitsplatz der Anwender
› Dokumente, die nur von berechtigte Benutzer eingesehen und bearbeitet werden können
› ein funktionierendes Operator Shielding: weder Plattform-Betreiber noch IT haben Zugriff auf die Dokumente
› eine Lösung, bei der kein Austausch von Schlüsseln erforderlich ist

Konzernweit

› die Möglichkeit der Integration in vorhandene Anwendungssysteme (z.B. Mail, SAP) und automatisierte Lösungen
› eine Lösung, bei der keine Bedarfsplanung und kein unternehmensweiter Roll-Out erforderlich ist
› eine automatisierte Bereitstellung an die Fachbereiche
› die Möglichkeit konzernspezifischer Konfigurationen

Mit gutem Gewissen sicher kommunizieren

Einmal eingeführt, ist das Brainloop Document Compliance Management auch für neue Aufgaben bestens gerüstet: Man könnte sagen, es ist „future proof", auch Herausforderungen, von denen zum Zeitpunkt der Installation noch niemand etwas ahnt, kann problemlos begegnet werden. Ein Beispiel dafür ist die Brainloop iPad-App: Schon kurz nach der rasanten Verbreitung des Apple-Tablets wurden es in die Brainloop Sicherheitszone integriert. Auch Daten aus anderen Systemen im Unternehmen (zum Beispiel SAP oder E-Mail-Systemen) können einfach und schnell integriert werden. Das Brainloop Document Compliance Management ist damit eine Investition, die nachhaltig und langfristig für das Unternehmen großen Nutzen bringt. Einen Nutzen, der vor allem auch darin besteht, dass Brainloop die Arbeit mit vertraulichen Daten im Hintergrund schützt und alle Mitarbeiter den Kopf frei haben für ihr Kerngeschäft.

Kontakt

Die Brainloop AG mit Zentrale in München und Standorten in Boston, Wien und Zürich ist der führende Anbieter von Document Compliance Management-Lösungen (DCM) für den hochsicheren Umgang mit vertraulichen Dokumenten. Weitere Informationen zur Brainloop AG finden Sie im Internet unter www.brainloop.de.

Brainloop AG
Franziskanerstraße 14
81669 München · Deutschland
T: +49 (89) 444 699 0
info@brainloop.de
www.brainloop.de

Brainloop Austria GmbH
Josefstädter Straße 44/2/1
1080 Wien · Österreich
T: +43 (1) 402 4851 700
info@brainloop.at
www.brainloop.at

Brainloop Switzerland AG
Gotthardstraße 52
8800 Thalwil ZH · Schweiz
T: +41 (44) 720 37 31
info@brainloop.ch
www.brainloop.ch

Brainloop Inc.
One Broadway, 14th floor
Cambridge, MA 02142 · USA
T: +1 (800) 517 3171
info@brainloop.com
www.brainloop.com

brainloop