

Risiken des unternehmensübergreifenden Austauschs sensibler Dokumente

Sichere Zusammenarbeit in der Cloud durch Document Compliance Management

Deutschland ist eine technologie- und exportorientierte Nation, deren Stärke auf Wissensvorsprung und Innovationen basiert. Dieses Wissen weckt weltweit immer wieder großes Interesse. Dokumente, die Einblick in Patente, Best Practices, finanzielle Transaktionen und geheime Absprachen geben, müssen vor fremdem Zugriff geschützt werden. Dieses Vorgehen sichert das Überleben der Unternehmen und sollte zentrale Bestandteil jeder Unternehmensstrategie sein.

Wie aber kann dieser Schutz gelingen, wenn immer mehr Unternehmen von der Verlagerung ihrer Anwendungen, Daten und Dokumente in die sogenannte »Cloud« sprechen und die Abhängigkeit von web-basierten Verfahren damit Kernbestandteil unternehmensinterner Prozessabläufe wird? Was bedeutet das für den Umgang mit vertraulichen Dokumenten, in denen überlebenswichtiges Wissen zu Papier gebracht wurde, das nicht für jedermann einsehbar sein darf? Offensichtlich erfordert diese völlig neue Situation Lösungen, die in der »Cloud« eine sichere Umgebung für die gemeinsame Bearbeitung und die regelkonforme Verwaltung sensibler Inhalte garantieren.

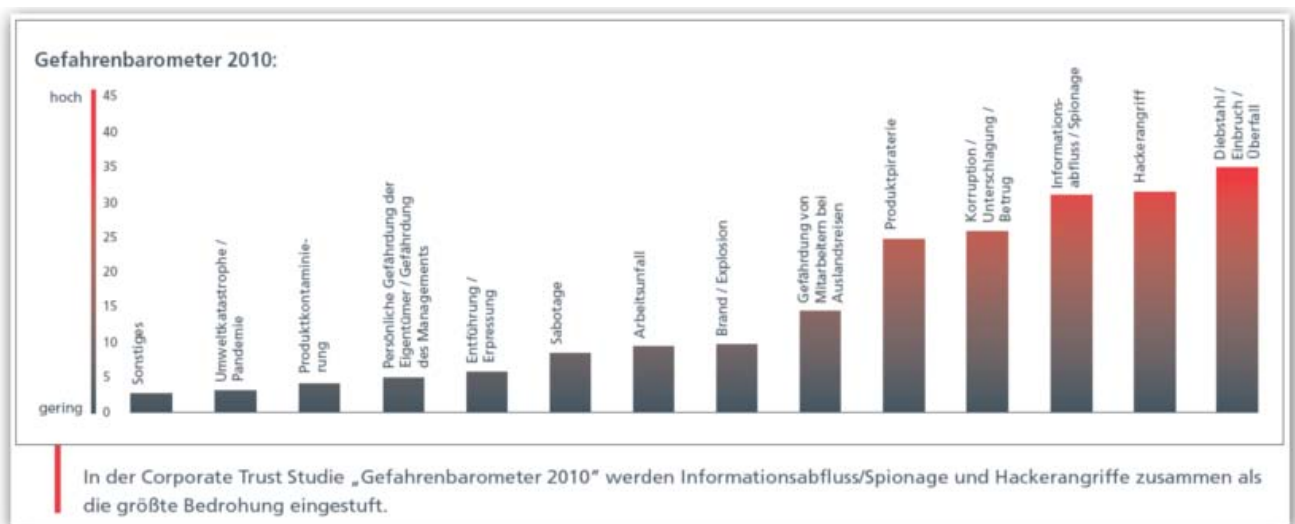
Beispiele für aktuelle Fälle von Datenverlust durch Fehlverhalten oder Wirtschaftskriminalität lassen sich schnell finden. So tauchten im vergangenen Jahr Bilder und Daten der neu designten E-Klasse Fahrzeuge von Mercedes Wochen vor der offiziellen Vorstellung im Internet auf. Gleiches widerfuhr Audi mit seinem Modell A5. Der Hintergrund dieser Datenpannen: Beide Automobilhersteller beauftragten externe Unternehmen damit, Handbücher, Werbematerialien und Vertriebsunterlagen zu erstellen. Über diese Wege gelangten die noch geheimen Informationen an die Öffentlichkeit. Wesentlich problematischer als diese Vorfälle dürfte die Veröffentlichung von hoch vertraulichen internen Unterlagen von Firmen und Regierungen sein, die Online-Portale wie WikiLeaks veröffentlicht haben und auch weiter veröffentlichen werden. Die Betreiber von Wikileaks erhalten tausende von internen Memos, Geschäftsunterlagen, Verträge und andere, als hochvertraulich eingestufte, elektronische Dokumente. Der Schaden, der sich durch die Veröffentlichung dieser Informationen, für die betroffenen Unternehmen ergeben wird, ist derzeit noch gar nicht abzuschätzen.

Firmenübergreifende Zusammenarbeit macht den Schutz sensibler Dokumente notwendig

Ein Grund dafür, dass sensible Informationen in falsche Hände geraten, ist die Art und Weise, wie Firmen mit ihren Kunden und Partnern heute zusammenarbeiten: Räumlich verteilte Arbeitsgruppen kommunizieren via E-Mail, Instant Messaging-System oder Collaboration-Plattformen. Sensible Dokumente werden als E-Mail-Anhang oder über Online-Plattformen ausgetauscht und gemeinsam bearbeitet. Zudem müssen Mitarbeiter von Zulieferfirmen, Konstruktionsbüros oder Beratungsunternehmen in den Informationsfluss mit einbezogen werden. Diese Faktoren machen die Kommunikation zwar schneller und effizienter, aber auch unsicher.

In der Corporate Trust Studie »Gefahrenbarometer 2010« werden Informationsabfluss/Spionage und Hackerangriffe zusammen als die größte Bedrohung eingestuft.

Gefahrenbarometer 2010:



Eine E-Mail, an die ein Word-Dokument mit dem Entwurf eines Vertrags angehängt ist, landet aus Versehen schnell einmal beim falschen Adressaten. Neben der Fehlhantierung ergibt sich die Gefahr des Missbrauchs vertraulicher Informationen durch interne Mitarbeiter. Vor allem IT-Administratoren haben wegen ihrer privilegierten Position oft Zugang zu Daten, die nicht für ihre Augen bestimmt sind. Dies ist nicht verwunderlich, sind es doch die IT-Spezialisten im eigenen Haus, die Rechner, Datenbanken und Speichersysteme verwalten und den Nutzern der Arbeitsplatzrechner ihre Passwörter zuteilen. Aus diesem Grund zählen IT-Administratoren zu den bevorzugten Zielen von Wirtschaftsspionen. Betrachtet man offizielle Berichte, wie beispielsweise den Bericht des Bundesamts für Verfassungsschutz (Juni 2010) so nehmen digitale Angriffe auf Unternehmensinformationen drastisch zu:

Der 2010 veröffentlichte Bericht des Bundesamtes für Verfassungsschutz befasst sich im Kapitel »Spionage und sonstige nachrichtendienstliche Aktivitäten« mit der Situation Deutschlands, die auf Grund der geopolitischen Lage, ihrer wichtigen Rolle in EU und NATO sowie als Standort zahlreicher Unternehmen der Spitzentechnologie für Spionage besonders interessant ist.

Im Bericht wird festgestellt, dass »...Die Aufklärungsziele ausländischer Nachrichtendienste reichen von der Informationsbeschaffung aus Politik, Wirtschaft und Militär bis hin zur Ausspähung und Unterwanderung in Deutschland ansässiger Organisationen ... Eine zunehmende Bedeutung erlangen internetgebundene Angriffe auf Computersysteme von Wirtschaftsunternehmen und Regierungsstellen ... «.

Ein eigenes Kapitel widmet der Bericht im Rahmen seiner Spionage-Betrachtung den elektronischen Angriffen. Hier heißt es: »...Mit dem Begriff »Elektronische Angriffe« werden gezielte Maßnahmen mit und gegen IT-Infrastrukturen bezeichnet. Neben der Informationsbeschaffung fallen darunter auch Aktivitäten, die zur Schädigung beziehungsweise Sabotage dieser Systeme geeignet sind. Dazu gehören das Ausspähen, Kopieren oder Verändern von Daten ... Die Angriffe können dabei sowohl von außen über Computernetzwerke, wie beispielsweise das Internet, erfolgen als auch durch einen direkten, nicht netzgebundenen Zugriff auf einen Rechner, beispielsweise mittels manipulierter Hardwarekomponenten wie Speichermedien....«

Abschließend kommt der Bericht zu dem Ergebnis, dass seit dem Jahr 2005 auf breiter Basis durchgeführte zielgerichtete elektronische Angriffe auf Behörden und Wirtschaftsunternehmen in Deutschland erkannt werden, die bis heute in unverminderter Intensität anhalten. Als die größte aktuelle Bedrohung werden vom Verfassungsschutz internetbasierte Angriffe auf Computersysteme und mobile Kommunikation deutscher Wirtschaftsunternehmen und Behörden angesehen. Dieses Gefahrenpotenzial sieht der Bericht noch gesteigert durch einen Abbau von Sicherheitsstrukturen in der deutschen Wirtschaft, ausgelöst durch Einsparungen auf Grund der Turbulenzen im internationalen Finanzmarkt der jüngsten Zeit.

Angesichts dieser Entwicklungen ist ein neuer Ansatz für den Umgang mit vertraulichen Inhalten gefordert, der den gesamten Lebenszyklus eines vertraulichen Dokuments erfasst und dieses zu jeder Zeit umfassend schützt: Das Document Compliance Management (DCM).

Eine ganzheitliche Document-Compliance-Lösung sollte neben dem zuverlässigen Schutz der Dokumente und neben dem revisions sicheren Protokollieren aller Aktivitäten insbesondere das effiziente Arbeiten der Anwender im Blick haben. Idealerweise ist es ganz einfach, zu jeder Zeit und von jedem Ort aus auf die Anwendung und die Dokumente zuzugreifen. Genau diese Flexibilität bieten Anwendungen in der Cloud, wie man es von Social-Media-Plattformen, beispielsweise Facebook kennt, aber auch Business-Applikationen wie Salesforce.com oder Online Office-Versionen wie Google Docs oder Microsoft Office 365 sind überall und einfach über die Cloud verfügbar, jedoch ohne Sicherheit für die Inhalte. Letzte erfüllen nur ganzheitliche DCM-Lösungen, die zuverlässige Sicherheit in der Cloud bieten.

DCM BIETET:

- › Durchgehenden Schutz vertraulicher Dokumente
- › Sicherheit bis auf den Arbeitsplatz und darüber hinaus
- › Geschützte unternehmensübergreifende Zusammenarbeit
- › Ausschluss der IT-Abteilung, sowie des Serverbetreibers

Die auf Document Compliance Management aufbauende »Secure Cloud«

Der Service-Provider richtet im Auftrag eines Unternehmens oder einer Organisation in einem, dem Kunden bekannten, hochsicheren und zertifizierten Rechenzentrum einen Datentresor für unternehmenskritische Informationen ein. Zugang haben etwa ausschließlich dazu autorisierte Mitglieder eines Projektteams (dieses kann Unternehmens- und standortübergreifend aufgestellt sein). Die Hauptvorteile dieses Ansatzes: Die Nutzer können via Web-Browser jederzeit, von jedem Ort auf Dokumente zugreifen, und dies auf sichere Weise.

Vorteilhafte Kombination aus SaaS und DCM

Um Document Compliance zu nutzen, sollte ein Software-as-a-Service Angebot aus der »Sicheren Cloud« genutzt werden: Der Lösungsanbieter richtet für den Anwender eine hochsichere DCM-Umgebung ein, auf die dieser via Internet, geschützt durch eine Mehrfach-Authentifizierung, zugreift. Eine solche Lösung ist von jedem Arbeitsplatz auf der ganzen Welt aus für Berechtigte zugänglich. Zudem ist es nicht erforderlich, auf den Arbeitsplatzrechnern Software zu installieren. Der Zugriff auf die Dokumente erfolgt über den Browser. Der Projektleiter verantwortet eigenständig die Zugriffsrechte für die Teilnehmer seines Projekts. Er benötigt aufgrund der einfachen Benutzeroberfläche keine Hilfe eines Administrators. Vereinfacht gesagt: DCM gibt den Fachabteilungen die Hoheit über die sensiblen Daten, die sie bearbeiten. Die Fachabteilung legt fest, wer Zugang den Dokumenten erhält. Eine hoch sichere Zwei-Faktor-Authentifizierung mittels Passwort und Einmal-PIN stellt sicher, dass nur dazu autorisierte Personen die für sie freigegebenen Dokumente zu Gesicht bekommen. Ein derartiges Document Compliance System bietet somit vergleichbare Funktionen wie ein komfortables Dokumentenmanagement mit Versionskontrolle und einer Änderungshistorie, oder die Möglichkeit, Dokumente gegen Änderungen zu schützen (Read-only-Modus). Die Vorteile liegen jedoch in der Sicherheit, die auch das abgesicherte Arbeiten über Firewalls ohne Installation auf den End-Rechnern ermöglicht.

Das Herzstück: Schutz vor dem unbefugten Zugriff des IT-Administrators

Natürlich schwebt eine »Secure Cloud« nicht im luftleeren Raum. Das heißt, Mitarbeiter des Service-Providers müssen eine solche Umgebung einrichten und verwalten. Dies bedeutet aber nicht, dass dadurch erneut ein Administrator vorhanden ist, der sich Zugang zu den sensiblen Daten verschaffen kann. Denn Sicherheitsfunktionen wie Operator Shielding (Betreiberabschirmung) stellen sicher, dass das IT-Personal des Service-Providers keine Möglichkeit hat, in die abgesicherte Arbeitsumgebung Einblick zu nehmen oder auch die

Dokumente einzusehen. Weitere Sicherheits-Features, etwa eine starke Verschlüsselung des Datenraums und der Daten verhindern Zugriffe Unbefugter.

Voraussetzungen für einen sicheren Umgang mit vertraulichen Dokumenten in der Cloud

Das Management von sensiblen Daten in die »Wolke« zu verlagern, also über Plattformen abzuwickeln, die nicht unter Kontrolle der hauseigenen IT stehen, mag auf den ersten Blick paradox erscheinen. Bei näherer Betrachtung gibt diese Möglichkeit, unter bestimmten Voraussetzungen, jedoch noch mehr Sicherheit.

Dies beginnt schon mit der Auswahl des externen Rechenzentrums. Hier kann sich der Kunde detailliert über die Sicherheitslevels und Gewährleistungsbedingungen der verschiedenen Rechenzentren sowie über den Standort des Rechenzentrums in verschiedenen Ländern mit unterschiedlichen gesetzlichen Bestimmungen, beispielsweise für Datenschutz, informieren. Professionelle Rechenzentren sind zertifiziert und stellen eine hochredundante Infrastruktur bereit, in der Server mit minimalen geplanten Ausfallzeiten arbeiten können. Sämtliche für den Betrieb benötigten Anlagen sind mehrfach vorhanden.

Die Cloud bietet vor allem für Dokumente, die über Firmengrenzen hinweg von vielen Externen bearbeitet werden sollen, durch deren einfache Verfügbarkeit via Browser einen großen Vorteil. Jedoch muss gewährleistet werden, dass jeder Zugriff, jede Änderung an den Dokumenten sorgfältig mit Datumstempel, Namen vom Document Compliance Management protokolliert wird.

Um die Gefahren von »Mitlesern« auszuschließen, werden die Kommunikationsströme vom Anwender zur Cloud häufig verschlüsselt. Handelt es sich um vertrauliche Dokumente, so muss nicht nur der Kommunikationsweg zum Server verschlüsselt sein, sondern selbstverständlich auch die Arbeitsumgebung auf dem Server. Ebenfalls werden die Dokumente nur verschlüsselt in die »Cloud« abgelegt.

Durch ein intelligentes und fein granuliertes Berechtigungssystem wird jedem einzelnen Projektmitglied ein eigenes Rechteprofil bereitgestellt. Um in das Document Compliance System in der »Wolke« eintreten zu können, ist ein kontrollierter und maximal abgesicherter Zugang von Nöten. Selbstverständlich muss auch der Betreiber des Rechenzentrums und Servers ausgeschlossen werden. Bei hochvertraulichen Dokumenten können Administratoren definitiv keinen Einblick in die Arbeitsumgebung oder gar in die Dokumente nehmen.

Document Compliance in der »Secure Cloud« bietet maximale Sicherheit

Zusammenfassend lässt sich festhalten, dass eine Document Compliance Strategie, die auf einem Cloud- oder Software-as-a-Service-Modell basiert, die höchstmögliche Sicherheit bieten kann. Hochsicherheits-Datencenter erfüllen in der Regel höhere Sicherheitsstandards als die der meisten Unternehmen, deren Kernkompetenz nicht im Betreiben großer Serverfarmen mit der notwendigen Sicherung besteht. Redundant ausgelegte Stromversorgungen und Internet-Leitungen, moderne IT-Komponenten und aktuelle IT-Security-Standards sind dort die Regel.

Investitionskosten werden zu operativen Kosten

Für den Kunden haben Cloud-/SaaS-Services generell Vorteile: Die größere Flexibilität und eine bessere Kostenkontrolle. Er kann nicht nur IT-Ressourcen aller Art schnell und einfach ordern, sondern im Rahmen von DCM auch die gesamte vertrauliche Kommunikation und somit wichtige Informationsprozesse über die Firewall hinaus geschützt in die Cloud verlagern. Da Cloud-Computing-Lösungen in hohem Maße skalierbar sind, ist dies in fast unbegrenztem Maße möglich. Ein weiterer Vorzug dieses Konzepts: Kapitalkosten werden zu operativen Kosten. Statt Geld in eigene Server, Speichersysteme und Software zu stecken, kauft der Kunde nach Bedarf Ressourcen ein. Aus Investitionskosten werden somit operative Kosten, die sich klar kalkulieren lassen. Versteckte Kosten oder unabsehbare Folgeinvestitionen gibt es nicht. So wird zum einen kein Kapital gebunden, zum anderen lassen sich Dienste »on demand« hinzubuchen oder abbestellen, je nach Bedarfslage.

Resümee

Ganzheitliche Document-Compliance-Lösungen schaffen einen sicheren Raum für vertrauliche Dokumente auch in der Cloud. So bieten sie Unternehmen eine Alternative zu Lösungen, die das Unternehmen in Eigenregie implementiert. Der Nutzer einer DCM-Lösung arbeitet mit sensiblen Dokumenten, ohne Abstriche bei Sicherheit und Komfort machen zu müssen. Im Gegenteil: Unternehmenskritische Daten sind in einem zertifizierten Hochsicherheits-Daten-Center eines spezialisierten Anbieters in der Regel besser aufgehoben als auf hauseigenen Servern und Speichersystemen. Hinzu kommt der Faktor Kosten. Sie lassen sich im Rahmen eines Software-as-a-Service-Modells besser kontrollieren. Durch DCM entstehen nützliche Vorteile für alle Unternehmen und Organisationen.



Die **Brainloop AG** mit Sitz in München und Boston ist der führende Anbieter von Document Compliance Management-Lösungen, die den hochsicheren und jederzeit nachvollziehbaren Austausch vertraulicher Dokumente ermöglichen.

Weitere Informationen zur Brainloop AG finden Sie im Internet unter

www.brainloop.de

Brainloop AG

Franziskanerstr. 14

81669 München · Deutschland

T: +49 (89) 444 699 0

info@brainloop.de

www.brainloop.de

Brainloop Inc.

One Broadway, 14th floor

Cambridge, MA 02142 · USA

T: +1 (800) 517 3171

info@brainloop.com

www.brainloop.com