



SearchSecurity.de
Entscheiderwissen für Security-Professionals

Sicherer Datenaustausch beim Finanzdienstleister Deloitte

Dokumente zeitnah, ortsunabhängig und sicher in der Gruppe bearbeiten

09.03.2010 | Autor: Ulrike Dreischer-Wanner



Speziell im Bereich der Finanzdienstleistungen ist Vertraulichkeit und Verlässlichkeit der Informationen oberstes Gebot. Wenn es um den Kauf oder die Verschmelzung von Unternehmen (M&A) geht, kann jede Indiskretion und jedes Dokument in falschen Händen Millionen kosten. Die Brainloop-Technologie für sichere Datenräume – virtuelle Datenbereiche auf besonders gesicherten Servern – hilft hier auch beim sicheren Datenaustausch zwischen Personen aus unterschiedlichen Unternehmen.

Deloitte Financial Advisory GmbH mit Sitz in Wien ist einer der führenden Transaktionsberater im österreichischen M&A Markt. Das angebotene Leistungsspektrum umfasst neben der Unternehmensbewertung und der Durchführung von Due Diligence Prüfungen auch die Begleitung und Beratung von Unternehmensveräußerungen und -übernahmen sowie Fusionen.

Bei Deloitte Financial Advisory erfolgt während der Phase der Due Diligence die sorgfältige Analyse, Prüfung und Bewertung des Zielunternehmens. Virtuelle Datenräume bieten in diesem Zusammenhang den entscheidenden Vorteil, Dokumente mehreren Parteien zeitnah und ortsunabhängig zur Verfügung stellen zu können. Potentielle Bietergruppen haben so die Möglichkeit, gleichzeitig und dennoch getrennt voneinander Einsicht in entscheidungsrelevante Unterlagen zu nehmen.

„Wir waren schon lange auf der Suche nach einer Anwendung, um dieses Prozedere auf ein sicheres Fundament zu stellen. Die DCM (Document Compliance Management)-Lösung von Brainloop Secure Dataroom entspricht unserem Wunsch, Dokumente für den Unternehmensverkauf potentiellen Investoren zeitnah, ortsunabhängig und vor allem für alle Parteien sicher zur Verfügung zu stellen. Die Anwendung ist browserbasiert, leicht bedienbar und angriffsicher gestaltet.

Mehrere Bietergruppen können parallel und zugleich getrennt voneinander Einsicht in die vertraulichen Unternehmensinformationen nehmen. Alle Zugriffe der unterschiedlichen Parteien während des Prozesses werden vollständig und lückenlos aufgezeichnet. So können sämtliche Datenraumzugriffe auf Dokument- und Userbene nachvollzogen werden.“, erläutert Paul Günther, Senior Consultant bei Deloitte Financial Advisory GmbH, die Entscheidung.

Einfache und sichere Kommunikation weltweit

Durch das integrierte Versionsmanagement können Adressaten weltweit jederzeit auf die Letztversion eines Dokuments zugreifen, welches verschlüsselt übertragen wird. Paul Günther kommentiert: „Die Datensichtung soll schnell erfolgen können und nicht durch zusätzliche Einarbeitungs- und Inbetriebnahmezeiten unnötig verzögert werden. Die intuitive Benutzeroberfläche des Datenraums ist an Windows Explorer angelehnt und dementsprechend einfach zu bedienen. Einschulungen können daher entfallen.“

Der Datenraum zeichnet sich durch einen End-to-End Schutz vom Einloggen in den Datenraum bis hin zum Download eines Dokuments auf den eigenen Rechner aus. Jede Form der Datenübertragung, ob es nun ein Up- bzw. Download oder die Anzeige von Datenraumgehalten betrifft, wird über eine 128-Bit Verschlüsselung geschützt. Durch die Nutzer-Authentifizierung mittels Password und SMS-PIN und das rollenbasierte Rechtekonzept stellt der Brainloop Secure Dataroom sicher, dass der Anwender ausschließlich Zugriff auf die für ihn bestimmten Informationen erhält und diese dann – je nach vordefinierter Rolle - „nur lesen“, herunterladen oder sogar bearbeiten darf.

Die lückenlose Aufzeichnung und Archivierung aller Informationsflüsse in Form des integrierten Audit-Trails des Brainloop Secure Dataroom schafft Transparenz und entspricht modernen Compliance-Anforderungen. Eine nachvollziehbare Protokollierung aller Zugriffe während des gesamten M&A Projektes ist damit sichergestellt. „Diese Funktionalität rundet das Profil der Lösung in idealer Weise ab, da alle Bearbeitungsschritte detailliert aufgezeichnet werden und damit jederzeit nachvollzogen werden können“, begründet Paul Günther.

Redakteur: Peter Schmitz

<http://www.searchsecurity.de/themenbereiche/sicherheits-management/risk-management/articles/253946/index.html>