

Erfolg rund um den Globus

Union Investment Real Estate verwahrt vertrauliche Dokumente in virtuellem Hochsicherheitstrakt

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 diesem nicht oder nicht direkt angehören. Die für diese Geschäftsprozesse relevanten digitalen Dokumente können nicht hinter den Firewall-Systemen des eigenen Hauses gehalten werden, sondern müssen auf sichere Art unter den berechtigten Personen zirkulieren können. Die Union Investment Real Estate AG nutzt deshalb für den nachvollziehbaren Dokumententransfer mit unabhängigen Sachverständigen den virtuellen Datenraum der Brainloop AG.



Entspanntes Arbeiten - auch über interne und externe Unternehmensgrenzen hinweg.

Zu den vertraulichen Kommunikationsprozessen, die die Union Investment Real Estate AG über den Datenraum abwickelt, gehört der Austausch großer Datenvolumina (Pläne in Auto-Cad, Bilder, Exposés) mit externen Fachkundigen im Rahmen ihres weltweiten Immobilienankaufs. „Wenn wir Immobilien bewerten und kaufen, sind wir auf den schnellen und vollständigen Austausch von Informationen mit vielen verschiedenen Sachverständigen im In- und Ausland angewiesen“, so Friedlind Krause, Controlling, Union Investment Real Estate AG.

Hochsicherheitstrakt für vertrauliche digitale Dokumente

Ganzheitlich konzipierte Document Compliance Management (DCM) Systeme benötigen eine Art digitalen Hochsicherheitstrakt, in dem allen Zugangsberechtigten vertrauliche Dokumente gemäß ihrem jeweiligen Rechtstatus zugänglich sind. Dieser Sicher-

heitstrakt muss problemlos über einen Web-Browser durch Endanwender z.B. aus der Vorstands- oder Geschäftsführungsebene bedient werden können. Durch digitales Dokumentenmanagement und dessen Einbindung in die geschäftlichen Workflows werden indes nicht nur die Verarbeitungsmöglichkeiten erweitert, sondern es werden vor allem auch die Entscheidungsprozesse erheblich beschleunigt. Ganz gleich, ob es sich um die Vorbereitung von Firmenkäufen, um Abstimmungsprozesse im Vorfeld von Hauptversammlungen oder den Schutz geistigen Eigentums handelt. Der Ort, an dem heute Dokumente vor unbefugter Einsichtnahme und Änderung geschützt werden müssen, ist das Extranet. Unternehmen sind gegenwärtig in größere Beziehungsgeflechte integriert, außen und innen verschwimmen zusehends. Doch gerade an diesen Stellen gilt es, brisante Dokumente auszutauschen. Um die vom Gesetzgeber geforderte Sicherheit zu erreichen, taugt der traditionelle Firewall-Ansatz nicht viel. Schließlich sind gerade hier Dokumente und Daten zu sichern, die ständig zwischen den Firewalls der verschiedenen Protagonisten hin und her reisen. Wegsperrern nutzt also wenig, zerstört vielmehr die geschäftlichen Abläufe. Ein adäquater Sicherheitsansatz muss ganz im Gegenteil das „Reisen der Dokumente“ zum Ausgangspunkt nehmen und dann die Reiseroute und die zusteigenden Personen absichern und dokumentieren. Für vertrauliche Dokumente können die verschiedenen technischen Komponenten der Verschlüsselungstechnik unter einer integrierenden Applikationsoberfläche zusammengeführt werden, die keine IT-technischen Kenntnisse voraussetzt, sondern vom Endanwender quasi intuitiv bedient werden kann.

Was ist der Secure Dataroom?

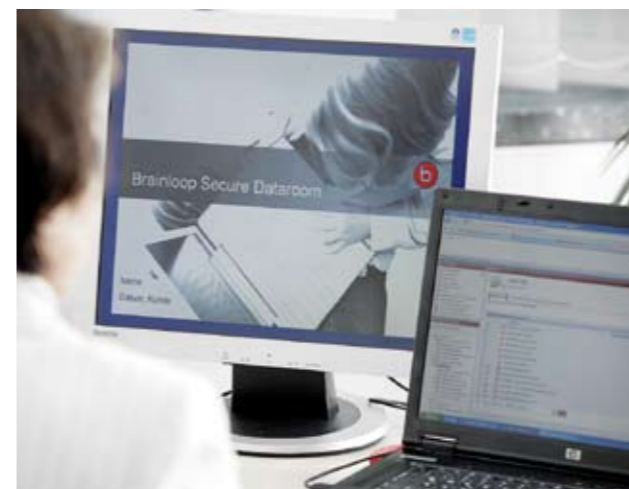
Der Secure Dataroom ist ein virtueller Dokumententrezor, mit dem die Ablage, Bearbeitung und Verteilung von streng vertraulichen Dokumenten im Unternehmen und über Unternehmensgrenzen hinweg abgesichert sowie vor internen und externen Angreifern geschützt werden können. Sämtliche Zugriffe und Aktionen werden protokolliert und damit nachvollziehbar. Der Raum lässt sich nutzen für die sichere Ablage, nachvollziehbare Bearbeitung und Verteilung von vertraulichen Dokumenten wie Verträge, Quartalsberichte, Personal- und Projektunterlagen. Beispiele von Einsatzgebieten sind Vertragverhandlungen, Projektdurchführung, Erstellen von Quartalsberichten und die Kommunikation zwischen Vorstand und Aufsichtsrat.

„Wenn wir Immobilien bewerten und kaufen, sind wir auf den schnellen und vollständigen Austausch von Informationen mit vielen verschiedenen Sachverständigen im In- und Ausland angewiesen.“

Friedlind Krause, Controlling, Union Investment Real Estate AG

Union Investment Real Estate AG

Die Union Investment Real Estate AG ist einer der in Europa führenden Investment-Manager für Immobilien. Das Unternehmen verbindet über 40 Jahre Expertise im Asset Management von Immobilien mit der Kapitalmarkterfahrung der Union Investment Gruppe. Als eine der größten Kapitalanlagegesellschaften verwaltet das Unternehmen heute ein Fondsvermögen von 14,5 Milliarden Dollar.



Über den Datenraum kann zügig auf aktuelle Dokumente zugegriffen werden.

Kontrolle über den gesamten Lebenszyklus

Eine DCM-Lösung hat den gesamten Lebenszyklus eines Dokuments 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 gelöscht. So kann schnell auf neue Gegebenheiten reagiert und ein Dokument auch nach dem Übertragen auf den Arbeitsplatzrechner gesperrt beziehungsweise seine Verwendung zeitlich und funktional begrenzt werden.

Die betreffenden Informationen müssen in Sekundenschnelle zwischen den beteiligten Personen ausgetauscht oder auch gemeinsam bearbeitet werden können. Bei diesen digitalen Abläufen und Kooperati-

onen muss zu jedem Zeitpunkt und an jeder Stelle des Prozesses sicher gestellt 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. Das ist durch entsprechende Verfahren und Kontrollsysteme zu gewährleisten, wobei die diesbezüglichen Regeln die gesetzlich vorgeschriebenen Vorsorge- und Sorgfaltspflichten ebenso umfassen wie branchenspezifische Normen. Solche Systeme müssen vertrauliche Dokumente von ihrer Entstehung bis zur Archivierung oder Löschung begleiten. Ebenso ist nahtlos zu dokumentieren, wer wann diese Dokumente eingesehen, verschickt oder verändert hat.

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 sicher gestalten.

DCM als SaaS

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-beziehungswise Funktionstrennungsprinzip zu binden. Die Administration der IT-Infrastruktur kann und sollte überdies in verschiedene Zuständigkeits Ebenen aufgeteilt werden. Daher erscheint für ein DCM-System eine browserbasierte Mietlösung (Software-as-a-Service, SaaS) ideal. Es wird dabei keine Client-Software benötigt und die IT-Infrastruktur wird von Spezialisten quasi unsichtbar, aber effizient bereitgestellt und gepflegt. Die zu bedienende Oberfläche stellt sich für die Nutzer als eine Anwendung ähnlich einem Office-Programm dar. Das Strukturspektrum reicht von einer durchgängigen Verschlüsselung, die den gesamten Lebenszyklus abdeckt, und einer starken Authentifizierungskomponente über eine stringente Transportsicherung, unter anderem für E-Mail oder Dokumentenkennzeichnungsverfahren 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.