

Virtueller Datenraum

Kommentar von Nicole Dietrich, Senior Director Marketing bei der Brainloop AG, über webbasierte Dokumententresore, die neben der elektronischen Signatur eine weitere Möglichkeit darstellen, um Dokumente sicher vom Sender zum Empfänger zu transportieren.

> Die in webbasierte Dokumententresore eingestellten Dokumente können ausschließlich vom berechtigten Empfänger abgerufen und bearbeitet werden. Das hinterlegte Sicherheitskonzept schützt die Dokumente vor unbefugtem Zugriff und gewährleistet eine lückenlose Nachvollziehbarkeit aller Aktivitäten.

Zu den Schutzfunktionalitäten zählen serverseitig die Zwei-Faktor-Zugangskontrolle, die verschlüsselte Ablage und Datenübertragung, die Abschirmung des Betreibers und die revisionssichere Protokollierung. Dabei stellt die Zwei-Faktor-Zugangskontrolle eine hochsichere Authentisierungsmethode dar, die beispielsweise auf kurzlebigen Einmalschlüsseln basiert, die per SMS verschickt werden. Ein flexibles Berechtigungssystem sorgt für die genaue Definition und Überwachung von Rollen und Rechten für die Teilnehmer des Datenraums.

Zur verschlüsselten Ablage und Datenübertragung zählt die Ablage vertraulicher Dokumente auf dem Server mit 256-Bit-Verschlüsselung. Auf diese Weise werden Dokumente vor unbefugtem Zugriff geschützt. Jede Datenübertragung zwischen Client und Server wird über 128-Bit-Verschlüsselung geschützt.

Durch die Trennung von Anwendungs- und Systemadministration sowie Freigabeprozesse mit Vier-Augen-Prinzip für sicherheitsrelevante Administrationsfunktionen werden vertrauliche Dokumente auch vor dem Zugriff durch IT-Administratoren des Betreibers geschützt. Zudem werden alle Aktionen in einem Audit-Trail unveränderbar aufgezeichnet. Dies gewährleistet die Transparenz von Änderungen und Zugriffen und die Dokumentation aller Informationsflüsse.



Name: Nicole Dietrich
Position: Senior Director Marketing bei Brainloop

Auch nach dem Download werden die Dokumente geschützt, indem sie als automatisch generierte Brainmark-Version auf den Client heruntergeladen werden. Dabei kann eine solche Version je nach Schutzbedürftigkeit des Dokumentes technisch unterschiedliche Ausprägungen haben. Brainmark-Versionen basieren auf den Standardformaten PDF oder XPS, versehen mit zusätzlichen Schutzmethoden.

Die Vergabe von Sicherheitskategorien definiert die Schutzbedürftigkeit eines Dokumentes und damit die anzuwendende Schutzmethode. So können unternehmensinterne Informationsschutzrichtlinien direkt umgesetzt werden. Typische Sicherheitsstufen sind etwa »intern«, »geheim« und »streng vertraulich«. An diese Kategorien sind definierbare Berechtigungen gebunden, die bestimmen, wie der Dokumentenempfänger zugreifen kann. Des Weiteren verhindert der integrierte Secure Document Viewer den Download von Dokumenten aus dem Datenraum. Statt einer Originaldatei werden so bei der Präsentation von Dokumenten nur gekachelte Bildfragmente auf den Arbeitsplatz übertragen. Dort verbleiben also keine vertraulichen Daten.

Dynamisch generierte Wasserzeichen bieten zusätzlichen Schutz vor der unberechtigten Weitergabe von Unterlagen. Inhalt und Layout des Wasserzeichens sind konfigurierbar. Eingesetzt werden derartige Datenräume für vertrauliche, unternehmensübergreifende Vorgänge sowie für die vertrauliche Kommunikation mit Kunden und Partnern. Zu den Anwendern zählen u.a. Deutsche Telekom, T-Systems, ThyssenKrupp, Postbank, Premiere oder die Landesbank Berlin. <

„Dynamisch generierte Wasserzeichen bieten zusätzlichen Schutz vor der unberechtigten Weitergabe von Unterlagen.“