

# Virtueller Datentresor

Schutz vertraulicher Dokumente über Unternehmensgrenzen hinweg

Heutzutage werden wichtige Geschäftsvorgänge nicht mehr ausschließlich intern abgewickelt. Der Austausch und die Zusammenarbeit mit externen Dienstleistern werden immer wichtiger. Dabei verlassen auch vertrauliche Dokumente die Unternehmensgrenzen. Diese neuen Formen der Zusammenarbeit in und außerhalb von Unternehmen erfordern eine neue Form der Datensicherheit. Gefragt ist daher eine Sicherheitslösung zur gemeinsamen und sicheren Nutzung von vertraulichen Informationen.

■ Markus Seyfried



Bild: Getty Images

**D**er Austausch mit Partnern, Subunternehmern und anderen externen Fachleuten ist für viele Unternehmen zum essentiellen Bestandteil ihrer Arbeit geworden. Aber auch interne Arbeitsprozesse können die Sicherheit von vertraulichen Dokumenten gefährden. Leistungen externer Dienstleister werden immer häufiger in Anspruch genommen. Auch vertrauliche interne Dokumente von Unternehmen werden zur Bearbeitung außer Haus gegeben. Quartalsberichte etwa werden oft noch vor ihrer Veröffentlichung außerhalb des Unternehmens verschickt. Übersetzer, Agenturen und andere externe Dienstleister erhalten sie zur weiteren Bearbeitung. Vielen werden auf Anhieb mehrere Beispiele für kooperationsintensive, die Grenzen von Unternehmen überschreitenden Geschäftsprozesse in den Sinn kommen. Der Trend zur Zusammenarbeit von Personen, die weltweit an weit verstreuten Orten tätig sind, wird sich weiter intensivieren.

Aber auch interne Arbeitsprozesse können die Sicherheit von vertraulichen Dokumenten gefährden. Zum Beispiel sind an der Vorbereitung eines wichtigen Meetings und den zu-

gehörigen Unterlagen oftmals viele Personen unterschiedlicher Hierarchieebenen eingebunden. Ein weiteres Risiko sind auch die im Zuge der flexiblen Arbeitsmodelle – wie Homeoffices – gewährten externe Zugriffe auf interne Unternehmensdaten. Diese Möglichkeiten nutzen inzwischen nicht nur Führungskräfte, die unterwegs arbeiten wollen.

Durch die genannten Beispiele und noch viele weitere Faktoren entstehen Sicherheitsrisiken. Zwar soll die firmeninterne IT-Abteilung das Unternehmen sicher machen, doch auch sie können nicht alle entstehenden Sicherheitslücken schließen. Diese Formen der Zusammenarbeit in und außerhalb von Unternehmen erfordern eine neue Datensicherung. Für Firmen ist es essenziell, dass die Prozesse zur erfolgreichen Zusammenarbeit sicher sind. Gleichzeitig dürfen sie nicht durch eine schwerfällige IT-Infrastruktur behindert werden. Anstehende Aufgaben dürfen nicht durch umständliche Sicherheitsfunktionen unnötig in die Länge gezogen werden. Gefragt ist daher eine Sicherheitslösung zur gemeinsamen und sicheren Nutzung von vertraulichen Informationen.



**Markus Seyfried**  
ist CTO bei Brainloop in München  
T +49-89-4444699-77  
F +49-89-4444699-99  
presse@brainloop.com

## Die Lösung

Der Brainloop Secure Dataroom beispielsweise ermöglicht das benutzerfreundliche und gleichzeitig hochsichere unternehmensübergreifende Management vertraulicher Dokumente. Der Datenraum ist ein so genannter elektronischer Safe, in den Dokumente eingestellt und hochgeladen werden können. Ausschließlich berechtigte Empfänger, innerhalb und außerhalb des Unternehmens, können sie abrufen und bearbeiten. Üblicherweise verlassen die Dokumente den Safe nicht. Besonders wichtig ist die Möglichkeit, Berechtigungen aufgrund der Rolle des einzelnen Mitarbeiters zu vergeben. So kann der Zugriff auf ein Dokument kontrolliert werden. So gibt es die Möglichkeit einem Mitglied ein „Nur-Lesezugriffsrecht“ zuzuweisen. Dokumente werden in diesem Fall automatisch konvertiert und mit Wasserzeichen versehen.

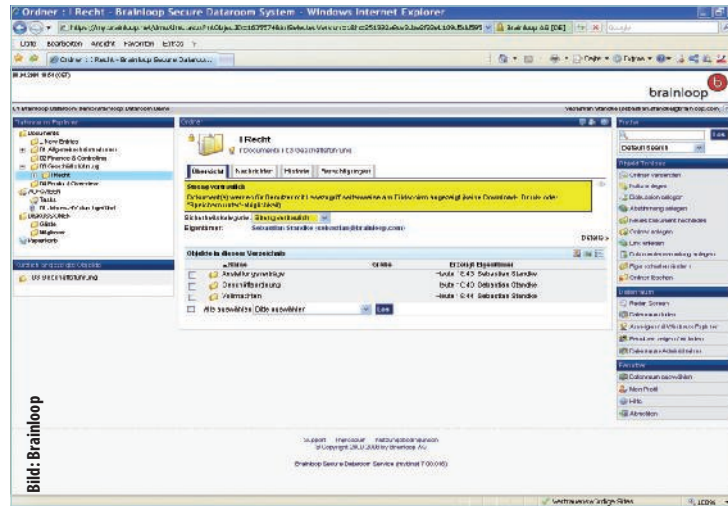
Der Datenraum wird vornehmlich für vertrauliche, unternehmensinterne und unternehmensübergreifende Vorgänge eingesetzt, etwa als elektronischer Boardroom zur Kommunikation und Beschlussfassung zwischen Vorstand und Aufsichtsrat, für vertrauliche unternehmensübergreifende Projekte oder als virtueller Dealroom bei M&A-Transaktionen, sowie für die nachvollziehbare, vertrauliche Kommunikation mit Kunden und Partnern.

Als Online-Anwendung ist der Datenraum von jedem Ort der Welt und zu jeder Zeit verfügbar. Aufgrund der intuitiven Benutzeroberfläche ist kein Training notwendig, sodass auch weniger EDV-erfahrene Anwender sich sofort gut zurechtfinden können. Mit dem Brainloop Secure Dataroom erhält der Anwender eine End-to-End-Sicherheitslösung. Jeder Anwender kann diesen umfangreichen und durchgängigen Dokumentenschutz auch ohne spezielles Know-how in seiner täglichen Arbeit einsetzen und dabei die unternehmensinternen Sicherheitsvorgaben einhalten. Zusätzlich werden nicht nur Dokumente, sondern auch die E-Mails zwischen Datenraumnutzern jederzeit effektiv geschützt. Zum verbesserten Schutz der Kommunikation zwischen den Datenraummitgliedern werden die E-Mails verschlüsselt oder als Stellvertreternachricht verschickt, die der Anwender dann im Datenraum in seinem persönlichen Posteingang sicher lesen kann.

## Überblick

Der Datenraum ist ein wertvolles Tool bei sicherheitskritischen Geschäftsprozessen. Die Vorteile eines solchen Datenraums sind

- Konsequenter Schutz auf der Seite des Servers: Zwei-Faktor Zugangskontrolle /



Screenshot aus dem Datenraum: Per Auswahlmenü kann ein einzelnes Dokument mit einer bestimmten Sicherheitskategorie – hier „streng vertraulich“ – ausgestattet werden.

Zugriffsrechte, Verschlüsselte Ablage & Datenübertragung, Abschirmung des Betreibers, Revisions sichere Protokollierung, Integrierter Virens scanner

- Konsequenter Schutz auf dem Client Rechner: Sichere Dokumentenauslieferung nach dem Download, Wahl der Sicherheitskategorien, Secure Document Viewer, Wasserzeichen, geschützte Dokumentenanzeige und -bearbeitung mit Microsoft XPS und Microsoft RMS
- Durchgängiger und flexibler Schutz vertraulicher Email Inhalte
- Einfaches Nachvollziehen der gesamten Kommunikation im Datenraum
- Integriertes Dokumentenmanagement
- Effizientes, zentrales Bereitstellen der Dokumente für alle Beteiligte
- Erfüllung von Compliance-Anforderungen durch revisions sichere Protokollierung
- Intuitive Nutzung ohne Training, intelligente und benutzerfreundliche Handhabung
- Weltweite Verfügbarkeit, sicherer Zugriff jederzeit und überall per Web Browser
- Höchste Sicherheit, starke Authentifizierung sowie Verschlüsselung der Datenübertragung und Datenablage
- Schutz vor Zugriff des IT-Betreibers

## Die Anwender

Einige Unternehmen nutzen bereits den sicheren Datenaustausch mittels des Datenraums. Bei der Premiere AG etwa sollten Vorstandsunterlagen sicher versandt werden. Bisher erfolgte die Protokollierung und Ablage in Papierform, also beispielsweise per Fax. Dies war für das Unternehmen zu unsicher und ineffizient. Als Lösung kam der Brainloop Secure Dataroom ins Spiel. Premiere hat sich für den Einsatz des Datarooms entschieden, um die sichere Übertragung vertraulicher Informationen zu gewährleisten. Die

Zustellung von Dokumenten sollte flexibler gestaltet werden und auch die Kommunikation zwischen Aufsichtsrat und Vorstand sollte effizienter durchführbar sein. Durch den webbasierten Dokumententresor können die Mitglieder des Premiere Aufsichtsrats weltweit von jedem beliebigen Ort aus auf wichtige Informationen und Unterlagen zugreifen. Neben der hochsicheren Zustellung von vertraulichen Dokumenten wie Sitzungsprotokollen und Aufsichtsratsbeschlüssen nutzt Premiere den Secure Dataroom unter anderem auch zur Archivierung der Aufsichtsratsunterlagen. In einem zweiten Schritt will Premiere die Funktionen des Datarooms über die Grenzen von Vorstand und Aufsichtsrat hinaus zur hochsicheren Abwicklung vertraulicher Geschäftsprozesse nutzen.

## Fazit

Für die elektronische Kommunikation zwischen Personen, die an einem Projekt beteiligt sind, wird eine hochsichere und vor allem räumlich flexible Infrastruktur benötigt, die allen Beteiligten den permanenten Zugriff auf sämtliche Protokolle und Beschlüsse ermöglicht – egal von welchem Ort. Zum umfassenden Sicherheitskonzept der Brainloop Secure Dataroom Software gehören daher die verschlüsselte Ablage im virtuellen Datenraum, die kodierte Übertragung sensibler Dokumente und die verlässliche Authentifizierung der Anwender. Für den Zugriff auf unternehmenskritische Dokumente wie Aufsichtsratsunterlagen gibt es auch eine Zweifaktoren-Authentifizierung, die außer den Passwörtern zusätzliche Token benutzt, beispielsweise Mobiltelefone mit SMS oder Einmalschlüsseln. Zugleich wird jede Aktion im Datenraum, jeder Lesezugriff und jede Veränderung eines Dokuments, automatisch protokolliert. ■

Weiterführende Infos auf [www.sui24.net](http://www.sui24.net)

**more @ click** **S1068250**