

# Dokumente vor IT-Zugriff und Insidern schützen!

Der Umgang mit vertraulichen Dokumenten stellt hohe Anforderungen. Die heute eingesetzten Schutzmechanismen weisen oft Lücken auf. Auch dort, wo höchste Sicherheitsvorkehrungen herrschen, bleibt die Gefahr von Zugriffen Unberechtigter.

Die von Elca Informatik AG angebotenen Lösungen Brainloop «Secure-Boardroom»- und «Secure-Dataroom» schliessen diese Lücke. Bereits viele Verwaltungsrats- und Geschäftsleitungsorganisationen sowie auch Firmen, die Merger-&-Acquisitions-Prozesse durchführen oder externe Prüfungen von Geschäftsdaten benötigen, profitieren bereits von diesen Lösungen.

Es ist kein Geheimnis: Aufgrund zunehmend transparenter werdender Unternehmensgrenzen nehmen die unbeabsichtigten oder auch bewusst in Kauf genommenen Risiken bei der Sicherheit von vertraulichen Informationen ständig zu. Führungskräfte, die an unterschiedlichen Standorten arbeiten, lückenhafte Sicherheitsvorkehrungen, die Verfügbarkeit der Informationen rund um die Uhr, internetgestützte Applikationen sowie virtuelle Arbeitsgruppen tragen dazu bei, dass sich der Schutz von elektronisch gehaltenen Dokumenten oft zu einer grossen Herausforderung entwickelt. In Sachen Sicherheit für den Schutz dieser Dokumente wird vieles getan. Leitungen werden verschlüsselt, der Zugang zu Computer abgesichert. Lücken bleiben dennoch, speziell dann, wenn externe Stellen einbezogen werden müssen, aber auch gegenüber Insidern und der firmeninternen IT bestehen wesentliche Missbrauchsgefahren.

Gelangen höchst vertrauliche Dokumente in falsche Hände, richten sie oft grossen Schaden an. Die Auswirkungen reichen von einer schlichten Unannehmlichkeit bis hin zu gewaltigen Imageschäden für ein Unternehmen. Beispiele gibt es genügend.

## Hohe Risiken bei Dokumenten und E-Mail

Vorstands-, Geschäftsleitungs- und Kadermitglieder sowie deren Vertraute arbeiten laufend mit hoch sensiblen Dokumenten. Damit Vorteile wie rasche Aktualisierung und Verteilung genutzt werden können, sind die

vertraulichen Dokumente in elektronischer Form verfasst und werden auch auf elektronischem Weg verteilt. Es hat sich gezeigt, dass je relevanter ein Dokument ist, es umso häufiger auch wichtigen externen Personen, die nicht im Firmennetz eingebunden sind, zur Verfügung gestellt werden muss. Dokumente werden dabei meist via E-Mail oder Fax verteilt, manchmal auch umständlich mit einem Kurier. Die Verteilung von Dokumenten via diese klassischen Kanäle ist nicht mehr umfänglich kontrollierbar, die Gefahren lauern überall.

Die Probleme der Dokumentenverteilung durch E-Mail sind mannigfach und vielfältig:

- Unverschlüsselte E-Mail und Dokumente öffnen Tür und Tor für Missbrauch;
- Der E-Mail-Fluss und die Verteilung der Dokumente ist unkontrollierbar;
- Von einem Dokument können rasch viele Kopien existieren und sind im Nu überall verteilt;

- E-Mail-Verschlüsselungstechniken sind fehleranfällig und bedienungsunfreundlich;
- Ungeschützte Dateiablage erlaubt interne Angriffe;
- Verschlüsselte Serverablage schützt nicht vor böswilligen IT-Administratoren;
- Ohne gemeinsamen Dateiorder fehlt die Übersicht und die zielgerichtete Kommunikation;
- Versionierung von Dokumenten ist nicht nachvollziehbar;
- Eindeutige Kennzeichnung von Dokumenten ist nur mit hohem manuellem Aufwand möglich.

Die Brainloop-«Secure-Boardroom»- und «Secure-Dataroom»-Lösungen adressieren genau diese Schwachstellen. Nachfolgend werden zwei Anwendungen beschrieben, bei denen die hohen Sicherheitsanforderungen der Kunden vollumfänglich erfüllt wurden.

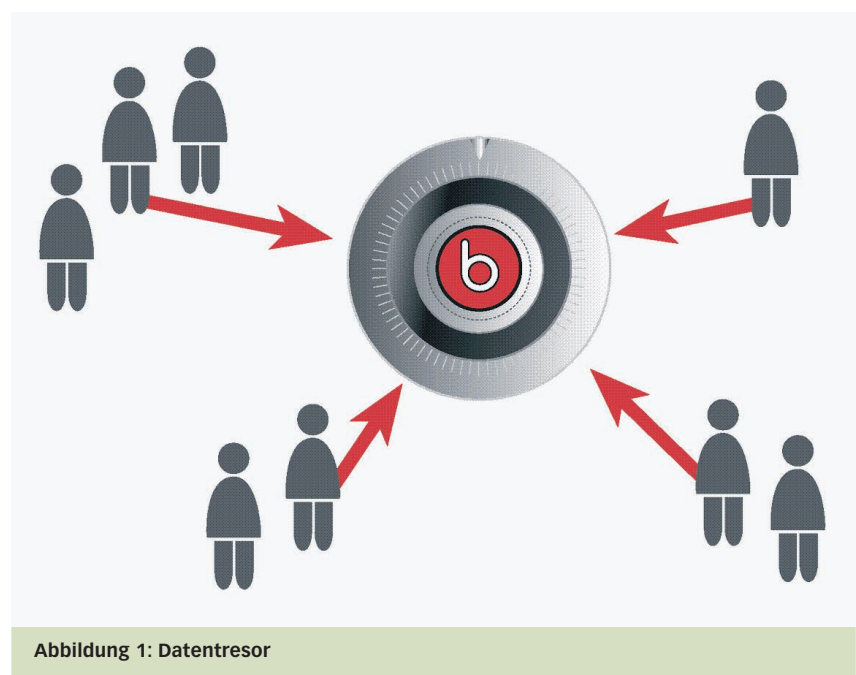


Abbildung 1: Datentresor

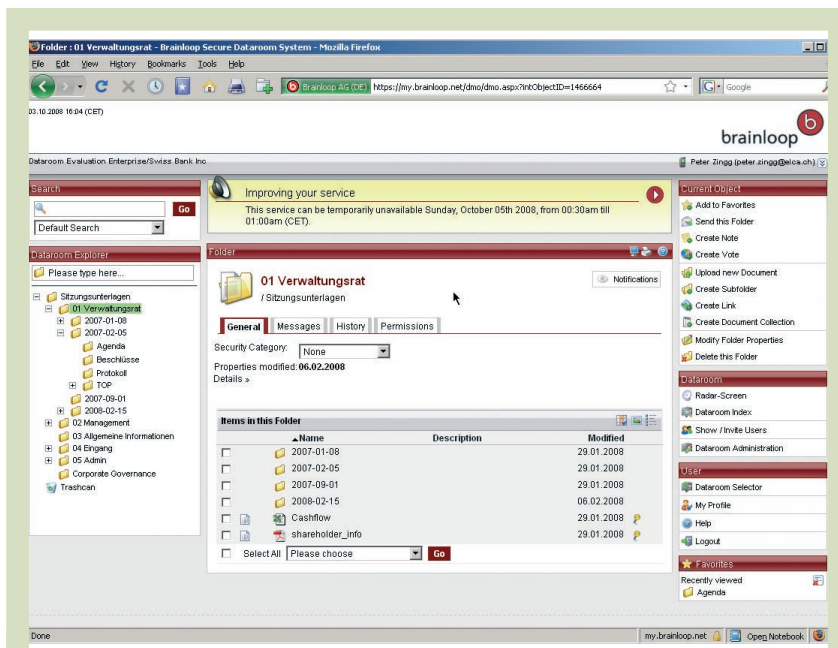


Abbildung 2: Beispiel einer Ansicht auf die Sitzungsordner

### Einsatz im Verwaltungsrat oder in der Geschäftsleitung

Der Verwaltungsrat eines grossen Finanzinstituts hat einen virtuellen, sicheren Datenraum («Secure-Boardroom») eingerichtet, in dem alle für die VR-Mitglieder relevanten Dokumente aufbewahrt und verwaltet werden. Selbstverständlich sind alle Dokumente verschlüsselt, und nur wer eine entsprechende Berechtigung besitzt, kann die Unterlagen ansehen. Das Sekretariat und registrierte Vertraute können Dokumente und Unterlagen zuliefern, haben aber nur Zugriff auf genau ihren Teil. Dokumente wie Sitzungseinladung, Traktanden mit allen dazugehörigen Unterlagen (Texte, Zeichnungen, Excel-Tabellen, Präsentationen usw.) werden übersichtlich strukturiert und in elektronische Ordner abgelegt. Der Sitzungsleiter verschickt mit der Einladung eine E-Mail mit einem Link auf diesen Ordner. Alle Unterlagen sind so gegliedert, dass jeder einzelne Verwaltungsrat sofort und einfach damit arbeiten kann. Jedes Dokument kann einzeln angesehen oder mit einem einzigen Befehl der Sitzungsordner ausgedruckt werden. Vertrauliche Dokumente sind über ein Wasserzeichen mit dem Benutzernamen markiert.

Auf diese Art gelangen keine Informationen in falsche Hände, die Dokumente sind immer sicher im Datentresor (siehe Abbildung 1). Nach ersten positiven Erfahrungen hat der Verwaltungsrat die Verwendung sicherer Datenräume auf zusätzliche Bereiche, die routinemässig mit sensiblen Informationen umgehen, ausgeweitet. Alle beteiligten Parteien, wie das Top-Ma-

nagement oder die Personalabteilung, die mit der Erstellung von Geschäftsberichten, Strategien und Firmenübernahmen vertraut sind, nutzen heute diesen virtuellen Datenraum.

### Einsatz im M&A-Prozess

Ein Institut bereitet den Verkauf eines grossen und bekannten Unternehmens vor. Für den Due-Diligence-Prozess mussten deshalb höchst sensible Dokumente an eine grosse Zahl potenzieller Bieter weitergeleitet werden. Die Herausforderung bestand darin, die Daten so zu verteilen, dass die Empfänger die Informationen nicht «behalten» also in irgendeiner Art speichern konnten. Nachgereichte detaillierte Informationen sollten dann ausschliesslich qualifizierten Bietern vorbehalten bleiben. Das für den Verkauf zuständige Team des Unternehmens wollte den Due-Diligence-Prozess in eigener Regie abwickeln, anstatt sich hierbei auf die IT-Abteilung zu verlassen.

Das Unternehmen richtete einen sicheren Verhandlungsraum (Secure-Dataroom) für die gesamte Dauer der Transaktion ein. Diese erstreckte sich von der anfänglichen Strategieplanung über das Einholen aller vertraulichen Informationen, die streng kontrollierte Due Diligence, die Verhandlungsführung, den Abschluss der Transaktion bis hin zur Integration nach der erfolgten Fusion. Der gesamte Prozess war zu 100 Prozent gesichert, vollständig kontrolliert, einfach in der Anwendung und erforderte keinerlei IT-Ressourcen. Eine verhältnismässig grosse Fusion liess sich dadurch sicher und erfolgreich abwickeln.

### Hauptmerkmale der Lösungen von Elca: Brainloop «Secure-Dataroom» und «Secure-Boardroom»

- Alle Dokumente sind im zentralen Datentresor verschlüsselt abgelegt.
- Die Dokumente sind jederzeit verschlüsselt.
- Anstelle von Dokumenten werden Links verschickt.
- Der Zugriff auf Dokumente kann von jedem beliebigen Ort über einen Internetbrowser sicher erfolgen.
- Der Zugriff auf Dokumente kann zeitlich limitiert und eingeschränkt werden.
- Der Zugriff auf den Datentresor erfolgt über ein starkes Authentisierungsverfahren.
- Jedem einzelnen Dokument kann zugeordnet werden, ob und wer dieses lesen, drucken, bearbeiten oder exportieren darf.
- Die aus dem System ausgedruckten Dokumente sind über ein Wasserzeichen markiert, womit jederzeit verfolgt werden kann, aus welcher Quelle dieses kommt.
- Die Verwaltung von Berechtigungen erfolgt durch die Benutzer und nicht durch die IT.
- Über «Backup und Restore» sind die Daten jederzeit gesichert, trotzdem gibt es keine Einsicht der IT/des RZ-Betreibers in die Dokumente.
- Die Bedienung ist einfach und selbsterklärend.
- Die revisionssichere Nachvollziehbarkeit aller Aktionen ist gewährleistet.

### Für weitere Auskünfte:

ELCA Informatik AG  
Steinstrasse 21, Postfach  
CH-8003 Zürich  
Tel. +41 44 456 32 11  
info@elca.ch  
www.elca.ch