

Sicherheit und Betriebsführung

Die Document Compliance Lösung der Brainloop AG ermöglicht die Bearbeitung und Verteilung streng vertraulicher Dokumente über Unternehmensgrenzen hinweg. Durch eine starke Verschlüsselung und eine Abschirmung aller Dokumente vor unbefugtem Zugriff interner und externer Angreifer wird die Zusammenarbeit in ein hochsicheres Umfeld verlagert. Durch vollständige Nachvollziehbarkeit und Protokollierung aller Zugriffe und Aktionen werden weitere Compliance-Voraussetzungen erfüllt. Angewandt werden die Lösungen u.a. in der Gremienkommunikation, in Personalabteilungen sowie beim Finanz- und Vertragsmanagement.

Ihre Vorteile im Überblick:

- › Konsequente Abschirmung der System- und Applikations-Administration
- › Restriktive Zugangskontrolle
- › Durchgehende Verschlüsselung in allen Phasen
- › Audit-Trail für vollständige Nachvollziehbarkeit aller Aktionen
- › Sicherheitskategorien für die durchgängige Umsetzung von Unternehmens-Sicherheitsrichtlinien
- › Integration von Information Rights Management Technologien zum Schutz von Dokumenten bis hin zum Empfänger und auf seinem Rechner
- › Als SaaS-Service verfügbar – gehostet im hochsicheren, zertifizierten Rechenzentrum
- › Keine Client-Installation
- › Server sind in verschiedenen Ländern mit unterschiedlich restriktiven Datenschutzgesetzen verfügbar, z.B.: Schweiz, Luxembourg, Deutschland

Absicherung der vertraulichen Dokumente durch Document Compliance im gesamten Unternehmen

Um die Sicherheit und den Compliance Anspruch bei allen schützenswerten Unterlagen eines Konzerns zu gewährleisten, ist eine sichere und abteilungsübergreifend einsetzbare Lösung notwendig. Überall, wo vertrauliche Dokumente, wie Finanzzahlen, personenbezogene Daten, Strategiepapiere oder ähnliches bearbeitet und mit externen Dritten ausgetauscht oder vor Unbefugten geschützt werden müssen, sind besonders hohe Maßnahmen zum Schutz anzuwenden.

DOCUMENT COMPLIANCE DURCH SICHERHEIT

Abschirmung des Betreibers

Der Brainloop Server ist eine Applikationsplattform, auf der mehrere Mandanten und ihre virtuellen Datenräume, parallel voneinander abgeschirmt, koexistieren. Jeder Datenraum verfügt über seine eigenen Schlüssel und Schutzkonfigurationen und kann unabhängig vom Applikationsmanagement verwaltet werden. Wesentliches Merkmal der Architektur ist die konsequente Trennung von Aufgaben des Datenraum-Managements, der Applikations-Administration und der System- bzw. Infrastrukturadministration. Technologisch ist die Applikation eine

Microsoft .NET Anwendung, die MS SQL für die Speicherung von Konfigurations- und Systemdaten nutzt. Die zu schützenden Dokumente werden nicht in der Datenbank gespeichert, sondern in verschlüsselter Form auf einem NAS-Server abgelegt.

Datenraum-Center

Ein Datenraum-Center ist ein gekapselter und unabhängig administrierbarer, logischer Mandant, der seinerseits mehrere Datenräume enthält. Das Datenraum-Center erlaubt die einheitliche Verwaltung von Nutzern, Sicherheitsrichtlinien, Templates, Stylesheets, Reporting und Abrechnung über Datenräume hinweg.



Integrierte Benutzerverwaltung

Jeder Datenraum verfügt über seine eigene Benutzerverwaltung. Benutzer werden über eine E-Mail Adresse und ein vom jeweiligen Benutzer selbst gewähltes Passwort identifiziert. Anforderungen bezüglich eines Passworts sind über eine Passwort-Policy festgelegt (Passwortlänge und Passwort-Aging). Pro Datenraum sind zusätzliche Methoden zur Authentisierung konfigurierbar.

Steuern der Sicherheitskategorien

Es können individuelle Sicherheitskategorien definiert werden, die die kundenspezifischen Informationsschutzrichtlinien direkt umsetzen. Dadurch wird die Berechtigungspflege stark vereinfacht. Durch einen einzigen Mausklick des berechtigten Benutzers wird die entsprechende Sicherheitskategorie ausgewählt und legt so den Zugriff auf einzelne Dokumente oder ganze Ordner fest. Typische Sicherheitsstufen sind zum Beispiel „intern“, „geheim“ und „streng vertraulich“. An die Sicherheitskategorien sind definierbare Berechtigungen gebunden, die z. B. die Ausprägung der Brainmark-Version für einen Benutzer bestimmen.

Zugangskontrolle

Schutz der Passwörter

Um das manuelle oder maschinelle Testen von Passwörtern und Token zu verhindern, werden Fehlversuche zusammen mit der IP-Adresse protokolliert und stehen dem Applikationsadministrator zur Einsicht zur Verfügung. Außerdem wird der Benutzer-Account nach einer vordefinierten Anzahl von Fehlversuchen für eine konfigurierbare, begrenzte Zeit gesperrt.

Zwei-Faktor-Authentisierung

Optional kann eine zusätzliche, Token-basierte Authentisierung aktiviert werden. Hierbei werden über SMS kurzlebige Einmalschlüssel verschickt, die dann zur Authentisierung eingegeben werden. Diese Option kann für jeden Datenraum separat oder auch nur für sicherheitskritische Operationen, wie z. B. das erstmalige Registrieren der Benutzer oder den Zugriff auf die Sicherheitskonfiguration eines Datenraums, aktiviert werden. Es ist einstellbar, wie oft ein Benutzer seine Identität über den Token bestätigen muss: Bei jeder Anmeldung, einmal täglich oder nur einmal wöchentlich. Die Verwendung von per SMS versendeten Einmalschlüsseln eignet sich insbesondere für den unternehmensübergreifenden Einsatz, denn ein Mobiltelefon ist meistens verfügbar. Darüber hinaus wird der Verlust eines Mobiltelefons schnell bemerkt und das Gerät sofort gesperrt. Benutzer ohne Mobiltelefon können den Token optional per E-Mail empfangen.

Zertifikatsbasierte Authentisierung

Eine bestehende Infrastruktur für die Authentisierung, basierend auf Zertifikaten, kann nahtlos integriert werden. Dabei werden sowohl software- als auch hardwarebasierte Zertifikatssysteme wie z. B. Chipkarten unterstützt.

Session Timeouts

Um Angriffe auf einen nicht beobachteten Rechner zu verhindern, werden Sitzungen bei Nichtaktivität automatisch beendet. Die Länge des Timeouts ist konfigurierbar.

URL Hashing

URL Hashing erlaubt der Applikation zu erkennen, ob eine URL vom System

generiert wurde oder nicht. Dadurch werden Attacken durch manuelles oder automatisches URL-testen erschwert.

DOKUMENTENSCHUTZ AUF DEM SERVER

Stark verschlüsselte Dokumentenablage

Vertrauliche Dokumente können auf dem Server stark verschlüsselt abgelegt und so konsequent vor unbefugtem Zugriff geschützt werden. Dabei werden die Dokumente mit dem Advanced Encryption Standard (Rijndael-Algorithmus) mit 256-Bit Schlüssellänge verschlüsselt. Jeder Datenraum hat dafür einen separaten Schlüssel. Die Schlüssel werden, transparent für alle Benutzer, von der Anwendung selbst verwaltet.

Betreiber transparente Verschlüsselung

Verschlüsselung und Schlüsselverwaltung arbeiten für den Betreiber völlig transparent. Das Personal des internen oder externen Systembetreibers kann den ordnungsgemäßen Betrieb des Systems garantieren, das System überwachen, Datensicherungen durchführen und Daten wiederherstellen, ohne dafür Kenntnisse oder Zugriffe auf vertrauliche Dokumente oder einzelne Schlüssel zu benötigen. Die konsequente Trennung von Anwendungs- und Systemadministration plus integrierte Freigabeprozesse nach dem Vier-Augen-Prinzip für sicherheitsrelevante Administrationsfunktionen garantieren höchste Vertraulichkeit. Dies gilt auch beim Betrieb des Anwendungsservers durch einen externen IT-Dienstleister in einem externen Rechenzentrum.



Berechtigungssystem

Ein flexibles, rollenbasiertes Berechtigungssystem ermöglicht die genaue Definition und Überwachung von Rollen und Rechten für jeden Teilnehmer eines Datenraums. Die Rechtevergabe findet nur innerhalb eines Datenraums statt.

Anwendungsadministratoren können sich daher keinen Zugriff auf vertrauliche Dokumente verschaffen. Die Rechte können hochgranular vergeben werden und auf diese Weise sehr genau das gewünschte Nutzungsverhalten abbilden. Insbesondere erlaubt das Berechtigungssystem die Konfiguration im Sinne einer sogenannten „Chinese Wall“, d.h. von Gruppen, die sich gegenseitig nicht sehen können, auch innerhalb eines Datenraums. Die Vergabe von Rechten kann durch Vererbung über eine Ordnerhierarchie vereinfacht werden. Darüber hinaus können einmal erarbeitete, komplexe Rechteschemata in Vorlagen wieder verwendbar abgelegt werden.

Schutz der Datenintegrität

Der Dokumenten-Fingerabdruck ist eine Kennung, die eindeutig aus dem Inhalt einer Dokument-Version erzeugt wird. Sobald Änderungen an einem Dokument vorgenommen werden, ändert sich auch der Fingerabdruck. Dadurch kann die Anwendung sicherstellen, dass der Dokumentinhalt auch außerhalb der Brainloop Anwendung nicht verändert wurde, z. B. nach Versand und Download eines Dokumentes oder durch einen Angriff von außen. Ähnlich werden auch andere Datenbank-Einträge durch Querbezüge und Prüfsummen geschützt, um nicht autorisierte Zugriffe durch einen Angreifer mit Datenbank-Privilegien zu verhindern.

Revisionssicherer Audit-Trail

Alle Ereignisse auf Applikations-, Datenraum- und Objektebene werden in einem Audit-Trail mit Zeitstempel revisionssicher erfasst. Erfasste Ereignisse sind Konfigurationsänderungen und Aktionen wie z. B. Zugriff, Editieren, Herunterladen oder Einstellen von Dokumenten und die Anzeige einzelner Seiten im Secure Document Viewer. Dem Anwender werden jeweils nur die für ihn freigegebenen Informationen angezeigt. Die Zugangsberechtigung zum Audit-Trail können eingeschränkt werden. Die Applikation stellt sicher, dass der Audit-Trail nicht nachträglich verändert werden kann.

Schutz der Dokumente Bei der Übertragung

Verschlüsselte Datenübertragung
Jede Datenübertragung vom lokalen Browser zum Server und umgekehrt (Upload und Download von Dokumenten, Anzeige von Datenraumgehalten) erfolgt über HTTPS und wird über 128-Bit Standard-SSL-Verschlüsselung geschützt. Dies gilt auch für die Übertragung von Dateien und Dateinamen bei der Kommunikation über die WebDAV-Schnittstelle.

Für den Betrieb eines Brainloop Secure Dataroom Servers werden sowohl für die Web-Browser- als auch für die WebDAV-Schnittstelle jeweils eine eigene IP-Adresse, ein DNS-Name und ein gültiges SSL-Zertifikat benötigt.

Sicherer Dokumenten-Versand

Ein Benutzer kann anderen Benutzern ein Dokument zu kommen lassen, ohne dass dafür das Dokument ohne Schutz des Datenraums übermittelt wird. Es wird lediglich ein Link auf das Dokument versendet. Auch können nur Empfänger ausgewählt werden, die die Berechtigungen auf das Dokument

haben. Der Empfänger kann dann den Link direkt aus der E-Mail öffnen. Optional steht diese Funktion zum Versand auch an Nicht-Datenraumbenutzer zur Verfügung. Hierbei wird ein zeitlich befristeter Verweis verschickt, der jederzeit vom Datenraum aus zurückgezogen werden kann. Über eine Sicherheitsrichtlinie kann festgelegt werden, in welcher Form einem Externen das Dokument zur Verfügung gestellt werden kann und in welcher Granularität der Zugriff protokolliert wird.

Sichere E-Mail

Zur Unterstützung von Zusammenarbeit und Kommunikation können sich Benutzer aus dem Datenraum verschlüsselte E-Mails zuschicken. Dabei erhält Empfänger mit Client-Zertifikat (x.509 v3) die E-Mails dann verschlüsselt. Empfänger, die kein entsprechendes Zertifikat in ihrem Benutzerprofil hinterlegt haben, erhalten eine Ersatz-E-Mail, die auf die Original-Nachricht verweist. Die Original-Nachricht wird in diesem Fall im persönlichen Posteingang des Empfängers im Datenraum hinterlegt. So wird verhindert, dass Unbefugte an vertrauliche Informationen gelangen. Diese Art des Schutzes wird auch auf E-Mails, die das System an den Anwender schickt, angewendet.

DOKUMENTENSCHUTZ AUF DEM RECHNER DES EMPFÄNGERS

„Brainmark“-gesicherte Dokumenten-Auslieferung

Alternativ zum Originalformat kann der Zugriff auf ein Dokument auf einen Brainmark-gesicherten Download eingeschränkt werden. Ein so gesicherter Download liefert eine automatisch generierte, geschützte Dokumenten-Version an den Client. Sicherheitsricht-



linien bestimmen, ob ein Brainmark-gesicherter Download das Dokument als einfache, aber eindeutig gekennzeichnete Druckversion, die von allen Bearbeitungsvermerken bereinigt ist, ausgeliefert wird, ob die ausgelieferte Version zusätzlich ein personalisiertes Wasserzeichen enthalten soll, oder ob das Dokument nur zur Anzeige, ohne Möglichkeit zur Weiterverteilung oder Ausdrucken, ausgeliefert werden soll. Das Basisformat für die Brainmark-Darstellung ist PDF. Die Anwendung passt sich dabei automatisch an die spezifischen Fähigkeiten des Client-Rechners an, z. B. ob entsprechend Client-Zertifikate, Microsoft RMS oder Adobe Live Cycle eingesetzt werden kann.

Brainmark:

Ein Brainmark-gesicherter Download liefert eine automatisch generierte, geschützte Dokumentenversion an den Client. Der Anwender kann zwischen verschiedenen Sicherheitsstufen wählen.

Einige Beispiele:

- › Ein Dokument wird als einfache, aber eindeutig gekennzeichnete Druckversion, die von allen Bearbeitungsvermerken bereinigt ist, ausgeliefert.
- › Die ausgelieferte Version kann zusätzlich ein personalisiertes Wasserzeichen enthalten.
- › Das Dokument wird nur zur Ansicht, ohne Möglichkeit zur Weiterverteilung oder zum Druck, ausgeliefert werden.

Eindeutige Kennzeichnung von Ausdrucken

Brainmark-Versionen der Dokumente sind gegen Veränderungen geschützt und mit einer eindeutigen Kennung versehen. Diese eindeutige Nummer ermöglicht die lückenlose Verfolgung eines Dokumentes, auch nachdem es ausgedruckt, kopiert oder verschickt worden ist.

Wasserzeichen in den Dokumenten

Es können frei konfigurierbare Wasserzeichen hinterlegt werden, die beim Download über den geschützten Anzeigemodus für jeden Anwender personalisiert in die Dokumenten-Ansicht eingefügt werden. Empfängern eines vertraulichen Dokumentes wird so effektiv das unabsichtliche oder absichtliche Weitergeben z. B. durch abfotografieren des Bildschirms erschwert.

Dokumentenanzeige mit Secure Document Viewer

Der Secure Document Viewer liefert Dokumente am Browser zum Nur-Lesen ohne Speichermöglichkeit aus. Die Form der Anzeige ist für jeden Benutzer mit einem Browser möglich. Das Server-Side-Rendering ermöglicht die Anzeige von Dokumentinhalten in gekachelten Teilbildern. Dadurch werden die Informationen so zerstückelt, dass die einzelnen Einheiten nicht oder nur mit erheblichem Aufwand gedruckt oder weitergeleitet werden können.

Dokumentenanzeige mit Information Rights Management (IRM)

Für besonders hohe Schutzanforderungen kann mit IRM Technologien, sichergestellt werden, dass ein Leser

ein Dokument nur zum Lesen auf den Client heruntergeladen und öffnen kann. Eine Sicherheitsrichtlinien auf dem Dokument sorgt dafür, dass ein Office Dokument automatisch in PDF konvertiert werden, ggf. mit Wasserzeichen versehen und mit dem Rechte Management von Adobe Live Cycle versehen wird. Die Dokumentendatei wird dann verschlüsselt auf dem Client abgelegt und enthält die Information, was der Benutzer damit machen darf. Wenn der Benutzer das Dokument auf dem Client öffnet, muss er sich explizit gegenüber dem IRM Server ausweisen und seine zeitlich begrenzte Leselizenz vorweisen. Dieser Vorgang ist aber i.d.R. für den Benutzer transparent und wird über den Acrobat Reader 9.0 oder höher durchgeführt. Benutzer, die keinen passenden Acrobat Reader haben, bekommen das Dokument im Secure Document Viewer angeboten. Der IRM Schutz von Adobe Live Cycle kann auch in einer Form angeboten werden, die das zeitlich begrenzte Öffnen eines Dokumentes im Offline-Modus unterstützt. Dafür ist es jedoch erforderlich, dass der Benutzer seinem Profil ein von Brainloop generiertes Zertifikat zuweist, das dann zur Bestätigung der Leselizenz am IRM Server vorgelegt werden muss.

Sicheres Bearbeiten mit Information Rights Management Technologien

Die Integration von Microsoft Windows Rights Management Services (RMS) und Adobe Live Cycle Server steht auch für den geschützten Download zur Bearbeitung zur Verfügung. Die kombinierte Lösung aus Brainloop Secure Dataroom und IRM Technologie



unterstützt die Formate von Microsoft Office und PDF. Der IRM-Schutz wird bei entsprechend konfigurierter Sicherheitskategorie automatisch beim Download erzeugt.

Client-seitige Microsoft RMS Funktionen sind in den neueren Microsoft Windows Versionen enthalten. Weitere Client-Software wird nicht benötigt. Die Auslieferung der für die Zugriffskontrolle benötigten Zertifikate und Berechtigungen erfolgt durch den Server an den Client.

SICHERE BETRIEBSFÜHRUNG

Keine Client-Software

Es werden keine Plugins oder OCX-Module installiert, die ggf. von Angreifern kompromittiert werden könnten.

Keine Objekte im Browser Cache

Durch entsprechende Einstellungen des Browsers kann sichergestellt werden, dass keine Objekte unverschlüsselt im Browser Cache des lokalen Rechners gespeichert und von dort nachträglich ausgelesen werden können.

IP Einschränkungen für die Administration

Der Zugriff auf die Funktionen sowohl des Applikations-Managements als auch für die Datenraum-Center und Datenraum-Administration kann auf bestimmte Netze bzw. IP-Bereiche eingeschränkt werden.

Applikationsadministration

Die Aufgaben innerhalb der Applikations-Administration sind an Berechtigungen gebunden, so dass unterschiedliche Qualitäten von Administratoren (Monitoring & Analyse, Veränderungen, Konfiguration, Software Upgrades) eingerichtet bzw. Aufga-

ben auf verschiedene Personen oder Gruppen verteilt werden können. Alle Veränderungen, die der Applikations-Administrator vornimmt, werden protokolliert. Zusätzlich wird durch Hardware Finger-Printing sichergestellt, dass Änderungen an der System-Konfiguration sofort bemerkt werden.

Applikations Überwachung

Eine Monitoring-Komponente überwacht den Betrieb und meldet Änderungen, wie etwa an den Berechtigungen am Filesystem, an sicherheitskritischen Datenbank-Inhalten, oder Verfälschungen von Dateien auf dem Dateisystem. Die Applikationsadministratoren definieren selbst, über welchen Weg (SMS, E-Mail) sie über Alarme informiert werden möchten.

Gekapselte Benutzerverwaltung

Der Applikations-Administrator kann kritische Benutzerdaten wie z. B. E-Mail oder Mobiltelefon nicht verändern. Daher kann er keinen Benutzeraccount so verändern, dass er selbst Zugriff auf die Dokumente des Benutzers bekommt. Über alle weiteren Änderungen durch den Applikationsadministrator an seinem Profil wird der Benutzer über E-Mail informiert.

Datenraum-Center Administration

Die Datenraum-Center Administration umfasst das Anlegen und Konfigurieren von Datenräumen und das Provisionieren von Benutzer-Lizenzen. Die weitere Verwaltung erfolgt innerhalb eines Datenraums in der Datenraum-Administration. Der Datenraum-Center-Administrator hat keinen Zugriff auf die Dokumente eines Datenraums.

Datenraum-Administration

Die Verwaltung der Konfiguration und

Inhalte eines Datenraums liegt i.d.R. beim Projekt- oder Fachbereichsverantwortlichen. Er bestimmt unabhängig von der Applikations-Administration, wer in den Datenraum eingeladen wird und wer welche Berechtigungen besitzt.

Integration Virens scanner

Kunden- oder betreiberspezifische Virens scanner können integriert werden. Infizierte Dateien werden isoliert und der Applikations-Administrator per E-Mail informiert.

Schutz der Schlüssel Infrastruktur

Die Datenraum-Schlüssel werden über einen Masterkey verschlüsselt. Der Masterkey wird während der Installation des Systems generiert und wiederum verschlüsselt im Speicher gehalten. Nach der Erzeugung kann der Masterkey in mehrere Teile aufgeteilt und auf unterschiedliche Personen verteilt werden. Um z. B. nach einem Totalausfall den Masterkey wieder herzustellen muss mindestens ein Benutzer pro Schlüsselteil zur Verfügung stehen. Es wird empfohlen, den Schlüssel in 2-3 Teile aufzuteilen und diese an 4-6 Personen zu verteilen.

Umzug von Datenräumen

Beim Umzug von Datenräumen werden ebenfalls spezielle Schlüssel benötigt, die zwischen dem Applikationsadministrator und dem Datenraum-Manager aufgeteilt werden. Um den Datenraum in einem neuen System wieder herzustellen sind beide Schlüsselteile notwendig.

Datenbank-Administration

Passwörter u.ä. liegen nicht im Klartext in der Datenbank. Des Weiteren sorgen Datenintegritätsprüfungen



dafür, dass Manipulationsversuche sofort entdeckt werden und der Datenraum gesperrt wird. Der Datenbank-Administrator erhält keinen Systemlogin auf der Servermaschine. Der Zugriff auf die Datenbank aus dem Netz ist gesperrt.

DATENSICHERUNG

Zur Sicherung der Datenverfügbarkeit werden unterschiedliche Stufen der Datensicherung durchgeführt:

- › **Systembackup:** wird regelmäßig und jeweils nach Softwareupdates durchgeführt. Ein Systembackup kann nur für ein komplettes System-Recovery verwendet werden. Es können keine einzelnen Dateien aus einem Datenraum restauriert werden.
- › **Datenbankbackup:** wird kontinuierlich durchgeführt.
- › **Datenbereiche des Servers:** sollte in regelmäßigen Abständen erfolgen. Ein Differenzbackup durch Backup Software ist möglich.
- › **Datenraum Backup:** Um eine Rekonstruktion eines einzelnen Datenraumes zu ermöglichen, bietet die Applikation die Möglichkeit an, Datenräume in definierten Abständen zu sichern und diese in mehreren Versionen aufzubewahren. Die Backups werden mit dem Datenraum-schlüssel verschlüsselt im Filesystem

des Servers abgelegt. Der Applikationsadministrator übernimmt die Parametrisierung (maximales Zeitintervall zum letzten Backup, Anzahl der Backups die aufbewahrt werden, Backup Zeiten, wann Backups ausgeführt werden sollen).

Integration in bestehende IT-Infrastruktur

Der Server kann nahtlos in bestehende Netzwerkinfrastrukturen wie Firewall, Intrusion Detection sowie in System- und Applikationsmanagement-Infrastruktur etc. integriert werden.

KOMMUNIKATIONSKONFIGURATION
Die Firewall vor dem Brainloop System kann sehr restriktiv konfiguriert werden. Das System verwendet nur sehr wenige Kommunikationsprotokolle. Minimal benötigt wird:

- › **HTTPS Zugriff:** Die normale Kommunikation vom Client zum Server verwendet HTTPS. HTTP kann aus Gründen der Sicherheit abgeschaltet werden.
- › **E-Mail:** Für den Versand von Benachrichtigungen an Benutzer baut das System Verbindungen nach extern auf.
- › **SMS:** Der SMS Versand erfolgt über einen Webservice. Dazu muss der Server Zugriff über HTTPS auf einen externen Server haben. Für Software-Updates und Wartungs-

arbeiten ist ggfls. Terminalserver Zugriff notwendig. Dieser kann durch IP Restrictions oder andere übliche Schutzmechanismen geschützt werden. Software-Updates für das Betriebssystem und dessen Komponenten müssen über den Microsoft Update Service oder über eine RZ interne Lösung eingespielt werden.

Hochverfügbarkeitskonfiguration

Durch geclusterte Datenbank-Server und verteilte Applikations-Server mit entsprechender Unterstützung für das Systemmanagement und Systemmonitoring kann eine sehr hohe Verfügbarkeit sichergestellt werden. Dabei können die Komponenten zum Schutz für Katastrophen geografisch verteilt werden.

KONTAKT

Die **Brainloop AG** mit Sitz in München und Boston ist der führende Anbieter von Document Compliance Management-Lösungen, die den hochsicheren und jederzeit nachvollziehbaren Austausch vertraulicher Dokumente ermöglichen.

Weitere Informationen zur Brainloop AG finden Sie im Internet unter www.brainloop.de

Europa
Brainloop AG
Franziskanerstr. 14
81669 München · Deutschland
T: +49 (89) 444 699 0
info@brainloop.de
www.brainloop.de

USA
Brainloop Inc.
One Broadway, 14th floor
Cambridge, MA 02142 · USA
T: +1 (800) 517 3171
info@brainloop.com
www.brainloop.com

