

Internetbasiertes System hält vertrauliche Inhalte unter Verschluss

Abrechnungen landen im Web-Safe

Eine Lösung für den sicheren Austausch von Unterlagen schützt beim Versicherer Janitos die Kommunikation mit Maklern und Gutachtern. Das System regelt und protokolliert jeden einzelnen Zugriff.

Sowohl den Datenaustausch mit Maklern als auch mit Dienstleistern wie etwa Gutachtern wickelt das Versicherungsunternehmen Janitos auf elektronischem Weg ab. „Bei den Informationen handelt es sich um sensible Daten, etwa Provisionsabrechnungen und vertrauliche Kundeninformationen“, erläutert Christian Moser, Abteilungsleiter IT-Betrieb.

Als Janitos noch Teil der MLP-Gruppe war, wurden diese vertraulichen Informationen über einen zentralen Server ausgetauscht. Nach dem Verkauf an den Versicherungskonzern Gothaer musste eine neue Lösung her. Sie sollte unter anderem ein hohes Maß an Sicherheit bieten, keine Änderungen an bestehenden Arbeitsabläufen erfordern und alle Kommunikationsvorgänge lückenlos dokumentieren. Eine weitere Forderung: Die Sicherheitslösung musste mit den vorhandenen SAP-Systemen zusammenarbeiten.

Das Unternehmen entschied sich für Secure Dataroom von Brainloop. In diesem webbasierten Datenraum lassen sich alle Arten von sicherheitsrelevanten Informationen ablegen, ähnlich wie Papierdokumente in einem Safe. Janitos nutzt die Lösung als Software as a Service.

Bevor ein Anwender Zugang zum Datenraum erhält, muss er sich authentifizieren. Dies geschieht durch eine Zwei-Faktor-Authentifizierung – mittels eines Einmalpass-

worts, das durch ein Token oder eine Smartcard bereitgestellt wird, und durch das persönliche Passwort des Nutzers.

Das integrierte Rechtemanagement regelt, welche Person oder Anwendergruppe was wann mit welchen Dokumenten tun darf: Lesen, editieren, ausdrucken, kopieren oder weitergeben. Zudem registriert das System, wer zu welchem Zeitpunkt auf Dokumente zugegriffen hat. Document Viewer-Funktionen verhindern, dass geschützte Unterlagen vom Server auf einen Rechner heruntergeladen werden. Selbst das Erstellen von Screenshots lässt sich verhindern, indem der Server Dokumente in Form von kachelförmigen Teilbildern übermittelt.

Beim Hoch- und Herunterladen werden die Inhalte des Datenraums mit einer 128-Bit-Verschlüsselung geschützt. Dabei kommt der Advanced Encryption Standard (AES) zum Einsatz. Auf dem Datenraumserver werden Schlüssel von 256-Bit-Länge verwendet.

„Die Sicherheitslösung hat den Austausch vertraulicher Informationen erheblich vereinfacht“, erläutert Moser. „Zudem wird der gesamte Datenaustausch protokolliert. Die Kommunikation ist transparent und nachvollziehbar.“

Nicole Dietrich,
Senior Marketing
Manager EMEA, Brainloop/ms

Screenshots lassen sich durch kachelförmige Teilbilder verhindern