

Sicherer Dokumentenaustausch bei Versicherungsunternehmen

Janitos setzt auf den sicheren Datenraum von Brainloop



Hauptgebäude von Janitos.

Dass vertrauliche Daten von Kunden oder Geschäftspartnern an die Öffentlichkeit geraten oder gar bei Konkurrenten landen, ist bei der Janitos AG ausgeschlossen. Das Versicherungsunternehmen schützt solche Informationen mithilfe eines elektronischen Dokumententresors. Secure Dataroom der Münchener Firma Brainloop erlaubt den sicheren und jederzeit nachvollziehbaren Austausch unternehmenskritischer Daten zwischen Mitarbeitern, Kunden und Dienstleistern.

„Wir sind nicht die Größten, dafür aber wahrscheinlich die Schnellsten“, lautet einer der Slogans der Janitos AG. Das Versicherungsunternehmen mit Hauptsitz in Heidelberg gehört seit 2005 zum Versicherungskonzern Gothaer. Im Geschäftsjahr 2007 lag das Volumen der verdienten Beiträge von Janitos bei rund 87 Millionen Euro und verwaltete über 700.000 Verträge.

„Wir verstehen uns als leistungsstarker Sachversicherer für Makler“, umreißt Manfred Bauer, Vorstandsvorsitzender der Janitos AG, das Geschäftsfeld des Unternehmens. Die Angebotspalette umfasst unter ande-

rem Haftpflicht- und Kfz-Versicherungen. Hinzu kommen Policen für das Absichern von Wohngebäuden sowie Angebote, die vor den finanziellen Folgen von Unfällen oder Erkrankungen schützen.

Um als kleines Unternehmen mit den Großen der Branche mithalten zu können, muss Janitos nicht nur konkurrenzfähige Produkte anbieten, sondern seinen Kunden auch einen besseren Service offerieren. Und das wäre ohne eine leistungsfähige Informationstechnik nicht möglich. »Sobald ein Makler über unser Online-Portal einen Antrag zur Policierung freigegeben hat, sind die Unterlagen innerhalb von 72 Stunden beim Kunden«, beschreibt Manfred Bauer eine der Stärken des Unternehmens.



„Mit Secure Dataroom haben wir eine Lösung gefunden, die den Austausch vertraulicher Bestandsdaten mit unseren Versicherungsmaklern erheblich vereinfacht.“

Christian Moser, Abteilungsleiter IT-Betrieb bei Janitos

Sicherer Datenraum als Informationsdrehscheibe

Nicht nur der Austausch von Daten zwischen den Maklern und der Firmenzentrale wird auf elektronischem Weg abgewickelt. Dasselbe gilt für die Kommunikation mit Dienstleistern, etwa Gutachtern, die Schadensfälle aufnehmen. »Bei den Informationen handelt es sich um sensible Daten, etwa Provisionsabrechnungen mit den Maklern und vertrauliche Kundeninformationen«, erläutert Christian Moser, Abteilungsleiter IT-Betrieb bei der Janitos AG. »Es muss hundertprozentig sichergestellt sein, dass diese Daten nicht in falsche Hände geraten.« Als Janitos noch Teil der MLP-Gruppe war, wurden vertrauliche Informationen über einen zentralen Server ausgetauscht. Nach dem Verkauf an die Gothaer musste eine neue Lösung her. Sie sollte folgende Anforderungen erfüllen:

- ein hohes Maß an Sicherheit bieten,
- für die Benutzer intuitiv zu bedienen sein,
- keine Änderungen an bestehenden Arbeitsabläufen erfordern,
- innerhalb kürzester Zeit zu implementieren sein,
- keine Vorlaufkosten erfordern und
- alle Kommunikationsvorgänge lückenlos dokumentieren.

Eine weitere Forderung: Die Sicherheitslösung musste mit den vorhandenen SAP-Systemen zusammenarbeiten. Mit Hilfe von SAP-Programmen werden unter anderem Kundendaten, Versicherungspolicen und Schadensakten verwaltet. Außerdem ist die Betriebswirtschafts-Software für die Abrechnung mit Maklern und Dienstleistern zuständig.

Dokumente werden im elektronischen Tresor aufbewahrt

Nach Tests entschied sich die Janitos AG für Secure Dataroom der Münchener Firma Brainloop AG. »Die Software von Brainloop erfüllte als einziges Produkt alle unsere Vorgaben«, begründet Christian Moser. Secure Dataroom ist eine webbasierte Anwendung, die sicheren Zugriff auf Dokumente und Informationen ermöglicht. In diesem Datenraum lassen sich alle Arten von sicherheitsrelevanten Informationen ablegen, ähnlich wie Papierdokumente in einem Safe. Bevor ein Anwender Zugang zum Datenraum erhält, muss er sich authentifizieren. Secure Dataroom unterstützt eine Zwei-Faktor-Authentifizierung – mittels eines Einmal-Passwortes, das beispielsweise durch ein Token oder eine Smartcard bereitgestellt wird, und durch das persönliche Passwort des Nutzers.

Janitos setzt Secure Dataroom als zentrale Plattform für die Kommunikation ein. »Mit Secure Dataroom haben wir eine Lösung gefunden, die den Austausch vertraulicher Bestandsdaten mit unseren Versicherungsmaklern erheblich vereinfacht«, erläutert Christian Moser. »Auch Provisionsabrechnungen werden künftig auf diesem Wege übermittelt. Zudem wird der gesamte Informationsaustausch protokolliert; die Kommunikation ist transparent und nachvollziehbar.« Über den sicheren Datenraum von Brainloop tauscht Janitos zudem Informationen mit seinen externen Dienstleistern und den Outsourcing-Partnern aus: »Wir stellen ihnen mit Hilfe von Secure Dataroom beispielsweise vertrauliche Vertragsinformationen zur Verfügung«, so Moser.

Rechtmanagement regelt Zugriff auf Dokumente

Das integrierte Rechtmanagement von Secure Dataroom regelt bei Janitos, welche Person oder Personengruppe was wann mit welchen Dokumenten tun darf: lesen, editieren, ausdrucken, kopieren oder weitergeben. Die Lösung versieht dazu Dokumente

Janitos Versicherung AG

Die Janitos Versicherung AG wurde 1997 als MLP Service GmbH durch den Finanzdienstleister MLP gegründet. Vor sieben Jahren stieg die Firma in das Segment Sachversicherungen ein. Seit 2005 gehört Janitos zum Versicherungskonzern Gothaer. Dieser benannte das Unternehmen in Janitos AG um. Mit rund 200 Mitarbeitern, verdienten Beiträgen von rund 87 Millionen Euro und über 700.000 Versicherungsverträgen zählt Janitos in Deutschland zu den kleinen Versicherungen. Secure Dataroom von Brainloop ermöglicht es etwa 100 Mitarbeitern von Janitos, vertrauliche Daten wie Kundendaten, Schadensakten und Provisionsabrechnungen intern, mit externen Maklern sowie mit Dienstleistern auszutauschen.



„Wir sind ein leistungsstarker Sachversicherer für Makler.“

Manfred Bauer, Vorstandsvorsitzender der Janitos AG

mit Attributen, wie etwa „Nur Lesezugriff“. Zudem registriert sie, wer zu welchem Zeitpunkt auf Dokumente zugegriffen hat. Document-Viewer-Funktionen verhindern, dass geschützte Unterlagen vom Server auf einen Rechner heruntergeladen und dort gespeichert werden. Dazu autorisierte User können Informationen zwar einsehen, aber nicht lokal abspeichern. Selbst das Erstellen von Screenshots lässt sich verhindern, indem der Server Dokumente in Form von kachelförmigen Teilbildern übermittelt.

Ein Versionsmanagement dokumentiert den Lebenszyklus eines Dokuments und verhindert, dass unterschiedliche Varianten in Umlauf geraten. Das ist beispielsweise wichtig, wenn ein Kunde Änderungen an einem Versicherungsvertrag durchführen lässt. Der Makler und die Mitarbeiter der Janitos AG sind stets darüber im Bilde, welche Version eines Dokuments die derzeit gültige ist.

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

Datenraum wird als Service bereitgestellt

Für die Lösung von Brainloop sprach aus Sicht von Janitos zudem, dass Secure Dataroom im Rahmen eines Software-as-a-Service-Angebots (SaaS) bereitgestellt werden konnte. Der Datenraumserver wird in einem speziell gesicherten Rechenzentrum gehostet.

Eine Trennung der Rollen von System- und Anwendungsmanager, wie sie das Operator Shielding des Secure Dataroom vorsieht, stellt sicher, dass die Daten vor dem Zugriff durch allzu neugierige IT-Manager sicher sind. Die Authentifizierung und Verwaltung von Anwendungen und Dokumenten ist unterschiedlichen Instanzen anvertraut: Der Systemverwalter ist für die Authentifizierung zuständig, der Anwendungsmanager für die Schlüsselverwaltung von Dokumenten.

„Als Software-as-a-Service-Lösung war Secure Dataroom sofort einsetzbar“, sagt Christian Moser. Sein Gesamtresümee fällt rundum positiv aus: „Die Lösung erfüllt vollständig unsere fachlichen Anforderungen, und das bei einem minimalen Trainingsaufwand für die Mitarbeiter und die IT-Abteilung.“