

## SICHERER DATENAUSTAUSCH

# Projektarbeit sicher gestalten

Um sich gegen Wirtschaftskriminalität und Industriespionage zu wappnen und die Kommunikation innerhalb des Unternehmens und mit externen Partnern abzusichern, führte Voith IT-Solutions die kommerzielle Standardlösung Brainloop Secure Dataroom ein. Sie erlaubt den sicheren Versand von Dokumenten und erfüllt zugleich die Compliance-Vorgaben zur Dokumentenklassifizierung. **VON NICOLE DIETRICH**



Der Hauptsitz der Voith AG liegt im baden-württembergischen Heidenheim.

**VOITH IST EIN** weltweit tätiger Anbieter für Spitzentechnologie und Industriedienstleistungen. Das breite Portfolio aus Anlagen, Produkten und Services bedient mit Energie, Öl & Gas, Papier, Rohstoffe sowie Transport & Automotive weltweit fünf Märkte. Gegründet 1867, ist Voith heute mit knapp 40.000 Mitarbeitern, 5,2 Milliarden Euro Umsatz und Standorten in rund 50 Ländern der Welt eines der großen Familienunternehmen Europas.

In punkto sicherer Datenaustausch bringen die weltweite Präsenz und die internationale Zusammenarbeit Risiken in den Bereichen Wirtschaftskriminalität und Industriespionage mit sich. Um sich gegen diese Herausforderungen zu wappnen und die Kommunikation intern und mit externen Partnern abzusichern, prüfte die Voith IT Solutions GmbH die auf dem Markt verfügbaren Lösungen für sicheren Dokumentenversand. Ausgewählt wurde schließlich die webbasierte Standardlösung Brainloop Secure Dataroom. Dieser wurde in das Voith-Extranet eingebunden und erfüllt die Compliance-Auflagen des ISO-27001-zertifizierten Unternehmens für den sicheren und nachvollziehbaren Austausch und die Bearbeitung vertraulicher Dokumente.

„Die unverschlüsselte Übertragung von sensiblen Dokumenten per E-Mail ist zu unsicher und nicht mehr zeitgemäß. Da der Weg der Daten durch das Internet unkalkulierbar ist, können unverschlüsselt versendete Dokumente abgefangen werden. Folglich haben wir eine Lösung gesucht, die neue Maßstäbe für den sicheren und schnellen Versand von Dateianhängen und deren vertrauliche Ablage setzt. Gleichzeitig sollten die Compliance-Vorgaben zur Dokumentenklassifizierung sowie die Wünsche unserer Geschäftspartner erfüllt werden“, berichtet Ralf Pichler, der das IT-Projekt bei Voith IT-Solutions geleitet hat.

In enger Zusammenarbeit zwischen Voith IT-Solutions und Brainloop wurde die Lösung für den sicheren Versand von Dokumenten in Microsoft Office Outlook integriert. Dokumente, die ausgetauscht werden, wechseln auf diese Weise geschützt den Empfänger. Verschickt wird lediglich ein Link, um das im Datenraum hinterlegte Dokument zu öffnen.

## Integration in das Extranet

Seit der Integration des Brainloop Secure Dataroom in das Voith-Extranet wird der Datenraum in diversen Unternehmensbe-

reichen eingesetzt. Dazu zählt der Konstruktions- und Entwicklungsbereich, der Dokumente mit externen Ingenieurbüros austauscht. Aber auch ein Teil des Personalbereichs nutzt den Brainloop-Datenraum zur verschlüsselten Ablage von Dokumenten. Er steuert damit einen Teil zur Erfüllung der Anforderung aus dem Bundesdatenschutzgesetz im Blick auf die im §9 BDSG geforderten Maßnahmen bei der Verarbeitung personenbezogener Daten bei. Der Datenraum wird vom jeweiligen Eigentümer verwaltet, er allein bestimmt, welche Personen Zugriff haben.

Jeder Zugriff wird automatisch protokolliert, so dass jederzeit nachvollzogen werden kann, wer wann welche Informationen eingesehen hat. Auch nach dem Download von Dokumenten bleiben die vergebenen Bearbeitungsberechtigungen aktiv. Somit haben nur Befugte die Möglichkeit, Daten zu lesen, zu verändern, zu drucken oder weiterzuleiten.



**Autor: Nicole Dietrich, Senior Director Marketing bei der Brainloop AG**

Kennziffer: DBM22216

## Der Lösungsanbieter: Brainloop AG

Die Brainloop AG mit Firmensitz in München und Boston ist Anbieter einer Document-Compliance-Management-Lösung. Der Brainloop Secure Dataroom, ein webbasierter Dokumententresor, sichert die Ablage, Bearbeitung und Verteilung vertraulicher Dokumente im Unternehmen und über Firmengrenzen hinweg ab. Dabei werden diese vor Angreifern bei gleichzeitiger Wahrung der gesetzlich vorgeschriebenen Nachvollziehbarkeit durch Protokollierung aller Zugriffe und Aktionen geschützt. Einsatzbeispiele sind Vertragsverhandlungen, Projektabwicklungen oder die Erstellung von Quartalsberichten.