

Nutzerfreundliche E-Mail-Sicherheit

Tresorit sichert Datenaustausch zwischen Spitälern und externen Dienstleistern

Für Cyberkriminelle sind E-Mails ein beliebtes Einfallstor. Um dieses zu schliessen und die sichere Kommunikation zwischen Spitälern und Dienstleistern zu vereinfachen, hat der schweizerisch-ungarische Spezialist für Cloud-Zusammenarbeit Tresorit die Lösung «Tresorit E-Mail Encryption» entwickelt. Die kürzlich veröffentlichte neue Version ermöglicht nun auch die automatische Zero-Knowledge-Verschlüsselung aller E-Mail-Nachrichten und -Anhänge ihrer Endnutzer.

Schon mit der Einführung der ersten Version von Tresorit E-Mail Encryption im April dieses Jahres stellte Tresorit Kunden im Gesundheitswesen eine leistungsstarke Lösung zum sicheren E-Mail-Austausch zur Verfügung: Sie ermöglicht den einfachen Versand sicherer E-Mails mit nur einem Klick und bietet erweiterte Kontrolle über die gesendeten Daten, darunter den Widerruf der Zugriffserlaubnis oder die Möglichkeit, die Anzahl der Downloads zu begrenzen. Nur Absender müssen hierzu über ein Tresorit-Konto verfügen. Somit können Anwender nicht nur die ausgehende E-Mail-Korrespondenz – zum Beispiel mit Medizintechnik-Unternehmen – absichern, sondern auch die eingehende: Denn Antworten werden ebenfalls automatisch verschlüsselt.

Im Vergleich zu Legacy-E-Mail-Sicherheitslösungen bietet Tresorit höhere Benutzerfreundlichkeit und Sicherheit. Als Built-in-Modul arbeitet Tresorit E-Mail Encryption mit gängigen E-Mail-Services zusammen. Im ersten Schritt ist die Lösung für Microsoft Office Desktop verfügbar. Weitere Plattformen, darunter Gmail

und Microsoft 365, werden im Rahmen zukünftiger Versionen folgen.

Tresorit E-Mail Encryption 2.0: Was ist neu?

Mit der zweiten Version von Tresorit E-Mail Encryption können IT-Administratoren nun ab sofort auch E-Mail-Verschlüsselungsregeln für Endnutzer festlegen. Damit erfüllen Organisationen regulatorische Anforderungen und gewinnen die Kontrolle zurück über den Transfer geschäftskritischer Daten per E-Mail. Administratoren minimieren das Risiko menschlichen Versagens, indem sie E-Mails auf Basis eigener Regeln automatisch verschlüsseln – und das zum Beispiel abhängig davon, ob es sich um vertrauenswürdige Empfänger handelt oder die Nachricht einen Anhang enthält.

Darüber hinaus hilft Tresorit, die Arbeitsabläufe für Endnutzer zu vereinfachen: Denn diese müssen Verschlüsselung nicht länger aktivieren oder deaktivieren. Das System selbst führt die Verschlüsselung aus. Zudem lassen sich verschlüsselte Anhänge über eine separate siche-



Istvan Lam, CEO und Mitgründer von Tresorit

re Benutzeroberfläche verwalten. Nutzer können Anhänge mit einer Grösse von bis zu fünf Gigabyte senden und empfangen, ohne Warnmeldungen in Outlook zu erhalten.

Komfortabel und konform: Sicherer Austausch kritischer Daten

«Eines unserer Ziele besteht darin, den Austausch kritischer Daten im Gesundheitswesen mithilfe unserer Zero-Knowledge-Verschlüsselung so sicher und nutzerfreundlich wie möglich zu gestalten», so Istvan Lam, CEO und Mitgründer von Tresorit. «Dazu wenden wir unsere zehnjährige Expertise im Bereich Cloud-Verschlüsselung auch auf die E-Mail-Kommunikation an: Unser E-Mail-Dienst ist der nächste grosse Schritt auf unserem Weg, eine sichere, Ende-zu-Ende-verschlüsselte Workspace- und Kollaborationsplattform für Spitälern und Unternehmen aller Grössenordnungen zu schaffen. Die neue Version von Tresorit E-Mail Encryption ist das Ergebnis empfangenem Anwender-Feedbacks, das wir direkt zu

Über Tresorit

Tresorit ist eine Ende-zu-Ende-verschlüsselte Produktivitätslösung für hochsichere Zusammenarbeit, die das Verwalten, Speichern, Synchronisieren und Übertragen von Dateien gewährleistet. Mehr als 10 000 Organisationen nutzen Tresorit bereits, um ihre geschäftskritischen Daten zu schützen und Informationen sicher zu teilen. Seit Juli 2021 ist die Schweizerische Post AG Mehrheitsgesellschafter von Tresorit.

dringenden zusätzlichen Funktionen verarbeitet haben. Mit Ende-zu-Ende-verschlüsselten E-Mails durch Tresorit geht der sichere Austausch geschäftskritischer Daten nie zu Lasten der Nutzerfreundlichkeit.»

Tresorit wird die Regeln für E-Mail Encryption auf Basis von Kundenrückmeldungen und internen Richtlinien zur Produktsicherheit (z. B. Zero-Knowledge-Protokolle) kontinuierlich noch weiter verbessern. Zu den künftig geplanten Weiterentwicklungen zählt auch Verschlüsselung, die zum Beispiel bei Nutzung bestimmter Begriffe und Datentypen automatisiert stattfindet. Bereits heute ist die Lösung mit dem «Digital Trust Label» der Swiss Digital Initiative zertifiziert.

Weitere Informationen

Tresorit AG, Stefan Killer-Haug
Franklinstrasse 27, 8050 Zürich
Telefon +49 160 8434 133
stefan.killer@tresorit.com
www.tresorit.com/de

