Vertraulichkeit und Datenschutz in Microsoft Teams

Microsoft Teams ist die Zentrale für Team-Arbeit in Microsoft 365. Es ermöglicht Instant-Messaging, Online-Meetings mit Audio- sowie Video-Calls und enthält umfangreiche Funktionen für Web-Konferenzen. Darüber hinaus bietet Teams File- and Data-Collaboration sowie Online-Datenspeicher. Microsoft Teams nutzt Online-Dienste wie SharePoint und Exchange Online. Über Teams geteilte Daten werden in SharePoint gespeichert und können von praktisch jedem Gerät abgerufen werden. Cloud-Daten sind allerdings größeren Risiken ausgesetzt und bedürfen zusätzlichem Schutz. Für Daten in Microsoft Teams und SharePoint Online ist eine Client-seitige Verschlüsselung eine einfach zu realisierende Möglichkeit, um den Schutz zu gewährleisten.

Wie können Sie Daten mit conpal LAN Crypt schützen?

conpal LAN Crypt ist eine Client-seitige Lösung für Verschlüsselung auf Dateiebene. Ihre Verwaltung von Keys und Policys unterstützt Anwendungsfälle wie etwa Datenaustausch mit verschiedenen Schlüsseln für geschäftlich, persönlich und gemeinsam genutzte Daten. Die Ver- und Entschlüsselung erfolgt ausschließlich auf dem Endgerät. Somit sind Daten auf dem lokalen Rechner und bei der Übertragung geschützt. Weder Microsoft noch andere haben Zugriff auf die Klartext-Daten oder den verwendeten Key. conpal LAN Crypt hilft Unternehmen dabei, die Sicherheit ihrer Daten auch in Cloud-gehosteten Umgebungen zu wahren.

Schutz aktivieren

1 Definieren Sie, welche Teams oder Channels sie schützen

Definieren sie in der Admin-Konsole von conpal LAN Crypt eine Verschlüsselungsregel für die Teams oder Channels, die Sie schützen möchten. Eine einzige Regel für alle Teams reicht aus, um zu gewährleisten, dass alle hochgeladenen Daten verschlüsselt sind. Definieren Sie zusätzliche Regeln, wenn sie eine feingliedrigere Kontrolle wünschen. Sollten Sie mit dem Resultat nicht zufrieden sein, können Sie jederzeit die geschützten Bereiche nachjustieren, um sie so weiter an Ihre Bedürfnisse anzupassen.

2 Aktivierung der Policy

Stellen Sie sicher, dass der Client von conpal LAN Crypt auf Ihrem Gerät installiert ist. Prüfen Sie dafür auf ihrem Mobilgerät bzw. in der Taskleiste (Windows) oder in der Menüleiste (Mac OS), ob das betreffende App-Symbol vorhanden ist. Lassen Sie als nächstes die Policy aktualisieren. Dadurch werden die soeben eingestellten Verschlüsselungsregeln auf Ihr System angewendet. Sämtliche Daten, welche Sie in Ihrem lokalen Sync-Ordner erstellen, werden nun automatisch verschlüsselt.

Synchronisation mit Microsoft Teams

3 Verbindung mit dem Datenspeicher von Teams

Stellen Sie sicher, dass der Client von conpal LAN Crypt auf Ihrem Gerät installiert ist. Prüfen Sie dafür auf ihrem Mobilgerät bzw. in der Taskleiste (Windows) oder in der Menüleiste (Mac OS), ob das betreffende App-Symbol vorhanden ist. Aktivieren Sie die lokale Synchronisation für jene Teams/Channels, in welchen Ihre Daten verschlüsselt werden sollen.

Zugriff von überall

4 Windows oder Mac

Verwenden Sie Ihren lokalen Sync-Ordner, um auf in Teams gespeicherte Daten zuzugreifen. Ver- und Entschlüsselung erfolgen on-the-fly im Hintergrund. Client-seitige Verschlüsselung gewährleistet, dass Daten vor dem Upload auf den Server oder in die Cloud verschlüsselt werden. Dokumente können geteilt werden, auch wenn sie verschlüsselt sind. Beachten Sie jedoch, dass derjenige, mit dem Sie das jeweilige Dokument teilen möchten, ebenfalls Zugriff auf den entsprechenden Verschlüsselungs-Key benötigt.

5 Smartphone oder Tablet

Die App von conpal LAN Crypt erlaubt Ihnen das Öffnen von verschlüsselten Dateien, welche via Teams gespeichert wurden. Starten Sie die Teams-App und navigieren Sie durch Ihre Ordner. Dateien können mit der conpal LAN Crypt App oder direkt aus der Teams-App heraus geöffnet werden. Verschlüsselte Dateien werden entschlüsselt, bevor sie angezeigt werden. Die Verschlüsselung erfolgt lokal innerhalb der App, um die Vertraulichkeit Ihrer Daten zu gewährleisten.

Copyright © 2021 conpal GmbH