# Keeper unterstützt Compliance nach Sarbanes-Oxley (SOX)

DATENBLATT

SOX-Compliance

Das Sarbanes-Oxley Act (SOX) ist ein US-Bundesgesetz des Jahres 2002, mit dem eine Reihe von Kontrollmechanismen zur Betrugsbekämpfung eingeführt wurden, die für öffentliche Unternehmen und Unternehmen, die einen Börsengang in Erwägung ziehen, gelten. Das unter den Kürzeln SOX oder SarbOx bekannte Gesetz gilt auch für hundertprozentige Tochtergesellschaften und ausländische Unternehmen, die an der Börse gehandelt werden und in den USA Geschäfte betreiben, sowie für Wirtschaftsprüfungsgesellschaften, die SOX-Compliance-Audits durchführen.

Ziel des SOX ist es, die Genauigkeit und Transparenz der von Unternehmen offengelegten Daten zu gewährleisten und sowohl Aktionäre als auch die Öffentlichkeit vor Bilanzierungsfehlern und betrügerischen Praktiken zu schützen.

## Automatisierung als Schlüssel zu SOX-Compliance im Zeitalter von Remote Work

Die COVID-19-Pandemie löste weltweit eine Welle von Cyberangriffen aus, die von INTERPOL als „alarmierend“ bezeichnet wird. Da Unternehmen gezwungen waren, in kürzester Zeit Technologien bereitzustellen, um einer Vielzahl von Mitarbeitern die Remote Arbeit zu ermöglichen, nutzen Cyberkriminelle die dadurch entstandenen Sicherheitslücken aus.

In diesem risikoreichen Umfeld versuchen SOX-Compliance-Experten, ihre bestehenden Compliance-Technologien und -Prozesse anzupassen.

Bei SOX-Audits müssen Unternehmen umfassend belegen, dass sie in fünf Schlüsselbereichen interne Kontrollen eingerichtet haben und diese effektiv umsetzen:

1. Kontrollumgebung
2. Risikobewertung
3. Kontrollmaßnahmen
4. Information und Kommunikation
5. Monitoring

Während SOX-Auditberichte jährlich erstellt werden, müssen Unternehmen nachweisen, dass ihre Kontrollen das ganze Jahr über ununterbrochen stattfinden. Mit anderen Worten müssen audit-relevante Maßnahmen das gesamte Jahr über durchgeführt werden, was die ohnehin schon überforderten IT-Mitarbeiter zusätzlich belastet. Daher ist es wichtig, dass Unternehmen so viele SOX-Compliance-Prozesse wie möglich automatisieren.

## Stärkung der SOX-Compliance mit Keeper

Der Schutz von Daten und Prozessen für den Zugang zu Finanzsystemen ist für Unternehmen entscheidend für die Einhaltung der SOX-Vorschriften für die Berichterstattung und Offenlegung ihrer Finanzdaten. In einem Unternehmensnetzwerk ist jeder Benutzer ein potenzieller Risikofaktor. Daher sind Risikominderung und Datenschutz für jeden Mitarbeiter, Subunternehmer und Lieferanten und für jedes Gerät, mit dem auf das Unternehmensnetzwerk zugegriffen wird, von entscheidender Bedeutung.

Keeper vereinfacht das Monitoring und Reporting im Bereich der SOX-Compliance und bietet IT-Administratoren vollumfängliche Transparenz und Kontrolle über die Passwortnutzung der Mitarbeiter und den rollenbasierten Systemzugriff in ihren Datenumgebungen mit anpassungsfähigen Audit-Protokollen und Event Reporting. Keeper unterstützt robuste interne Kontrollmechanismen durch delegierte Verwaltung, Durchsetzungsrichtlinien, Event Tracking, Monitoring und Reporting.

## IT-Administrator

Jeder Mitarbeiter wird mit einem gesicherten digitalen Tresor ausgestattet. Ein Sicherheits-Dashboard in der Admin-Konsole gibt einen Überblick über schwache Passwörter, die Mehrfachverwendung von Passwörtern und die Durchsetzung von 2FA sowie über rollenbasierte Zugriffskontrollen (RBAC) zur Durchsetzung von Richtlinien nach dem Prinzip der minimalen Berechtigung. Die Administration kann je nach Abteilung oder durch den Teamleiter delegiert werden, und Ordner und Datensätze können sicher freigegeben und widerrufen werden. Verlässt ein Administrator oder ein Mitarbeitender das Unternehmen, wird der zugehörige Datentresor automatisch gesperrt und kann sicher übertragen werden. Die Zugriffsprotokolle der Tresore von Keeper können im Rahmen einer Compliance-Kontrolle zu forensischen Zwecken geprüft werden.

## SOX-Audit-Reporting

Mit dem Keeper Commander SDK erstellen Administratoren und autorisierte Endnutzer Berichte, die für die Einhaltung der SOX-Compliance-Anforderungen relevant sind:

**Shared Access Report –** Der Befehl Share-Report liefert eine Aufschlüsselung darüber, welche Benutzer innerhalb des Unternehmens Zugriff auf Datensätze im Tresor haben. Dieser Bericht wird auf der Grundlage des gegenwärtig in Commander angemeldeten Benutzers generiert.

Mit dem Advanced Reporting & Alerts Module (ARAM) von Keeper Security können IT-Administratoren beliebig große Benutzerkreise überwachen, gezielt Verlaufsdaten zusammenfassen, Echtzeit-Meldungen über riskante oder ungewöhnliche Verhaltensweisen erhalten und benutzerdefinierte Berichte erstellen. Beispielsweise können über den Befehl Audit-Report ausführliche, ereignisbasierte Berichte auf Benutzer-, Datensatz- oder allgemeiner Systemebene erstellt werden.

Mit Keeper verfügen Administratoren über ein praktisches Tool zur Erstellung benutzerdefinierter SOX-Berichte mit ausführlichen Ereignisdaten im Zusammenhang mit der Freigabe von Informationen, darunter die Personen, mit denen die Informationen geteilt wurden, und sämtliche Änderungen der Zugriffsberechtigung. Mehr Informationen zu ARAM finden Sie im **Datenblatt zu Keeper ARAM**.

## Automatische E-Mail-Provisionierung

Mit den Datentresoren von Keeper können problemlos und in kürzester Zeit zehntausende von Benutzern mit E-Mail-Adressen unter derselben Domain ausgestattet werden. Mit minimalem Verwaltungsaufwand lässt sich über einen bestehenden E-Mail-Kanal oder ein vorhandenes Portal eine umfangreiche Implementierung vornehmen.

## Flexible Provisionierung

Keeper unterstützt die nahtlose Provisionierung von Benutzern und Teams ausgehend von Microsoft Azure AD oder anderen Identitätsplattformen mit Hilfe des SCIM-Protokolls. Außerdem unterstützt Keeper die API-basierte Befehlszeilen-Provisionierung mit dem Keeper Commander SDK. Das Keeper Commander SDK ist ein Open Source-Python-Code, der im Keeper Github-Repository zum Download bereitsteht.

## Sichere Dateispeicherung

Keeper schützt nicht nur die Passwörter von Mitarbeitern, sondern hilft Unternehmen auch dabei, Datenverluste zu vermeiden, indem es ihnen ermöglicht, sensible Dateien, Dokumente, digitale Zertifikate, private Schlüssel, Fotos und Videos in einem hochsicheren, verschlüsselten digitalen Tresor zu speichern. So können Mitarbeiter Dateien sicher mit Kollegen austauschen und sich darauf verlassen, dass nur die vorgesehenen Empfänger auf die freigegebenen Dateien zugreifen können.

Keeper verwendet PBKDF2 zur Ableitung von Authentifizierungsschlüsseln auf der Grundlage des Master-Passworts des Benutzers und generiert dann persönliche AES-256-Verschlüsselungscodes auf Datensatzebene lokal auf dem Gerät, um jede gespeicherte Datei zu verschlüsseln. Die Keeper-Cloud enthält ausschließlich den verschlüsselten Chiffretext der einzelnen Dateien. Die Freigabe zwischen Nutzern erfolgt über PKI, um sicherzustellen, dass nur der Empfänger einer freigegebenen Datei diese entschlüsseln kann. Mit Hilfe seiner Zero Knowledge-Verschlüsselungsverfahren stellt Keeper sicher, dass nur der Benutzer auf seine gespeicherten Dateien zugreifen und sie entschlüsseln kann.

## Schutz vor Sicherheitsverletzungen durch externe Lieferanten

Selbst wenn Sie über eine zuverlässige Passwortsicherheit verfügen, kann Ihr Unternehmen durch einen Ihrer Lieferanten gefährdet werden. Angesichts der rasanten Entwicklung der Remote Arbeit nutzen Cyberkriminelle die unzähligen SaaS-Lösungen, die Unternehmen zur Unterstützung ihrer Remote-Arbeitskräfte einsetzen. Keeper unterstützt granulare Kontrollen, mit denen Administratoren den Zugriff von externen Lieferanten auf Informationen und kritische Systeme einschränken und gleichzeitig eine strenge Zugriffskontrolle und Kontenüberwachung gewährleisten können. Benutzerdefinierte Warnmeldungen und Berichte können konfiguriert werden, um Lieferanten zu überwachen und zu tracken, und um Administratoren über riskante Verhaltensweisen zu benachrichtigen. Daraufhin können Administratoren Maßnahmen ergreifen und beispielsweise die Konten externer Lieferanten sperren.

Keeper BreachWatch™ für Unternehmen schützt Ihr Netzwerk, einschließlich der Konten externer Lieferanten, vor Sicherheitsverletzungen durch kompromittierte Zugangsdaten. BreachWatch™ für Unternehmen ist nicht auf öffentliche Meldungen über Sicherheitsverletzungen angewiesen. Es scannt Dark Web-Foren und benachrichtigt Unternehmen in Echtzeit, wenn die Passwörter von Mitarbeitern kompromittiert werden. Dadurch können IT-Administratoren die sofortige Rücksetzung von Passwörtern erzwingen und somit das Risiko minimieren, dass Cyberkriminelle diese zum Eindringen in die Systeme des Unternehmens missbrauchen.

## Über Keeper Security, Inc.

Keeper Security, Inc. (Keeper) ist die marktführende und top-bewertete Cybersicherheitsplattform zur Vermeidung passwortbezogener Datenverletzungen und Cyberbedrohungen. Millionen von Menschen und Tausende von Unternehmen weltweit vertrauen auf die Zero Knowledge-Sicherheits- und Verschlüsselungssoftware von Keeper, um das Risiko von Cyberdiebstahl zu mindern, die Mitarbeiterproduktivität zu steigern und Compliance-Standards zu erfüllen. Keeper wurde vom PC Magazine zum besten Passwort-Manager des Jahres und zum Editors' Choice gekürt. Auch von PCWorld erhielt Keeper den Editors' Choice-Award und von G2 vier Auszeichnungen für die beste Software. Keeper ist nach SOC-2 und ISO 27001 zertifiziert und für die Nutzung durch die US-Bundesregierung über das System for Award Management (SAM) gelistet. **Mehr Informationen finden Sie unter https://keepersecurity.com/enterprise.html.**