KEEPER

Datenblatt

Erfüllen Sie Anforderungen von ISO 27001 Anhang A.9 ganz einfach mit Keeper

ISO 27001 ist eine internationale Norm für Informationssicherheit, die einen Rahmen und Leitlinien für die Einrichtung, Implementierung und Verwaltung von Managementsystemen für Informationssicherheit bereitstellt. ISO 27001 wurde entwickelt, um Unternehmen beim Schutz wichtiger Ressourcen und der Einhaltung regulatorischer Anforderungen in der jeweiligen Branche zu helfen.

Zur Einhaltung von ISO 27001 müssen Unternehmen unter anderem dafür sorgen, dass Mitarbeiter ausschließlich Daten anzeigen können, die für ihre Rolle relevant sind. So wird die Wahrscheinlichkeit, dass Daten unbefugte Benutzer erreichen und offengelegt werden, reduziert.

Durch Nutzung führender Cybersicherheitslösungen von Keeper Security können Unternehmen jeder Größe einfach und kostengünstig Anhang A.9 von ISO 27001 einhalten und so ihren Sicherheitsstatus verbessern.

Anforderung	Lösung
A.9.1.1: Zugriffskontrollrichtlinie	Die Zugriffskontrollrichtlinie definiert Regeln und Verfahren, um die Sicherheit von Datenressourcen zu gewährleisten und das Prinzip der geringsten Privilegien durchzusetzen. Keeper sorgt mit rollenbasierten Zugriffskontrollen (RBAC), die von Administratoren festgelegt werden, um im gesamten Unternehmen das Prinzip der geringsten Privilegien durchzusetzen, für Konformität. Das Advanced Reporting and Alerts Module (ARAM) von Keeper stellt Unternehmen nahtlos übersichtliche Berichte zum Zugriff auf privilegierte Ressourcen zur Verfügung.
A.9.2.1: Registrierung und De-Registrierung von Benutzern	Unternehmen müssen sicherstellen, dass es einen formellen Prozess dafür gibt, wie Benutzer Zugriff erhalten und wie Zugriff auf Dateien und Dienste des Unternehmens widerrufen werden kann. RBAC von Keeper definiert Zugriffsrichtlinien für Benutzer auf der Rollenebene und setzt das Prinzip der geringsten Privilegien durch. Außerdem bietet Keeper zeitlich begrenzten Zugriff, damit Benutzer Datensätze für eine bestimmte Zeit teilen können, wobei der Zugriff nach Ablauf automatisch widerrufen wird. In Kombination mit der Passwortrotation von Keeper Secrets Manager können Benutzer und Administratoren dafür sorgen, dass Empfänger niemals dauerhaften Zugriff haben. Das Deaktivieren von Benutzern innerhalb der Keeper-Plattform ist ganz leicht. Administratoren können Benutzer schnell und einfach löschen und den Inhalt von Tresoren an geeignete Kollegen übertragen, was eine nahtlose Fortführung des Geschäftsbetriebs ermöglicht.
A.9.2.2: Bereitstellung von Benutzerzugriff	Ein System, vorzugsweise automatisiert, ist erforderlich, um Rechte im gesamten Unternehmen zuzuweisen und zu widerrufen. Keeper SSO Connect erlaubt eine zentralisierte Zugriffsverwaltung, sodass IT-Teams den Zugriff auf autorisierte Ressourcen überwachen und steuern können. Dieser Ansatz vereinfacht die Zugriffsverwaltung, erhöht die Transparenz und gewährleistet die Einhaltung von Sicherheitsrichtlinien.
A.9.2.3: Verwaltung privilegierter Zugriffsrechte	Privilegierter Zugriff gewährt Systemadministratoren und Personen mit Zugriff auf sensible Daten bestimmte Rechte. Privilegierte Benutzer sind oft IT- und Sicherheitsadministratoren, HR-Personal, Führungskräfte auf C-Ebene oder andere Mitarbeiter, die Zugriff auf privilegierte Systeme benötigen. ISO 27001 erfordert eine regelmäßige Prüfung von Administratorkonten und Protokollierung aller privilegierten Rechte. Keeper erlaubt die Verwaltung von Passwörtern, Geheimnissen und privilegierten Verbindungen auf Enterprise-Niveau in einer einheitlichen Plattform. Mit der Lösung von Keeper können Unternehmen vollständige Transparenz, Sicherheit, Kontrolle und Berichterstattung für jeden privilegierten Benutzer auf jedem Gerät erreichen.

Anforderung	Lösung
A.9.2.4: Verwaltung geheimer Authentifizierungsdaten von Benutzern	Geheime Authentifizierungsdaten müssen stark verschlüsselt werden und zusätzliche Mechanismen nutzen, um die erforderliche Sicherheit zu gewährleisten. Die entsprechenden Systeme müssen effizient verwaltet werden und vertraulich bleiben. Keeper Secrets Manager (KSM) ist eine vollständig verwaltete cloudbasierte Zero-Knowledge-Plattform zum Schutz von Geheimnissen wie API-Schlüsseln, Datenbankpasswörtern, Zugriffsschlüsseln, Zertifikaten und anderen vertraulichen Daten. KSM speichert alle Geheimnisse und Anmeldeinformationen im Keeper Vault, wobei Verschlüsselung auf Datensatzebene für maximal sichere Verschlüsselung sorgt. Administratoren können zusätzliche Sicherheitsmaßnahmen wie Multifaktor-Authentifizierung (MFA) und Rotation von Anmeldeinformationen durchsetzen, um zu erreichen, dass Geheimnisse stets sicher bleiben.
A.9.4.1: Einschränkung des Datenzugriffs	Richtlinien zur Zugriffskontrolle müssen für alle Systeme in einem Unternehmen gelten. Maßnahmen müssen so implementiert werden, dass sie unterschiedliche Ebenen von Zugriffsbeschränkungen im gesamten Unternehmen widerspiegeln. Keeper bietet zur Einhaltung von Anforderungen folgende Funktionen: • Rollenbasierte Zugriffskontrollen • Granulare Freigabe zur Durchsetzung von Regeln (wie z. B. Speicherung von Anmeldeinformationen mit Schreibschutz oder obligatorische Speicherung in Freigabeordnern) sowie die Möglichkeit, den Zugriff auf Freigaben zu widerrufen und Benutzer darauf zu beschränken, Anmeldeinformationen nur intern zu teilen oder zu empfangen. • Privilegierte Zugriffskontrollen für sensible Informationen und Daten
A.9.4.2: Sichere Anmeldeverfahren	Unternehmen sollten neben Passwörtern weitere Methoden anwenden, um Anmeldeverfahren zu schützen. Erfolgreiche und fehlgeschlagene Versuche sollten protokolliert werden. Keeper bietet neben Passwörtern verschiedene Optionen für Anmeldemethoden. So unterstützt Keeper verschiedene MFA-Lösungen und erlaubt ein automatisches Speichern und Ausfüllen von Passkeys. Zudem unterstützt Keeper Unternehmen, die Single Sign-on (SSO)-Lösungen nutzen, um über ihren SSO-Anbieter Zugriff auf Tresore zu gewähren, was für einen nahtlosen und sicheren Zugang sorgt. Keeper ARAM ermöglicht es Teams, Compliance und Auditing mit über 200 verschiedenen Ereignisarten zu unterstützen, einschließlich erfolgreicher und fehlgeschlagener Anmeldeversuche. Dabei helfen benutzerdefinierte Berichte, Echtzeitbenachrichtigungen und Integration mit SIEM-Lösungen von Drittanbietern.
A.9.4.3: Passwortverwaltung-slösung	Unternehmen sollten ein Passwortverwaltungssystem bereitstellen, das starke Passwörter generieren und durchsetzen sowie Wiederherstellungsverfahren unterstützen kann. Keeper ist branchenweit führend bei Sicherheits- und Compliance-Zertifizierungen und verschlüsselt auf der Datensatzebene, was für branchenweit maximale Sicherheit sorgt. Alle Keeper-Benutzer haben einfachen Zugriff, um für alle Einträge Passwörter und Passphrasen zu erstellen. Dadurch wird gewährleistet, dass sichere Passwörter zum Einsatz kommen. BreachWatch von Keeper übernimmt die Darknet-Überwachung, um Benutzer und Administratoren vor offengelegten Anmeldeinformationen zu warnen.
A.9.4.5: Zugriffskontrolle für Quellcode von Programmen	Quellcode ist durch Cyberkriminelle, die versuchen, auf Systeme von Unternehmen zuzugreifen, kontinuierlich bedroht. Darum müssen Unternehmen strenge Zugriffskontrollen implementieren, um ihre Systeme zu schützen. Keeper Secrets Manager schützt Ihre Umgebung und verhindert die Ausbreitung von Geheimnissen, indem hartcodierte Anmeldeinformationen aus Quellcode, Konfigurationsdateien und CI/CD-Systemen entfernt werden. Benutzer und Administratoren sollten alle Anmeldeinformationen sicher in ihrem Keeper Vault speichern, um eine Ausbreitung zu verhindern, und einfache Berichte und Warnungen nutzen. Benutzer von Keeper können unbegrenzt viele Geheimnisse, Anwendungen und Umgebungen verwalten.