Pressemitteilung

Keeper Security führt quantenresistente Verschlüsselung zum Schutz gegen zukünftige Quantengefahren ein

Die Enterprise-Security-Plattform stärkt die Abwehr gegen aktuelle Cyberbedrohungen und bereitet Kunden auf das Zeitalter des Quantencomputings vor.

MÜNCHEN, 25. Februar 2026 – Keeper Security, eine führende Plattform für Zero-Trust- und Zero-Knowledge-Identitätssicherheit sowie Privileged-Access-Management (PAM), gibt heute bekannt, dass ihre Lösungen nun quantenresistent sind. Keeper hat den Kyber-Schlüsselkapselungsmechanismus in seine Plattform integriert. Dies ist ein quantenresistenter Verschlüsselungsalgorithmus, der vom U.S. National Institute of Standards and Technology (NIST) zugelassen wurde.

Aufbauend auf seinem langjährigen Ruf für die Verwendung der branchenweit vertrauenswürdigsten Verschlüsselungsstandards bietet Keeper durch die Integration von Kyber doppelten Schutz: Schutz vor aktuellen Cyber-Bedrohungen und Vorbereitung der Kunden auf die Zukunft des Quantencomputings.

Die Quantengefahr ist real

Aktuelle Verschlüsselungsstandards wie RSA und Elliptic Curve Cryptography (ECC) sind zwar gegen heutige Angreifer robust, aber sie sind nicht für die besonderen Rechenfähigkeiten von Quantencomputern ausgelegt. Sobald Quantencomputer im großen Maßstab einsatzbereit sind, können sie diese Algorithmen brechen und die öffentliche Schlüsseltechnologie, auf der die heutige Internetsicherheit basiert, obsolet machen.

Die Gefahr besteht bereits heute durch „Harvest-now-decrypt-later"-Angriffe, bei denen Cyberkriminelle verschlüsselte Übertragungen abfangen und speichern, um sie später zu entschlüsseln, sobald die Quantentechnologie ausgereift ist. Das bedeutet, dass sensible Informationen, die heute übertragen werden – darunter Finanzdaten, Gesundheitsakten und geistiges Eigentum – in Zukunft möglicherweise offengelegt werden.

Das NIST hat in Anbetracht dieses Risikos Kyber im Jahr 2024 als einen der ersten Post-Quanten-Kryptografie-Standards fertiggestellt und Organisationen dazu aufgefordert, mit der Einführung zu beginnen. In Deutschland wird die Quantenbereitschaft als strategische Priorität im Rahmen eines mit 3 Milliarden Euro Aktionsplans für Quantentechnologien (Handlungskonzept Quantentechnologien) vorangetrieben. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Post-Quanten-Kryptografie in seine technischen Leitlinien (TR-02102-1) aufgenommen und damit signalisiert, dass regulierte Branchen und Betreiber kritischer Infrastrukturen mit einer strukturierten Migrationsplanung beginnen sollten.

Proaktive Verteidigung mit Keeper

Die Implementierung quantenresistenter Verschlüsselung in der Client-Server-Kommunikation durch Keeper stärkt die Führungsposition des Unternehmens beim Schutz privilegierter Zugriffe, Geheimnisse, Anmeldedaten und Verbindungen und steht im Einklang mit der breiten Einführung von Post-Quanten-Standards durch Apple iMessage, Signal, Google Chrome und Cloudflare, die seit 2024 ähnliche Schutzmaßnahmen einsetzen.

„Die Public-Key-Kryptografie, einschließlich RSA und ECC, bietet weiterhin starken Schutz gegen moderne Bedrohungen, aber Quantencomputing verändert die Spielregeln", erklärt Dr. Adam Everspaugh, Cryptography Advisor bei Keeper Security. „Keepers hybrider Ansatz kombiniert bewährte elliptische Kurven-Primitive mit der gitterbasierten Kryptografie von

Kyber. Diese mehrschichtige Abwehr stellt sicher, dass Kunden sowohl gegen heutige Angreifer als auch gegen zukünftige Gegner mit Quantenfähigkeiten geschützt sind.“

Keepers Implementierung von Kyber ist krypto-agil und ermöglicht schnelle Updates der kryptografischen Protokolle, während die Abwärtskompatibilität bei Software-Upgrades erhalten bleibt. Durch die Absicherung von Client-Server-Authentifizierungs-Handshakes und der verschlüsselten Datenübertragungskanäle stellt Keeper sicher, dass seine Zero-Trust- und Zero-Knowledge-Architektur sich parallel zu neuen Standards weiterentwickeln kann. Die quantenresistente Kryptografie wird Kunden automatisch mit dem Upgrade auf die neueste Version bereitgestellt – ohne Konfigurationsänderungen oder Benutzeraktionen.

„Cybersicherheit darf nicht reaktiv sein. Würden Organisationen warten, bis Quantencomputer verfügbar sind, wären sie gefährdet“, betont Darren Guccione, CEO und Mitgründer von Keeper Security. „Bei der Einführung von Kyber in Keeper geht es um Weitsicht. Wir helfen unseren Kunden, Resilienz aufzubauen, die sowohl die heutigen Bedrohungen als auch die bevorstehenden tektonischen Veränderungen abdeckt. So stellen wir sicher, dass sensible Systeme, Anmeldedaten und Geheimnisse auch in den kommenden Jahrzehnten sicher bleiben.“

Die Einbindung der Kyber quantumresistenten Verschlüsselung unterstreicht Keepers Führungsrolle beim Aufbau sicherer, widerstandsfähiger Infrastruktur. Dieser Meilenstein ergänzt Keepers langjährige Erfolgsbilanz bei der Erfüllung höchster Compliance-Standards, darunter SOC 2 Type II, ISO 27001, ISO 27017, ISO 27018, FedRAMP High Authorization, GovRAMP Authorization und FIPS 140-3-Validierung.

Die Bereitstellung der Kyber-basierten quantenresistenten Verschlüsselung ist nun in den Backend-APIs von Keeper und Keeper Commander verfügbar. In Kürze wird sie auch auf mobilen Plattformen verfügbar sein und schrittweise auf die gesamte Keeper-Plattform ausgeweitet werden, um Kompatibilität und Leistung in großem Maßstab zu gewährleisten.

Weitere Informationen zu Keeper finden Sie unter www.keepersecurity.com.

###

Über Keeper Security:
Keeper Security ist eines der am schnellsten wachsenden Unternehmen für Cybersicherheitssoftware, das Tausende von Organisationen und Millionen von Menschen in über 150 Ländern schützt. Keeper ist ein Pionier der Zero-Knowledge- und Zero-Trust-Sicherheit für jede IT-Umgebung. Das Herzstück, KeeperPAM®, ist eine KI-fähige, Cloud-native Plattform, die alle Benutzer, Geräte und Infrastrukturen vor Cyberangriffen schützt. Keeper wurde für seine Innovationen im Gartner Magic Quadrant für Privileged Access Management (PAM) ausgezeichnet und sichert Passwörter und Passkeys, Infrastrukturgeheimnisse, Remote-Verbindungen und Endpunkte mit rollenbasierten Durchsetzungsrichtlinien, Least-Privilege und Just-in-Time-Zugriff. Erfahren Sie auf KeeperSecurity.com, wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Erfahren Sie mehr unter KeeperSecurity.com
Folgen Keeper: Facebook Instagram LinkedIn X YouTube TikTok

Pressekontakt für Keeper in DACH:
Alexandra Schmidt, +49 170 387 10 64
Thilo Christ, +49 171 622 06 10
keeper@tc-communications.de