Trust and Technology Blog
By PwC Deutschland | 08. Oktober 2024

Risiken der Verwahrung von Kryptowerten

Finanzinstitute in der Welt der Kryptowerte-Dienstleistungen - Risiken der Verwahrung von Kryptowerten im eigenen Haus und bei Auslagerung der Verwahrung.

Der Aufstieg von Kryptowährungen und Blockchain-Technologie hat das Potenzial, die Finanzindustrie nachhaltig zu verändern. Neben den zahlreichen Chancen, wie der Unabhängigkeit von (Zahlungs)-Vermittlern und der Geschwindigkeit sowie der Sicherheit von Transaktionen, ergeben sich auch neue Risiken, die zu beachten sind. Besonders in der Kryptoverwahrung (**Crypto Custody**), die die Generierung (**Key Generation**) sowie Verwaltung (**Key Management**) von privaten Schlüsseln (**Private Keys**) umfasst, ergeben sich neuartige Risiken. Daher sollten sich Kreditinstitute beim Eintritt in die Welt der Kryptowerte-Dienstleistungen im Rahmen der organisatorischen Ausgestaltung intensiv mit der Frage beschäftigen, ob Sie die Kryptoverwahrung im eigenen Hause behalten oder an Dritte auslagern.

Das wesentliche Risiko wurde bereits von der deutschen Finanzaufsicht erkannt und mit der Einführung der **Markets in Crypto-Assets Regulation (MiCAR)** hat die Europäische Union einen umfassenden regulatorischen Rahmen geschaffen, welcher auch die Verwahrung von Kryptowerten betrifft. MiCAR fordert von Unternehmen, die Kryptowerte -Dienstleistungen erbringen, eine Zulassung durch die jeweiligen nationalen Aufsichtsbehörden. Diese Regulierung, die im Jahr 2023 verabschiedet wurde und im Laufe des Jahres 2024 vollständig in Kraft tritt, dient dazu, ein einheitliches und sicheres Umfeld für Kryptowerte zu schaffen und die Risiken für Endkunden und Investoren zu minimieren.

Durch die MiCAR sind Unternehmen angehalten, sich mit den Risiken in Bezug zur Kryptoverwahrung auseinanderzusetzen. Zu den wesentlichsten Risiken der Kryptoverwahrung gehören folgende:

1. Verlust der privaten Schlüssel: Der private Schlüssel ist essenziell für den Zugriff zu den Kryptowerten. Der Verlust von privaten Schlüsseln kann somit den unwiederbringlichen Verlust der Zugriffe auf die digitalen Vermögenswerte bedeuten.

2. Unautorisierter Zugriff auf private Schlüssel: Wenn sich unautorisierter Zugang zu den privaten Schlüsseln verschafft wird, können die Kryptowerte irreversibel entwendet werden. Dies kann durch unzureichende Sicherheitsmaßnahmen, Schwachstellen im Zugangs-/Zugriffsmanagement oder Cyber-Angriffe geschehen.

3. Technische Fehler: Software- oder Hardwarefehler können dazu führen, dass auf die Kryptowerte nicht mehr zugegriffen werden kann. Dies könnte durch Bugs in der Software oder physische Schäden an den Speichermedien verursacht werden.

4. Insider-Bedrohungen: Mitarbeiter:innen oder Dienstleister, die Zugang zu den privaten Schlüsseln haben, könnten diese missbrauchen oder unbefugt weitergeben.

5. Fehlerhafte Transaktionen: Transaktionen auf der Blockchain sind unumkehrbar. Fehlerhafte Transaktionen, sei es durch menschliches Versagen oder durch technische Fehler, können nicht rückgängig gemacht werden und führen zu Verlusten.

Für die Vertraulichkeit, Verfügbarkeit und Integrität der privaten Schlüssel bestehen weitere Risiken, die nicht durch den Erhalt der Zulassung abgedeckt sein müssen und daher mit gesonderten Maßnahmen zu versehen sind. Daher ist es essenziell, sich mit den Risiken frühzeitig auseinanderzusetzen, unabhängig davon, ob Sie selbst die Kryptoverwahrung erbringen oder ein Dritter für Sie.

In Anbetracht der Risiken ist der Aufbau von Internen Kontrollsystemen (**IKS**) bei Kryptoverwahrern ein entscheidender Aspekt, um diese zu angemessen mitigieren zu können. Auch die MiCAR stellt Anforderungen an interne Kontrollsysteme und das Risikomanagement. Ein effektives IKS für Kryptoverwahrer sollte unteranderem die fünf vorweg genannten Risiken adressieren, hierfür folgen beispielhaft Maßnahmen:

1. Verlust der privaten Schlüssel: Ein IKS sollte Verfahren für die sichere Generierung, Speicherung und Verwaltung privater Schlüssel beinhalten. Hierzu gehört die Implementierung von zertifizierten Hardware-Sicherheitsmodulen (HSMs) und geeigneten Passwortmanager Systemen.

2. Unautorisierter Zugriff auf private Schlüssel: Um unautorisierten Zugriff zu verhindern, sollten Kryptoverwahrer strenge Zugriffs- und Zugangsmanagement-Prozesse einführen. Die Implementierung spezifischer Verwaltungsrichtlinien zur Verwahrung und Management der privaten Schlüssel ist hierzu empfehlenswert.

3. Technische Fehler: Ein robustes IKS sollte Maßnahmen zur Sicherstellung der Systemverfügbarkeit und -integrität umfassen. Dies umfasst die Durchführung und Kontrolle von regelmäßige Software-Updates und die Überwachung von Systemen auf Anomalien.

4. Insider-Bedrohungen: Zur Minimierung von Insider-Bedrohungen sollten beispielsweise das Need-to-know-Prinzip sowie organisatorische Trennungen bei Rollenvergaben umgesetzt werden. Des Weiteren sollten strenge und wiederkehrende Hintergrundüberprüfungen der Mitarbeiter:innen durchgeführt werden.

5. Fehlerhafte Transaktionen: Zur Vermeidung fehlerhafter Transaktionen sollten Kryptoverwahrer Kontrollmechanismen implementieren, die sicherstellen, dass Transaktionen vor ihrer Ausführung gründlich überprüft werden. Dies kann durch Multi-Signatur-Verfahren oder Transaktions-Review-Prozesse erreicht werden.

Darüber hinaus sind regelmäßige Schulungen und Sensibilisierungen für verantwortliche Mitarbeiter empfohlen, um fortlaufend das Bewusstsein für die Risiken zu schärfen. Die Umsetzung solcher Maßnahmen trägt nicht nur zur Sicherheit und Verlässlichkeit der Kryptoverwahrung bei, sondern ist auch zur Einhaltung der regulatorischen Vorgaben durch MiCAR notwendig.

Durch unser Expertenwissen im Bereich Crypto & Digital Assets sowie der weitreichenden Prüfungserfahrung für Finanzinstitute können wir Sie optimal bei dem Aufbau und der Implementierung eines robusten IKS unterstützen.

Gerne können Sie sich bei Fragen zu diesem Thema an uns wenden!

Falls weitere Fragen zu MiCAR bestehen, haben wir für Sie hier die wichtigsten Informationen zusammengefasst:https://www.pwc.de/de/MiCAR

Laufende Updates zum Thema erhalten Sie über das regulatorische Horizon Scanning in unserer Recherche-Applikation PwC Plus. Lesen Sie hier mehr über die Möglichkeiten und Angebote.

Zu weiteren PwC Blogs

Schlagwörter

Cryptocurrencies (Virtual Currencies), Finanzmarkt, IT-Sicherheit, Informationstechnologie (IT), Prozesse, Risk Management Banking

Kontakt

Konstantin Dagianis

Düsseldorf

konstantinos.dagianis@pwc.com