NACHRICHTEN
Österreich

Krypto-Sicherheit: Bitcoin-Genie Buterin warnt vor Hardware-Wallets!

Vitalik Buterin erläutert, warum er MultiSig-Wallets statt Hardware-Wallets für die Krypto-Sicherheit bevorzugt. Mehr dazu in unserem Artikel.

Im Bereich der Kryptowährungen stellt sich für viele Anleger die entscheidende Frage: Wie bewahre ich meine digitalen Vermögenswerte sicher auf? Insbesondere angesichts der jüngsten Skandale in der Branche, wie dem Fall der Kryptobörse FTX, ist Sicherheit ein heiß diskutiertes Thema. Dabei fallen oft die Begriffe „Hardware Wallet“ und „MultiSig Wallet“, die unterschiedliche Sicherheitsansätze repräsentieren.

Traditionell gelten Hardware Wallets als die sicherste Methode zur Aufbewahrung von Kryptowährungen. Diese sogenannten Cold Wallets haben den Vorteil, dass sie nicht mit dem Internet verbunden sind, was sie theoretisch vor Hackern schützt. Dennoch sollten Nutzer dabei beachten, dass menschliche Fehler eine erhebliches Risiko darstellen können. So besteht die Möglichkeit, dass der Besitzer seinen Zugangscode, den sogenannten Seed, vergisst oder verliert. Ein solcher Verlust kann dazu führen, dass der gesamte Zugriff auf die Kryptowährungen verloren ist.

Neue Sicherheitskonzepte durch MultiSig-Wallets

Vitalik Buterin, Mitbegründer von Ethereum, hat sich mittlerweile für die Nutzung von MultiSig-Wallets ausgesprochen. Diese Wallets basieren auf einem anderen Sicherheitsprinzip, das die

Gefahr eines einzelnen Ausfallpunkts minimieren soll. Bei einer MultiSig-Wallet werden mehrere Schlüssel benötigt, um eine Transaktion durchzuführen. Buterin beschreibt dieses Modell als „M-of-N“, wobei eine bestimmte Anzahl von Schlüsseln (M) aus einer Gesamtanzahl von Schlüsseln (N) erforderlich ist, um eine Transaktion abzuschließen. So können Wallet-Besitzer ihre Sicherheit auf viele Schultern verteilt, anstatt sich allein auf einen einzigen Schlüssel zu verlassen.

„Die Verwendung einer MultiSig-Wallet erfordert strategisches Denken“, sagt Buterin. „Einige Schlüssel haltet ihr selbst, aber nicht genug, um die Wiederherstellung zu blockieren. Der Rest wird von anderen vertrauenswürdigen Personen gehalten.“ Diese Dezentralisierung schafft eine zusätzliche Sicherheitsebene, da selbst im Falle eines Passwortverlusts oder Diebstahls eine Wiederherstellung möglich bleibt, solange die anderen Schlüssel vorhanden sind. Ein weiteres Plus: Hacker hätten es wesentlich schwerer, alle nötigen Schlüssel zu ergattern.

Kritik an traditionellen Hardware-Wallets

Details