DIGITAL ASSET
INTELLIGENCE

RESEARCH REPORT
NR. 15 · 2026

KRYPTOVERWAHRUNG · FORENSIK

Hardware Wallets im Sicherheitscheck

Bekannte Sicherheitsvorfälle, Angriffsmethoden und forensische Möglichkeiten nach dem Diebstahl von Kryptowerten — von der Seed-Erzeugung über Supply-Chain- und Evil-Maid-Szenarien bis zur strukturierten Ursachenanalyse.

12 KAPITEL · RISIKOMATRIX · FALLSTUDIEN

FINANZ FORENSIK GMBH · FINANCIAL INTELLIGENCE

EXECUTIVE SUMMARY

Nicht das Gerät allein entscheidet, sondern die gesamte Sicherheitskette

Hardware Wallets reduzieren viele klassische Risiken erheblich — sie beseitigen sie aber nicht. Der COLDCARD-Vorfall 2026 zeigt: Schlüssel können bereits bei ihrer Erzeugung angreifbar sein, ohne dass ein Angreifer das Gerät je berührt oder aus der Ferne übernommen hat.

FINANZ·FORENSIK · FINANCIAL INTELLIGENCE & BLOCKCHAIN FORENSICS RESEARCH REPORT 15 / 2026

≈1.816 BTC
im COLDCARD-Vorfall 2026 betroffen (TRM Labs, 05.08.2026)

≈116 Mio. $
Gegenwert der betroffenen Coins zum Stichtag 08/2026

40 Bit
effektive Schlüsselstärke Mk2/Mk3 statt 128 Bit Sicherheitsziel

>5.200
betroffene Adressen in vier Angriffswellen

Hardware Wallets gelten als eine der sichersten Möglichkeiten, Bitcoin und andere Kryptowährungen selbst zu verwahren. Der zentrale Sicherheitsgedanke ist nachvollziehbar: Private Keys sollen nicht auf einem gewöhnlichen Computer oder Smartphone gespeichert werden, sondern innerhalb einer speziell dafür entwickelten Hardware. Daraus wird jedoch häufig eine Aussage abgeleitet, die technisch zu weit geht: „Wenn die Kryptowährungen auf einer Hardware Wallet liegen, können sie nicht gehackt werden." Hardware Wallets reduzieren bestimmte Risiken erheblich. Sie beseitigen sie aber nicht.

KERNAUSSAGE

Die Sicherheit eines Hardware Wallets ist nicht allein eine Eigenschaft des Geräts. Sie entsteht aus einer Sicherheitskette: Herstellung, Lieferweg, Initialisierung, Seed-Erzeugung, Firmware, Hardware, App oder Hostsystem, Transaktionsfreigabe, Backup und Nutzerverhalten.

Dokumentierte Vorfälle der vergangenen Jahre zeigen unterschiedliche Angriffsmöglichkeiten. Dazu gehören physische Seed-Extraktion, Fault-Injection- und Voltage-Glitching-Angriffe, fehlerhafte Zufallszahlenerzeugung, Schwachstellen in Firmware, kompromittierte Softwarebibliotheken, Supply-Chain- und Evil-Maid-Szenarien sowie die unbeabsichtigte Speicherung sensibler Schlüsseldaten in Anwendungsprotokollen.

Besonders folgenreich ist der COLDCARD-Vorfall des Jahres 2026. Nach Darstellung des Herstellers und unabhängiger Analysen führte ein Build- und Link-Integrationsfehler dazu, dass die Seed-Erzeugung nicht die vorgesehene Hardware-TRNG-Implementierung, sondern einen in der Laufzeitumgebung enthaltenen Software-PRNG verwendete. Die effektive Sicherheitsstärke sank dadurch auf rund 40 Bit bei älteren und rund 72 Bit bei neueren Modellen, gegenüber einem Sicherheitsziel von 128 Bit. Ab dem 30. Juli 2026 wurden betroffene Adressen in mehreren Wellen

geleert; nach der Analyse von TRM Labs vom 5. August 2026 waren rund 1.816 BTC aus mehr als 5.200 Adressen betroffen. Der Hersteller betont zugleich, die Geräte selbst seien weder aus der Ferne übernommen noch physisch angegriffen worden. [1][2][4]

Für die forensische Praxis folgt daraus ein Prüfschritt, der bislang selten vorgenommen wird: Vor jeder Einzelfallhypothese ist zu klären, ob der Geschädigte zu einer bekannten Geräte- und Firmwarekohorte gehört. Trifft ein Abfluss zahlreiche nicht miteinander verbundene Geschädigte in einem engen Zeitfenster, spricht dieses Muster dafür, zunächst nach einer gemeinsamen technischen oder organisatorischen Ursache zu suchen — Gerät, Firmware, App, eingebundene Softwarebibliothek oder eine koordinierte Kampagne —, bevor ein individuelles Fehlverhalten des einzelnen Geschädigten angenommen wird.

Aus forensischer Sicht bedeutet ein Diebstahl von einer Hardware Wallet deshalb keineswegs automatisch, dass der Geschädigte seinen Seed weitergegeben haben muss. Ebenso wenig beweist ein unautorisierter Transfer für sich genommen einen Hardware-Hack. Die technische Ursache muss im Einzelfall anhand von Gerät, Seed-Prozess, Softwareumgebung, Lieferkette und Blockchain-Spuren untersucht werden.

Sicherheit ist ein Prozess, kein Bauteil. *Ein Hardware Wallet isoliert den privaten Schlüssel gegenüber dem Hostsystem — vorausgesetzt, Seed-Erzeugung, Firmware, Lieferkette und Transaktionsfreigabe sind ebenfalls intakt.*

01 Einleitung und Zielsetzung

Der Grundsatz „Not your keys, not your coins“ gehört zu den bekanntesten Aussagen innerhalb der Kryptowelt. Nach Insolvenzen und Zusammenbrüchen zentraler Anbieter entscheiden sich viele Anleger dafür, Kryptowährungen nicht mehr bei Börsen oder anderen Verwahrstellen zu halten, sondern selbst zu verwahren.

Hardware Wallets spielen dabei eine zentrale Rolle. Hersteller wie Ledger, Trezor, Tangem, BitBox, COLDCARD, OneKey, SafePal, Keystone oder Ellipal verfolgen unterschiedliche technische Konzepte zur Aufbewahrung und Nutzung kryptografischer Schlüssel.

Die Unterschiede betreffen nicht nur Form und Bedienung. Wesentlich sind unter anderem Mikrocontroller, Secure Elements, Firmwarearchitektur, Seed-Erzeugung, Backup-Verfahren, Display- und Eingabesysteme, Kommunikationswege wie USB, Bluetooth, NFC oder QR sowie der Anteil offen einsehbarer Softwarekomponenten.

Eine pauschale Bewertung nach dem Muster „Hersteller A ist sicher, Hersteller B ist unsicher“ wäre daher weder technisch noch forensisch sinnvoll. Dieses Whitepaper untersucht stattdessen typische Sicherheitsarchitekturen, dokumentierte Vorfälle, Angriffsmethoden, mögliche forensische Spuren und die Bedeutung dieser Erkenntnisse für Geschädigte, Rechtsanwälte und Ermittlungsbehörden.

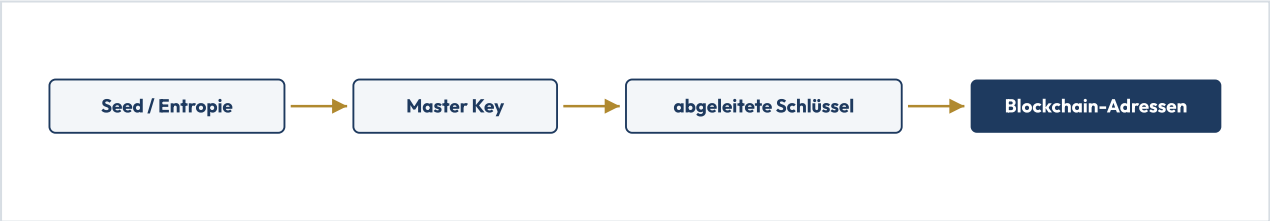
1.1 Quellenlage, Methode und Grenzen

Grundlage dieses Papiers sind Sicherheitsmitteilungen der Hersteller, veröffentlichte Forschungs- und Auditberichte sowie Fachberichterstattung. Eigene Laborprüfungen an Geräten wurden für diese Fassung nicht durchgeführt. Daraus ergeben sich Grenzen, die bei jeder Verwendung mitzulesen sind:

- Herstellerangaben sind Parteivortrag. Sie werden als solche gekennzeichnet und nicht als bestätigte Tatsache geführt.
- Angaben zu Schadenshöhen laufender Vorfälle sind Momentaufnahmen; sie schwanken je nach Quelle, Stichtag und Kurs und werden deshalb als Stichtagswert oder, soweit sinnvoll, als Spanne angegeben.
- Eine nachgewiesene Schwachstelle belegt keinen Vermögensdiebstahl; ein Vermögensdiebstahl belegt keine Schwachstelle des Geräts.
- Das Papier bewertet keine Produkte, spricht keine Kaufempfehlung aus und ersetzt keine Einzelfallprüfung.
- Maßgeblich ist der im Deckblatt genannte Stand. Spätere Erkenntnisse, insbesondere zu den Vorfällen des Jahres 2026, sind nicht berücksichtigt.

02 Was schützt eine Hardware Wallet?

Eine Hardware Wallet speichert streng genommen keine Bitcoin oder sonstigen Kryptowährungen. Die Assets befinden sich innerhalb der jeweiligen Blockchain. Das Gerät verwaltet die kryptografischen Schlüssel, mit denen Transaktionen autorisiert werden können.



Eine Transaktion wird häufig außerhalb der Hardware Wallet vorbereitet. Das Gerät erhält anschließend die zu signierenden Daten. Die Signatur soll innerhalb der geschützten Umgebung erfolgen; der private Schlüssel soll gegenüber dem Smartphone, dem Computer oder einem sonstigen Hostsystem nicht offengelegt werden. Je nach Architektur kann ein geschützter Schlüsseltransfer zwischen mehreren Sicherheitsgeräten Bestandteil des Backup-Verfahrens sein; das ist kein Widerspruch zu diesem Grundsatz, verschiebt aber die entscheidende Frage darauf, wer bei der Erstinitialisierung beteiligt war. Diese Isolation gegenüber dem Hostsystem ist der wesentliche Sicherheitsvorteil gegenüber klassischen Software Wallets.

Sie schützt jedoch nur dann, wenn der Seed korrekt und zufällig erzeugt wurde, nicht anderweitig offengelegt ist, die Firmware korrekt arbeitet, das Gerät nicht manipuliert wurde und der Nutzer tatsächlich die beabsichtigte Transaktion bestätigt.

03 Das Sicherheitsmodell als Kette

Die Sicherheit einer Hardware Wallet sollte nicht auf einen einzelnen Chip reduziert werden. Aus forensischer Sicht ist die gesamte Sicherheitskette zu betrachten:

- Hersteller und Entwicklungsprozess
- Produktion und Lieferweg
- Gerät und Hardwarearchitektur
- Firmware und Updateprozess
- Initialisierung und Seed-Erzeugung
- Backup und Recovery-Verfahren
- Wallet-App, Smartphone oder Computer
- Transaktionsdarstellung und Signatur
- Nutzerverhalten und physische Aufbewahrung

FORENSISCHE KONSEQUENZ

Ein Fehler an nur einer Stelle kann das Gesamtsystem schwächen. Deshalb muss nach einem Diebstahl zunächst geklärt werden, auf welcher Ebene ein Angriff technisch möglich war und welche Hypothesen durch die vorhandenen Spuren tatsächlich gestützt werden.

04 Zentrale Angriffsklassen

4.1 Kompromittierung des Recovery Seeds

Wer über einen vollständigen Seed verfügt, benötigt die ursprüngliche Hardware Wallet grundsätzlich nicht mehr. Der Seed kann auf einer anderen kompatiblen Wallet wiederhergestellt werden. Ein Täter kann deshalb Assets transferieren, während sich das originale Gerät weiterhin im Besitz des Opfers befindet.

- Phishing oder gefälschter Support
- Fotografieren oder Kopieren des Seeds
- Cloud- oder Datei-Backups
- Eingabe des Seeds auf einem Computer oder einer Website
- Gefälschte Wallet-Software
- Vorgegebener Seed bei manipulierten Geräten

4.2 Fehlerhafte oder vorhersehbare Seed-Erzeugung

Eine Hardware Wallet ist nur so sicher wie die Zufallswerte, aus denen ihre Schlüssel entstehen. Wird statt kryptografisch sicherer Entropie ein vorhersehbarer oder zu kleiner Wertebereich verwendet, kann ein Angreifer mögliche Seeds offline berechnen und mit öffentlich sichtbaren Blockchain-Adressen abgleichen.

4.3 Firmware-Schwachstellen

Firmware steuert zentrale Sicherheitsfunktionen. Fehler können unter anderem die Schlüsselerzeugung, Signaturprüfung, Updateprozesse, Speicherzugriffe oder die Kommunikation zwischen Sicherheitskomponenten betreffen.

4.4 Physische Angriffe

Physische Angriffe erfordern Zugriff auf das Gerät. Dazu zählen Fault Injection, Voltage Glitching, Side-Channel-Analysen, Speicherextraktion und Bus Sniffing. Sie sind von klassischen Remote-Angriffen klar zu trennen.

4.5 Kompromittierte Host- oder App-Umgebung

Auch wenn der Private Key das Gerät nicht verlässt, können Malware oder manipulierte Anwendungen die Benutzeroberfläche verändern, Empfangsadressen austauschen, schädliche Transaktionen vorbereiten oder den Nutzer zur Preisgabe des Seeds bewegen.

4.6 Lieferketten- und Manipulationsangriffe

Ein Gerät kann vor der ersten Nutzung kompromittiert werden. Denkbar sind ausgetauschte Geräte, manipulierte Verpackungen, veränderte Firmware, vorgegebene Seeds, gefälschte Begleitkarten oder nachgeahmte Herstellerseiten und Apps.

05 Dokumentierte Vorfälle und Fallstudien

5.1 COLDCARD – geschwächte Seed-Erzeugung 2026

Der COLDCARD-Vorfall des Sommers 2026 ist ein besonders folgenreiches dokumentiertes Beispiel dafür, dass ein Hardware Wallet kompromittiert sein kann, ohne dass ein Angreifer es je berührt oder aus der Ferne übernommen hat. Ursache war nach den veröffentlichten Analysen kein Angriff auf die Geräte, sondern ein Fehler in der Erzeugung der Schlüssel selbst. [1][2][4]

Mechanismus: Ursache war kein Laufzeitproblem des Hardware-Zufallsgenerators. Nach der technischen Darstellung des Herstellers führte ein Build- und Link-Integrationsfehler dazu, dass die Seed-Erzeugung nicht die vorgesehene Hardware-TRNG-Implementierung, sondern den in MicroPython enthaltenen Software-PRNG Yasmarang verwendete: Bei der Umstellung auf eine neue Kryptobibliothek im März 2021 wanderte die Schlüsselerzeugung auf einen Pfad, auf dem das Symbol rng_get() zur Software-Implementierung aufgelöst wurde. Eine Schutzabfrage, die genau das hätte verhindern sollen, prüfte lediglich, ob ein Konfigurationswert gesetzt war — nicht, ob er von null verschieden war. Der Hardware-Generator fiel also nicht aus; er wurde für die Seed-Erzeugung schlicht nicht erreicht. Auf Mk2 und Mk3 speiste sich der wirksame Generator im Wesentlichen aus Geräte- und Zeitzuständen. [2]

Bemerkenswert für die Bewertung offener Quellen: Der Quellcode lag über Jahre öffentlich vor, ohne dass der Fehler auffiel — auch eine kurz zuvor durchgeführte KI-gestützte Prüfung des eigenen Codes förderte ihn nach Herstellerangaben nicht zutage. Offenheit ersetzt keine gezielte Prüfung der tatsächlich erreichten Codepfade. [2]

Auswirkung: Die effektive Sicherheitsstärke — also der Suchraum, der einem Angreifer tatsächlich verbleibt — sank nach Angaben des Herstellers auf rund 40 Bit bei den Modellen Mk2 und Mk3 und auf rund 72 Bit bei Mk4, Mk5 und Q vor der Korrektur, gegenüber dem vorgesehenen Sicherheitsziel von 128 Bit; bei den neueren Modellen wirkte zusätzlich eingemischte Entropie der Sicherheitselemente dämpfend. Beide Werte sind vorläufige Schätzungen des Herstellers. Ein effektiver Suchraum von rund 40 Bit liegt in einem Bereich, der mit moderner Rechenleistung praktisch angreifbar ist; TRM Labs bezeichnet die betroffenen Schlüssel als ohne physischen Zugriff durchsuchbar. Genau darin liegt die Besonderheit des Falls: Der Angreifer benötigt weder das Gerät noch Schadsoftware beim Geschädigten, sondern nur die öffentlich einsehbare Blockchain, um Treffer zu erkennen. [2][4]

Ausmaß: Ab dem 30. Juli 2026 wurden betroffene Adressen in mehreren Wellen geleert. In der ersten Welle flossen binnen rund 25 Minuten etwa 594 BTC aus rund 500 Wallets in eine einzige Konsolidierungsadresse. Nach der Analyse von TRM Labs vom 5. August 2026 waren insgesamt rund 1.816 BTC aus mehr als 5.200 Adressen betroffen, verteilt auf vier Angriffswellen; der Gegenwert wurde zu diesem Zeitpunkt mit etwa 116 Millionen US-Dollar angegeben. Da weitere Betroffene auch nachträglich bekannt werden können, stellen diese Zahlen keine abschließende Schadensbilanz dar. [4]

Bemerkenswert ist das Nachtatverhalten: Die Mittel sammelten sich nach der Analyse von TRM Labs auf wenigen Adressen der Täterseite, mit nur einem weiteren Konsolidierungsschritt und ohne erkennbare Verschleierungsschichten; lediglich eine Wasabi-Einzahlung über 64,9 BTC und 200 ETH an Tornado Cash am 4. August 2026 wurden festgestellt. Unterschiede im Aufbau der Transaktionen je Welle sprechen dafür, dass mehrere Täter beteiligt sein könnten; eine Zuordnung zu einem bestimmten Akteur erfolgte nicht. [4]

Ausnahmen — und hier ist genau zu unterscheiden: Nach der Sicherheitsmitteilung gelten Seeds, bei deren Erzeugung mindestens 50 faire, unabhängige und nicht dokumentierte Würfelwürfe eingebracht wurden, hinsichtlich dieses RNG-Problems allein als nicht gefährdet. Eine starke, nur einmal verwendete BIP-39-Passphrase wirkt dagegen anders: Sie erschwert die unmittelbare Ausnutzung erheblich, weil der Angreifer zusätzlich die Passphrase erraten müsste, repariert den schwach erzeugten Seed aber nicht. Der Hersteller empfiehlt auch diesen Nutzern die Migration. Kurze, gängige, gemusterte oder mehrfach verwendete Passphrasen bieten ohnehin keinen verlässlichen Schutz. [1][2]

Der Angriff lässt sich vereinfacht als Kette darstellen:

1. Seed wird mit zu geringer beziehungsweise vorhersehbarer Entropie erzeugt.
2. Angreifer berechnet den begrenzten Raum möglicher Seeds beziehungsweise Private Keys.
3. Daraus werden Bitcoin-Adressen abgeleitet.
4. Die abgeleiteten Adressen werden mit öffentlich sichtbaren Blockchain-Daten abgeglichen.
5. Bei einem Treffer kann der Angreifer eine gültige Transaktion signieren.

Entscheidend für Betroffene: Ein Firmwareupdate repariert einen bereits erzeugten schwachen Seed nicht. Der Schlüssel war ab dem Moment seiner Erzeugung angreifbar. Betroffene Wallets müssen auf einen neu erzeugten Seed migriert werden — mit Prüfung von Fingerprint und Empfangsadresse und einer kleinen Testtransaktion vor der vollständigen Übertragung. [1][3]

Reaktion des Herstellers: Ab dem 30./31. Juli 2026 wurden Sicherheitsmitteilungen veröffentlicht, für sämtliche betroffenen Modellreihen korrigierte Firmwarestände bereitgestellt und nach eigenen Angaben der Versand betroffener Lagerbestände gestoppt. Stand September 2026 nennt der Hersteller als empfohlene Standardversionen 5.6.2 für Mk4/Mk5 und 1.5.2Q für Q; als Mindestversionen gelten 4.2.0 für Mk2/Mk3, 5.6.0 für Mk4/Mk5 und 1.5.0Q für Q sowie die entsprechenden Edge-Stände. Die aktuellen Standardversionen verlangen bei jeder neuen Seed-Erzeugung zusätzlich eigene Nutzerentropie — mindestens 65 Tastendrücke mit unvorhersehbarem Zeitverhalten, 50 Würfelwürfe oder 128 Münzwürfe — und erlauben die Anzeige und Nachrechnung des eingemischten Geräteanteils. Der Hersteller weist zugleich darauf hin, dass die veröffentlichten unabhängigen Prüfungen gezielte Einzelkontrollen und kein vollständiges Audit darstellen. [1][3][22]

FORENSISCHE BEDEUTUNG

Das Opfer kann den Seed niemals digitalisiert, das Gerät nie aus der Hand gegeben und keine unbekannte Transaktion bestätigt haben – und dennoch können Assets entwendet werden, wenn die Schlüssel schon bei ihrer Erzeugung unzureichend geschützt waren.

5.1.1 Woran sich ein Kohortenfall erkennen lässt

Fehler in der Schlüsselerzeugung erzeugen ein Schadensbild, das sich vom Bild einer individuellen Kompromittierung unterscheidet. Die folgenden Merkmale helfen bei der ersten Einordnung:

MERKMAL	HINWEIS AUF KOHORTEN-/RNG-FALL	HINWEIS AUF EINZELKOMPROMITTIERUNG
Zeitliche Verteilung	viele nicht verbundene Geschädigte innerhalb weniger Stunden oder Tage	einzelner Geschädigter, kein zeitliches Muster
Gemeinsamkeiten	gleiches Modell, gleiche Modellreihe, Seed-Erzeugung im selben Firmwarezeitraum	keine gemeinsame technische Grundlage erkennbar
Vorgeschichte	kein Phishing, kein Support-Kontakt, kein digitalisierter Seed	Phishing-Nachricht, Support-Chat, Screenshot oder Cloud-Backup nachweisbar
Adressauswahl	Abfluss von Adressen ohne jede vorherige Interaktion mit dem Täter	gezielte Ansprache oder vorherige Kontaktaufnahme
Transaktionsmuster	Sweeps über viele Adressen in kurzer Folge, häufig ohne Rücksicht auf Gebühren	einzelner Abfluss, oft nach einer Testtransaktion
Wirkung von Gegenmaßnahmen	Bei bereits schwach erzeugtem Seed: Firmwareupdate repariert den Seed nicht; Migration erforderlich	Neueinrichtung oder Bereinigung der Umgebung kann genügen

Keines dieser Merkmale beweist für sich genommen eine Ursache. In der Zusammenschau erlauben sie jedoch eine belastbare Priorisierung — und sie verhindern den in der Praxis häufigen Fehler, dem Geschädigten vorschnell einen Sorgfaltsverstoß zu unterstellen.

5.2 Trezor – physische Seed-Extraktion

Ledger Donjon veröffentlichte 2019 einen physischen Angriff gegen Trezor One, Trezor Model T und verwandte Designs. Kraken Security Labs demonstrierte 2020 einen Voltage-Glitching-Angriff, bei dem mit physischem Zugriff Speicherinhalte ausgelesen und ein Seed extrahiert werden konnten. [7][8]

Diese Angriffe sind keine Remote-Hacks. Sie setzen physischen Zugriff, spezielles technisches Know-how und Ausrüstung voraus. Für gewöhnliche Internetbetrugsfälle ist diese Angriffsklasse deshalb anders zu gewichten als Seed-Phishing oder kompromittierte Software.

5.3 Trezor Safe 7 / TROPIC01 – Laser Fault Injection 2026

Ledger Donjon prüfte im Rahmen eines unabhängigen Audits das Sicherheitselement TROPIC01 des Herstellers Tropic Square, das im Trezor Safe 7 verbaut ist. Die Forscher öffneten das Gehäuse, belichteten die Rückseite des Chips mit einem 1064-nm-Laser und brachten damit die Ed25519-Signaturprüfung dazu, eine ungültige Signatur als gültig zu bewerten. In Verbindung mit einem

zweiten Fehlereinschuss beim Startvorgang ließ sich dadurch eigene Firmware auf dem Chip ausführen. Der erste vertrauliche Hinweis an Tropic Square datiert vom 27. Januar 2026, die koordinierte Veröffentlichung erfolgte am 3. Juni 2026. [5][6][19]

Für die Bewertung wichtig ist, was damit noch nicht erreicht war: Die im Chip gespeicherten Geheimnisse liegen hinter einem Hardwaremechanismus (MAC-and-Destroy), auf den auch eine vollständig übernommene Firmware zunächst keinen Zugriff hatte. Tropic Square fand anschließend in eigener Analyse einen Weg, diese Schutzgrenze aus einer solchen Position heraus zu überwinden, und hielt die Einzelheiten bis zur Verfügbarkeit einer überarbeiteten Chipversion zurück; Ledger Donjon gelangte daraufhin ebenfalls zu Schwachstellen, die den Mechanismus in Kombination kompromittieren — nach eigener Darstellung jedoch nur, wenn zuvor eigene Firmware auf dem Chip ausgeführt werden kann. Als Feldmaßnahme wurde vorgeschlagen, den Wartungsmodus des Chips zu deaktivieren; das erhöht den Aufwand, ohne den Angriff im Laborversuch unmöglich zu machen. [19] [20]

Der Gerätehersteller stellt dazu fest, dass der Safe 7 auf drei unabhängigen Sicherheitsebenen beruht und die Schwachstelle nur eine davon betrifft; Zugriff auf PIN, Wallet oder Guthaben ergebe sich daraus nicht, und ein Nachweis realer Ausnutzung liege nicht vor. Der Befund liegt auf Siliziumebene und lässt sich nicht durch ein gewöhnliches Firmwareupdate beheben. Herstellerangabe und Forschungsergebnis stehen hier nicht im Widerspruch, betonen aber unterschiedliche Seiten desselben Sachverhalts: die verbleibenden Schutzschichten einerseits, die praktische Durchführbarkeit der Laborangriffe andererseits. [5][6][19]

Der Chiphersteller stuft die Schwachstelle mit einem CVSS-3.1-Basiswert von 5,7 (mittel) ein und weist darauf hin, dass sich das Risiko je nach Einsatzumgebung weiter verringern kann, weil der Angriff den vollständigen physischen Besitz des Geräts, eine präzise rückseitige Entkapselung des Chips, Expertenwissen und Laborausrüstung im Wert von mehr als 30.000 Euro voraussetzt. Ein Nachweis realer Ausnutzung liegt nicht vor. Als Sofortmaßnahmen werden das Abschalten des Wartungsmodus und ein besonderes Aktualisierungsverfahren genannt; eine überarbeitete Siliziumversion war für Ende 2026 angekündigt, der vollständige technische Bericht für das Frühjahr 2027. [20]

Für die forensische Praxis ist vor allem der Maßstab wichtig: Ein Angriff, der Entkapselung, Laborausrüstung und den physischen Besitz des Geräts voraussetzt, ist in gewöhnlichen Betrugs- und Diebstahlsfällen keine plausible Erklärung. Er gehört in die Bewertung, wenn ein Gerät nachweislich längere Zeit außerhalb der Kontrolle des Eigentümers war. Zugleich zeigt der Fall, dass auch ein Secure Element nicht mit absoluter Sicherheit gleichzusetzen ist; entscheidend bleibt die Kombination aus Chip, Firmware, Integrationsdesign und weiteren Schutzschichten.

5.4 Ledger – Kundendatenleck 2020

2020 erhielt ein Angreifer über einen API-Schlüssel Zugriff auf Ledgers E-Commerce- und Marketingdatenbank. Später wurde bekannt, dass mehr als eine Million E-Mail-Adressen sowie ungefähr 272.000 Datensätze mit weitergehenden personenbezogenen Informationen wie Namen, Anschriften und Telefonnummern betroffen waren. [9]

Private Keys wurden dadurch nicht unmittelbar kompromittiert. Der Vorfall erhöhte jedoch das Risiko gezielter Phishing-, Social-Engineering- und gegebenenfalls physischer Angriffe auf bekannte Hardware-Wallet-Besitzer.

5.5 Ledger Connect Kit – kompromittierte Softwarelieferkette 2023

Im Dezember 2023 veröffentlichte ein Angreifer nach einem Phishing-Angriff auf einen ehemaligen Ledger-Mitarbeiter manipulierte Versionen des Ledger Connect Kit über NPMJS. DApps, die die Bibliothek einbanden, konnten schädlichen Code laden und Nutzer zu Transaktionen veranlassen, durch die Assets abflossen. [10]

Die Hardware Wallet selbst war dabei nicht kompromittiert. Der Fall zeigt vielmehr die Bedeutung der Software- und Integrationsumgebung, in der ein Hardware Wallet verwendet wird.

5.6 Tangem – private Schlüssel in App-Protokollen 2024

Tangem veröffentlichte Ende 2024 eine Sicherheitsmitteilung zu einer mobilen App. Bei Wallets, die mit einer Seed Phrase aktiviert wurden, konnte der Private Key irrtümlich in App-Logs erscheinen. Potenziell betroffen waren nach Angaben des Herstellers Nutzer, die zusätzlich innerhalb von sieben Tagen über die App den Support kontaktierten und dabei Logs übermittelten. Tangem erklärte, dass keine Nutzerverluste festgestellt worden seien. [11]

Der Vorfall verdeutlicht, dass eine Schwachstelle außerhalb des eigentlichen Wallet-Chips entstehen kann. Für die forensische Bewertung muss daher auch die mobile App und deren Protokollierung betrachtet werden.

5.7 OneKey Mini – Kommunikation zwischen Sicherheitskomponenten

Unciphered demonstrierte einen physischen Angriff gegen den OneKey Mini. Nach der veröffentlichten Darstellung lag ein Problem in der unzureichend geschützten Kommunikation zwischen CPU und Secure Element. OneKey erklärte, die Schwachstelle behoben zu haben. Ein Remote-Angriff war für das demonstrierte Szenario nicht erforderlich beziehungsweise nicht vorgesehen; entscheidend war der physische Zugriff auf das Gerät. [12]

5.8 SafePal S1 – Schwachstellen in der Geräte- und Updatearchitektur

Kraken Security Labs berichtete 2021 über mehrere Schwachstellen beim SafePal S1, darunter Fragen zur Manipulationserkennung und die Möglichkeit eines Firmware-Downgrades. Die Forscher erklärten zugleich, dass es ihnen in dieser Untersuchung nicht gelungen sei, Kryptowährungen aus dem Gerät zu stehlen. [13]

Diese Abgrenzung ist wichtig: Eine nachgewiesene Schwachstelle ist nicht automatisch gleichbedeutend mit einem nachgewiesenen Vermögensdiebstahl.

5.9 Ellipal – physische Seed-Extraktion

Ledger Donjon untersuchte 2019 ein Ellipal-Wallet und berichtete über mehrere Schwachstellen. Eine davon ermöglichte nach Darstellung der Forscher bei physischem Zugriff die Extraktion des Seeds. Weitere Feststellungen betrafen reaktivierbare Kommunikationsschnittstellen und damit mögliche Supply-Chain- oder Evil-Maid-Szenarien. Der Hersteller wurde vor Veröffentlichung informiert. [14]

Der Fall ist bemerkenswert, weil Ellipal mit einer weitgehend „air-gapped“ Architektur warb. Air Gap kann die Angriffsfläche reduzieren, ist aber keine Garantie gegen Fehler in Hardware oder Firmware.

5.10 Keystone 3 – Auditierte Firmware- und Hardwarethemen

Keylabs veröffentlichte 2023 einen Sicherheits-Audit des Keystone 3. Der Bericht identifizierte unter anderem eine hoch eingestufte Firmware-Schwachstelle im Bereich der Manipulationsreaktion sowie mehrere niedrig eingestufte Feststellungen. Nach Angaben des Prüfers wurden die hoch eingestufte

und weitere Firmwarefeststellungen behoben und erneut getestet. [15]

Veröffentlichte Audits sind nicht nur ein Hinweis auf vorhandene Schwachstellen. Sie können zugleich ein Zeichen dafür sein, dass ein Hersteller externe Prüfungen zulässt und gefundene Probleme nachvollziehbar bearbeitet.

5.11 BitBox02 – Beispiel einer mehrschichtigen Architektur

BitBox beschreibt für die BitBox02 eine Dual-Chip-Architektur mit Mikrocontroller und separatem Secure Chip. Der Seed wird verschlüsselt auf dem Mikrocontroller gespeichert; mehrere voneinander unabhängige Geheimnisse und Entropiequellen sollen die Seed-Erzeugung und den Zugriff zusätzlich absichern. Hinzu kommen Secure Bootloader, Geräteauthentisierung und die Prüfung von Transaktionsdaten am Display. [16]

Im Rahmen der für diese Fassung ausgewerteten Quellen wurde kein mit dem COLDCARD-Vorfall 2026 vergleichbarer öffentlich bestätigter Fall identifiziert, bei dem eine aktuelle BitBox02-Schwachstelle zu einer bekannten Serie von Vermögensdiebstählen geführt hätte. Dies ist ausdrücklich keine Aussage über absolute Sicherheit.

5.12 Einordnung der dokumentierten Beispiele

HERSTELLER / FALL	EBENE	ZUGRIFF	REALER NUTZERVERLUST DOKUMENTIERT?	KERNAUSSAGE
COLDCARD 2026	Seed-Erzeugung / Firmware	kein physischer Zugriff nötig	**Ja; mehrere Sweep-Wellen ab 30.07.2026**	Schwach erzeugte Schlüssel lassen sich offline rekonstruieren — ohne Gerätezugriff.
Trezor 2019/2020	Hardware / physischer Angriff	physisch	Kein realer Nutzerverlust belegt; Seed-Extraktion demonstriert	Physischer Besitz kann bei älteren Designs entscheidend sein.
TROPIC01 2026	Secure Element	Labor, Entkapselung, physisch	Kein realer Nutzerverlust belegt; Laborangriff demonstriert	Auch Sicherheitschips können angreifbar sein.
Ledger 2020	Kundendaten / Infrastruktur	remote gegen Datenbank	Nicht durch den Datenabfluss selbst; Folgeangriffe möglich	Herstellerdaten können Folgeangriffe ermöglichen.
Ledger Connect Kit 2023	Software-Lieferkette	remote / DApp-Umfeld	**Ja**	Wallet-Hardware war nicht selbst kompromittiert.
Tangem 2024	Mobile App / Logs	spezifische Support-Konstellation	Nein, nach Herstellerangabe	Schlüsseldaten können außerhalb des Chips exponiert werden.
OneKey Mini	Hardware-Integration	physisch	Kein realer Nutzerverlust belegt; Extraktion demonstriert	Die Verbindung CPU ↔ Secure Element ist Teil der Sicherheitsarchitektur.
SafePal S1	Firmware / Manipulationsschutz	physisch	Kein realer Nutzerverlust belegt; kein Diebstahl im Test gelungen	Schwachstelle ist nicht automatisch Vermögensdiebstahl.
Ellipal 2019	Hardware / physisch	physisch	Kein realer Nutzerverlust belegt; Seed-Extraktion demonstriert	Air Gap schützt nicht vor jeder Hardware-/Firmware-Schwachstelle.
Keystone 3 Audit	Firmware / Hardware	Audit	Kein realer Nutzerverlust belegt; Auditbefunde behoben	Externe Audits können Risiken sichtbar und behebbar machen.

06 Supply Chain, Evil Maid und gefälschte Geräte

Eine besonders problematische Angriffsklasse entsteht, bevor der Anwender das Wallet erstmals verwendet. Das Ziel muss dabei nicht darin bestehen, unmittelbar Kryptowährungen zu stehlen. Ein Täter kann einen kompromittierten Seed oder eine manipulierte Geräteumgebung vorbereiten und

anschließend auf eine größere Einzahlung warten.

- Öffnen und erneutes Verpacken eines Geräts
- Austausch durch ein manipuliertes oder gefälschtes Gerät
- Manipulierte Firmware oder Elektronik
- Vorgefertigter oder dem Täter bereits bekannter Recovery Seed
- Manipulierte Begleitkarten oder Setup-Anweisungen
- Gefälschte Herstellerwebsite oder Wallet-App

6.1 Zeitverzögertes Angriffsszenario

ZEITPUNKT	EREIGNIS
Tag 1	Manipulation oder Kenntnis des Seeds
Tag 5	Nutzer aktiviert die vermeintlich neue Wallet
Tag 6	kleine Testtransaktion
Tag 8	größere Bitcoin-Übertragung
kurz danach	vollständiger Transfer auf eine unbekannte Adresse

Aus Sicht des Nutzers wirkt der Vorgang wie ein unmittelbarer Angriff auf die neue Hardware Wallet. Tatsächlich kann der Angreifer den Schlüssel bereits Tage oder Wochen zuvor gekannt haben.

6.2 Evil-Maid-Angriffe

Bei einem Evil-Maid-Szenario erhält ein Angreifer vorübergehend physischen Zugriff auf ein Gerät und manipuliert es, ohne dass der Eigentümer die Veränderung bemerkt. Relevante Situationen können Transport, Lagerung, Hotelaufenthalt, Reparatur, Versand oder persönliche Übergabe sein.

6.3 Gefälschte Hardware Wallets

Ein Nutzer kann glauben, ein Produkt eines bekannten Herstellers zu verwenden, obwohl es sich um eine Kopie, ein modifiziertes Originalgerät oder ein manipuliertes Gebrauchtgerät handelt. Echtheitsprüfungen und eine kontrollierte Lieferkette sind deshalb Teil des Sicherheitsmodells.

6.4 Voraktivierte Geräte und Übergabe durch Dritte

Ein praktisch besonders relevantes Szenario dieser Angriffsklasse ist zugleich das unspektakulärste: Der spätere Eigentümer richtet die Wallet nicht selbst ein. Er erhält ein Gerät, das bereits initialisiert wurde, oder lässt sich die Einrichtung von einem Händler, Vermittler, Bekannten oder vermeintlichen Experten abnehmen. Wer die Erstinitialisierung kontrolliert und dabei Kenntnis des erzeugten Schlüssels erlangt oder eine gleichwertige Sicherungskopie zurückbehält, kann später weiterhin Zugriff auf die Wallet besitzen — unabhängig davon, wer das Gerät anschließend besitzt.

Hersteller warnen inzwischen ausdrücklich vor diesem Muster. Tangem etwa weist darauf hin, dass Geräte niemals mit vorgenerierten Schlüsseln oder Zugangscodes ausgeliefert werden und ein beiliegendes „Initialisierungspasswort“ ein eindeutiges Warnzeichen ist; die Anwendung zeigt beim ersten Scan an, ob ein Gerät bereits aktiviert wurde. [17][18][21]

Für Tangem sind hierbei insbesondere zwei technische Eigenschaften relevant, die sich in ähnlicher Form auch bei anderen Herstellern finden können, dort aber jeweils gesondert zu prüfen sind:

- Kartensets bestehen aus mehreren Geräten, die bei der Erstinitialisierung miteinander verbunden werden. Wurde dabei ein weiteres Gerät als Sicherung eingebunden und anschließend von einem Dritten zurückbehalten, enthält dieses Sicherungsgerät denselben privaten Schlüssel und ermöglicht — bei Kenntnis der erforderlichen Zugangsdaten — denselben Wallet-Zugriff wie das ausgehändigte Gerät. Den Zugangscode legt fest, wer die Wallet einrichtet.
- Das Kopieren des Schlüssels auf Sicherungsgeräte erfolgt regelmäßig nur einmalig bei der Erstinitialisierung. Eine bereits eingerichtete Wallet lässt sich deshalb nicht nachträglich bereinigen — sie muss vollständig zurückgesetzt und neu erzeugt werden.

Das erklärt auch das typische Schadensbild: Der Abfluss erfolgt nicht bei der Übergabe, sondern kurz nach der ersten nennenswerten Einzahlung. Aus Sicht des Geschädigten wirkt das wie ein Angriff auf ein neues Gerät; tatsächlich kann der Schlüssel dem Täter seit Wochen bekannt gewesen sein.

07 Forensische Untersuchung nach einem Diebstahl

Nach einem Diebstahl von einer Hardware Wallet sollte nicht vorschnell eine Ursache angenommen werden. Sinnvoll ist eine strukturierte Untersuchung in mehreren Ebenen.

Die Spur bleibt auf der Kette. *Unabhängig von der technischen Ursache liegt die Nachverfolgung entwendeter Kryptowerte in der lückenlosen Rekonstruktion der Blockchain-Transaktionen — von der Ausgangsadresse bis zum identifizierbaren Endpunkt.*

7.1 Ebene Blockchain

- Ausgangsadresse und Transaktionshash
- Zeitpunkt, Betrag und Netzwerkgebühr
- Zieladresse und nachgelagerte Wallets
- Konsolidierungen und Aufsplittungen
- Swaps, Bridges und andere Protokolle
- Einzahlungen auf zentrale Börsen oder andere identifizierbare Dienstleister

7.2 Ebene Zeitablauf

Besonders wichtig ist die zeitliche Rekonstruktion. Ein sehr kurzer Abstand zwischen Eingang und unautorisiertem Abfluss kann auf eine automatisierte Überwachung oder einen bereits vorhandenen Schlüsselzugriff hinweisen. Er beweist dies jedoch nicht.

EREIGNIS	BEISPIELZEITPUNKT
Wallet aktiviert	**14:05 Uhr**
Empfangsadresse erstellt	**14:08 Uhr**
BTC gesendet	**14:23 Uhr**
Bestätigung im Netzwerk	**14:31 Uhr**
Unbekannte Ausgangstransaktion	**14:37 Uhr**

7.3 Ebene Gerät

- Hersteller und Modell
- Serien- oder Geräteinformationen
- Firmwareversion
- Kaufdatum und Verkäufer
- Verpackung und sichtbare Manipulationsmerkmale
- durchgeführte Updates
- verwendete Wallet-App und Kopplungsart

Bei ungeklärtem Sachverhalt sollte das Gerät möglichst nicht zurückgesetzt, aktualisiert oder anderweitig verändert werden. Veränderungen können spätere technische Prüfungen erschweren oder unmöglich machen. Festzuhalten sind außerdem der Zeitpunkt der Seed-Erzeugung und die damals installierte Firmwareversion: Nur damit lässt sich prüfen, ob der Geschädigte zu einer von einem bekannten Herstellervorfall betroffenen Kohorte gehört. Gerät, Verpackung und Begleitmaterial sind mit dokumentierter Beweiskette zu verwahren.

7.4 Ebene Smartphone und Computer

- Installationsquelle und Version der Wallet-Software
- verdächtige Apps, Browsererweiterungen oder Downloads
- Supportkontakte und Kommunikationsverläufe
- Screenshots, Dateien und mögliche Seed-Abbildungen
- Hinweise auf Remote-Zugriffe oder Schadsoftware
- Browserhistorie rund um Einrichtung und Transaktionen

7.5 Ebene Beschaffungskette

Zu klären ist, ob das Gerät direkt vom Hersteller, über einen autorisierten Händler, einen Online-Marktplatz, eine Privatperson, einen Berater, einen Vermittler oder einen angeblichen Finanzdienstleister bezogen wurde. Die Antwort kann die Risikoeinschätzung erheblich verändern.

7.6 Hardware-Wallet-Hack oder Seed-Diebstahl?

Die Aussage „Meine Hardware Wallet wurde gehackt“ beschreibt zunächst nur die Wahrnehmung des Geschädigten. Technisch können dahinter sehr unterschiedliche Ursachen stehen:

1. Seed kompromittiert
2. Seed vorhersehbar oder schwach erzeugt
3. Hardware kompromittiert
4. Firmware kompromittiert
5. Software beziehungsweise App kompromittiert
6. Transaktion manipuliert oder irreführend dargestellt
7. Lieferkette kompromittiert
8. Social Engineering oder gefälschter Support

PRÜFGRUNDSATZ

Ein Gutachten sollte die Ursache nur dann als feststehend bezeichnen, wenn sie durch technische oder dokumentarische Belege gestützt wird. Plausible Alternativhypothesen sind ausdrücklich zu kennzeichnen.

7.7 Von der Wahrnehmung zur belastbaren Hypothese

Die Reihenfolge der Prüfung entscheidet über die Qualität des Ergebnisses. Bewährt hat sich, von den überprüfbaren zu den unüberprüfbaren Annahmen zu arbeiten:

- Zuerst die Kohortenfrage: Gibt es zu Gerät, Modellreihe und Erzeugungszeitraum eine bekannte Sicherheitsmitteilung? Diese Frage ist ohne Mitwirkung Dritter zu beantworten.
- Dann die dokumentierbaren Umstände: Beschaffungsweg, Erstinitialisierung, Seed-Handhabung, Support- und Phishing-Kontakte, App-Quelle.
- Dann die Blockchain: Zeitachse, Zielstruktur, Weiterleitungsmuster, Endpunkte.
- Erst zuletzt die technischen Restszenarien, die nur im Labor oder mit physischem Zugriff erklärbar wären.

Ergibt die Prüfung keine eindeutige Ursache, wird das im Gutachten so festgehalten. Ein als offen gekennzeichneter Befund ist für Ermittlungsbehörden verwertbar; eine zu früh festgelegte Ursache ist es nicht.

08 Forensische Risikomatrix

ANGRIFFSSZENARIO	PHYSISCHER ZUGRIFF	SEED DIREKT BENÖTIGT	OHNE PHYSISCHEN GERÄTEZUGRIFF MÖGLICH?	TYPISCHE BLOCKCHAIN-SPUREN
Seed-Phishing	Nein	Ja	Ja	Abfluss wie regulär signierte Transaktion
Schwache Seed-Erzeugung	Nein	Nein	Ja (Offline-Rekonstruktion des Schlüssels)	Abfluss wie regulär signierte Transaktion
Manipuliertes Gerät	Vor Nutzung / physisch	Nicht zwingend	Ja, nach der vorgelagerten Manipulation	Abfluss nach Einzahlung
Supply Chain	Vor Nutzung	Nicht zwingend	Ja, nach der vorgelagerten Manipulation	oft zeitnah oder ereignisgesteuert
Fault Injection	Ja	Nein	Nein	Abfluss nach Schlüsselgewinnung
Side Channel	Ja	Nein	Nein	Abfluss nach Schlüsselgewinnung
Firmware-Schwachstelle	abhängig	abhängig	abhängig vom konkreten Angriff	abhängig vom Angriff
App-/Software-Kompromittierung	Nein	nicht zwingend	Ja	manipulierte oder autorisierte Transaktion
Seed in Logdateien	Nein	indirekt	Ja, sofern die Daten abgeflossen sind	regulär signierter Abfluss

Die Matrix dient der ersten Strukturierung. Sie ersetzt keine Einzelfallprüfung. Insbesondere können verschiedene Angriffsklassen miteinander kombiniert werden.

09 Empfehlungen für Anwender

GERÄT AUS NACHVOLLZIEHBARER QUELLE BEZIEHEN

Bevorzugt direkt beim Hersteller oder über eindeutig autorisierte Vertriebspartner. Bei gebrauchten oder weitergegebenen Geräten ist zusätzliche Vorsicht erforderlich.

KEINE VORGEFERTIGTE RECOVERY PHRASE AKZEPTIEREN

Ein neues Gerät sollte seinen Seed im vorgesehenen Initialisierungsprozess selbst erzeugen. Ein bereits beiliegender oder vorgegebener Seed ist ein deutliches Warnsignal.

RECOVERY PHRASE NICHT DIGITALISIEREN

Keine Fotos, Cloudspeicher, E-Mails, Messenger-Nachrichten oder unverschlüsselte Textdateien verwenden.

FIRMWARE UND APP AKTUELL HALTEN

Sicherheitsupdates können bekannte Schwachstellen beseitigen. Ein Update repariert jedoch nicht zwingend einen bereits kompromittierten oder schwach erzeugten Seed.

TRANSAKTIONSDATEN AM VERTRAUENSWÜRDIGEN GERÄT PRÜFEN

Wo technisch möglich, Adresse, Betrag und weitere relevante Daten direkt am Hardware Wallet kontrollieren.

BEI GROSSEN VERMÖGENSWERTEN ZUSÄTZLICHE SCHUTZKONZEPTE PRÜFEN

Je nach Risikoprofil können Passphrase, Multisignature, getrennte Backups und getrennte Wallets für langfristige Verwahrung und laufende Nutzung sinnvoll sein.

TESTTRANSAKTION RICHTIG EINORDNEN

Eine Testtransaktion dient dazu, Empfangsadresse, Wallet und Übertragungsweg zu prüfen — insbesondere nach einer Migration auf einen neuen Seed. Sie ist kein Sicherheitsnachweis dafür, dass der private Schlüssel ausschließlich dem Eigentümer bekannt ist: Ein Täter mit bereits vorhandenem Schlüsselzugriff kann einen kleinen Testbetrag bewusst unangetastet lassen und erst bei einer größeren Einzahlung reagieren. Der Schutz liegt deshalb in der kontrollierten Erstinitialisierung, nicht in der Wartezeit.

EIGENE ENTROPIE EINBRINGEN, SOFERN DAS GERÄT DIES VORSIEHT

Bei größeren Beträgen kann die Seed-Erzeugung durch eigene, ausreichend viele Würfelwürfe ergänzt werden; im COLDCARD-Vorfall 2026 galten so erzeugte Seeds hinsichtlich des RNG-Fehlers als nicht gefährdet. Eine zusätzliche starke Passphrase erschwert die Ausnutzung, ersetzt aber keine saubere Schlüsselerzeugung: Ein schwach erzeugter Seed bleibt schwach und muss migriert werden. [1][2]

SICHERHEITSMITTEILUNGEN DES HERSTELLERS VERFOLGEN

Wer weiß, welches Modell mit welcher Firmware den eigenen Seed erzeugt hat, kann im Ernstfall innerhalb von Minuten beurteilen, ob er betroffen ist. Diese Angaben sollten zusammen mit dem Kaufbeleg dokumentiert werden — getrennt vom Seed selbst.

BEI MEHREREN GERÄTEN AUF UNABHÄNGIGE IMPLEMENTIERUNGEN ACHTEN

Multisignature-Konstruktionen aus Geräten verschiedener Hersteller und mit getrennt erzeugter Entropie verringern die Abhängigkeit von einer einzelnen Implementierung. Der Zugewinn an Sicherheit geht mit höherer Komplexität einher und will geübt sein.

WICHTIG

Zusätzliche Sicherheitsmaßnahmen erhöhen häufig auch die Komplexität. Ein Sicherheitskonzept muss deshalb nicht nur gegen Angreifer schützen, sondern vom Eigentümer dauerhaft und fehlerarm bedient werden können.

10 Bedeutung für Rechtsanwälte und Ermittlungsbehörden

Der Begriff „Hardware Wallet“ sollte bei der Sachverhaltsaufnahme nicht als Beweis dafür behandelt werden, dass ausschließlich der Geschädigte Zugriff auf die Private Keys gehabt haben kann. Umgekehrt darf ein unautorisierter Transfer nicht automatisch als Produktfehler des Herstellers eingestuft werden.

Für eine belastbare Ersteinschätzung sollten insbesondere folgende Punkte dokumentiert werden:

- Hersteller, Modell und Gerätegeneration
- Kaufquelle und Zeitpunkt der Beschaffung
- Zeitpunkt und Ablauf der Initialisierung
- Firmwareversion und Updatehistorie
- Art der Seed-Erzeugung und Aufbewahrung
- verwendetes Smartphone oder Computer
- Wallet-App und Installationsquelle
- letzter legitimer Zugriff
- Zeitpunkt des Asset-Eingangs
- Zeitpunkt des unautorisierten Transfers
- Zieladresse und weitere Transaktionswege

Gerade bei schnellen Abflüssen nach einer Einzahlung ist die Kombination aus Zeitachse und Blockchain-Analyse besonders wichtig. Muster können Hinweise auf bereits bekannte Schlüssel, automatisierte Überwachung oder einen vorher vorbereiteten Angriff geben.

Zwei Punkte werden in der Praxis regelmäßig übersehen. Erstens sollte das Gerät frühzeitig gesichert und nicht zurückgesetzt werden; für eine spätere technische Untersuchung ist der unveränderte Zustand entscheidend. Zweitens ist zu prüfen, ob weitere Geschädigte mit demselben Gerätetyp im selben Zeitfenster bekannt sind. Fällt der Sachverhalt in eine bekannte betroffene Geräte- oder Firmwarekohorte, kann dies deutlich gegen eine ausschließlich nutzerseitige Ursache sprechen. Die rechtliche Bewertung eines möglichen Mitverschuldens bleibt davon getrennt und ist anhand des konkreten Einzelfalls vorzunehmen.

11 Forensisches Fazit

Hardware Wallets reduzieren eine Vielzahl klassischer Cyberrisiken erheblich. Sie stellen jedoch keine absolute Sicherheitsgrenze dar. Die dokumentierten Vorfälle zeigen Angriffsmöglichkeiten auf Hardware, Firmware, Seed-Erzeugung, Software, Lieferkette, Support-Infrastruktur und Nutzerprozesse.

Ein besonders wichtiger Befund ergibt sich aus dem COLDCARD-Vorfall 2026: Ein Angreifer muss ein Hardware Wallet nicht zwingend physisch besitzen oder aus der Ferne kompromittieren. Ist die kryptografische Schlüsselerzeugung fehlerhaft, kann das Sicherheitsmodell bereits an seinem

Ausgangspunkt versagen.

Auf der anderen Seite darf auch nicht jeder unautorisierte Transfer vorschnell als „Hardware-Wallet-Hack“ bezeichnet werden. In der Praxis können kompromittierte Recovery Seeds, Phishing, manipulierte Software, Lieferkettenrisiken oder andere Angriffe außerhalb der eigentlichen Hardware die Ursache sein.

LEITGEDANKE

Nicht das einzelne Hardware Wallet entscheidet über die Sicherheit der Kryptowährungen, sondern die gesamte Kette von der Erzeugung des Private Keys bis zur Freigabe einer Transaktion.

Für die Blockchain-Forensik ist anschließend entscheidend: Wann wurden die Assets transferiert? Welche Adresse hat sie erhalten? Wie wurden sie weitergeleitet? Welche Börsen, Bridges oder anderen Dienstleister wurden genutzt? Und welche technische Erklärung ist mit den vorhandenen Beweisen tatsächlich vereinbar?

12 Quellen und Hinweise

Die nachfolgenden Quellen bilden die wesentliche Grundlage für die dargestellten Vorfälle. Herstellerangaben werden als solche behandelt; sie ersetzen keine unabhängige technische Bewertung. Sämtliche Verweise wurden zuletzt im September 2026 abgerufen. Angaben zu Schadenshöhen laufender Vorfälle sind Momentaufnahmen und können sich ändern.

[1] Coinkite: Coldcard Security Advisory (Seed-Erzeugung Mk2/Mk3), 30.07.2026, aktualisiert 01.08.2026 – blog.coinkite.com/coldcard-mk3-seed-generation-warning/
[2] Coinkite: Technical Deep Dive into the Entropy Issue, 07/2026 – blog.coinkite.com/entropy-technical-backgrounder/
[3] Coinkite: COLDCARD Security Update – Seed Generation, Transaction Integrity, and Data Isolation, 20.08.2026 – blog.coinkite.com/coldcard-security-update-5.6.1-1.5.1q/
[4] TRM Labs: The Largest Hardware Wallet Exploit of 2026 – Inside the Coldcard Hack, 08/2026 – trmlabs.com/resources/blog/the-largest-hardware-wallet-exploit-of-2026-inside-the-usd-116-million-coldcard-hack
[5] Trezor: TROPIC01 chip vulnerability disclosure – what happened, 06/2026 – trezor.io/learn/security-privacy/how-trezor-keeps-you-safe/tropic-01-chip-vulnerability-disclosure-what-happened
[6] Trezor: Trezor response – TROPIC01 chip disclosure (no impact to your funds), 03.06.2026 – trezor.io/blog/news/Trezor-response-TROPIC01-chip-disclosure-no-impact-to-your-funds
[7] Ledger Donjon: Unfixable Seed Extraction on Trezor – A practical and reliable attack, 01.07.2019 – ledger.com/blog/unfixable-key-extraction-attack-on-trezor
[8] Kraken Security Labs: Kraken Identifies Critical Flaw in Trezor Hardware Wallets, 31.01.2020 – blog.kraken.com/product/security/kraken-identifies-critical-flaw-in-trezor-hardware-wallets
[9] Ledger: Update – Efforts to Protect Your Data and Prosecute the Scammers, 2020 – ledger.com/blog/update-efforts-to-protect-your-data-and-prosecute-the-scammers
[10] Ledger: Security Incident Report – Ledger Connect Kit, 20.12.2023 – ledger.com/blog/security-incident-report
[11] Tangem: Tangem Identifies and Resolves Potential Vulnerability, 31.12.2024 – tangem.com/en/blog/post/tangem-resolves-log-issue/
[12] Unciphered: OneKey says it has fixed flaw that got its hardware wallet hacked in 1 second, 2023 – unciphered.com/onekey-says-it-has-fixed-flaw-that-got-its-hardware-wallet-hacked-in-1-second/
[13] Kraken Security Labs: Finds Flaws in SafePal S1 Hardware Wallet, 2021 – blog.kraken.com/product/security/kraken-security-labs-finds-flaws-in-safepal-s1-hardware-wallet
[14] Ledger Donjon: Extracting seed from Ellipal wallet, 25.06.2019 – ledger.com/blog/ellipal-security
[15] Keylabs: Keystone 3 Security Audit, 11/2023 – keylabs.io/reports/2023-11-keystone3/
[16] BitBox / Shift Crypto: Security on every level – BitBox02 security features – bitbox.swiss/bitbox02/security-features/
[17] Tangem: Scam Alert – How to Identify and Avoid Pre-Activated Wallets, 03.10.2025 – tangem.com/en/blog/post/preactivated-wallets/
[18] Tangem Hilfe-Center: Firmware & Echtheit – tangem.com/de/help-center/security/firmware-authenticity/
[19] Ledger Donjon: Laser Fault Injection on the TROPIC01 Open-Source Secure Element, 03.06.2026 – donjon.ledger.com/blog/tropic01-laser-fault-injection/
[20] Tropic Square: TROPIC01 Security Advisory – LFI Vulnerability Disclosure and Mitigation, 03.06.2026 – tropicsquare.com/news-and-events/tropic01-security-advisory-lfi-vulnerability-disclosure-and-mitigation
[21] Tangem Hilfe-Center: Wie die Sicherung funktioniert – tangem.com/de/help-center/security/how-backup-works/
[22] COLDCARD (Coinkite): Current COLDCARD Security Status — laufend aktualisierte Remediation-Übersicht, zuletzt geprüft 04./06.09.2026 – coldcard.com/security/status

HINWEIS ZUR EINORDNUNG

Dieses Whitepaper dient der technischen und forensischen Einordnung von Sicherheitsrisiken bei Hardware Wallets. Die Darstellung dokumentierter Schwachstellen bedeutet nicht, dass sämtliche Geräte eines Herstellers betroffen waren oder aktuell betroffen sind. Sicherheitsarchitekturen, Firmware und Gerätegenerationen verändern sich laufend. Sicherheitsvorfälle müssen deshalb stets hinsichtlich Modell, Firmwareversion, Zeitpunkt und konkretem Angriffsszenario bewertet werden.

ÜBER FINANZ-FORENSIK.DE

David Lüdtke

Geschäftsführer · OSINT-Analyst & Krypto-Forensiker · Finanz Forensik GmbH

finanz-forensik.de unterstützt Geschädigte, Kanzleien und Behörden bei der forensischen Nachverfolgung betrügerisch erlangter Vermögenswerte, insbesondere im Bereich Kryptowährungen und digitaler Zahlungsverkehr — von der Sicherung der Beweismittel über die Blockchain-Analyse bis zur gutachterlichen Aufbereitung. **Kontakt:** postfach@finanz-forensik.de · +49 6057 9189145 · www.finanz-forensik.de

Herausgeber: Finanz Forensik GmbH · Würzburger Str. 59, 63639 Flörsbachtal · HRB 100521, Amtsgericht Hanau · USt-IdNr. DE454473675 · Geschäftsführung: Lydia Bonhard-Lüdtke, David Lüdtke. Fassung 1.2, Stand 19. September 2026. Zitiervorschlag: Finanz-Forensik GmbH, Hardware Wallets im Sicherheitscheck, Fassung 1.2, 2026.