

21 OAKS INSIGHTS

Binance-Hack: Angriff über Bewerbungsgespräche

6,34 Mrd. US-Dollar betroffen: Das schwächste Glied war nicht die Kryptografie

Am 29. Oktober 2026 haben Angreifer Hot Wallets von **Binance** auf mehreren Blockchains geleert. Betroffen waren digitale Vermögenswerte im Wert von rund **6,34 Mrd. US-Dollar**, ein Vielfaches des Bybit-Hacks vom Februar 2025 mit rund 1,5 Mrd. US-Dollar. Nach Angaben des FBI steckt Nordkorea hinter dem Angriff. Den Schaden trägt laut Binance die Börse selbst, nicht ihre Kunden. Am 3. November hat Binance einen ersten Untersuchungsbericht veröffentlicht. Er zeigt: Der Angriff lief in zwei Phasen, monatelange Vorarbeit über einzelne Mitarbeitende, dann knapp vier Stunden Zugriff auf die Wallets.

WHAT'S THE NEWS

1. Monatelange Vorbereitung

- **Juni, manipulierte Installation:** Ein Wallet-DevOps-Ingenieur lud über eine Suchmaschine eine manipulierte Homebrew-Installation, um ein KI-Coding-Tool einzurichten. Binance ersetzte das Gerät, doch Rolle und Team waren den Angreifern damit bekannt.
- **September, falsches Bewerbungsgespräch:** Ein zweiter Ingenieur wurde über eine seriöse Jobplattform zu zwei Interviews eingeladen und sollte eine „Probeaufgabe" auf seinem Arbeitsrechner ausführen. Der Code tauschte unbemerkt ein Entwicklerwerkzeug gegen eine Schadversion aus; der Endpunktschutz erkannte die bis dahin unbekannte Malware nicht.
- **20. Oktober, internes KI-Tool als Sprungbrett:** Über ein internes KI-Werkzeug übernahmen die Angreifer die Rechner zweier Wallet-Ingenieure und fanden ein Zugangstoken für Container-Deployments. Damit starteten sie am 29. Oktober das Skript, das den Signierdienst erreichte.

2. Der Angriff am 29. Oktober

- **Zugriff auf den Signierdienst:** Die Angreifer nutzten einen internen Signierdienst für Wallets, um Transaktionen außerhalb des regulären Auszahlungsprozesses auszulösen.
- **Vier Minuten für XRP:** Zwischen 20:05 und 20:09 UTC schickten fünf Hot Wallets **233,46 Mio. XRP** an die Angreifer. Danach folgten rund 970.500 SOL, 44,2 Mio. OP und 18.270 BTC.
- **EIP-7702 als Hebel:** Mit 50 signierten Transaktionen verschafften die Angreifer einem eigenen Smart Contract Ausführungsrechte über eine Ethereum-Hot-Wallet. Diese Delegation lag on-chain und wirkte weiter, als Binance die Auszahlungen bereits gestoppt hatte.
- **MPC verlängert die Abwehr:** Die Wallet war per Multi-Party Computation gesichert. Es gab daher keinen einzelnen Schlüssel, mit dem sich die Delegation sofort widerrufen ließ. Die letzte Abbuchung über 2.961,9 ETH wurde um 23:56 UTC bestätigt, die Delegation um 00:10 UTC am 30. Oktober gelöscht.

3. Schadensbegrenzung

- **Eingefroren:** Rund **2,85 Mrd. US-Dollar** sind eingefroren oder abgefangen.
- **Ersetzt:** Bis zum 31. Oktober hat Binance **98 %** der abgeflossenen Token ersetzt, nachprüfbar über den Proof of Reserves; weniger liquide Werte kauft die Börse noch nach.
- **Neu aufgebaut:** Betroffene Systeme wurden neu aufgesetzt, Geräte ersetzt und Zugänge widerrufen. Unabhängige Sicherheitsfirmen prüfen den Vorfall.

GOOD TO KNOW

- **Der Mensch ist die Angriffsfläche:** Allein 2026 hat Binance nach eigenen Angaben **57** mutmaßlich nordkoreanische Angriffsversuche abgewehrt: gefälschte Bewerbungsgespräche, präparierte Entwicklerwerkzeuge, falsche Videokonferenz-Apps. Hier reichte ein Treffer.
- **KI-Werkzeuge erweitern das Risiko:** Der Einstieg im Juni und die Ausbreitung im Oktober liefen beide über KI-Tools. Wer Entwicklern solche Werkzeuge gibt, muss sie wie privilegierte Zugänge absichern.
- **On-chain-Rechte überdauern den Notstopp:** EIP-7702 macht Wallets flexibler, schafft aber Berechtigungen, die ein Auszahlungsstopp nicht berührt. Für Verwahrer gehört der Widerruf solcher Delegationen in jeden Notfallplan.
- **Börsenrisiko bleibt Gegenparteirisiko:** Dass Kunden keinen Verlust tragen, liegt an der Kapitalkraft von Binance, nicht an einer Garantie. Ein Guthaben auf einer Börse ist eine Forderung gegen die Börse; Selbstverwahrung oder regulierte Verwahrstellen verteilen dieses Risiko.

Quellen: Binance, „29 October 2026 Binance Security Incident: Initial Findings and Response Update" (3. November 2026, vorläufiger Bericht); FBI, Public Service Announcement zur Zuordnung an Nordkorea (31. Oktober 2026). Die Untersuchung läuft noch, Zahlen können sich mit der Abstimmung der Bestände ändern.

Dieser Beitrag dient ausschließlich der Information und stellt keine Anlageberatung oder Aufforderung zum Kauf oder Verkauf von Wertpapieren dar.

21 Oaks Capital GmbH
Breite Straße 22
40213 Düsseldorf

+49 (0)211 54215240
info@21-oaks.com
www.21-oaks.com

Geschäftsführer: Edgar Heimbach
Amtsgericht Düsseldorf, HRB 98023
USt-Id-Nr.: DE355967929

„21 Oaks Insights" wird herausgegeben von der 21 Oaks Capital GmbH und hat keinerlei konkreten Bezug zu Finanzprodukten der Gesellschaft. Die 21 Oaks Capital GmbH erbringt ihre Dienstleistungen in der Anlagevermittlung von und der Anlageberatung in Finanzinstrumenten im Sinne des § 2 Abs. 2 Nr. 3 und Nr. 4 des Wertpapierinstitutsgesetzes („WpIG") als vertraglich gebundene Vermittlerin ausschließlich für Rechnung und unter der Haftung der AHP Capital Management GmbH, Weißfrauenstraße 12-16, 60311 Frankfurt am Main.