JARXE analysiert die Krypto-Sicherheitslage 2025

Von dem Bybit-Hack bis zu DNS-Hijacks – ein Jahr voller Warnsignale

Von dem Bybit-Hack bis zu DNS-Hijacks – ein Jahr voller Warnsignale

GERMANY, November 28, 2025 /EINPresswire.com/ -- JARXE analysiert die Krypto-Sicherheitslage 2025: Von dem Bybit-Hack bis zu DNS-Hijacks – ein Jahr voller Warnsignale
2025 entwickelt sich für die globale Kryptobranche zu einem Jahr, das die bisherigen Vorstellungen von Sicherheit grundlegend erschüttert hat. Milliardenverluste, ausgefeilte Angriffe und eine wachsende Professionalisierung der Täter zeichnen ein deutliches Bild: Sowohl zentrale Börsen als auch DeFi-Protokolle und Infrastrukturprojekte sind unter zunehmendem Druck geraten.

Das Forschungsteam von JARXE hat die bestätigten Vorfälle des Jahres ausgewertet und liefert eine Einschätzung, wie sich die Sicherheitslandschaft verändert – und warum 2025 als Wendepunkt gelten könnte.

1. Bybit-Hack: 1,4–1,5 Mrd. USD Verlust – der größte Einzelfall der Kryptogeschichte
Im Februar erschütterte ein Angriff auf die zentralisierte Börse Bybit die gesamte Branche. Über kompromittierte Schlüssel oder Schwachstellen im Hot-Wallet-System verschafften sich die Angreifer Zugang zu hochsensiblen Komponenten und entwendeten Vermögenswerte im Wert von rund 1,4 bis 1,5 Milliarden US-Dollar.

Mehrere Analysen deuten auf die nordkoreanische Hackergruppe Lazarus hin – ein Hinweis darauf, dass staatlich unterstützte Akteure weiterhin eine zentrale Rolle in großangelegten Kryptoangriffen spielen.

Nach Einschätzung des JARXE-Forschungsteams zeigt dieser Vorfall, dass selbst global führende Börsen nicht immun sind und Hot-Wallet-Infrastrukturen ein strukturelles Risiko darstellen.

2. Regionale Börsen im Fadenkreuz: Nobitex, BtcTurk und CoinDCX
Neben Bybit gerieten auch mehrere regionale Marktführer unter massiven Beschuss:
* Nobitex (Juni) – rund 90 Mio. USD Schaden; die Angreifer veröffentlichten sogar Teile des Source-Codes und stellten einen politischen Hintergrund heraus.
* BtcTurk (August) – 54 Mio. USD Verlust durch Hot-Wallet-Kompromittierung; bereits der zweite Großangriff innerhalb eines Jahres.
* CoinDCX (Juli) – 44 Mio. USD Schaden infolge eines Servereinbruchs; das Unternehmen sicherte seinen Kunden jedoch vollständige Erstattung zu.

Diese Serie zeigt, dass regionale Börsen zwar große Nutzerzahlen aufweisen, jedoch nicht immer über denselben Sicherheitsapparat verfügen wie globale Marktführer.

3. DeFi bleibt Hochrisikozone: 2025 zeigt erneut die Schwächen komplexer Ökosysteme
(1) Cetus Protocol – 225 Mio. USD Verlust (Mai)
Der bislang größte DeFi-Vorfall des Jahres. Ein raffinierter Angriff auf die Geschäftslogik mehrerer Smart-Contracts auf Sui und Aptos führte zu einer massiven Kapitalverschiebung. Trotz späterer Rückgewinnung eines großen Teils bleibt ein zweistelliger Millionenbetrag verschwunden.

(2) Infini – 50 Mio. USD durch Insider-Manipulation (Februar)
Ein ehemaliger Entwickler nutzte zurückgelassene Sonderrechte im Contract-System – ein seltener, aber äußerst gefährlicher Fall von Insiderbedrohung.

(3) Abracadabra.Money – 13 Mio. USD (März)
Ein Rechenfehler („rounding error“) wurde ausgenutzt, um Kontrollmechanismen zu umgehen. Selbst etablierte Protokolle bleiben somit anfällig für kleine, aber fatale Ungenauigkeiten.

JARXE hebt hervor, dass Smart-Contract-Design, interne Governance-Prüfungen und Orakel-Mechanismen 2025 stärker denn je im Fokus stehen müssen.

4. DNS-Hijacking und Frontend-Manipulationen: Die Rückkehr einer unterschätzten Bedrohung
Mehrere prominente Projekte kämpften 2025 mit Angriffen, die nicht den Code selbst ins Visier nahmen, sondern den Zugang der Nutzer:

* Aerodrome & Velodrome (November): DNS-Umleitungen führten Nutzer auf gefälschte Webseiten, wo sie manipulierte Transaktionen bestätigten.
* Curve Finance (Mai): Erneuter Angriff über ein kompromittiertes Domain-Registry-System.

* Binance (März): Kein finanzieller Schaden an der Börse selbst, aber ein Leak von rund 100.000 Datensätzen löste eine Welle zielgerichteter Phishing-Angriffe aus.

Diese Vorfälle zeigen: Der Angriffspunkt hat sich verschoben – weg vom Protokoll, hin zur Benutzeroberfläche und ihrer Infrastruktur.

5. Sozialtechnische Angriffe eskalieren: Der Fall des Venus-Protokolls
Im September wurde ein Großinvestor beim Venus Protocol Opfer eines perfiden Plans: Ein gefälschtes Zoom-Meeting, Malware-Platzierung über Bildschirmfreigabe, anschließender Privatkey-Diebstahl – Schaden rund 13 Mio. USD.

Dieser Fall verdeutlicht, dass Sicherheitslücken längst nicht mehr nur im Code liegen, sondern oft in menschlichen Prozessen.

6. JARXE: Sicherheit wird zum zentralen Wettbewerbsfaktor der Branche
Das Forschungsteam von JARXE sieht in den Ereignissen des Jahres mehrere übergeordnete Trends:
(1) Hot-Wallet-Management wird regulatorisch neu bewertet – Vorfälle wie bei Bybit und BtcTurk verschieben den Fokus auf strengere operative Standards.
(2) MPC-Wallets und Cold-Storage-Strategien werden zur Branchenbasis – um Single-Key-Risiken zu minimieren.
(3) Transparenz durch On-Chain-Proofs (PoR) gewinnt an Bedeutung – Nutzer verlangen nachvollziehbare Sicherheiten.
(4) Frontend-Sicherheit rückt ins Zentrum – DNS-Hijacks werden 2025 zu einer der häufigsten Angriffsmethoden.
(5) Interne Risiken werden neu priorisiert – Infini zeigt: Governance und Audit-Prozesse sind Teil der Sicherheitsarchitektur.

7. 2025 markiert einen Wendepunkt
Die enorme Zahl und Professionalität der Angriffe setzt neue Maßstäbe. Der Wettbewerb der Plattformen verschiebt sich sichtbar: von Liquidität und Produktvielfalt hin zu Sicherheit, Transparenz und operativer Resilienz.

Wie JARXE in seinem Fazit schreibt:
„Die Zukunft des Marktes entscheidet sich nicht an der nächsten Trendwelle, sondern an der Fähigkeit, Sicherheit als Fundament des gesamten Ökosystems zu verstehen."

Eric Foo
Exabytes
email us here