expertenReport

Quelle: Redaktion experten.de / KI-generiert

Rekord-Hack bei Binance: Wenn die Verwahrung zum Risiko wird

Michael Fiedler

Bei der Kryptobörse Binance wurden digitale Vermögenswerte im Milliardenwert gestohlen. Das FBI macht nordkoreanische Hacker verantwortlich, ein Teil der Beute konnte eingefroren werden. Der Vorfall zeigt, welche Risiken entstehen, wenn Anleger ihre Kryptowährungen zentralen Plattformen anvertrauen. Auch die wachsende Bedeutung künstlicher Intelligenz für die Cybersicherheit rückt in den Fokus.

Milliarden aus Binance-Wallets abgezogen

Nach Angaben von Elliptic wurden innerhalb weniger Stunden Kryptowährungen aus sogenannten Hot Wallets von Binance über elf verschiedene Blockchains abgezogen. Hot Wallets sind mit dem Internet verbundene digitale Geldbörsen, die Handelsplattformen für laufende Transaktionen benötigen. Binance hatte zunächst erklärt, dass möglicherweise der kompromittierte Laptop eines Mitarbeiters aus dem technischen Betrieb den Angriff ermöglicht habe. Später berichtete das Unternehmen von weiteren identifizierten Einfallstoren. Die Untersuchung ist noch nicht abgeschlossen. Nach bisherigen Angaben gibt es keine Hinweise darauf, dass private Schlüssel der betroffenen Wallets offengelegt wurden. Das schließt andere Formen unberechtigter Zugriffe auf Transaktionssysteme jedoch nicht aus. Elliptic beziffert die bislang eingefrorenen oder sichergestellten Vermögenswerte auf rund 2,85 Milliarden Dollar. Das entspricht etwa 44 Prozent der gesamten Beute. Die übrigen Werte werden teilweise über verschiedene Kryptowährungen und Netzwerke bewegt.

Binance will Kundenverluste ausgleichen

Binance hat zugesagt, die finanziellen Auswirkungen des Angriffs für seine Kunden aufzufangen. Nach Angaben des Unternehmens wurden bis zum Wochenende bereits Vermögenswerte im Gegenwert von rund 5,7 Milliarden Dollar wiederbeschafft beziehungsweise aus eigenen Mitteln ersetzt. Das entspricht etwa 90 Prozent des ursprünglich bezifferten Schadens. Auch den verbleibenden Betrag will Binance ausgleichen. Die Kryptobörse hatte Ein- und Auszahlungen nach Bekanntwerden des Vorfalls vorübergehend ausgesetzt. Seit dem 1. November werden Auszahlungen schrittweise wieder ermöglicht. Die finanziellen Folgen für das Unternehmen und die abschließende Schadenhöhe lassen sich derzeit noch nicht sicher beurteilen.

Julius Bär: Nicht die Blockchain, sondern die Verwahrung ist entscheidend

Für Carsten Menke, Head Next Generation Research bei Julius Bär, liegt die zentrale Erkenntnis des Angriffs in der Unterscheidung zwischen der Sicherheit einer Blockchain und der Sicherheit eines Unternehmens, das Kryptowährungen für Kunden verwahrt. Wer digitale Vermögenswerte auf einer zentralisierten Handelsplattform hält, überträgt die Kontrolle über deren Verwahrung an einen Dritten. Dadurch entstehen zusätzliche operative Risiken – etwa durch kompromittierte Zugänge, fehlerhafte interne Prozesse oder Sicherheitslücken in der technischen Infrastruktur. Der Angriff auf Binance zeigt, dass auch große Handelsplattformen mit umfangreichen Sicherheitsmaßnahmen nicht vor solchen Vorfällen geschützt sind. Als Alternative verweist Menke auf die eigenständige Verwahrung digitaler Vermögenswerte, die sogenannte Self-Custody. Insbesondere Hardware-Wallets mit offline gespeicherten privaten Schlüsseln können bestimmte Risiken zentralisierter Plattformen reduzieren. Allerdings verlagert sich damit die Verantwortung auf die Anleger selbst. Wer den Zugang zu seiner privaten Wallet verliert oder seine Schlüssel nicht ausreichend schützt, kann ebenfalls erhebliche Verluste erleiden.

Welche Rolle spielt künstliche Intelligenz?

Ob beim Angriff auf Binance künstliche Intelligenz eingesetzt wurde, ist bislang nicht belegt. Unabhängig vom konkreten Vorfall sieht Julius Bär jedoch eine wachsende Herausforderung durch KI-gestützte Cyberangriffe. Automatisierte Werkzeuge können Angreifern helfen, Schwachstellen schneller zu identifizieren, Angriffe vorzubereiten und technische Abläufe zu beschleunigen. Gleichzeitig entstehen durch den zunehmenden Einsatz autonomer KI-Agenten neue Sicherheitsfragen. Wenn solche Systeme eigenständig auf sensible Daten, Anwendungen oder Transaktionsprozesse zugreifen können, müssen Unternehmen auch die Berechtigungen und Handlungsmöglichkeiten dieser Agenten absichern. Für Finanzdienstleister bedeutet dies, dass klassische Schutzmaßnahmen allein nicht mehr ausreichen dürften. Gefragt sind unter anderem eine kontinuierliche Überwachung der Systeme, ein wirksames Berechtigungsmanagement und die schnelle Erkennung verdächtiger Aktivitäten. Auch automatisierte Sicherheitsprüfungen und zeitnahe Softwareaktualisierungen gewinnen an Bedeutung.

Cybersicherheit wird zum strategischen Risiko

Der Binance-Angriff verdeutlicht, dass Sicherheitsvorfälle bei digitalen Vermögenswerten weit über den unmittelbaren finanziellen Schaden hinausreichen können. Handelsunterbrechungen, gesperrte Auszahlungen, Vertrauensverluste und hohe Kosten für die Wiederherstellung betroffener Systeme können die wirtschaftlichen Folgen erheblich vergrößern. Julius Bär sieht deshalb weiterhin langfristige Wachstumschancen für Unternehmen aus dem Bereich Cybersicherheit. Die zunehmende Digitalisierung von Finanzdienstleistungen und der Einsatz künstlicher Intelligenz erhöhen nach Einschätzung der Privatbank den Bedarf an spezialisierten Schutzmaßnahmen. Für Anleger bleibt die Unterscheidung entscheidend: Die Sicherheit einer Kryptowährung hängt nicht allein von ihrer Blockchain ab. Ebenso wichtig ist, wie und von wem die digitalen Vermögenswerte verwahrt werden.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4952775/Rekord-Hack-bei-Binance-Wenn-die-Verwahrung-zum-Risiko-wird/