KRYPTO NEWS
PART OF THE GLOBAL WOM NEWS NETWORK

29. Juni 2022

Kettenübergreifende Brückendiebstähle übersteigen 2022 die 1-Milliarde-Dollar-Marke

Nur wenige DeFi-Unternehmen beschäftigen engagiertes Sicherheitspersonal Branchenexperten glauben, dass Brücken mit zunehmender Reife von DeFi sicherer werden Mit zunehmender Investition in Kryptowährung steigt auch der Anreiz für kriminelle Akteure, den DeFi-Raum (dezentralisierte Finanzen) auszunutzen. Kettenübergreifende Bridge-Hacks waren im Jahr 2022 die Waffe der Wahl für Kryptodiebe. Bridge-Hacks haben in diesem Jahr mehr als eine Milliarde Dollar an gestohlenen Geldern ausgemacht, so Untersuchungen des Blockchain-Analyse- und Compliance-Unternehmens Elliptic. Cross-Chain-Bridges ermöglichen das Verschieben von Assets zwischen verschiedenen Blockchain-Protokollen, was bedeutet, dass die Netzwerke eine große Konzentration von Krypto-Assets enthalten. Die jüngste Reihe von Bridge-Angriffen hat einige Branchenführer dazu veranlasst, sich zu fragen, …

- Nur wenige DeFi-Unternehmen beschäftigen engagiertes Sicherheitspersonal
- Branchenexperten glauben, dass Brücken mit zunehmender Reife von DeFi sicherer werden

Mit zunehmender Investition in Kryptowährung steigt auch der Anreiz für kriminelle Akteure, den DeFi-Raum (dezentralisierte Finanzen) auszunutzen. Kettenübergreifende Bridge-Hacks waren im Jahr 2022 die Waffe der Wahl für Kryptodiebe. Bridge-Hacks haben in diesem Jahr mehr als eine Milliarde Dollar an gestohlenen Geldern ausgemacht, so Untersuchungen des Blockchain-Analyse- und Compliance-Unternehmens Elliptic.

Cross-Chain-Bridges ermöglichen das Verschieben von Assets zwischen verschiedenen Blockchain-Protokollen, was bedeutet, dass die Netzwerke eine große Konzentration von Krypto-Assets enthalten. Die jüngste Reihe von Bridge-Angriffen hat einige Branchenführer dazu veranlasst, sich zu fragen, ob die Vorteile von Bridges ihre Risiken überwiegen. Ein Top-Analyst bei Elliptic glaubt, dass Bridge-Hacks nur wachsende Schmerzen sind, die DeFi schließlich überwinden wird.

Harmony, Sky Mavis und Wormhole erlitten in diesem Jahr alle Blockchain-Exploits von über 100 Millionen US-Dollar. Mudit Gupta, Chief Information Security Officer bei Polygon, glaubt, dass Brückenunsicherheit ein branchenweites Problem ist.

„Die meisten Hacks passieren, weil Unternehmen keine geeigneten Sicherheitsexperten haben und nicht wissen, was sie selbst tun sollen", sagte Gupta in einer Twitter-DM. „Es gibt nur sehr wenige DeFi-Unternehmen mit [dedicated] Sicherheitspersonal."

DeFi-Protokolle haben sich in den letzten sechs Jahren rasant verbreitet, aber die Sicherheitsinfrastruktur hat nicht mit der Industrie mit einem Volumen von mittlerweile über 900 Milliarden US-Dollar Schritt gehalten. Aus diesem Grund sind Hacks in dreistelliger Millionenhöhe nicht verwunderlich.

Am 1. April twitterte ein Händler seine Befürchtung, dass ein großer Harmony Horizon Bridge-Exploit nur erfordern würde, dass ein Hacker zwei der fünf Validierungsschlüssel des Protokolls erhält. Im Juni trat genau dieses Szenario ein ج und Harmony wurde für 100 Millionen Dollar geplündert.

> Da Bridges & Bridge Hacks das aktuelle Narrative Du Jour sind, wollte ich etwas über die Harmony Bridge auf Ethereum graben, die Token im Wert von ~330 Millionen Dollar sichert.
>
> ج Ape Dev (@_apedev) 1. April 2022

Vitalik Buterin, Mitbegründer von Ethereum, glaubt, dass Cross-Chain-Brücken von Natur aus anfällig für Sicherheitsverletzungen sind.

ذDie grundlegenden Sicherheitsgrenzen von Bridges sind eigentlich ein Hauptgrund, warum ر ich pessimistisch bin, was Cross-Chain-Anwendungen angehتذ, schrieb Buterin in einem langen Reddit-Beitrag vom Januar. Der einflussreiche Gründer brachte weiter seine Überzeugung zum Ausdruck, dass Vermögenswerte im selben Blockchain-Ökosystem gehalten werden sollten, anstatt zwischen Ketten gemischt zu werden.

Tara Annison, Head of Technical Crypto Advisory beim Krypto-Forschungsunternehmen Elliptic, ist anderer Meinung.

ȝWir werden nicht in einer Single-Chain-Welt lebenȝ, sagte Annison. Es wird immer notwendig sein, Assets zwischen Blockchains zu verschieben, daher sollten ȝwir Bridges nicht im Allgemeinen als schlecht charakterisieren, nur weil einige gehackt wurdenȝ.

Annison glaubt, dass Bridge-Hacks durch die Wertkonzentration innerhalb von Cross-Chain-Bridges verursacht werden, nicht durch die Bridges selbst.

> ȝWenn Sie an Kriege denken, versuchen Sie, Brücken zu bombardieren, um den Transport von Waren und Dienstleistungen zu stoppenȝ, sagte Annison. Die jüngsten Cross-Chain-Bridge-Hacks finden nicht statt, ȝweil Bridges von Natur aus eine schwache Infrastruktur sind, sondern weil sie eine Konzentration von Wert habenȝ.

Annison glaubt, dass alle Krypto-Assets mit Risiken verbunden sind, und Bridges sind nach Stablecoins im Mai und NFTs davor nur das Risiko ȝGeschmack des Monatsȝ. Brücken sollten sicherer werden, wenn Protokolle technologisch ausgereifter werden.

Es bleibt abzuwarten, ob die Marktteilnehmer zustimmen.

Die Ronin Bridge von Sky Mavis, die im April für 625 Millionen Dollar kompromittiert wurde, wurde heute Morgen wiedereröffnet. Laut Messari haben Vermögenswerte in Höhe von fast 9 Millionen US-Dollar die Kette bereits verlassen.

. .

Der Post Cross-Chain Bridge Thefts Top $1B in 2022 ist keine finanzielle Beratung.

Details

Besuchen Sie uns auf: krypto-news.at