NACHRICHTEN Österreich
25. Juli 2025

Arizona-Frau verurteilt für nordkoreanisches Tech-Arbeitsprogramm

Eine Frau aus Arizona wurde zu über 8 Jahren Haft verurteilt, nachdem sie ein Betrugsnetzwerk geleitet hatte, um nordkoreanischen IT-Arbeitern zu helfen, sich als Amerikaner auszugeben und Jobs in den USA zu erhalten.

Eine Frau aus Arizona wurde am Donnerstag zu mehr als 8 Jahren Gefängnis verurteilt, weil sie ein komplexes Betrugssystem orchestrierte, um nordkoreanischen Cyber-Operativen zu helfen, sich als Amerikaner auszugeben und remote IT-Jobs bei hunderten von US-Unternehmen, darunter Fortune-500-Unternehmen, zu erhalten.

Die Dimension des Betrugsplans

Der Plan, den das Justizministerium als eines der größten Betrugsprogramme nordkoreanischer IT-Arbeiter beschreibt, nutzte die gestohlenen Identitäten von 68 Amerikanern. Über

300 US-Unternehmen wurden betrogen, und es wurden Einnahmen von mehr als 17 Millionen US-Dollar generiert – Gelder, die dem atomwaffenbesitzenden nordkoreanischen Regime zugutekommen könnten, wie das Ministerium in einer **Mitteilung** erklärte.

Die Rolle von Christina Chapman

Christina Chapman, 50, bekannte sich im Februar schuldig, nachdem sie beschuldigt wurde, von ihrem Zuhause aus eine „Laptop-Farm“ betrieben zu haben. Dort „erhielt und hostete“ sie von Unternehmen ausgegebene Computer im Auftrag ausländischer IT-Arbeiter, um die Firmen davon zu überzeugen, dass die Arbeiter in den USA lebten.

Sie wurde mit neun Anklagepunkten belastet, darunter Verschwörung zur Begehung von Betrug und schwerer Identitätsdiebstahl.

Globale Implikationen und Vorgehensweisen

In der Mitteilung des DOJ wurde erwähnt, dass Nordkorea weltweit Tausende hochqualifizierter IT-Arbeiter eingesetzt hat, auch in den USA, um Kontrollen, die von US-Unternehmen zur Verhinderung illegaler Einstellungen eingesetzt werden, zu umgehen, indem sie die Hilfe von US-basierten Komplizen in Anspruch nehmen.

Chapman verschickte 49 Laptops und andere Geräte an verschiedene Standorte im Ausland, darunter eine Stadt in China nahe der nordkoreanischen Grenze. Bei einer Durchsuchung ihres Hauses im Oktober 2023 wurden mehr als 90 Laptops gefunden.

Finanzielle Strukturen und Auswirkungen

Chapman erhielt und fälschte auch Gehaltsunterlagen, wobei sie gestohlene Identitäten verwendete. Gelder wurden auf ihre persönlichen Konten in den USA eingezahlt und dann an Personen im Ausland überwiesen.

Zu den von dem Betrugsplan betroffenen Unternehmen gehören Fortune-500-Unternehmen, ein nationales Fernsehnetzwerk, ein Luft- und Raumfahrtunternehmen, ein amerikanischer Autohersteller und ein Luxus-Einzelhändler, wie in der Anklageschrift vom Mai **vermerkt**, ohne die Unternehmen namentlich zu nennen.

Warnungen vor weiteren Betrugsversuchen

Beamte berichteten, dass ausländische IT-Arbeiter erfolglos versuchten, Anstellungen bei zwei US-Regierungsbehörden zu erhalten. Das Staatsministerium und andere Behörden gaben 2022 eine **Warnung** zu Programmen heraus, in denen nordkoreanische IT-Arbeiter, die vorgaben, andere Nationalitäten zu haben, anboten, remote zu arbeiten und sich um Stellen in den Bereichen elektronische Spiele, IT-Support und künstliche Intelligenz zu bewerben.

Zusammenhang mit nordkoreanischen Hackergruppen

Einige dieser IT-Arbeiter arbeiten eng mit nordkoreanischen Hackern zusammen, die ebenfalls eine bedeutende Einnahmequelle für das Regime darstellen, so Experten, die mit CNN sprachen. Etwa die Hälfte von **Nordkoreas** Raketenprogramm wurde durch Cyberangriffe und Kryptowährungsdiebstahl finanziert, wie ein Beamter des Weißen Hauses **2024** mitteilte.

„Indem Nordkorea seine IT-Arbeiter anweist, bei westlichen Unternehmen eine Anstellung zu suchen, hat das Regime sein technisches Talent als Waffe eingesetzt und eine ultimative

Insider-Bedrohung geschaffen“, sagte Michael Barnhart, ein Nordkorea-Spezialist bei dem Google-eigenen Cybersicherheitsunternehmen Mandiant, 2024 im Gespräch mit CNN. „Diese Operativen umgehen Sanktionen, indem sie ihre Gehälter umleiten, um Nordkoreas Atomprogramm zu finanzieren. Gleichzeitig verschaffen sie Nordkoreas fortgeschritteneren Bedrohungsgruppen Zugang zu großen Organisationen“, so Barnhart weiter.

Details