NACHRICHTEN
Österreich
31. Mai 2025

Hacker-Trick: Deepfake-Angriff auf Trumps Stabschefin Wiles enthüllt!

US-Präsident Trump reagiert gelassen auf einen Hackerangriff auf sein Stabschefin Handy; Deepfake-Technologie könnte beteiligt sein.

Washington, D.C., USA - Eine alarmierende Cyberattacke hat das Handy von Susie Wiles, der Stabschefin von US-Präsident Donald Trump, ins Visier genommen. Während Trump sich gelassen zu den Hack-Berichten äußert und versichert, dass es „nur eine Susie“ gebe, wirft der Vorfall jedoch Fragen zur Cybersicherheit auf. Wiles informierte ihre Mitarbeiter über gehackte Kontakte auf ihrem privaten Gerät, während offizielle Kommunikationskanäle unberührt bleiben. Laut dem **Wall Street Journal** untersuchen Bundesbehörden den Fall eingehend.

Bei bereits eingeleiteten Ermittlungen wird vermutet, dass in dem Vorfall künstliche Intelligenz eingesetzt wurde, um die

Stimme von Wiles nachzuahmen. „Jemand hat versucht, sich als Wiles auszugeben“, erläuterte Trump, beschrieb sie jedoch als „wunderbare Frau“, die gut mit der Lage umgehen könne. Der Vorfall könnte Teil eines Phishing-Angriffs sein, bei dem nicht nur Wiles, sondern auch andere prominente Republikaner und Führungspersönlichkeiten getäuscht wurden. Dabei wurden hochrangige Zielpersonen kontaktiert, was auf eine potenziell weitreichende Cyberbedrohung hindeutet.

Die Rolle von Deepfake-Technologie

Die Methode der Angreifer setzt auf Deepfake-Technologie, die zunehmend im Untergrund von Cyberkriminellen genutzt wird. Diese Technologie ermöglicht es, Stimmen und Gesichter künstlich zu erzeugen und täuschend echte Inhalte zu erstellen. Laut Sicherheitsforschern ist dies eine wachsende Bedrohung, die politische und wirtschaftliche Strukturen destabilisieren könnte. Experten warnen, dass moderne Cyberangriffe schwerer zu erkennen und zu verhindern sind, da sie oft auf einem Mix aus Social Engineering und hochentwickelten Algorithmen beruhen, die durch maschinelles Lernen unterstützt werden.

Deepfakes, wie sie im Angriff auf Wiles zum Einsatz kamen, können für Identitätsdiebstahl und andere kriminelle Handlungen genutzt werden. In einem weiteren bemerkenswerten Vorfall half eine Deepfake-Stimme dabei, in Hongkong, Millionenbeträge von bankgeschäften zu transfersieren. Die Risiken dieser Technologie sind nicht zu unterschätzen, insbesondere in einer Zeit, in der sie weiterhin an Verbreitung gewinnt.

Notwendige Sicherheitsmaßnahmen

Um solchen Angriffe vorzubeugen, müssen Unternehmen und Regierungen ihre Sicherheitsstrategien überdenken. Experten empfehlen die Nutzung sicherer Kommunikationsplattformen wie Signal zur Identitätsverifizierung. Weitere Maßnahmen sind der Einsatz fortschrittlicher KI-/ML-Lösungen zur Erkennung von

Deepfakes sowie Authentifizierungsmethoden wie Blockchain und Zwei-Faktor-Authentifizierung (2FA).

Des Weiteren ist es entscheidend, Mitarbeiter über aktuelle Cybersecurity-Praktiken zu schulen und für die Gefahren von Deepfakes zu sensibilisieren. In Anbetracht der Zunahme von Cyberangriffen, die laut Check Point Research 2021 um 50% im Vergleich zum Vorjahr angestiegen sind, stehen Unternehmen vor der Herausforderung, ihre Sicherheitsprotokolle kontinuierlich anzupassen und zu optimieren.

Die Vorfälle rund um Susie Wiles zeigen nicht nur die Verletzlichkeit von Regierungsbeamten, sondern verdeutlichen auch die dringende Notwendigkeit, sich gegen die wachsende Bedrohung durch Cyberangriffe zu wappnen.

Details	
Vorfall	Cyberkriminalität
Ursache	Phishing-Angriff, Hacking
Ort	Washington, D.C., USA
Quellen	• **www.oe24.at** • **www.it-boltwise.de** • **cybersecurity-magazine.com**