NACHRICHTEN AG

06. Mai 2025

Hackerangriff auf US-App: Sicherheit von Daten in Gefahr!

Hackerangriffe auf die Messenger-App TM SGNL zwingen Betreiber zur Abschaltung. Sensible Daten könnten erbeutet worden sein.

USA - Die Anwendung „TM SGNL“, ein Klon des etablierten Signal-Messengers, wurde jüngst durch zwei Hackerangriffe schwer getroffen, was dazu führte, dass die Betreiber die App vorübergehend abgeschaltet haben. Bereits in der Vergangenheit hatte die App Beachtung gefunden, als sie von US-Beamten, einschließlich Mike Waltz, einem ehemaligen Sicherheitsberater von Donald Trump, genutzt wurde. Die Hacker konnten Berichten zufolge sensible Informationen erbeuten, darunter archivierte Daten aus Einzel- und Gruppenchats, was die Sicherheit der Nutzerdaten stark gefährdet.

Die App „TM SGNL“ wird von der israelischen Firma

Telemessage entwickelt, die sich auf die Archivierung von Nachrichten aus verschiedenen Plattformen wie Signal, WhatsApp und Telegram spezialisiert hat. Der Dienst richtet sich insbesondere an Unternehmen und staatliche Stellen, was die ernsten Sicherheitsrisiken noch verstärkt. Der Mutterkonzern Smarsh beschreibt die Vorfälle als „potenziellen Sicherheitsvorfall“ und hat eine Untersuchung durch eine externe Cybersicherheitsfirma eingeleitet, um die Hintergründe der Angriffe zu klären. Diese Enthüllungen erfolgten kurz nach Waltz‘ Degradierung am 1. Mai, als er aufgrund eines Kommunikationsskandals, bei dem er versehentlich den Chefredakteur der Zeitschrift „The Atlantic“ in eine geheime Signal-Gruppe einlud, unter Druck geriet.

Ein Sicherheitsvorfall mit weitreichenden Folgen

Die Sicherheitslage rund um „TM SGNL“ wirft erneut Fragen über die Verwundbarkeit von Kommunikationsdiensten auf. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtet ständig über aktuelle Entwicklungen und Risiken in der Cyberwelt. Die Vorfälle rund um „TM SGNL“ sind ein weiteres Beispiel für die Bedrohungen, denen digitale Dienste ausgesetzt sind, und verdeutlichen die Notwendigkeit, Cybersicherheitsmaßnahmen konsequent zu verbessern. Informationen zu akuten IT-Sicherheitsvorfällen können über die Plattform des BSI gemeldet werden.

Der BSI-Lagebericht zur IT-Sicherheit in Deutschland befasst sich darüber hinaus mit verschiedenen Methodologien der Cyberkriminalität, wie etwa Schadsoftware Emotet, digitalem Identitätsdiebstahl und Phishing-Angriffen. Der Newsletter „Einfach • Cybersicher“ bietet monatliche Updates zu solchen Themen sowie praktisches Wissen für eine bessere Cyber-Sicherheit.

Die Sicherheitslücken bei „TM SGNL“ sind nicht nur für die Nutzer der App alarmierend, sondern werfen auch ein Licht auf

die Herausforderungen, denen sich Sicherheitsbehörden und Unternehmen in der digitalen Kommunikation gegenübersehen. Die Untersuchung durch die externe Cybersicherheitsfirma könnte entscheidende Erkenntnisse liefern, wie ähnliche Vorfälle in der Zukunft vermieden werden können.

Für weitere Informationen zu Cybersicherheit und aktuellen Bedrohungen besuchen Sie bitte **BSI**, **CSO** sowie **T-Online**.

Details	
Vorfall	Cyberkriminalität
Ort	USA
Quellen	• **www.t-online.de** • **www.csoonline.com** • **www.bsi.bund.de**