Iranischer Cyberangriff auf EU-Abgeordnete: Neumann schlägt Alarm!

Das EU-Parlament bestätigt einen iranischen Spionageangriff auf Abgeordnete Neumann, der mit Menschenrechtsarbeit in Verbindung steht.

Köln, Deutschland - Das Europäische Parlament hat einen iranischen Spionageangriff auf die deutsche Europaabgeordnete Hannah Neumann bestätigt. Der Cyberangriff auf Neumanns Büro zeigt deutliche Ähnlichkeiten zu Techniken, die von iranischen, staatlich unterstützten Cyber-Spionagegruppen genutzt werden. Ziel dieser Attacke war vermutlich die Informationsgewinnung, was Neumann veranlasst, den Verdacht zu äußern, dass der Angriff mit ihrem Engagement für Menschenrechte und Demokratie im Iran zusammenhängt. Die Täter scheinen mit der Hackergruppe „Charming Kitten“ in Verbindung zu stehen, die mutmaßlich im Auftrag der iranischen Revolutionsgarden agiert. Neumann, die aktuell die Delegation für die Beziehungen des Parlaments zu Iran leitet, hat sich

zudem für die Einstufung der Revolutionsgarden als Terrororganisation ausgesprochen.

Über einen Zeitraum von mehreren Wochen kontaktierte die Hackergruppe Neumanns Büro unter falscher Identität und versuchte, Spionagesoftware über einen Link zu installieren. Glücklicherweise verhinderte das Abwehrsystem der IT des Parlaments, dass Informationen ausgespäht wurden. Der Vorfall wurde von Neumann gemeldet, nachdem der deutsche Verfassungsschutz sie über einen möglichen Angriff informiert hatte. In der Folge alarmierte sie das Parlament, das umgehend eigene Nachforschungen einleitete. Parlamentspräsidentin Roberta Metsola verurteilte diesen Angriff entschieden und forderte erhöhte Wachsamkeit seitens der Sicherheitsdienste des Parlaments.

Anhaltende Bedrohungen durch iranische Hacker

Das Bundesamt für Verfassungsschutz (BfV) in Deutschland warnt bereits seit Ende 2022 vor einer Zunahme von Cyberangriffen auf iranische Dissidenten und Organisationen. Die Angriffe richten sich häufig gegen Journalisten, Anwälte und Menschenrechtsaktivisten, und die Gruppe hinter diesen Attacken, bekannt unter Namen wie Charming Kitten, APT35, Mint Sandstorm, TA453 und Yellow Garuda, zeigt Fortschritte in ihren Methoden. Diese Gruppe nutzt ausgeklügelte Social Engineering-Techniken, um Vertrauen durch gefälschte Online-Identitäten aufzubauen.

Im jüngsten Vorfall wurde der iranische Umweltexperte Mansour Sohrabi in Köln Ziel eines ähnlichen Angriffs. Er erhielt ein vermeintliches Jobangebot über Instagram und wurde zu einem Vorstellungsgespräch über Messaging-Dienste eingeladen. Während des Gesprächs klickte er auf einen Link, was zur Kompromittierung seines Computers führte. Die Angreifer hinterließen oft Spuren, darunter IP-Adressen aus dem Iran, und werden verdächtigt, in etwa 40 ähnlichen Angriffen in den

letzten Jahren beteiligt gewesen zu sein.

Die Vorfälle verdeutlichen die anhaltende Bedrohung durch iranische Hacker, die auch international operieren. Die Sicherheitsanalysten, wie Mike Hart von Mandiant, bestätigen, dass die Aktivitäten von Charming Kitten stark mit der iranischen Revolutionsgarde verknüpft sind. Angesichts der Gefahren führt das BfV nun verstärkte Sicherheitsmaßnahmen ein, um die Ziele vor weiteren Angriffen zu schützen.

Diese jüngsten Entwicklungen werfen Fragen hinsichtlich der Sicherheit von Abgeordneten und der Notwendigkeit gezielter Maßnahmen zum Schutz von Menschenrechtsaktivisten und anderen potenziellen Opfern von Cyberangriffen auf. Das Europäische Parlament selbst hat im Zusammenhang mit den Angriffen darauf hingewiesen, dass die Gefahren durch solche Hackergruppen ernst genommen werden müssen.

Weitere Informationen zu diesen Vorfällen und zu den Methoden von Charming Kitten finden sich in den Artikeln von **sueddeutsche.de**, **thehackernews.com** und **tagesschau.de**.

Details	
Vorfall	Cyberkriminalität
Ursache	Spionage
Ort	Köln, Deutschland
Quellen	• **www.sueddeutsche.de** • **thehackernews.com** • **www.tagesschau.de**