NACHRICHTEN AG

20. August 2024

# Iranische Hacker zielen auf Wahlkampfmitarbeiter in den USA

Iranische Hackergruppe APT42 versucht, E-Mail-Accounts US-amerikanischer Wahlkampfteams zu kompromittieren. Experten warnen.

In einem alarmierenden Vorfall hat sich herausgestellt, dass eine Hackergruppe, die mit den iranischen Revolutionsgarden in Verbindung steht, einen gezielten Cyberangriff auf Wahlkampfteams in den USA unternommen hat. Diese Gruppe, bekannt als APT42, hat offensichtlich versucht, sich Zugriff auf die E-Mail-Konten von hochrangigen Mitarbeitern sowohl der Demokratischen Partei als auch des republikanischen Kandidaten Donald Trump zu verschaffen.

Die Offenbarung über diesen Angriff ist nicht nur besorgniserregend, weil sie die Integrität der Wahlkampagnen bedroht, sondern auch wegen der geopolitischen Implikationen, die damit einhergehen. Die iranischen Revolutionsgarden sind eine entscheidende militärische Institution im Iran, die für ihre aggressiven und oft geheimen Operationen bekannt ist. Die Tatsache, dass sie sich in die inneren Angelegenheiten eines anderen Landes einmischen, wirft ernsthafte Fragen auf.

## Details des Angriffs

Nach Informationen von Google, das ebenfalls ihre Erkenntnisse zur Cyberbedrohung veröffentlicht hat, fanden die Cyberangriffe zwischen Mai und Juni statt. Dabei wurden die persönlichen E-Mails von rund einem Dutzend hochrangiger Wahlkampfmitarbeiter ins Visier genommen. Zu dieser Zeit

wurde Joe Biden als der wahrscheinlichste Präsidentschaftskandidat der Demokraten betrachtet. Seit seinem Rückzug steht jedoch Vizepräsidentin Kamala Harris auf der Liste der Kandidaten, die gegen Trump antreten.

Dies offenbart die potenziellen Sicherheitsrisiken, mit denen Politiker und ihre Teams heutzutage konfrontiert sind. Mithilfe solcher Angriffe könnten ausländische Akteure wertvolle Informationen gewinnen, die sie möglicherweise für strategische Manipulationen während des Wahlprozesses nutzen könnten.

Die Einschätzung von Google macht deutlich, dass Cyberangriffe, die von Staaten ausgehen, zunehmend an Komplexität und Zielgenauigkeit gewinnen. APT42 und ähnliche Gruppen zählen zur neuen Generation von Bedrohungen, die nicht nur technisches Wissen besitzen, sondern auch strategisch handeln, um politische Ziele zu erreichen.

Die Behörden in den USA müssen sich diesen Herausforderungen stellen und sicherstellen, dass geeignete Maßnahmen zum Schutz der Wahlkampfteams getroffen werden. Da die Präsidentschaftswahl 2024 vor der Tür steht, ist es entscheidend, dass sich die politischen Parteien der Bedrohungen bewusst sind und proaktive Schritte unternehmen.

## Relevanz der Vorfälle

Die Vorfälle sind nicht nur technische Herausforderungen, sondern auch dringend zu lösende sicherheitspolitische Aufgaben. Cyberangriffe von ausländischen Akteuren stellen eine direkte Bedrohung der nationalen Sicherheit dar. Es ist wichtig, die Öffentlichkeit über diese Bedrohungen zu informieren und gleichzeitig die notwendigen Sicherheitsvorkehrungen zu fördern.

Zusätzlich muss die Reaktion auf solche Angriffe koordiniert werden, um Informationen und Ressourcen zwischen den verschiedenen politischen und sicherheitspolitischen

Institutionen zu bündeln. Die Frage, wie die USA auf Cyberangriffe reagieren können, ist komplex und erfordert eine umfassende Strategie.

Die Hacker von APT42 erweisen sich als ernstzunehmende Akteure im globalen Cyberkriegsfeld. Daher müssen sowohl Unternehmen als auch Regierungen zusammenarbeiten, um sicherzustellen, dass ihre digitalen Plattformen und Informationen geschützt sind. Die Notwendigkeit, in Cybersicherheit zu investieren und technologische Innovationen voranzutreiben, ist dringlicher denn je.

In Anbetracht der geopolitischen Spannungen und der bevorstehenden Wahlen wird sich die Überwachung und Absicherung der Wahlkampfteams als eine der wichtigsten Aufgaben für die US-Regierung erweisen müssen. Die Bedrohung durch Cyberangriffe ist eine Realität, mit der sich alle Beteiligten auseinandersetzen müssen, um die zukünftige Integrität demokratischer Prozesse zu gewährleisten.

## Kontext der Cyberangriffe

Die Cyberangriffe, die von der Hackergruppe APT42 ausgeführt wurden, sind Teil eines breiteren Trends, bei dem ausländische Akteure versuchen, Einfluss auf politische Prozesse in den USA zu nehmen. Solche Aktivitäten sind in der Vergangenheit immer wieder dokumentiert worden, insbesondere während der Präsidentschaftswahlen 2016, als Russland beschuldigt wurde, sich in die Wahl eingemischt zu haben. Derartige Angriffe dienen nicht nur der Informationsbeschaffung, sondern zielen auch darauf ab, das Vertrauen in demokratische Institutionen zu untergraben.

Im Kontext des aktuellen geopolitischen Klimas, in dem Spannungen zwischen den USA und dem Iran bestehen, könnten diese Angriffe auch die Absicht verfolgen, den politischen Diskurs in den USA zu destabilisieren. Die US-Regierung hat wiederholt gewarnt, dass ausländische Akteure versuchen

werden, sich in die Wahlen einzumischen, um ihre eigenen politischen Ziele voranzutreiben.

## Aktuelle Regierungsreaktionen

Die US-Regierung hat seit dem Vorfall mit APT42 auf verschiedene Weise reagiert. So haben die Sicherheitsbehörden verstärkt Maßnahmen zur Cyberabwehr ergriffen, um die Integrität der Wahlen zu schützen. Dazu gehört die Verbesserung der Sicherheitsprotokolle für Wahlkampfmitarbeiter und die Sensibilisierung für potenzielle Bedrohungen. Das Federal Bureau of Investigation (FBI) spielt eine zentrale Rolle bei der Überwachung und Untersuchung solcher Cyberaktivitäten.

Zudem wird die Zusammenarbeit zwischen staatlichen und privaten Unternehmen forciert, um Informationen über Cyberbedrohungen schnell zu teilen und abzuwägen, wie diese Bedrohungen sowohl auf ein internes Netzwerk als auch auf breitere Wahlprozesse wirken können.

## Statistiken und aktuelle Bedrohungen im Cyberraum

Eine Umfrage des Pew Research Center aus dem Jahr 2021 hat ergeben, dass 81% der Amerikaner der Ansicht sind, dass Cyberangriffe während der Wahlen eine ernsthafte Bedrohung darstellen. Zudem berichtete das Cybersecurity and Infrastructure Security Agency (CISA), dass bis Ende 2021 mindestens 40% aller verschiedenen Wahlen in den USA Opfer eines Cyberangriffs oder einer Cyberbedrohung geworden sind. Diese Statistiken verdeutlichen die Dringlichkeit, mit der diese Probleme angegangen werden müssen.

Der Anstieg solcher Bedrohungen führt auch dazu, dass Sicherheitsunternehmen weltweit ihre Strategien zur Erkennung und Abwehr von Cyberangriffen anpassen müssen. Dazu gehört

der Einsatz neuer Technologien und Künstlicher Intelligenz, um potenzielle Angriffe frühzeitig zu identifizieren und zu verhindern.

Details