

Spionage als Motiv für Cyberangriff

[01.08.2024] Das Bundesinnenministerium informiert über die Hintergründe eines schweren Cyberangriffs, der im Jahr 2021 auf das Bundesamt für Kartographie und Geodäsie ausgeübt wurde. Dieser ist demnach staatlichen chinesischen Angreifern zuzuordnen und diente der Spionage. Es besteht weiterhin eine erhebliche Gefahr durch chinesische Spionage und Cyberangriffe.

Ende 2021 wurde das [Bundesamt für Kartographie und Geodäsie](#) (BKG) – Deutschlands zentrale Behörde für Geo-Informationen – Ziel eines schweren Cyberangriffs. Nun liegt die umfassende Auswertung des Vorfalls vor. Demnach, so meldet jetzt das [Bundesministerium des Innern und für Heimat](#) (BMI), habe die Bundesregierung nach umfassenden Analysen und Ermittlungen der Sicherheitsbehörden die Verantwortung für den Angriff staatlichen chinesischen Akteuren zugeordnet. Die chinesischen Cyberakteure haben nach den Erkenntnissen der Sicherheitsbehörden das Netzwerk des BKG zu Spionagezwecken infiltriert. Dabei kompromittierten die Angreifer Endgeräte von Privatpersonen und Unternehmen, um diese für ihren Angriff zu nutzen. Eine Rolle spielte dabei vor allem die Nutzung so genannter Verschleierungsnetzwerke. Insbesondere das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatten seinerzeit das BKG bei der Bewältigung des Cyberangriffs unterstützt. Die Federführung für dieses nationale Attribuierungsverfahren lag beim Auswärtigen Amt, unterstützt von den Sicherheitsbehörden.

Cybersicherheitsniveau erhöht

Dieser chinesische Cyberangriff richtete sich gegen eine Bundesbehörde, die, so das BMI, eine wichtige Funktion für eine Vielzahl staatlicher und privatwirtschaftlicher Einrichtungen, auch im Bereich der Kritischen Infrastrukturen, wahrnimmt. „Dieser schwere Cyberangriff auf eine Bundesbehörde zeigt, wie groß die Gefahr durch chinesische Cyberattacken und Spionage ist. Die Bundesregierung verurteilt diesen Cyberangriff staatlich gesteuerter chinesischer Akteure auf das Schärfste. Wir fordern China auf, derartige Cyberattacken zu unterlassen und zu unterbinden“, sagte Bundesinnenministerin Nancy Faeser. „Diese Cyberangriffe bedrohen die digitale Souveränität Deutschlands und Europas. Wir stellen uns diesen Bedrohungen daher entschieden entgegen und haben den Schutz stark erhöht“, so Faeser weiter, die auch auf das [jüngst verabschiedete NIS2-Umsetzungsgesetz](#) verwies, welches dazu beitragen soll, die Cybersicherheit weiter zu erhöhen. Die Aufklärung des Cyberangriffs auf das BKG sei das Ergebnis der hervorragenden, eng vernetzten Arbeit der bundesdeutschen Sicherheitsbehörden, betonte Faeser.

Aktuelle Gefährdungslage

Im Rahmen der Untersuchungen wurde festgestellt, dass ein Netzbereich des BKG kompromittiert wurde. Weitere Schadsoftware konnte auf den Systemen des BKG nicht festgestellt werden. Ein Wiederaufbau des Netzwerks ist unter Beachtung der Empfehlungen des BSI erfolgt. Es gilt als gesichert, dass der Akteur erfolgreich aus den Netzen des BKG ausgeschlossen werden konnte. Das BKG hat nach diesem Cyberangriff ein umfangreiches Bündel von Maßnahmen ergriffen und konnte so sein Informationssicherheitsniveau deutlich verbessern. Das betrifft unter anderem die Protokollierung und

Detektion sicherheitsrelevanter Ereignisse, das IT-Risikomanagement und die Mitarbeiter-Sensibilisierung.

Wie das BMI berichtet, verübten im Jahr 2023 mutmaßlich staatliche oder staatlich gesteuerte chinesische Cyberakteure gezielt Cyberangriffe auf Unternehmen, Behörden und Privatpersonen sowie auch gegen politische Institutionen. Damit sollten Informationen über politische Meinungsbildungs- und Entscheidungsprozesse sowie Positionen der Bundesregierung zu Fragen der deutschen und europäischen Außenpolitik mit Auswirkungen auf den chinesischen Staat erlangt werden. Auch wurde seit Beginn 2023 eine Reihe von technisch hochversierten Cyberangriffen gegen verschiedene IT-Dienstleistungsunternehmen festgestellt, die schwerpunktmäßig in der Betreuung von Behördennetzwerken tätig sind. Die Sicherheitsbehörden erwarten eine weitere Intensivierung der staatlich betriebenen Spionage- und Einflussnahmeaktivitäten durch China. Cyberaktionen dürften auch zukünftig hochprofessionell und mit enormem Ressourcenaufwand umgesetzt werden, so das BMI.

(sib)

- Informationen über Spionage und Cyberangriffe im Verfassungsschutzbericht 2023

Stichwörter: IT-Sicherheit, BKG, BMI, Cyber-Angriff, Geodaten