

Schwerer Cyberangriff auf das Bundesamt für Kartographie und Geodäsie ist staatlichen chinesischen Angreifern zuzuordnen und diente der Spionage

Bundesministerium des Innern und für Heimat :: 7/31/2024

Typ: Pressemitteilung , Datum: 31.07.2024

Klare Erkenntnisse der Sicherheitsbehörden / Nationales Attribuierungsverfahren ist abgeschlossen / weiterhin erhebliche Gefahr durch chinesische Spionage und Cyberangriffe

Quelle: BKG

Die Bundesregierung hat heute nach umfassenden Analysen und Ermittlungen der Sicherheitsbehörden die Verantwortung für einen **schweren Cyberangriff Ende 2021 auf das Bundesamt für Kartographie und Geodäsie (BKG) staatlichen chinesischen Akteuren zugeordnet und auf das Schärfste verurteilt**. Diese 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 (Nutzung von sog. **Verschleierungsnetzwerken**).

Insbesondere das **Bundesamt für Verfassungsschutz (BfV)** und das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** haben seinerzeit das **BKG** bei der Bewältigung des Cyberangriffes unterstützt.

Die Federführung für dieses nationale Attribuierungsverfahren lag beim Auswärtigen Amt, unterstützt von den Sicherheitsbehörden.

Dieser chinesische Cyberangriff richtete sich gegen eine Bundesbehörde, die eine wichtige Funktion für eine Vielzahl staatlicher und privatwirtschaftlicher Einrichtungen, auch im Bereich der kritischen Infrastrukturen, wahrnimmt.

Bundesinnenministerin Nancy Faeser: "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. Diese Cyberangriffe bedrohen die digitale Souveränität Deutschlands und Europas. Wir stellen uns diesen Bedrohungen daher entschieden entgegen und haben den Schutz stark erhöht. Erst in der vergangenen Woche haben wir im Bundeskabinett ein weiteres Gesetz auf den Weg gebracht, um die Cybersicherheit weiter zu erhöhen und uns stärker gegen staatliche ebenso wie kriminelle Cyberattacken zu wappnen."

"Die Aufklärung dieses Cyberangriffe ist Ergebnis der hervorragenden, eng vernetzten Arbeit unserer Sicherheitsbehörden. Dafür danke ich allen beteiligten Behörden, insbesondere dem **Bundesamt für Verfassungsschutz** sehr herzlich."

Weitere Informationen:

- 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. In der Folge konnte das BKG sein Informationssicherheitsniveau deutlich verbessern. Das betrifft u.a., aber nicht nur, die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen, das IT-Risikomanagement und die noch stärkere Sensibilisierung der Mitarbeitenden für Informationssicherheit.
- Das **Bundesamt für Kartographie und Geodäsie (BKG)** gehört zum Geschäftsbereich des Bundesministeriums des Innern und für Heimat und ist ein modernes Kompetenz- und Dienstleistungszentrum des Bundes. Das BKG sorgt für ein **einheitliches Koordinatensystem** für das gesamte Bundesgebiet, stellt **aktuelle, amtliche Geodaten** von Deutschland über Internetdienste bereit, und unterstützt den Auf- und Ausbau der **Geodateninfrastruktur**, um es allen Bürgern zu ermöglichen, Geodaten von Bund, Ländern und Kommunen zu suchen, zu finden und zu nutzen. Sein Dienstleistungszentrum führt die amtlichen Geodaten des BKG und aller 16 Bundesländer sowie von Drittanbietern zusammen und stellt sie digital zur Verfügung.
- Das **Bundesamt für Verfassungsschutz** ist für die nachrichtendienstliche Aufklärung von Cyberangriffen, **Spionage** und Sabotage durch ausländische Nachrichtendienste zuständig und steht als vertraulicher Ansprechpartner für betroffene Einrichtungen zur Verfügung.
- **Zur aktuellen Gefährdungslage durch chinesische Cyberangriffe:** Im Jahr 2023 verübten mutmaßlich staatliche oder staatlich gesteuerte chinesische Cyberakteure **gezielt Cyberangriffe auf Unternehmen, Behörden und Privatpersonen** sowie auch gegen politische Institutionen. Damit sollen 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 Unternehmen im Umfeld politischer Stellen – wie beispielsweise IT-Dienstleistungsunternehmen für Behörden – gerieten intensiv in den Fokus und wurden als Einfallstor für darauf aufbauende Angriffe genutzt. Die Vorgehensweise der Cyberspionageakteure erfuhr eine deutliche qualitative und quantitative Weiterentwicklung, wodurch eine bislang kaum dagewesene Reichweite und Effektivität erreicht werden konnten.
- Seit Beginn 2023 wurde 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. Es verfolgt eine **offensive Cyberstrategie**, die durch umfangreichen Wissenstransfer einen wichtigen Beitrag zu den

industrie- und geopolitischen Zielen des Landes leisten soll. Cyberaktionen dürften auch zukünftig hochprofessionell und mit enormem Ressourcenaufwand umgesetzt werden.

- Weitere Informationen können Sie dem **aktuellen Verfassungsschutzbericht** entnehmen:
www.bmi.bund.de/VSB2023

© Bundesministerium des Innern und für Heimat, 2024