A serious cyberattack on the Federal Office of Cartography and Geodesy can be attributed to Chinese state attackers and was used for espionage

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

Type: Press release , Date: 31.07.2024

Clear findings from security authorities / National attribution process has been completed / still significant threat from Chinese espionage and cyber attacks

Source:*BKG*

Following comprehensive analyses and investigations by the security authorities, the Federal Government today assigned responsibility for a **serious cyber attack on the** Federal Office of Cartography and Geodesy **(BKG) at the end of 2021 to Chinese state actors and condemned them in the strongest possible terms . According to the findings of the security authorities, these Chinese cyber actors infiltrated the** BKG 's network **for espionage purposes** . In doing so, the attackers compromised end devices belonging to private individuals and companies in order to use them for their attack (use of so-called **obfuscation networks**).

In particular, the Federal Office for the Protection of the Constitution (BfV) and the Federal Office for Information Security (BSI) supported the BKG in dealing with the cyber attack.

The Federal Foreign Office was responsible for this national attribution procedure, supported by the security authorities.

This Chinese cyberattack targeted a federal agency that performs an important function for a variety of government and private sector institutions, including in the area of critical infrastructure.

Federal Minister of the Interior Nancy Faeser: “"This serious cyberattack on a federal authority shows how great the danger is from Chinese cyberattacks and espionage . The Federal Government condemns this cyberattack by state-controlled Chinese actors in the strongest possible terms. We call on China to refrain from and stop such cyberattacks. These cyberattacks threaten the digital sovereignty of Germany and Europe. We are therefore resolutely opposing these threats and have significantly increased protection. Just last week, we in the Federal Cabinet introduced another law to further increase cybersecurity and to better arm ourselves against state and criminal cyberattacks.”

“The investigation into this cyber attack is the result of the excellent, closely networked work of our security authorities. I would like to thank all the authorities involved, especially the Federal Office for the Protection of the Constitution ."”

Additional Information:

- During the investigation, it was determined that **a part of the BKG network had been compromised** . No other malware was found on the BKG systems. The network was rebuilt in accordance with the BSI 's recommendations . It is considered certain that the actor **was successfully excluded from the BKG** networks

- Following this cyber attack, the BKG took a comprehensive set of measures. As a result, the BKG was able to significantly improve its level of information security. This includes, but is not limited to, the logging and detection of security-relevant events, IT risk management and raising employees' awareness of information security even further.

- The Federal Office for Cartography and Geodesy **(BKG)** is part of the business area of the Federal Ministry of the Interior and Home Affairs and is a modern competence and service center of the federal government. The BKG ensures a **uniform coordinate system** for the entire federal territory, provides **current, official geodata** from Germany via Internet services, and supports the development and expansion of the geodata infrastructure to enable all citizens to search for, find and use geodata from the federal government, states and municipalities. Its service center brings together the official geodata of the BKG and all 16 federal states as well as from third-party providers and makes it available digitally.

- The Federal Office for the Protection of the Constitution is responsible for intelligence investigations into cyber attacks, espionage and sabotage by foreign intelligence services and is available as a confidential contact for affected institutions.

- **On the current threat situation posed by Chinese cyber attacks:** In 2023, suspected state or state-controlled Chinese cyber actors carried out **targeted cyber attacks on companies, authorities and private individuals** as well as on political institutions. The aim is to obtain information about political opinion-forming and decision-making processes as well as positions of the federal government on issues of German and European foreign policy with an impact on the Chinese state. Companies in the vicinity of political bodies - such as IT service companies for authorities - also came into intensive focus and were used as a gateway for attacks based on them. The approach of the cyber espionage actors underwent a significant qualitative and quantitative development, enabling a previously unseen reach and effectiveness to be achieved.

- Since the beginning of 2023, a number of sophisticated **cyber attacks have been detected against various IT service providers** that focus on supporting government networks.

- The security authorities expect China to **further intensify its state-run** espionage **and influence activities . It is pursuing an offensive cyber strategy** that is intended to make an important contribution to the country's industrial and geopolitical goals through extensive knowledge transfer. Cyber operations are likely to continue to be implemented in a highly professional manner and with enormous expenditure of resources.

- Further information can be found in the **current report of the Federal Office for the Protection of the Constitution** : www. *bmi.bund.de/VSB2023*