

"Inside Job": Russische IT-Expertin Kaspersky vermutet CIA hinter Hackerangriff auf US-Pipeline

14 Mai 2021 22:06 Uhr

Eine prominente russische Unternehmerin behauptet, dass es sich bei der Cyberattacke auf die Colonial Pipeline um einen "Inside-Job" handelt, um russische Hackergruppen dafür verantwortlich zu machen.



Colonial mit Sitz im Bundesstaat Georgia ist der Betreiber der größten Pipeline in den USA.

Eine der wichtigsten Pipelines der USA ist seit letzter Woche nach einem Hackerangriff lahmgelegt. Nach der Cyberattacke auf die Colonial Pipeline wurde das Benzin im Osten der USA teilweise knapp. Die Versorgung soll sich jedoch bald wieder normalisieren. US-Präsident Joe Biden betonte gestern, die Bürger sollten bis dahin "nicht in Panik verfallen".



Nach Hackerangriff auf Pipeline: Sprit wird knapp in den USA

Bei der Cyberattacke, die die Treibstoffversorgung an der Ostküste der USA stilllegte und die Gaspreise in die Höhe trieb, handele es sich eher um einen "Inside-Job", als dass ausländische Hacker dahintersteckten, behauptet nun die russische Unternehmerin Natalja Kaspersky. Die Gründerin und ehemalige CEO der Sicherheitssoftwarefirma Kaspersky Lab führte am Freitag mit *RIA Nowosti* ein Interview über den Vorfall. Sie behauptet, dass die CIA, der führende ausländische Geheimdienst der USA, eine Topmannschaft im digitalen Bereich zur Verfügung habe, die sich als ausländische Hacking-Gruppe tarnen könne. Ihr zufolge sei diese Gruppe, bekannt als UMBRAGE, geschickt darin, ihre "Online-Fußabdrücke" zu verbergen. Die Existenz dieser Topmannschaft war erstmals in einer Reihe von Dokumenten an die Öffentlichkeit durchgesickert, die von WikiLeaks im Jahr 2017 veröffentlicht und anschließend von US-Medien aufgegriffen wurden. Zu jener Zeit berichtete *USA Today*, dass deren verdeckte Agenten "möglicherweise Hacking-Methoden von ausländischen (externen) Hackern katalogisiert" hätten, auch unter anderem in Russland. Diese Methoden hätten es einem geheimen CIA-Team ermöglicht, seine Identität zu verbergen, indem es sie während der Spionage eingesetzt hätte.

Am Donnerstag gab Biden bekannt, dass dieser verheerende Schlag für die US-Infrastruktur aus dem Ausland verübt worden sei. "Wir glauben nicht, dass die russische Regierung an diesem Angriff beteiligt war, aber wir haben guten Grund zur Annahme, dass die Verbrecher, die den Angriff verübt haben, in Russland leben", behauptete er.



Nach Ausfall von US-Pipeline: Händler setzen auf Treibstoffimporte aus Europa

Kaspersky verwies auf die Liste der Länder, unter deren Hackergruppen-Signaturen sich UMBRAGE tarnte – "Russland, Nordkorea, China, Iran". Sie erklärte, man könne daher gar nicht mit Sicherheit sagen, dass der Angriff von einer Hackergruppe aus Russland durchgeführt worden sei.

Colonial soll nach Angaben der Nachrichtenagentur *Bloomberg* für die Freigabe seiner bei dem Angriff blockierten Daten rund fünf Millionen Dollar gezahlt haben und fährt dieser Tage den Betrieb seiner Anlagen wieder hoch. Das Wiederhochfahren der Anlage bis zum Normalbetrieb kann dennoch bis zu zwei Wochen dauern. Das generelle Problem mit Hackern aber ist damit noch lange nicht gelöst. Denn Ransomware-Angriffe auf Unternehmen häuften sich derzeit.

Woher die Hacker stammen, ist oft nicht zu klären. Vielfach wurden immer wieder Russland, China oder Iran für solche Attacken verantwortlich gemacht, ohne dass dafür vonseiten der USA überzeugende Beweise vorgelegt wurden. Das FBI machte als angebliche Angreifer auf die Colonial Pipeline mittlerweile eine Gruppe namens DarkSide aus. Ihre Mitglieder sind bislang unbekannt. Die Bande betreibt allerdings eine eigene Website. Darauf erklärte sie: "Unser Ziel ist es, Geld zu verdienen und nicht Probleme für die Gesellschaft zu produzieren", berichtet die *FAZ*.

Mehr zum Thema - [Hackerangriff legt Rohrleitungsnetz großer Benzin-Pipeline in USA lahm](#)

Quelle: <https://de.rt.com/international/117505-colonial-pipeline-wer-steckt-hinter/>
20210515 DT (<https://stopreset.ch>)