Medienkommentar

Behauptung der Washington Post über russische Hackerangriffe erweist sich als Falschmeldung

Seit dem vergangenen US-Wahlkampfjahr ist in den etablierten Medien immer wieder von angeblichen russischen Hackerangriffen auf US-Ziele die Rede. Russlands Präsident Wladimir Putin dementierte stets: Moskau beschäftige sich nicht mit Hackerangriffen auf Staatsniveau und habe mit den Angriffen nichts zu tun. Mit welcher Vorsicht die Anschuldigungen angeblich russischer Hackerangriffe betrachtet werden müssen, zeigt eines der neusten Beispiele.

Seit dem vergangenen US-Wahlkampfjahr ist in den etablierten Medien immer wieder von angeblichen russischen Hackerangriffen auf US-Ziele die Rede. Laut einem in der letzten Dezemberwoche veröffentlichtem Bericht des US-Auslandsgeheimdienstes CIA und der US-Bundespolizei FBI wollen diese genügend Beweise gefunden haben, die belegen, dass sich Russland mittels Hackerangriffe in unzulässiger Weise in den US-Präsidentschaftswahlkampf eingemischt habe. Im Zuge dieser angeblichen Beweise hat der amtierende US-Präsident Sanktionen gegen Russland verhängt: So wurden 35 russische Diplomaten des Landes verwiesen.
Russlands Präsident Wladimir Putin dementierte stets: Moskau beschäftige sich nicht mit Hackerangriffen auf Staatsniveau und habe mit den Angriffen nichts zu tun. Mit welcher Vorsicht die Anschuldigungen angeblich russischer Hackerangriffe betrachtet werden müssen, zeigt eines der neusten Beispiele:
Am 30. Dezember 2016 schrieb die amerikanische Tageszeitung „The Washington Post“, dass es russischen Hackern gelungen sei, in das Netzwerk eines Stromversorgers im US-Bundesstaat Vermont einzudringen. Im System des Stromversorgers sei eine „Malware“ – ein sogenannt „bösartiges“ Computerprogramm – entdeckt worden, das einer russischen Cyberattacke namens „Grizzly Steppe“ zugeordnet werden könne. So berichtete die Zeitung unter Berufung auf namentlich nicht genannte US-Behörden.
Schnell hat diese von der Washington Post und der Nachrichtenagentur Reuters verbreitete Meldung den Weg in die deutschsprachigen Leitmedien gefunden. Etablierte Medien wie der „SPIEGEL“, die FAZ, DIE WELT, DER STANDARD sowie die Schweizer NZZ und der Tages-Anzeiger, um nur einige zu nennen, übernahmen diese 1:1 – ohne auch nur im Geringsten überprüft zu haben. Auch Politiker wie US-Senator Patrick J. Leahy zeigten sich besorgt: Es handle sich um einen Versuch … um möglicherweise unser Stromnetz mitten im Winter abschalten zu können.
Jedoch erschien nur einen Tag später in der Washington Post folgende Richtigstellung des Chefredakteurs: „Eine frühere Version dieser Geschichte hat inkorrekt behauptet, dass russische Hacker ins US-Stromnetz eingedrungen sind. Behörden sagen, es gibt kein Anzeichen dafür. Der Computer von Burlington Electric war nicht am Netz angeschlossen.“ Anstatt „Russische Hacker drangen in US-Stromnetz ein …“ hieß es nun am nächsten Tag

nur noch, dass eine russische Malware auf einem Dienstcomputer Vermonts die Risiken des US-Stromnetzes aufzeigen würde.
Doch auch diese Behauptung hielt nicht lange Stand. Am 3. Januar berichtete die Washington Post unter Berufung auf Experten und Behördenvertreter, dass Ermittler keine Indizien gefunden hätten, die den Vorfall auf die russische Regierung zurückführen ließ.
Inzwischen griffen auch einige der deutschsprachigen Leitmedien – bei weitem nicht alle – die Richtigstellung auf. So schrieb die österreichische Tageszeitung „Der Standard“ am 3. Januar wörtlich: „Dem (neusten) Bericht (der Washington Post) zufolge stellte sich nun heraus, dass ein Mitarbeiter des Burlington Electric Departments vergangenen Freitag über einen Laptop nur seine Yahoo Mails aufgerufen habe. Das habe zum Alarm geführt, da das Unternehmens-Netzwerk eine angesteuerte IP (Internetprotokoll)-Adresse als verdächtig einstufte. Die vermeintlich schadhafte Adresse sei aber auch vielfach landesweit aufgerufen worden, hieß es. Deshalb gingen die Ermittler davon aus, dass der Stromversorger nicht Ziel russischer Hacker wurde.“
Auf dem Computer sollen die Ermittler Malware-Werkzeuge gefunden haben, die Kriminelle gern für Hackerangriffe nutzten. Jedoch seien keine Spuren zu russischen Hackern erkennbar gewesen.
Was das vom US-Ministerium für Innere Sicherheit getaufte Malware „Grizzly Steppe“ betrifft, sind sich Computerexperten einig, dass dieses im Netz jedermann und nicht nur den Russen zugänglich ist. Die mit freiberuflichen Journalisten arbeitende Nachrichtenwebseite „The Intercept“ zitierte einen Computerexperten. Dieser verglich die Anschuldigung, das Malware „Grizzly Steppe“ habe etwas mit Russen zu tun, mit der Annahme, dass ein russisches Kalaschnikow-Sturmgewehr, welches an einem Tatort gefunden wird, bedeute, dass der Killer ein Russe sei. Jedermann habe Zugang zu einer Kalaschnikow und zudem gebe es eine große Anzahl von Lizenzbauten und Kopien in anderen Staaten.
Dieses Beispiel über angebliche russische Hacker, die es auf US-Ziele abgesehen haben, macht wieder einmal deutlich:
1. Dass Falschmeldungen von etablierten amerikanischen Medien wie der Washington Post, bewusst oder unbewusst auf leichtfertigste Weise, weiterverbreitet werden.
2. Wie schnell und ohne zu überprüfen solche von den USA ausgehenden Falschmeldungen von den europäischen Leitmedien übernommen werden.
Deshalb können vergangene sowie zukünftige Behauptungen über angebliche russische Hackerangriffe nicht als bare Münze genommen werden. Vielmehr müssen sie sorgfältig geprüft werden, ob sie nicht als weitere gezielte Falschmeldungen im Informationskrieg gegen Russland eingestuft werden müssen.

von dd.

Quellen:

http://www.welt.de/politik/article160741870/Russische-Hacker-in-Stromversorger-Netzwerk-eingedrungen.html
http://www.srf.ch/news/international/trump-preist-putins-reaktion
http://alles-schallundrauch.blogspot.ch/2017/01/die-medien-verbreiten-wieder-fake-news.html
http://derstandard.at/2000050193323/Doch-keine-Spur-nach-Russland-nach-Angriff-aufStromversorger
http://www.broeckers.com/2017/01/01/hardware-der-grizzly-steppe-entdeckt/
https://deutsch.rt.com/international/44939-washington-post-fakenews-russland/

Das könnte Sie auch interessieren:

#Medienkommentar - www.kla.tv/Medienkommentare

#Hacker - www.kla.tv/Hacker

Kla.TV – Die anderen Nachrichten ... frei – unabhängig – unzensiert ...

- ➔ was die Medien nicht verschweigen sollten ...
- ➔ wenig Gehörtes vom Volk, für das Volk ...
- ➔ tägliche News ab 19:45 Uhr auf www.kla.tv

Dranbleiben lohnt sich!

Kostenloses Abonnement mit wöchentlichen News per E-Mail erhalten Sie unter: www.kla.tv/abo

Sicherheitshinweis:

Gegenstimmen werden leider immer weiter zensiert und unterdrückt. Solange wir nicht gemäß den Interessen und Ideologien der Systempresse berichten, müssen wir jederzeit damit rechnen, dass Vorwände gesucht werden, um Kla.TV zu sperren oder zu schaden.

Vernetzen Sie sich darum heute noch internetunabhängig!
Klicken Sie hier: www.kla.tv/vernetzung