

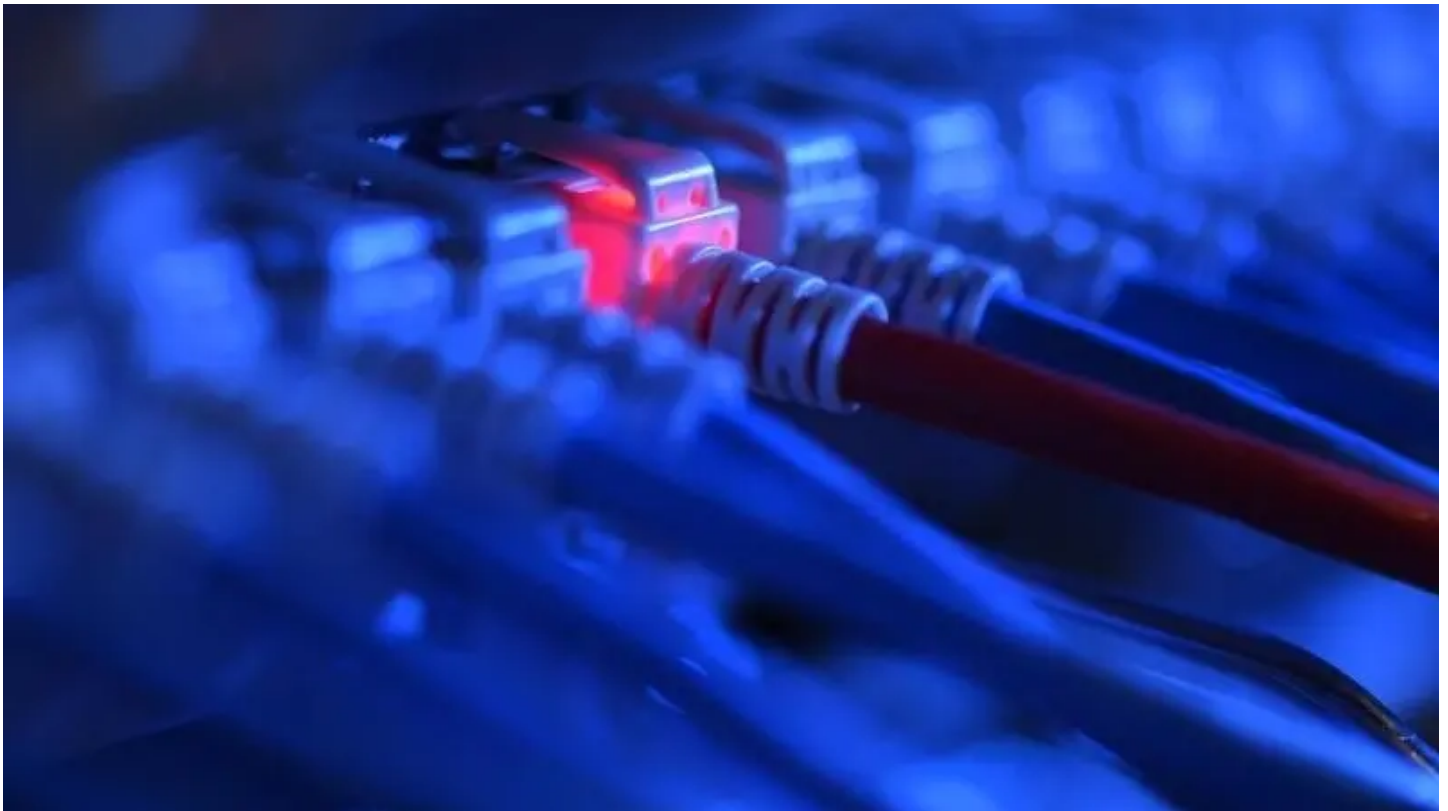
04.01.2019 16:52 Uhr

Gehackte Daten: Politiker beklagen schweren Angriff auf die Demokratie

Die lange unentdeckt gebliebene Hackerattacke auf Abgeordnete, Moderatoren, Aktivisten und YouTuber hat vor allem in den Parteien viele geschockt.

Von Stefan Krempl

 |  |  251



(Bild: dpa, Felix Kästle/Illustration)

Die massenhafte Veröffentlichung privater Daten deutscher Politiker, Journalisten, Moderatoren, Schauspieler, Sänger und YouTuber über ein mittlerweile gesperrtes Twitter-Konto hat viele der Betroffenen aus der Neujahrsruhe aufgeschreckt. Vor allem Vertreter der Bundesregierung und des Bundestags reagierten am Freitag entsetzt auf die tausende Datensätze umfassenden Leaks, die neben Kopien von Ausweisen, privaten Familien-Chats, Handy-Nummern und E-Mail-Adressen, Mietverträgen etwa auch eine Tageskarte für die Berliner Erotik-Messe "Venus" enthalten.

Ruf nach schneller Aufklärung

Bundjustizministerin Katarina Barley verurteilte das Vorgehen der unbekanntenen Cyberkriminellen auf Twitter scharf als einen "schwerwiegenden Angriff auf das Recht auf Privatsphäre und damit einen Grundpfeiler unserer Demokratie". Die Urheber wollten Vertrauen in den liberalen Rechtsstaat und seine Institutionen beschädigen. "Kriminelle und ihre Hintermänner dürfen keine Debatten in unserem Land bestimmen", betonte die SPD-Politikerin. Die Täter und ihre Motive müssten schnell aufgeklärt werden.

Der Fraktionsvorsitzende der Linkspartei, Dietmar Bartsch, zeigte sich "schwer geschockt" und sprach ebenfalls von einem "schweren Anschlag" auf die Demokratie und den sozialen Zusammenhalt in unserem Land. "Die zuständigen Behörden müssen jetzt schnell aufklären", forderte SPD-Generalsekretär Lars Klingbeil. Dabei müsse auch eine "mögliche politische Motivation dieses Angriffs" ausgelotet werden.

"Versuch der Destabilisierung"

"Wir erleben einen erneuten, sehr ernstzunehmenden Versuch, unsere Demokratie zu destabilisieren", konstatierte die parlamentarische Geschäftsführerin der Grünen, Britta Haßelmann. "Von diesem Angriff werden wir uns in unserer Arbeit nicht einschüchtern lassen."

Erste Hinweise auf die bereits größtenteils vor Weihnachten in Form eines "Adventskalenders" in einzelnen Teilen veröffentlichten Daten machten unter Bundestagsabgeordneten am Donnerstagnachmittag die Runde. Am Freitag erfolgten dann hektische Telefonkonferenzen zwischen den Geschäftsführern der meisten Fraktionen. Weder das Bundesamt für Sicherheit in der Informationstechnik (BSI) noch das Bundesamt für Verfassungsschutz (BfV) wussten offenbar vor Donnerstag etwas von den Vorfällen.

Mittlerweile ermitteln die beiden Behörden aber neben dem Bundeskriminalamt (BKA) und Staatsanwaltschaften bis hin zum Generalbundesanwalt, der ein "Beobachtungsverfahren" eingeleitet hat. Die Bundesanwaltschaft wäre etwa am

Drücker, wenn eine geheimdienstliche Agententätigkeit zu vermuten ist. Auch der Bundesnachrichtendienst (BND) soll in die laufenden Untersuchungen involviert sein. Das BSI twitterte, dass das nationale Cyber-Abwehrzentrum die zentrale Koordination übernommen habe. Regierungsnetze seien offenbar – im Gegensatz zum "Bundeshack" – nicht angegriffen worden.

Politiker aller Ebenen betroffen

Martina Fietz berichtete als Sprecherin der Bundesregierung, dass nach ersten Analysen Politiker und Mandatsträger aller Ebenen bis hinunter zu den Kommunen betroffen seien. Die Behörden arbeiteten derzeit "mit Hochdruck" daran, das Ausmaß zu ermitteln und den Geschädigten Hilfe zukommen zu lassen. Sensible Daten des Kanzleramts oder von Bundeskanzlerin Angela Merkel (CDU) sind laut Fietz nicht publik gemacht worden. Briefe an Merkel finden sich aber unter den Materialien. Die Sprecherin warnte, dass die Leaks "mit großer Vorsicht" zu handhaben seien, da sich auch gefälschte Materialien darunter befinden könnten.

Allgemein wird vermutet, dass die geklauten Daten aus verschiedenen Hacks etwa von Konten der Betroffenen auf der Amazon-Cloud, Facebook oder Twitter stammen und mit viel Fleißarbeit zusammengetragen wurden. Die SPD-Netzpolitikerin Saskia Esken forderte gegenüber heise online daher nicht nur einen bewussteren Umgang mit Passwörtern und mehr Verschlüsselung, sondern auch eine "Plakatkampagne des Bundesinnenministeriums zur IT-Sicherheit". Die Gesellschaft müsse lernen, besser mit Desinformationsstrategien im Netz umzugehen, um "resilient zu bleiben". Die von der Regierung erörterten "Hackbacks" brächten dagegen nichts.

Die Zielrichtung des Angriffs weist für Esken angesichts der Auswahl der vorgeführten Leute darauf hin, dass das rechte Spektrum dahinterstehen könnte. Die Behörden müssten daher Berichte genauer prüfen, wonach die Bundeswehr und Teile der Polizei von einem rechten Netzwerk in Form einer "Schattenarmee Hannibals" unterwandert seien. Die Vernetzung des Twitter-Kontos, über den die Leaks bekannt gemacht wurden, verweist auf die Neonazi-Szene. Die AfD war von den Hacks nicht betroffen und hat sich bislang auch nicht offiziell dazu geäußert.

Sondersitzungen im Bundestag

Die Grünen im Bundestag haben eine Sondersitzung der Kommission für den Einsatz neuer Informations- und Kommunikationstechniken sowie des Innenausschusses des Bundestags beantragt. "Wir brauchen endlich echte proaktive Maßnahmen zur Erhöhung der IT-Sicherheit", erklärte Fraktionsvize Konstantin von Notz. "Dazu gehören unter anderem ein Verzicht auf den staatlichen Handel mit Sicherheitslücken, durchgehende Ende-zu-Ende-Verschlüsselungen und die Stärkung unabhängiger Aufsichtsstrukturen."

Der parlamentarische Geschäftsführer der CDU/CSU-Bundestagsfraktion, Patrick Schnieder, gab sich eher schmallippig: "Wir stehen in Kontakt mit der Bundestagsverwaltung, die wiederum mit den Sicherheitsbehörden zusammenarbeitet", erklärte er. "Wir drängen auf eine rasche Aufklärung."

Sein Kollege von der SPD-Fraktion, Carsten Schneider, unterstrich: "Die IT-Infrastruktur der SPD-Bundestagsfraktion selbst ist nicht betroffen." Man habe Sicherheitsmaßnahmen eingeleitet, "um den Schutz der Kommunikation und die Funktionsfähigkeit der parlamentarischen Arbeit zu gewährleisten". Der demokratische Wettbewerb lasse sich nicht "durch auf illegale Weise gewonnene persönliche Daten kompromittieren".

Adressbuch als Angriffspunkt

"Wer private Angaben von Personen veröffentlicht, nimmt deren Gefährdung billigend in Kauf, und dagegen müssen wir uns gemeinsam wehren", sagte Jan Korte, Geschäftsführer der Linksfraktion. Es handle sich um "eine Folge der vernetzten Gesellschaft", befand die linke Digitalexpertin Anke Domscheit-Berg. Das schwächste Glied in einer Kette müsse dabei gar nicht "der Promi oder Politiker selbst sein". In Frage kämen auch Dritte, auf deren Adressbuch im Smartphone oder Plattformen bis hin zum Sexshop jemand Zugriff erlangt habe.

Der linke Abgeordnete Diether Dehm warnte davor, vorschnell Russland zu verdächtigen. Sollte im Laufe der nächsten Stunden "von den üblichen Medienagenten" Wladimir Putin für den Hackerangriff verantwortlich gemacht werden, werde er seinen gerade gestellten Strafantrag gegen Unbekannt zurückziehen.

"Diese Art der Hackerangriffe und Datenleaks sind leider kein Novum mehr und wird es in Zukunft öfter geben", prognostizierte der Vorsitzende des Bundestagsausschusses

Digitale Agenda, Jimmy Schulz. "Gerade weil es eine der zentralen staatlichen Aufgaben ist, die Privatsphäre der Menschen zu schützen, müssen wir dies zum Anlass nehmen, uns fraktionsübergreifend für die IT-Sicherheit Deutschlands einzusetzen." Die Liberalen hätten bereits einen Antrag zum "Recht auf Verschlüsselung" ins Parlament eingebracht. Darüber hinaus dürfte der Staat selbst "nicht an der Schwächung der IT-Sicherheit arbeiten".

Einfache Schutzmaßnahmen meist ausreichend

"Der grob fahrlässige Umgang diverser Politiker mit telefonischen und elektronischen Kontakten kann nicht nur hohe Funktionsträger erpressbar machen, sondern bringt auch ihr persönliches Umfeld und ihre Informanten in Gefahr", warnte Patrick Breyer, Spitzenkandidat der Piratenpartei zur Europawahl, vor den Folgen des erfolgten "Doxxing". Dass selbst prominente Bundespolitiker ihre Gesprächspartner großen US-amerikanischen Digitalkonzernen auslieferten, sei unverantwortlich. Der Bundestag müsse jetzt dringend einen "Verhaltenskodex zum Schutz der Sicherheit mandatsbedingter Kontakte" ausarbeiten.

Norbert Pohlmann, Vorstand für IT-Sicherheit beim eco-Verband der Internetwirtschaft, appellierte an die Bundesregierung, "die Entwicklung und Verbreitung einfach anwendbarer Verschlüsselungstechnologien stärker zu fördern und voranzutreiben". Von Maßnahmen wie Backdoors, Zero Day Exploits und Staatstrojaner müssten die Politik und die Behörden dagegen "entschieden Abstand nehmen", da sie den Aufbau sicherer IT-Systeme unterwanderten. Für Michael Littger von der Initiative "Deutschland sicher im Netz" zeigt die Attacke "den Nachholbedarf beim Thema digitale Aufklärung" auf. Es müsse darum gehen, "digitale Kompetenzen in allen Lebensbereichen zu verankern". Einfache Schutzfähigkeiten reichten, "um rund 90 Prozent der Cyberangriffe abzuwehren". (mho)

[Kommentare lesen \(251\)](#)

[Zur Startseite](#)

MEHR ZUM THEMA

HACKING

TEILE DIESEN BEITRAG



Kurzlink: <https://heise.de/-4265847>

Abonnieren

Top-News der Redaktion von heise online



Hackerangriff: Ehemaliges Twitter-Konto eines YouTubers missbraucht

Der Twitter-Account, der Daten von Parteien und Prominenten veröffentlichte, gehörte früher einem Minecraft-Troll-YouTuber.

Persönliche Dokumente von deutschen Politikern und Promis veröffentlicht

Faltphones, rollbare TVs und alles mit 5G

Neuer Mac Mini, Handy-Wechsel und Ultimaker-Klone

nach oben

Alle Angebote 

[Datenschutzhinweis](#)

[Impressum](#)

[Kontakt](#)

2572031

Content Management by **InterRed**

Hosted by Plus.line

Copyright © 2019 Heise Medien

