Hackerangriff auf Bundestag - Haftbefehl gegen Russen

SZ sueddeutsche.de/politik/hack-bundestag-angriff-russland-1.4891668

Georg Mascolo, Florian Flade

Hackerangriff auf Bundestag:Bärenjagd

5. Mai 2020, 9:36 Uhr
Lesezeit: 6 min

"Fancy Bear", der "schicke Bär": So heißt die Einheit des russischen Militärgeheimdienstes GRU, die hinter dem Cyberangriff auf den Bundestag von 2015 stecken soll.

(Foto: Getty Images)

Russlands Militärgeheimdienst GRU soll für den Cyberangriff auf den Deutschen Bundestag im Jahr 2015 verantwortlich sein. Nun hat die Bundesanwaltschaft einen Haftbefehl gegen einen Hacker erwirkt. Die Geschichte einer Jagd.

Von Florian Flade und Georg Mascolo

-
-
-
-
- Drucken

Ein blonder Junge blickt in die Kamera. Die Haare sind kurz, seine Miene ist ernst. Wann das ziemlich unscharfe Foto aufgenommen wurde, ist nicht bekannt. Dmitriy Sergeyevich (dt.: Dmitrij Sergejewitsch) Badin aber sieht darauf sehr jung aus. Heute soll er 29 Jahre alt sein, geboren am 15. November 1990 in Kursk, in Russland. So steht es auf dem Fahndungsplakat der amerikanischen Bundespolizei FBI. Sie sucht weltweit nach Badin, Hinweise nimmt auch jede US-Botschaft entgegen. Genau genommen sind es gleich zwei Plakate, auf denen sein Foto zu sehen ist - denn Badin gilt als Serientäter.

Der junge Russe, der so harmlos dreinblickt auf dem Foto, ist ein Soldat. Er fährt keinen Panzer, er fliegt auch keinen Kampfjet, vermutlich trägt er nicht einmal eine Waffe. Wenn Dmitrij Badin in die Schlacht zieht, dann macht er dies an einer Tastatur. Er soll ein Hacker im Staatsdienst sein, ein Cyber-Soldat im Auftrag Wladimir Putins. Badin soll einer berüchtigten Einheit des russischen Militärgeheimdienstes GRU angehören, die unter dem Namen "Fancy Bear", der "schicke Bär", bekannt ist.

Das FBI sucht nach Badin wegen zwei spektakulärer Hacker-Angriffe. Einer richtete sich gegen die Welt-Anti-Doping-Agentur Wada, aber das gilt auch in den USA eher als Kleinkram. Viel wichtiger ist ein anderer Fall: Es geht um die Manipulation der US-Wahlen im Jahr 2016, jener Wahl, aus der Donald Trump als Sieger und 45. Präsident der Vereinigten Staaten hervorging. Badin soll einer jener Männer gewesen sein, die Trump dabei halfen, indem sie E-Mails seiner Rivalin Hillary Clinton und der Demokratischen Partei stahlen und zielgerichtet veröffentlichten.

Die Fahndung nach Dmitrij Badin läuft nun bereits seit zwei Jahren. Inzwischen aber suchen nicht mehr nur die USA nach dem Russen - sondern auch der Generalbundesanwalt. Deutschlands Chefankläger hat in dieser Woche einen internationalen Haftbefehl gegen Badin erwirkt. Ihm wird "geheimdienstliche Agententätigkeit" und "Ausspähen von Daten" vorgeworfen. Die Ermittler sind sicher, dass er einer der führenden Köpfe hinter dem spektakulärsten Cyber-Angriff gewesen ist, den die Bundesrepublik je erlebt und erlitten hat: Dem Hack des Deutschen Bundestages. Auch Bundestagspräsident Wolfgang Schäuble wurde inzwischen über den Haftbbefehl informiert.

Fünf Jahre mühevolle Kleinarbeit haben nun auch den Ermittlungsrichter am Bundesgerichtshof überzeugt. Das Bundeskriminalamt (BKA) war beteiligt, ebenso die Bundespolizei. Es gab Hilfe aus den USA - und aus den Niederlanden. Der nun ausgestellte Haftbefehl gegen den Hacker ist aus Sicht der Strafverfolger ein großer Erfolg. Zwar haben die Sicherheitsbehörden mittlerweile eine relativ gute Übersicht über die Methoden und Werkzeuge der staatlich gesteuerten Cyber-Spionage, wer aber tatsächlich in Moskau, Peking oder Teheran an der Tastatur sitzt, bleibt oft unklar. Einzelne Hacker wie Dmitrij Badin zu identifizieren - von "naming and shaming" ist dann oft die Rede - gelingt so gut wie nie.

Cybersicherheit

"30 Prozent aller Angestellten klicken auf alles, was du ihnen schickst"

Dmitri Alperovitch, Mitgründer der IT-Sicherheitsfirma Crowdstrike, über die Frage, warum russische Hacker die schnellsten sind, was an Nordkorea innovativ ist und warum KI seine Firma nie ersetzen wird. Interview von Max Muth

Dass sich der Hacker, der in Russland vermutet wird, aus dem Land herauswagen wird, ist unwahrscheinlich. Einen schnellen Prozess darf man daher nicht erwarten. Und selbst wenn er irgendwo auf der Welt gefasst würde, dann wären da zunächst die USA. Bei allem Respekt, das haben die US-Kollegen die deutschen Ermittler schon wissen lassen, der Hack des Bundestages sei zwar eine schlimme Sache. Aber die Manipulation der Wahlen in den USA sei nun doch noch ein ganzes Stück schlimmer.

Überhaupt waren es nicht zuletzt die USA, die bei diesen Ermittlungen geholfen haben. Einer der Gründe hierfür war, dass der Angriff auf den Bundestag im Frühjahr 2015 vielen in Washington als der Fall Nummer eins gilt, als der Moment, in dem Russland, mit dem was man heute hybride Kriegsführung nennt, in den großen westlichen Demokratien beginnt. In US-Geheimdienstkreisen war man lange davon überzeugt, dass Wladimir Putin sich nichts sehnlicher wünsche, als Angela Merkel loszuwerden - etwa durch Beeinflussungen von Wahlen.

Bald schon kontrollierten die Eindringlinge auch Administratoren-Accounts

Der Angriff auf den Bundestag, er begann am 30. April 2015. An diesem Tag warfen die Hacker ihren Köder aus - und die Opfer bissen zu. Mehrere Abgeordnete des Bundestages bekamen nahezu gleichzeitig eine E-Mail, deren Absenderadresse auf "@un.org" endete. Sie wirkte wie eine echte Mail der Vereinten Nationen, in der Betreffzeile stand: *"Ukraine conflict with Russia leaves economy in ruins".* In der E-Mail befand sich ein Link zu einer angeblichen UN-Webseite. Tatsächlich aber war die Seite mit einer Schadsoftware präpariert, die sich unbemerkt auf dem Computer installierte, sobald man sie anklickte.

Die Angreifer waren nun im Netz des Bundestages - damals umfasste es mehr als 5600 Computer, rund 12 000 Nutzer waren registriert. Schritt für Schritt arbeiteten sich die Hacker durch das Bundestagsnetz, sie nutzten mehrere Schadprogramme, darunter "Mimikatz", ein

mächtiges Werkzeug, mit dem umfangreich Passwörter abgegriffen werden können. Bald schon kontrollierten die Eindringlinge auch Administratoren-Accounts, mit denen sie noch weitere Zugriffsrechte bekamen.

Die Bundesanwaltschaft ist überzeugt, Dmitrij Badin nachweisen zu können, dass er nicht nur persönlich am Bundestagshack beteiligt gewesen war - sondern auch genau wann und wie. So soll Badin am 7. Mai 2015 um 13.29 Uhr eine Schadsoftware namens "VSC.exe" zunächst erstellt, und dann um 13.31 Uhr eingesetzt und gesteuert haben. Mit dem Programm sollen Zugangsdaten abgegriffen worden sein.

Erst am 11. Mai 2015, fast zwei Wochen nach Beginn des Angriffs, meldete sich ein IT-Sicherheitsunternehmen beim Bundesamt für Verfassungsschutz (BfV) mit einer deutlichen Warnung. Die Firma beobachtet weltweit verdächtige Server, über die schon öfter Cyberattacken gesteuert worden waren. Einer dieser Server kommunizierte nun plötzlich mit zwei Computern in Deutschland - und die befanden sich im Bundestag.

Die Verfassungsschützer informierten daraufhin das Bundesamt für die Sicherheit in der Informationstechnik (BSI) in Bonn. Beim BSI kümmert man sich um den Schutz der Regierungsnetze, das Parlament gehört eigentlich nicht zum Zuständigkeitsbereich. Dennoch schickte das BSI kurze Zeit später ein Team nach Berlin, um die Bundestagsverwaltung zu unterstützen.

Es war eine digitale Abwehrschlacht, wie sie Deutschland bis dato noch nicht erlebt hatte. Zwischenzeitlich wurde das gesamte IT-System des Bundestages heruntergefahren. Erst am 20. Mai 2015 war die Attacke beendet - mindestens 16 Gigabyte Daten sollen bis dahin abgeflossen sein, darunter Zigtausende E-Mails von Abgeordneten.

Der Angriff konnte gestoppt werden. Wer aber war verantwortlich für die Cyberattacke auf den Bundestag? Die Identifizierung der Angreifer, Fachleute sprechen von "Attribution", ist alles andere als einfach. Es sind oft private IT-Sicherheitsunternehmen, die Angriffsmethoden und die eingesetzte Schadsoftware analysieren - und sozusagen die Handschrift einzelner Hackergruppen identifizieren. Die besonders fähigen Angreifer, die immer wieder auftauchen, werden als *Advanced Persistent Threat*, kurz APT, bezeichnet, als "fortgeschrittene andauernde Bedrohung". Dahinter werden Staaten und deren Geheimdienste vermutet.

In wenigen Wochen verjährt der Angriff auf den Bundestag

Beim Bundestagshack fiel der Verdacht schnell auf APT28, eine Gruppe auch bekannt als "Fancy Bear", die es in der Vergangenheit immer wieder auf staatliche Ziele in mehreren Ländern abgesehen hatte. Sicherheitsbehörden gehen davon aus, dass dahinter die "Einheit 26165" des russischen Militärgeheimdienstes GRU steckt. Sie soll ihren Sitz am Komsomol-

Prospekt Hausnummer 20 in Moskau haben. In einem unscheinbaren Gebäude auf einem Militärgelände. Zu Sowjetzeiten residierte hier jene Einheit der GRU, die mit dem Entschlüsseln von Codes beauftragt war.

Während den Geheimdiensten oft die sogenannten "glaubhaften nachrichtendienstlichen Hinweise" genügen, benötigen die Strafverfolger gerichtsfeste Belege. Und so beauftragte die Bundesanwaltschaft das BKA mit den Ermittlungen zum Bundestagshack. Die Angreifer sollten identifiziert und die Beweise für den virtuellen Raubzug gefunden werden. Eine Herausforderung, wie sie auch das BKA bislang selten hatte. Die Ermittler beschafften sich zunächst die einzig verfügbaren Beweismittel, das waren Log-Files aus dem Bundestagssystem und Serverdaten. Dann arbeitete man sich voran.

Auch die Bundespolizei - deren Spezialisten in Heimerzheim bei Bonn schon früher den Agentenfunk abhörten - wurde hinzugezogen. Hilfreich waren die Dossiers privater Sicherheitsunternehmen und die Hilfe von ausländischen Behörden. Es wurden zudem Server überwacht, auf denen "Fancy Bear" ab und an immer noch aktiv war. Von großer Bedeutung für die BKA-Ermittlungen war zudem eine spektakuläre Aktion in den Niederlanden.

Im April 2018 hatte die niederländische Spionageabwehr eine Gruppe Russen auffliegen lassen, die wohl der GRU-Einheit "26165" alias "Fancy Bear" angehörten. Die vier Männer waren mit Diplomatenpässen nach Amsterdam gereist und dann mit einem Mietwagen nach Den Haag gefahren. Sie hatten es wohl auf ein auffälliges rundes Gebäude abgesehen - den Hauptsitz der Organisation für das Verbot chemischer Waffen (OPCW).

Wenige Wochen zuvor waren in Großbritannien der russische Ex-Spion Sergej Skripal und seine Tochter mit dem Nervengift Nowitschok vergiftet worden - die britische Regierung machte Moskau für das Attentat verantwortlich. Die OPCW war in die Aufklärung eingebunden worden, die Labors untersuchten das eingesetzte Gift. Niederländische Sicherheitsbehörden gehen davon aus, dass das russische Hackerteam den Auftrag hatte, sich in die Computer der OPCW einzuhacken und Informationen zu stehlen.

Am 13. April 2018 schritten die niederländischen Ermittler ein, zerrten die Russen aus dem Auto und verwiesen sie umgehend des Landes - aufgrund des Diplomatenstatus konnten sie nicht festgenommen werden. Ihr Gepäck - darunter Laptops, Mobiltelefone - allerdings wurde beschlagnahmt. Eine wahre Schatztruhe - auch für die Ermittler in Deutschland. Man habe durch das Material wertvolle Informationen über Moskaus Cyberspione bekommen, heißt es. Zur "GRU-Einheit 26165" - und zu Dmitrij Badin.

Die BKA-Ermittler präsentierten schließlich den Karlsruher Staatsanwälten das Ergebnis ihrer jahrelangen Arbeit. Man habe zwei russische Hacker identifiziert und könne ihnen die Beteiligung an Cyberangriffen in Deutschland nachweisen. Am Ende reichte es - jedenfalls erst einmal - nur für einen: Dmitrij Badin. Die Zeit drängte auch. In wenigen Wochen verjährt der Angriff auf den Bundestag.

Die Russische Botschaft in Berlin erklärte am Dienstag auf Anfrage, ihr ständen "keine offiziellen Dokumente, Informationen oder Anfragen" zu dem Fall zur Verfügung. "Zur Klärung solcher Fragen gibt es konkrete Kanäle, die der deutschen Seite gut bekannt sind." Die Botschaft kommentiere "Medienberichte, Gerüchte und Vermutungen" nicht.

ExklusivIT-Sicherheit

:Warum Deutschland im Netz so wehrlos ist
Die Sicherheitsbehörden anderer Länder gehen aktiv gegen Cyber-Angreifer vor, Deutschland zögert bislang. Jetzt könnte der BND die Lizenz zum "Hack back" bekommen.