Hack gegen Abgeordnete: Russische Gruppe »Ghostwriter« attackiert offenbar Parlamentarier

spiegel.de/politik/deutschland/russischer-hack-erneute-attacke-hack-auf-bundestag-sieben-abgeordnete-betroffen-a-75e1adbe-4462-4e30-bd94-96796aed6b8a

Angriffsziel Bundestag

Foto: Paul Zinken/ dpa

Der Bundestag ist erneut das Ziel von mutmaßlich russischen Hackern geworden. Nach SPIEGEL-Informationen wurden die Rechner von mindestens sieben Bundestagsabgeordneten angegriffen. Die Attacke der Gruppe namens »Ghostwriter« soll über sogenannte Phishing-E-Mails an die privaten Mailadressen der Politiker gelaufen sein, also Nachrichten von vermeintlich vertrauenswürdigen Absendern, deren Ziel es ist, den gesamten Account zu kapern.

Ob Daten abgeflossen sind, ist zurzeit noch unklar. Die angegriffenen Politiker gehören mehrheitlich den Regierungsparteien CDU/CSU und SPD an. Außerdem sind von der Attacke nach SPIEGEL-Informationen auch 31 Landtagsabgeordnete betroffen.

Sicherheitsexperten vermuten den russischen Militärgeheimdienst GRU hinter den Attacken. In Deutschland wurden laut Regierungskreisen neben Abgeordneten auch politische Aktivisten in Hamburg und Bremen angegriffen, insgesamt sollen einige Dutzend Personen betroffen sein.

Fake News über Schändung eines jüdischen Friedhofs

Die Gruppe hinter den Angriffen existiert schon länger, das US-Sicherheitsunternehmen FireEye hat sie »Ghostwriter« getauft. Laut IT-Experten war sie bislang als »Hack&Leak«-Organisation und vor allem für Desinformationskampagnen bekannt.

Wie FireEye im vergangenen Jahr berichtete , habe sich die Gruppe »Ghostwriter« auf das Produzieren von Falschnachrichten spezialisiert. Die Hacker verschafften sich demnach Zugang zu populären Nachrichtenseiten oder Blogs, um dort gefälschte Artikel oder Fotos zu veröffentlichen. So wurde in einer auf einer baltischen Seite platzierten Meldung am 25. September 2019 behauptet, deutsche Nato-Soldaten hätten einen jüdischen Friedhof in Litauen geschändet. Illustriert wurde der frei erfundene Vorfall mit einem manipulierten Foto.

In einer Nachricht vom 7. Juni 2018 hieß es fälschlicherweise, ein litauisches Kind sei von einem Nato-Panzer überfahren worden. Und bereits am 28. März 2017 wurde ein deutscher Bundeswehroffizier, der bei der Nato in Litauen stationiert war, in einer Meldung beschuldigt, ein russischer Spion zu sein. Auch gefälschte Schreiben und Zitate von Nato-Generalen verbreiteten die Hacker.

Laut FireEye läuft die Kampagne seit 2017 und hat sich zunächst vor allem an Leserinnen und Leser in Litauen, Lettland und Polen gerichtet, um Stimmung gegen die Nato zu schüren. Die Gruppe richte sich deutlich an russischen Sicherheitsinteressen aus, heißt es in einer Analyse des IT-Unternehmens. Sicherheitsbehörden vermuten deshalb dahinter den russischen Geheimdienst GRU.

Der militärische Nachrichtendienst steckte nach Überzeugung deutscher Sicherheitsbehörden auch hinter dem Angriff auf den Bundestag im Jahr 2015. Damals wurden mehrere Rechner attackiert, auch jene im Abgeordnetenbüro von Bundeskanzlerin Angela Merkel. Insgesamt flossen damals mehr als 16 Gigabyte Daten ab. Der Generalbundesanwalt erwirkte im vergangenen Jahr einen Haftbefehl gegen den russischen Hacker Dmtiri Badin. Er soll maßgeblich an dem Cyberangriff beteiligt gewesen sein und für den GRU arbeiten.

Wegen der neuen Angriffswelle haben das Bundesamt für Sicherheit in der Informationstechnik und das Bundesamt für Verfassungsschutz inzwischen ein Warnschreiben an potenzielle Opfer verschickt. Darin heißt es nach SPIEGEL-Informationen, dass die Betroffenen im Fokus einer gezielten Phishing-Attacke stünden.

Der Verfassungsschutz, so heißt es in dem Schreiben weiter, gehe von einem »nachrichtendienstlichen Hintergrund« aus. Die Angreifer versuchten gezielt, E-Mail-Konten zu übernehmen, um diese für »weitere Aktivitäten« zu nutzen. Betroffen seien aktuell E-Mail-Adressen bei den Anbietern GMX und T-Online. Die Angreifermails erweckten den falschen Eindruck, offizielle Warnmails der Provider zu sein.

fis, kno, mba, mgb, rom, wow