Cyberattacken Angriff der "Chaostruppe"

tagesschau.de/investigativ/wdr/hackerangriffe-105.html

tagesschau

Exklusiv

Stand: 31.03.2021 05:00 Uhr

Die Hackergruppe "Ghostwriter" hat deutsche Politiker im Visier. Ersten Analysen zufolge führt die Spur nach Russland. Die Sicherheitsbehörden sind besorgt, dass es zu gezielten Desinformationskampagnen im Bundestagswahlkampf kommen könnte.

Von Florian Flade, WDR, und Hakan Tanriverdi, BR

Es ist Montag, der 18. Januar, kurz nach 10 Uhr, als der Twitter-Account des polnischen Politikers Marek Suski plötzlich ungewöhnliche Mitteilungen absetzt. "Das Verhalten einiger Frauen ist inakzeptabel und überschreitet jegliche moralische Grenzen", stand in einem Tweet. Er werde von einer Frau sexuell belästigt und müsse sich nun wehren, damit dies endlich aufhöre. Es folgte ein Tweet mit drei Fotos. Darauf zu sehen war eine blonde Frau, ebenfalls Politikerin. Die Aufnahmen zeigen sie leicht bekleidet, teilweise nur in Unterwäsche und Nachthemd.

Zum Zeitpunkt, als die Bilder gepostet wurden, hatte Suski rund 12.000 Twitter-Follower. Die Tweets mit den freizügigen Fotos aber hatte der Politiker gar nicht selbst veröffentlicht. Es waren Hacker, die heimlich sein Nutzerkonto übernommen hatten. Sie sollen zuvor auch die Social-Media-Kanäle der Politikerin gehackt und sich wohl auch die Bilder von ihrem Handy verschafft haben.

Exklusiv 26.03.2021

Russland unter Verdacht Cyberangriff auf Politiker
Hacker sollen die privaten E-Mail-Konten von Politikern angegriffen haben.

Russischer Geheimdienst unter Verdacht

Die Hackergruppe, die mit den gefälschten Politiker-Tweets in Polen für Aufsehen sorgte, beschäftigt nun auch deutsche Sicherheitsbehörden. Denn sie soll auch hierzulande Politiker ins Visier genommen haben. In der vergangenen Woche wurde bekannt, dass das Bundesamt für Verfassungsschutz (BfV) und das Bundesamt für die Sicherheit in der Informationstechnik (BSI) derzeit vor Cyberangriffen der Hacker warnen - und davon ausgehen, dass der russische Militärgeheimdienst GRU hinter den Attacken stecken könnte.

Sieben Bundestags- und mehr als 30 Landtagsabgeordnete sollen kürzlich sogenannte "Phishing-Mails" erhalten haben. Das sind harmlos wirkende E-Mails, in denen oft ein Link zu einer Webseite eingefügt ist, auf der Nutzer aufgefordert werden, ihre Passwörter einzugeben. Der Verfassungsschutz hatte die Angriffswelle frühzeitig bemerkt und anschließend die betroffenen Personen informiert. Betroffen sein sollen fast nur CDU- und SPD-Abgeordnete. Die Zahl der Empfänger der verdächtigen E-Mails soll in den vergangenen Tagen weiter gestiegen sein.

BfV vermutet "nachrichtendienstlichen Hintergrund"

In einem Schreiben des BfV und des BSI, das *WDR* und *BR* vorliegt, warnen die Behörden Parlamentarier, "dass Ihre dienstliche und/oder private E-Mail-Adresse im Fokus einer gezielten Phishing-Kampagne stehen könnte". Weiter heißt es, der Verfassungsschutz gehe "von einem nachrichtendienstlichen Hintergrund aus". Es sei zudem davon auszugehen, dass möglicherweise gestohlene Daten für weitere Aktivitäten genutzt werden sollten. Etwa "für den Zugriff auf Ihre Benutzerkonten bei sozialen Netzwerken oder zur Verbreitung von Falschmeldungen".

05.05.2020

Cyberangriff auf Bundestag Haftbefehl gegen russischen Hacker
Vor fünf Jahren griffen Hacker das IT-System des Bundestags an.

Die Behörden nehmen den Fall sehr ernst - vor allem wegen des brisanten Zeitpunktes. Im September findet die Bundestagswahl statt, zudem stehen noch mehrere Landtagswahlen und eine Kommunalwahl an. In den Sicherheitsbehörden ist daher die Sorge groß, dass russische Geheimdienste versuchen könnten, gerade im Superwahljahr 2021 die politischen Prozesse in Deutschland zu beeinflussen oder massiv zu stören. In den USA und in Frankreich war es in der Vergangenheit zu solchen Aktionen durch mutmaßlich russische Hackergruppen gekommen.

Hintergrund 21.04.2017

Russlands Einfluss in Frankreich Keine Kampagne, aber eine Strategie
Die Sorgen über russischen Einfluss auf den französischen Wahlkampf waren groß, eine Kampagne blieb bisher aus.

In der vergangenen Woche sprach BfV-Präsident Thomas Haldenwang den aktuellen Vorfall im geheim tagenden Parlamentarischen Kontrollgremium des Bundestages an, das die Arbeit der Geheimdienste kontrolliert. Haldenwang soll erklärt haben, dass die

Sicherheitsbehörden den russischen Militärgeheimdienst GRU hinter der Attacke vermuten.

Mehr als 200 E-Mail-Adressen sollen die Hacker angegriffen haben und zwar fast ausschließlich Nutzerkonten bei den Anbietern GMX und T-Online. Längst nicht alle Empfänger seien Politiker, es gebe oft auch nur eine Namensgleichheit oder Namensähnlichkeit.

Orthografische Fehler in den E-Mails

In den E-Mails werden die Empfänger aufgefordert, zu beweisen, dass "Sie kein Spam-Bot sind". Sie sollen deshalb eine Webseite besuchen und dort Name und Passwort eingeben, ansonsten werde das Postfach "innerhalb von drei Tagen gesperrt". Die Mail erzeugt also Druck und ist angeblich von GMX verschickt. Sie enthält viele orthografische Fehler, da die Hacker anscheinend ein Programm verwendet haben, das Probleme mit deutschen Umlauten hatte. Statt "müssen" steht in der E-Mail zum Beispiel "mÃ¼ssen" und statt "verstoßen" steht da "verstoÃŸen". Das sind Fehler, die in echten E-Mails von GMX nicht auftauchen.

Die Cyberkampagne, die nun offenbar auch auf deutsche Abgeordnete abzielt, wurde im Juli 2020 erstmals von der IT-Sicherheitsfirma Fireeye beschrieben und als "Ghostwriter" bezeichnet. Die Hacker würden sich "an russischen Sicherheitsinteressen" orientieren, so heißt es in einem Dossier der Firma. Sie beobachtet die Hacker bereits seit März 2017, wie der IT-Sicherheitsexperte Benjamin Read erklärt. "Was diese Gruppe auszeichnet, ist die Art und Weise, wie sie Hacking mit Desinformationskampagnen verbinden." Die Hacker hätten in vielen Fällen seriöse Webseiten gehackt und erfundene Inhalte hochgeladen. Fireeye selbst macht keine Angaben darüber, ob die Gruppe im Auftrag eines Staates agiert.

08.05.2020

Cyberangriff auf den Bundestag Wie lief die Suche nach dem Hacker?
Abgeordnete wollen wissen, wie die Behörden den russischen Spion enttarnt haben.

Desinformation über NATO-Mission

"Bemerkenswert ist, dass dies die erste größere beobachtete Aktivität der Gruppe in West-Europa darstellt", heißt es in einem aktuellen Bericht des BSI zum Hackerangriff auf die Politiker in Deutschland. Kampagnen durch Ghostwriter seien in der Vergangenheit vor allem

in Litauen, Lettland und Polen beobachtet worden. Auf Anfrage teilt die Behörde mit, sie beobachte den laufenden Angriff der Hacker bereits seit "Mitte Februar 2021".

Im September 2019 sollen die Hacker auf einer Nachrichtenseite in Litauen eine Falschmeldung platziert haben: Bundeswehrsoldaten, die als Teil einer NATO-Mission in Litauen stationiert sind, hätten einen jüdischen Friedhof nahe der Stadt Kaunas geschändet. Dazu veröffentlichten die Hacker ein gefälschtes Foto, das angeblich den Friedhof zeigte. Es folgten weitere Falschmeldungen. Zum Beispiel über den angeblichen Truppenabzug der NATO, oder über ein litauisches Kind, das angeblich von einem NATO-Panzer überrollt worden sei.


16.06.2017

Bundeswehr in Litauen Wenig Resonanz auf Propaganda
Ende Januar erreichten die ersten Bundeswehr-Soldaten im Rahmen eines NATO-Einsatzes Litauen.

Fälschungen und Desinformation

Die Mission von "Ghostwriter" scheint es offenbar zu sein, durch gezielte Desinformation, durch Lügen und Fälschungen nicht nur Verwirrung zu stiften, sondern auch die öffentliche Meinung zu beeinflussen, Wut und Empörung auf bestimmte Ziele zu lenken. Diese Hacker seien, so heißt es im Verfassungsschutz, nicht nur Datendiebe, sondern eine "Chaostruppe". Die Hacker gingen zwar relativ plump und technisch wenig ausgereift vor, aber könnten dennoch enormen Schaden anrichten. Dass die Hacker gerade in einem Wahljahr versuchen, Abgeordnete zu hacken, wird deshalb besonders aufmerksam verfolgt.

Reporter des *WDR* und *BR* haben über eine Datenbank der IT-Sicherheitsfirma "Domaintools" 35 Webseiten gefunden, die allem Anschein nach von "Ghostwriter" angemeldet wurden. Auch Fireeye bringt diese Webseiten mit den Hackern von "Ghostwriter" in Verbindung, wie IT-Sicherheitsexperte Ben Read bestätigt.

Viele der Seiten haben einen Bezug zu Polen oder der Ukraine, aber es finden sich auch Hinweise auf das Vorgehen der Hacker in Deutschland. Eine der Seiten trägt zum Beispiel "credentials-telekom" im Namen. Auch hier geht es also um Anmelde-Informationen. Die Hacker stellten die Seite am 24. März ins Netz, also vergangene Woche. An den beiden Folgetagen sollten Nutzer dort ihre Anmeldeinformationen bestätigen. Seit Montag ist die Seite nicht mehr aktiv.

Hintergrund 25.06.2020

Desinformation in Osteuropa Deutschland im Zerrspiegel
Ob Merkel, Flüchtlingspolitik oder die AfD: Es gibt zahlreiche Falschnachrichten, die in osteuropäischen Medien verbreitet wurden.

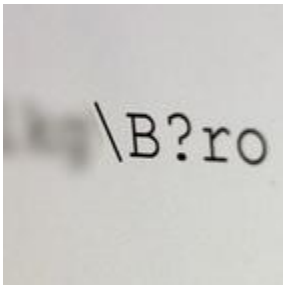
15.06.2021

Jetzt abonnieren tagesschau direkt auf Ihrem Messenger
Seien Sie immer auf dem Laufenden - mit dem Messenger-Angebot der tagesschau.

"Ghostwriter" Hackerangriff auf Politiker

Hakan Tanriverdi, BR, 31.3.2021 · 08:36 Uhr

Mehr zum Thema



08.05.2020 - 17:43 Uhr

Cyberangriff auf den Bundestag Die Sache mit dem "Ü"

Zurück zur Startseite Zurück