Internes Papier

Die Hackback-Pläne der Bundesregierung

Stand: 29.05.2019 12:38 Uhr

Vier Ministerien und das Kanzleramt stimmen Details zur Cyberabwehr ab. Im Falle eines schwerwiegenden Angriffs soll ein Gegenschlag möglich sein. Ein internes Papier zeigt, wie der Prozess ablaufen soll.

Von Hakan Tanriverdi, BR

Die Bundesregierung plant nach Informationen des *BR*, Cyberangriffe aktiv abzuwehren und dazu Server zu zerstören, über die die Angriffe laufen. Wie weit die Überlegungen mittlerweile fortgeschritten sind, ergibt sich aus einem internen "Konzeptpapier", das *BR Recherche* vorliegt. Dort wird der Abstimmungsprozess nach einem "erheblichen Cyber-Angriff aus dem Ausland" erstmals im Detail beschrieben.

Die Bundesregierung spricht von "aktiver Cyberabwehr", Kritiker von einem "Hackback". Mit dieser Wortwahl wollen sie deutlich machen, dass der Staat zurückschlägt.

Video: Bundesregierung plant Gegenangriffe bei Cyberattacken
tagesschau 16:00 Uhr, 29.05.2019, M. Stempfle/H. Tanriverdi, ARD Berlin

Papier beschreibt Vier-Stufen-Plan

Um Cyber-Angriffe abzuwehren, unterscheidet die Bundesregierung vier Stufen. In den ersten beiden Stufen "kann es erforderlich sein, Datenverkehre zu blockieren oder umzulenken", heißt es im Papier. Entweder werden dafür Telekommunikationsanbieter verpflichtet - zum Beispiel Telekom oder Vodafone - oder aber Polizeibehörden des Bundes werden selbst tätig. Diese beiden Stufen laufen ohne Eingriff in fremde Rechner und Server ab, von denen der Angriff ausgeht.

Für die dritte Stufe solle die zuständige Behörde das fremde Netzwerk hacken dürfen. "Hier kann es insbesondere erforderlich sein, Daten zu verändern oder Daten zu löschen", heißt es im Papier. So könne man das für den Cyber-Angriff verantwortliche Programm löschen.

Nach dem Bundestags-Hack im Jahr 2015 konnten Mitarbeiter des Bundesamtes für Verfassungsschutz ein größeres Datenpaket des Parlaments ausfindig machen. Es lag auf einem Server in Osteuropa. Gerne hätte man die Daten gelöscht - doch das wäre illegal. Zuerst berichteten SZ, *NDR* und *WDR* darüber.

Nach dem Bundestags-Hack hätten bereits Daten auf einem Server in Osteuropa vernichtet werden können. Doch das wäre illegal gewesen.

In der vierten Stufe geht es um "Maßnahmen, um auf die Funktionsfähigkeit des zum Angriff genutzten IT-Systems einzuwirken", zum Beispiel, indem man in die Systeme eindringt und sie herunterfährt.

Experten-
Gutachten

Staatliche Cyberangriffe verfassungswidrig

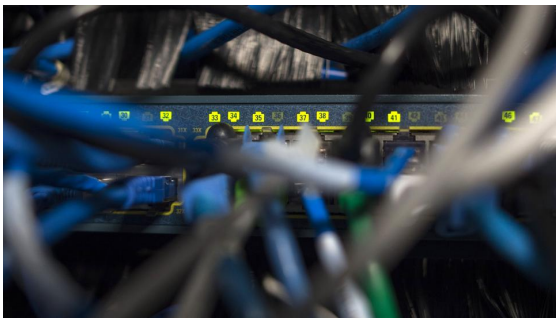
Bei Cyberangriffen wollen die Nachrichtendienste Gegenwehr leisten. Doch ein "Hackback" ist technisch komplex und juristisch heikel. Einem Gutachten zufolge müsste das Grundgesetz geändert werden. *Von Michael Götschenberg.* | mehr

Kritik: Eine übergreifende Strategie fehle

"Erstmal ist vollkommen verständlich, dass die Bundesregierung solch eine Fähigkeit haben möchte", sagt Isabel Skierka vom Digital Society Institute. Sie befasst sich dort mit der Rolle des Staates im digitalen Raum. Sie frage sich jedoch, was die Bundesregierung mit "Hackbacks" erreichen wolle: "Letztendlich müssen wir uns ja auch überlegen, wie sieht das denn real aus? Was kann man erreichen mit einem solchen Gegenangriff und wie würde man den Gegenangriff durchführen? Was mir hier fehlt, ist eine übergreifende Strategie."

Einvernehmliche Entscheidung erforderlich

In dem Papier werden solche Maßnahmen der aktiven Cyberabwehr "Computer Network Intervention" (CNI) genannt. Bevor es dazu kommen kann, soll laut Planungen ein Prozess durchlaufen werden.



Wenn ein "erheblicher Cyber-Angriff aus dem Ausland vorliegt", sollen die Maßanhmen greifen.

Im Cyber-Abwehrzentrum (Cyber-AZ) setzen sich schon heute Sicherheitsbehörden mit laufenden Hacker-Angriffen auseinander, darunter Bundesnachrichtendienst (BND), Bundesamt für Verfassungsschutz und Bundesamt für Sicherheit in der Informationstechnik (BSI).

In diesem Abwehrzentrum soll entschieden werden, ob "ein erheblicher Cyber-Angriff aus dem Ausland vorliegt", der sich gegen deutsche Infrastrukturen richtet und mit anderen zur Verfügung stehenden Mitteln nicht mehr abgewehrt werden kann.

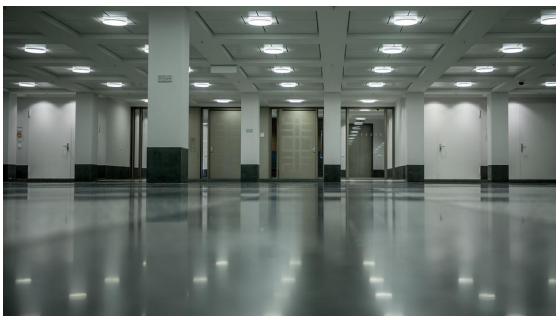
Löschpflicht, Gütesiegel und BSI-Stärkung

Nach den jüngsten Datendiebstählen hat das Innenministerium ein internes Eckpunktepapier verfasst, das dem *ARD-Hauptstadtstudio* vorliegt. Die Ideen sollen in ein IT-Sicherheitsgesetz münden. *Von Michael Stempfle.* | mehr

Die im Cyber-AZ vertretenen Behörden stimmen anschließend ab, ob eine derartige CNI-Maßnahme den Angriff schwächen oder beenden würde. Wird das bejaht, soll ein Gremium, in dem Kanzleramt, Auswärtiges Amt, Justiz-, Verteidigungs- und Innenministerium vertreten sind, "einvernehmlich" zu einem Urteil kommen. Erst nach diesem Schritt soll die aktive Cyberabwehr durchgeführt werden.

BND sei "geeignet" für diese Aufgabe

Das Papier argumentiert stark dafür, dass der BND diese Aufgabe übernehmen sollte. Schließlich verfüge dieser bereits heute über viele der notwendigen Kompetenzen. Der BND bewege sich unter anderem "in IT-Infrastrukturen im Ausland, sammelt konstant Informationen über Cyberangreifer, deren Vorgehen und Infrastrukturen" und werte diese detailliert aus. "Der BND ist somit für die Durchführung von CNI-Maßnahmen als direkten Anknüpfungspunkt zum bisherigen Auftrag auf Sicht der Praxis geeignet", heißt es im Papier. Für den Fall, dass eine Polizeibehörde die Aufgabe übernehmen sollte, müsste der BND "zwingend" mit einbezogen werden.



Geht es nach den Vorschlägen in dem Papier, soll der BND die Aufgabe übernehmen.

Grundgesetzänderung notwendig?

Für die aktive Cyberabwehr wäre wohl eine Grundgesetzänderung notwendig. Im Papier werden diverse Grundrechte genannt, die betroffen sein könnten: unter anderem das Grundrecht auf digitale Intimsphäre, die Unverletzlichkeit der Wohnung und das Fernmeldegeheimnis.

Notz sieht eine falsche Prioritätensetzung.

Der Bundestagsabgeordnete Konstantin von Notz von den Grünen kritisiert, dass die Regierung falsche Prioritäten setze. "Wir haben schon eklatante Schwächen bei der Frage der Verteidigung unserer Infrastruktur, dass diese ganzen Diskussionen und Überlegungen und Wolkenkuckucksheime in Richtung Cyberangriffe wirklich fehlgehen", sagt er im *BR*-Interview. "Die Hütte brennt lichterloh, aber nicht bei der Frage, ob wir selbst tolle Angreifer sind im Internet."

Das Konzept wird derzeit zwischen vier Ministerien und dem Kanzleramt abgestimmt. Die Federführung liegt beim Innenministerium. Dieses ließ eine *BR*-Anfrage unbeantwortet. Ein Regierungssprecher teilte mit, dass man zu regierungsinternen Abstimmungen keine Details mitteilen könne.

Im Juni wird sich die Regierung erneut mit dem Thema befassen, dann im geheim tagenden Bundessicherheitsrat.

Audio: Internes Papier der Bundesregierung skizziert Hackback-Pläne
Hakan Tanriverdi, BR
29.05.2019 14:41 Uhr

Über dieses Thema berichtete B5 aktuell am 29. Mai 2019 um 12:45 Uhr.

BSI warnt vor möglichen Cyberangriffen, 11.10.2018
Staatliche Cyberangriffe verfassungswidrig?, 16.06.2018
Hackback-Pläne der Bundesregierung, Hakan Tanriverdi, BR | audio
Nachrichtenatlas | Deutschland | Berlin