Deutscher Bundestag **Drucksache 19/5076**

19. Wahlperiode 17.10.2018

Kleine Anfrage

der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, Renata Alt, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg (Südpfalz), Britta Katharina Dassler, Bijan Djir-Sarai, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Reinhard Houben, Olaf in der Beek, Ulrich Lechte, Till Mansmann, Jimmy Schulz, Matthias Seestern-Pauly, Frank Sitta, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Katharina Willkomm und der Fraktion der FDP

Hackbacks als aktive digitale Gegenwehr

Die Debatte rund um die aktive Sicherung und Verteidigung digitaler Infrastrukturen im Cyberraum ist unter vielen Namen bekannt. Ob „digitaler Gegenangriff“, „digitaler Gegenschlag“, „aktive Cyberabwehr“, „finaler digitaler Rettungsschuss“ oder einfach nur „Hackback“. All diese Begriffe beschreiben die Suche nach Maßnahmen für die aktive, zivile und militärische Gegenwehr in einem Szenario eines Cyberangriffs auf deutsche Systeme (kritischer, staatlicher oder privater Natur). Der Terminus „Hackback“ soll in dieser Anfrage stellvertretend für alle verwendeten Termini in der Diskussion stehen.

Der Bundesminister des Innern, für Bau und Heimat Horst Seehofer wird in Medienberichten von August dieses Jahres mit den Worten zitiert, dass man in Bezug auf Cyberangriffe „nicht immer nur abwehren, sondern auch aktiv tätig werden“ müsse (u. a. www.sueddeutsche.de/digital/cyberkrieg-bundesregierung-1.4084810). Bereits 2017 äußerte sich der noch amtierende Verfassungsschutzpräsident Dr. Hans-Georg Maaßen Medienberichten zufolge mit folgenden Worten: „Wir halten es für notwendig, dass wir nicht nur rein defensiv tätig sind [...] Sondern wir müssen auch in der Lage sein, den Gegner anzugreifen, damit er aufhört, uns weiter zu attackieren“ (u. a. www.zeit.de/politik/deutschland/2017-01/cyberangriffe-verfassungsschutz-abwehrmassnahmen-gegenangriffe).

Die Wissenschaftlichen Dienste des Deutschen Bundestages haben in einer Ausarbeitung zum Thema Hackbacks auf ausländische Server (Ausarbeitung WD 3 - 3000 - 159/18) bereits festgestellt, dass die verfassungsrechtlichen Hürden für die Rechtfertigung von Hackbacks sehr hoch sind und nur durch eine Verfassungsänderung überhaupt erreicht werden könnten. Neben verschiedenen rechtlichen Fragen (völkerrechtlicher, verfassungsrechtlicher und sonstiger rechtlicher Natur) stellen sich auch grundsätzliche Kompetenzfragen. Welches Ressort, welche Behörde, welche Einheit ist zuständig für Hackbacks? Auch die Erweiterung von Kompetenzen oder die Schaffung neuer Zuständigkeiten wird debattiert.

Neben Kompetenzfragen und rechtlichen Erwägungen sind bei der Betrachtung von Cyberangriffen jedoch auch ganz praktische Fragen zu beachten, die wiederum für die rechtliche Bewertung von weitreichender Bedeutung sind. Etwa das Problem der Attribution oder auch die Betrachtung der Folgen von Gegenmaßnahmen. Die Erkennung eines geheimen Cyberangriffs an sich dauert im Schnitt schon etwa 150 bis 200 Tage. Wenn sich niemand zu der Attacke bekennt, bedarf es weiterer Zeit, um herauszufinden, woher die Attacke kam. Auch nachdem die Herkunft einer Attacke bekannt ist, ist die Attribution erst dann abgeschlossen, wenn klar ist, wer für den Cyberangriff verantwortlich war. Ähnliche Ausführungen ließen sich zu anderen praktischen Bereichen anführen.

Hackbacks waren teilweise bereits Gegenstand vergangener Kleiner Anfragen (z. B. Bundestagsdrucksachen 19/2009 und 19/2032). Wenn sich einzelne Fragen mit den in dieser Anfrage erfragten Informationen überschneiden, wird die Bundesregierung darum gebeten, explizit Fortschritte und neue Erkenntnisse im Rahmen der Prüfung von rechtlichen und technischen Möglichkeiten seit den Antworten (z. B. Bundestagsdrucksachen 19/2307 und 19/2645) auf die jeweiligen Fragen darzustellen.

Die Debatte um Hackbacks wirft insgesamt vielfältige rechtliche, technische, politische und ethische Probleme auf. Noch vor der Entscheidung, ob rechtliche Grundlagen geschaffen und technische Kapazitäten aufgebaut werden sollen, bedarf es demnach der Beantwortung einiger Fragen.

Wir fragen die Bundesregierung:

1. Welche rechtlichen Grundlagen hält die Bundesregierung bei der völkerrechtlichen, verfassungsrechtlichen und sonstigen rechtlichen Bewertung von Hackbacks für relevant?
2. Welche völkerrechtlichen, verfassungsrechtlichen oder sonstigen rechtlichen Vorschriften müssten nach Einschätzung der Bundesregierung geändert oder geschaffen werden, um Hackbacks zu ermöglichen?
3. Wären aus Sicht der Bundesregierung Hackbacks bei der Anwendung der bestehenden Rechtsgrundlagen auch heute schon möglich?

   Wenn ja, unter welchen Voraussetzungen?
4. Beabsichtigt die Bundesregierung, die Zuständigkeit für die Abwehr von Cyberangriffen grundsätzlich oder für einzelne Fälle auf die Bundesebene zu verlagern?

   Wenn nein, warum nicht?
5. Beabsichtigt die Bundesregierung im Hinblick auf Cyberangriffe, die Befugnisse und Zuständigkeiten zum Schutz ziviler Infrastrukturen zu erweitern?

   Wenn ja, inwiefern und an welcher Stelle?
6. Welche Fragen und Annahmen leiten die Bundesregierung bei der technischen, ethischen und politischen Bewertung von Hackbacks?
7. Welche Bundesministerien beschäftigen sich derzeit mit der Entwicklung eines Konzepts und konkreten gesetzgeberischen Maßnahmen zum Thema Hackback?

   Welche Abteilung ist jeweils für die Entwicklung zuständig?
8. Auf welcher Grundlage beschäftigt sich das Bundesministerium des Innern, für Bau und Heimat mit dem Thema Hackback?
9. Welches Bundesministerium und welche Behörde unterhalb des jeweiligen Bundesministeriums sind für den Aufbau technischer Kapazitäten für Hackbacks momentan zuständig?

10. Wäre aus Sicht der Bundesregierung eine ausreichende technische Ausstattung und Expertise zur Durchführung von Hackbacks bereits zum jetzigen Zeitpunkt gegeben?

    Welche Behörde oder Institution wäre aus Sicht der Bundesregierung hierzu bereits zum jetzigen Zeitpunkt technisch in der Lage?

11. Welche der in Frage kommenden Behörden oder Institutionen (namentlich BND – Bundesnachrichtendienst, BfV – Bundesamt für Verfassungsschutz, BKA – Bundeskriminalamt, BSI – Bundesamt für Sicherheit in der Informationstechnik, Zitis – Zentrale Stelle für Informationstechnik im Sicherheitsbereich, Bundeswehr) wäre bei Bestehen der notwendigen Rechtsgrundlagen nach Ansicht der Bundesregierung für die Durchführung von Hackbacks zuständig?

    Welche weiteren Behörden oder Institutionen kommen für die Bundesregierung in Betracht?

12. Wie beurteilt die Bundesregierung beim Thema Hackback das Trennungsgebot zwischen polizeilicher und geheimdienstlicher Tätigkeit?

    Wie wird dies von der Bundesregierung konkret berücksichtigt?

13. Welche der folgenden Ziele verfolgt die Bundesregierung mit dem Aufbau rechtlicher Grundlagen und technischer Kapazitäten für Hackbacks als Gegenmaßnahme zu Cyberangriffen (und warum):

    a) Prävention von Angriffen

    b) Schutz von Systemen

    c) Aufklärung von Cyberangriffen

    d) Übernahme und Infiltration der Angreifer-Infrastruktur

    e) Sonstige Reaktion auf Cyberangriffe (z. B. Rückerlangung von Informationen, Zerstörung von Angreifer-Infrastrukturen)?

    Welche darüberhinausgehenden Ziele verfolgt die Bundesregierung, und warum?

14. Für welche konkreten Szenarien eines Cyberangriffs werden in der Bundesregierung Gegenmaßnahmen diskutiert:

    a) Angriff auf staatliche Systeme und Infrastrukturen

    b) Angriff auf kritische Infrastrukturen

    c) Angriff auf sonstige private Systeme und Infrastrukturen

    d) Angriff unter Verwendung ausländischer Server oder Systeme

    e) Geheime Angriffe beziehungsweise angekündigte Angriffe?

15. Welche Maßnahmen werden für die unterschiedlichen Stadien beziehungsweise Zeitpunkte eines Cyberangriffs in der Bundesregierung konkret diskutiert

    a) im Vorfeld eines Cyberangriffs,

    b) während eines Cyberangriffs bzw.

    c) nach dem Abschluss eines Cyberangriffs?

16. Welche Alternativen zu Hackbacks zieht die Bundesregierung in Bezug auf die konkreten Szenarien und Stadien bzw. Zeitpunkte eines Cyberangriffs (s. Fragen 14 und 15) in Betracht?

17. Für wie wirkungsvoll hält die Bundesregierung passive Verteidigungs- und Sicherungsmaßnahmen, etwa die Stärkung der IT-Sicherheit?

    Welche defensiven Möglichkeiten der Cyberabwehr und der Cyberresilienz hält die Bundesregierung für wirksam?

18. Wie beurteilt die Bundesregierung das Problem der Attribution eines Angriffs in Bezug auf die konkreten Szenarien und Stadien bzw. Zeitpunkte eines Cyberangriffs?

    Wie beurteilt die Bundesregierung das Problem der Attribution in Bezug auf das völkerrechtliche Recht auf Selbstverteidigung?

    Wie schätzt die Bundesregierung generell die Möglichkeit einer zeitnahen Attribution von Angriffen ein?

    Wie soll nach Ansicht der Bundesregierung mit Zweifelsfällen umgegangen werden?

19. Wie beurteilt die Bundesregierung die Möglichkeit von Hackbacks für den Fall, dass die Angreifer

    a) Server von Unbeteiligten für ihren Angriff verwenden,

    b) Kritische Infrastrukturen für ihren Angriff verwenden bzw.

    c) Szenario a) oder b) aus dem Ausland heraus oder mithilfe ausländischer Infrastruktur durchführen?

20. Welche Rolle spielen bei den Überlegungen der Bundesregierung zu Hackbacks auf ausländischem Territorium Mittel der internationalen Amtshilfe bzw. Zusammenarbeit oder Rechtshilfeersuchen?

21. Wie soll die Nutzung von Hackbacks international bilateral oder multilateral abgestimmt werden?

    Bei welcher Gelegenheit gedenkt die Bundesregierung, eine solche Abstimmung voranzutreiben?

22. Wie schätzt die Bundesregierung die Wahrscheinlichkeit ein, dass Gegenangriffe auf im Ausland stehende Server oder Infrastrukturen als militärischer Angriff angesehen werden?

    Wie schätzt die Bundesregierung in diesem Zusammenhang die Möglichkeit der Eskalation von Cyberabwehrangriffen ein?

23. Plant die Bundesregierung die Einführung von Verpflichtungen für nichtstaatliche Akteure, bei der Abwehr von Cyberangriffen mit den durchführenden Sicherheitsbehörden zu kooperieren?

    Was sollen solche Kooperationsverpflichtungen umfassen?

Berlin, den 10. Oktober 2018

Christian Lindner und Fraktion

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333