Deutscher Bundestag **Drucksache 20/2079**

20. Wahlperiode 01.06.2022

Antrag

der Abgeordneten Anke Domscheit-Berg, Martina Renner, Nicole Gohlke, Gökay Akbulut, Clara Bünger, Dr. André Hahn, Jan Korte, Ina Latendorf, Petra Pau, Sören Pellmann, Dr. Petra Sitte und der Fraktion DIE LINKE.

Ausnutzung von IT-Sicherheitslücken durch Bundesbehörden verbieten

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die gesamtgesellschaftliche Bedeutung der IT-Sicherheit nimmt seit Jahrzehnten zu und auch im Zuge des aktuellen Krieges Russlands gegen die Ukraine werden wieder Forderungen nach sog. Hackbacks, d. h. digitalen Gegenschlägen nach einem Cyber- oder Hackerangriff, bzw. nach aktiver Cyberabwehr laut. Dabei wird häufig unterschlagen, dass für solche Maßnahmen bewusst Hintertüren in IT-Systeme eingebaut oder bekanntgewordene Sicherheitslücken absichtlich zurückgehalten werden müssen.

Auch hierzulande greifen Behörden, u. a. mittels sog. „Staatstrojaner“, auf fremde Informationssysteme und Daten zu, um Aufträge zu erfüllen. Für einen erfolgreichen Zugriff sind die für diesen Zweck beschafften oder entwickelten Software-Anwendungen jedoch auf die Ausnutzung von Schwachstellen in der anzugreifenden Software angewiesen. Dabei wird der Eindruck aufrechterhalten, dass die dadurch gewonnenen Informationen exklusiv kontrolliert werden können. Das größte Risiko besteht jedoch in der Gefährdung weiterer, auch eigener Systeme, die die gleiche Sicherheitslücke aufweisen.

Dabei stellen diese Anwendungen nicht nur einen unverhältnismäßigen Eingriff in das IT-Grundrecht der Betroffenen dar. Das bewusste Offenhalten von IT-Sicherheitslücken durch Sicherheitsbehörden gefährdet auch die IT-Sicherheit aller. Denn diese Sicherheitslücken können auch von Geheimdiensten oder Kriminellen ausgenutzt werden: ein erhebliches Risiko für Verbraucher*innen, Unternehmen und im Übrigen auch die Politik. Auch im Lagebericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit 2021 (siehe https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-cybersicherheit-2021.pdf?__blob=publicationFile&v=3) wurde deutlich auf die Risiken durch Sicherheitslücken hingewiesen – ohne jedoch die Handhabung durch die deutschen Sicherheitsbehörden zu problematisieren. Welche Gefahren entstehen, wenn staatliche Stellen Sicherheitslücken bewusst offen halten, zeigt der Fall „EternalBlue“. Der amerikanischen National Security Agency (NSA) war diese Schwachstelle jahrelang bekannt gewesen und sie hatte diese bewusst ausgenutzt, bevor sie 2017 durch die Gruppierung „Shadow Brokers“ publik gemacht wurde. Später wurde bekannt, dass u. a. die Trojaner WannaCry und NotPetya diese Hintertür für Angriffe ausnutzten und weltweit enorme Schäden verursachten. Offene Sicherheitslücken gefährden

kritische Infrastrukturen (KRITIS) erheblich und das absichtliche Offenhalten von Sicherheitslücken ist daher niemals verhältnismäßig. Der Schaden durch offen gehaltene Sicherheitslücken kann um ein Vielfaches über dem erwarteten Nutzen durch derartige Überwachungsmaßnahmen liegen. Besonders hoch sind die Gefahren von Kollateralschäden bei der „aktiven Cyberabwehr", da es sich hierbei um Angriffe auf IT-Systeme im Ausland handelt. Ob ein Cyberangriff ursprünglich genau von dort kam, ist fast nie sicher feststellbar. Eine Schädigung ziviler Infrastrukturen in einem Drittstaat kann nicht ausgeschlossen werden, wäre jedoch ein klarer Verstoß gegen das Völkerrecht. Die NATO hat zudem festgestellt, dass staatliche Angriffe im Cyberraum als militärische Angriffe gewertet werden können. Insofern kann ein Hackback deutscher Behörden gegen ausländische IT-Systeme auch als militärischer Angriff eines NATO-Staates gegen einen Drittstaat interpretiert werden und zur Eskalation führen.

Für Sicherheitsbehörden darf es deshalb, auch unter Berücksichtigung ihrer Ermittlungs- und Aufklärungsarbeit, keinerlei Ausnahmen geben. Erkannte Sicherheitslücken in IT-Systemen und -Produkten müssen konsequent und schnellstmöglich gemeldet sowie geschlossen werden. Das ist gleichzeitig effektive Prävention und trägt zum Schutz unserer kritischen Infrastrukturen vor Cyberangriffen durch Kriminelle oder ausländische staatliche Akteure bei.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

einen Gesetzentwurf vorzulegen, der es den deutschen Bundesbehörden konsequent verbietet, Sicherheitslücken in IT-Systemen auszunutzen.

Berlin, den 30. Mai 2022

Amira Mohamed Ali, Dr. Dietmar Bartsch und Fraktion

Begründung

Hackbacks und aktive Cyberabwehr bedeuten, dass Sicherheitslücken offen gehalten werden, um bei Bedarf auf andere Geräte und IT-Systeme zugreifen zu können. Solange bekannte Sicherheitslücken nicht geschlossen werden, können sie von allen ausgenutzt werden, denen sie bekannt sind. Das bedeutet eine erhebliche Gefährdung der IT-Sicherheit für alle Nutzer*innen der entsprechenden Software und verletzt damit in völlig unverhältnismäßiger Weise das IT-Grundrecht all dieser Nutzer*innen. Plausible Darlegungen über die zu erwartenden positiven Effekte einer Offenhaltung von Sicherheitslücken fehlen bislang.

Nach Auffassung der Antragstellenden strebt die Bundesregierung in ihrem Koalitionsvertrag zwar eine Abgrenzung zur IT-Sicherheitspolitik der Vorgängerregierung an, indem sie weitere Meldepflichten und ein Schwachstellenmanagement plant. Gerade deswegen ist es wenig nachvollziehbar, dass die Koalition einerseits feststellt, die Ausnutzung von Schwachstellen von IT-Systemen münde in ein Spannungsverhältnis zwischen IT-Sicherheit und Bürgerrechten, andererseits aber nur den Ankauf und das Offenhalten von Sicherheitslücken verbieten möchte – nicht aber das Ausnutzen von solchen Lücken, die den Sicherheitsbehörden auf anderem Weg bekannt werden (siehe dazu https://www.bundesregierung.de/resource/blob/974430/1990812/04221173eef9a6720059cc353d759a2b/2021-12-10-koav2021-data.pdf?download=1, S. 109). Ein konkretes Verbot, Sicherheitslücken auszunutzen, ist nicht vorgesehen. Damit wäre es den Sicherheitsbehörden weiterhin gestattet, z. B. auch während eines Meldeprozesses sog. Zero-Day-Schwachstellen auszunutzen. Solche Meldeprozesse können durchaus langwierig und herausfordernd sein, insbesondere wenn internationale Unternehmen ohne Kontaktstellen, ganze Lieferketten oder Vertriebseinheiten für das Schließen der Sicherheitslücken verantwortlich sind. Daher ist es umso notwendiger, dass Bundesbehörden Sicherheitslücken in IT-Systemen nicht länger ausnutzen dürfen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.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.bundesanzeiger-verlag.de
ISSN 0722-8333