Deutscher Bundestag **Drucksache 19/12974**

19. Wahlperiode 03.09.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Dr. Petra Sitte, Doris Achelwilm, weiterer Abgeordneter und der Fraktion DIE LINKE.
– Drucksache 19/12456 –

Erkenntnisse nach den „Prominenten-Doxing“-Fällen im Januar 2019

Vorbemerkung der Fragesteller

Vom 1. bis zum 28. Dezember 2018 wurden über die Plattform Twitter persönliche Daten von knapp 1 000 Politikerinnen und Politikern und weiteren Prominenten veröffentlicht. Dieses Vorgehen wurde als „Adventskalender“ bekannt, da jeden Tag neue Informationen veröffentlicht wurden (www.heise.de/newsticker/meldung/Politiker-und-Promi-Hack-Ehemaliges-Twitter-Konto-eines-YouTubers-missbraucht-42608.html). Die Daten wurden darüber hinaus auf zahlreichen Spiegelservern abgelegt, was die Löschung erheblich erschwerte (https://twitter.com/thegrugq/status/1081191019993915392).

Durch einen Tweet des selbst betroffenen YouTubers Unge und einen Bericht des Senders RBB am 4. Januar 2019 wurden die auch als „Doxing“ bezeichneten Veröffentlichungen von persönlichen Daten einer breiten Öffentlichkeit bekannt. Zwei Tage später wurde ein Verdächtiger ermittelt und festgenommen.

In vielen Fällen waren öffentlich bereits verfügbare Informationen wie Büroadressen, Telefonnummern oder Mailadressen zusammengetragen worden, in anderen wurden aber auch tatsächlich private Informationen wie Wohnadressen, Fotos oder Inhalte von Chats veröffentlicht.

Bereits vor Dezember 2018, nämlich mindestens seit dem Juli 2017, wurden über den Twitter-Account des Täters persönliche Daten veröffentlicht, u. a. die des Satirikers Jan Böhmermann (www.donaukurier.de/nachrichten/top news/inland/art388865,4037598).

Der Bundesregierung und den Sicherheitsbehörden waren die Doxingfälle nach eigener Aussage vor Januar 2019 nicht bekannt.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 30. August 2019 übermittelt.

Die Drucksache enthält – in kleinerer Schrifttype – den Fragetext.

Vorbemerkung der Bundesregierung

Dem Ermittlungsverfahren der Generalstaatsanwaltschaft Frankfurt a. M., Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT), Az. 60 Js 17/19, gegen den Beschuldigten wegen des Verdachts des Ausspähens von Daten, Verstoßes gegen das Bundesdatenschutzgesetz und andere Delikte, liegt die im Rahmen eines sogenannten „Adventskalenders“ im Dezember 2018 erfolgte Veröffentlichung persönlicher Daten von Personen des öffentlichen Lebens (Prominente, Politikerinnen und Politiker) zugrunde. Das Ermittlungsverfahren ist noch nicht beendet.

Trotz der grundsätzlichen verfassungsrechtlichen Pflicht der Bundesregierung, Informationsansprüche des Deutschen Bundestages zu erfüllen, tritt hier nach konkreter Abwägung der betroffenen Belange das Informationsinteresse des Parlaments hinter den berechtigten Geheimhaltungsinteressen zurück. Das Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege leitet sich aus dem Rechtsstaatsprinzip ab und hat damit ebenfalls Verfassungsrang. Die gewünschte Auskunft würde weitergehende Ermittlungsmaßnahmen erschweren oder gar vereiteln, weshalb aus dem Prinzip der Rechtsstaatlichkeit folgt, dass vorliegend das betroffene Interesse der Allgemeinheit an der Gewährleistung einer funktionstüchtigen Strafrechtspflege und Strafverfolgung (vgl. dazu BVerfGE 51, 324 (343 f.)) Vorrang vor dem Informationsinteresse hat.

Im Übrigen wird auf die gemeinsame Pressekonferenz von ZIT und BKA vom 8. Januar 2019 verwiesen.

1. Wie viele Personen waren nach Kenntnis der Bundesregierung insgesamt von diesen Doxing-Fällen betroffen?

2. Wie viele Personen waren direkt und wie viele waren mittelbar betroffen?

3. Fanden im Rahmen der Ermittlungen nach Kenntnis der Bundesregierung Durchsuchungen statt (bitte unter Nennung von Daten, beteiligter Behörden und ggf. sichergestellten Asservaten beantworten)?

4. Wurden nach Kenntnis der Bundesregierung im Rahmen der Ermittlungen nachrichtendienstliche Mittel angewandt, und wenn ja, welche, in welchem Zeitraum, und von welchen Behörden (bitte jeweils detailliert ausführen)?

5. Verfügt die Bundesregierung über Erkenntnisse über politische Neigungen oder politische Motive des Täters oder der Täterinnen und Täter (bitte jeweils detailliert ausführen)?

6. Wie ist der Täter oder sind die Täterinnen und Täter nach Kenntnis der Bundesregierung vorgegangen, um die dann veröffentlichten Daten zu erhalten (bitte Methoden und Häufigkeit je einzeln aufschlüsseln)?

7. Sind dabei nach Kenntnis der Bundesregierung Methoden des Social Engineering angewandt worden, und wenn ja, welche, und wie häufig (bitte einzeln aufschlüsseln)?

8. In wie viele Accounts von wie vielen Personen wurde nach Kenntnis der Bundesregierung von den Täterinnen und Tätern eingebrochen, also in wie vielen Fällen wurden Accounts tatsächlich gehackt?

9. Wie viele Ermittlungsverfahren gegen wie viele Personen wurden nach Kenntnis der Bundesregierung in der Folge eingeleitet (bitte nach Straftatbeständen und ermittelnder Behörde aufschlüsseln)?

10. Wurde das Bundesamt für Verfassungsschutz zu irgendeinem Zeitpunkt in die Ermittlungen einbezogen oder spielte sonst irgendeine Rolle in der Bewertung oder Ermittlung?

    Wenn ja, welche?

Die Fragen 1 bis 10 werden gemeinsam beantwortet.

Es wird auf die Vorbemerkung der Bundesregierung verwiesen.

11. Welche weiteren Fälle von Doxing sind der Bundesregierung bekannt?

    a) Wie viele Fälle von Politikerinnen und Politikern oder anderen in der Öffentlichkeit stehenden Personen sind darunter?

    b) Wie viele Fälle sind der Bundesregierung bekannt, in denen Gruppen von Menschen oder sonst jeweils größere Zahlen von Menschen betroffen waren?

Die Bundesregierung hält keine Daten vor, die eine Beantwortung im Sinne der Fragestellung ermöglichen.

12. Ist der Bundesregierung der Fall von 200 Namen und Adressen bekannt, die Anfang Januar 2019 bei Indymedia veröffentlicht wurden, darunter Journalisten, Politiker und Künstler, und hat es hierzu nach Kenntnis der Bundesregierung insbesondere strafrechtliche Ermittlungen gegeben, und wenn ja, mit welchem Ergebnis (www.neues-deutschland.de/artikel/1109331.indymedia-rechte-drohliste-auf-linkes-portal-geschmuggelt.html)?

Der Bundesregierung ist die im Januar 2019 bei Indymedia unter dem Begriff „#WirKriegenEuchAllee“ (Fehler im Original) veröffentlichte Datensammlung bekannt. Inzwischen sind die Beiträge nicht mehr abrufbar.

Das BKA führt diesbezüglich keine Ermittlungen. Über Ermittlungen der Länder liegen der Bundesregierung keine Informationen vor.

13. Welche konkreten Maßnahmen zum Schutz von betroffenen Politikerinnen und Politikern, Prominenten und anderen Nutzerinnen und Nutzern hat die Bundesregierung seit dem Bekanntwerden der Vorfälle im Januar 2019 ergriffen?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist für die Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes zuständig (§ 3 Absatz 1 Satz 2 Nummer 1 des BSI-Gesetzes – BSIG). Im genannten „Doxing“-Vorfall waren Informationstechnik und Daten außerhalb der Regierungsnetze betroffen.

Das BSI kann in solchen Fällen Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen beraten (§ 3 Absatz 1 Satz 2 Nummer 14 BSIG).

Entsprechende Beratungen hat das BSI mit großem personellen Einsatz durchgeführt.

Über das Informations- und Beratungsangebot „BSI für Bürger“ (www.bsi-fuer-buerger.de), das als Zielgruppe Privatanwenderinnen und -anwender hat, richtete das BSI nach dem „Doxing“-Vorfall ein Angebot zur Kontaktaufnahme an alle Betroffenen des Vorfalls, sodass die Inanspruchnahme einer Beratung durch das BSI für alle betroffenen Personen möglich war. Zudem wurden auf dieser Webseite Handlungsempfehlungen für Betroffene veröffentlicht, die unter anderem eine Anleitung zum Vorgehen beim Zurücksetzen von Passwörtern und Hinweise zu weiteren Maßnahmen zum Schutz persönlicher Daten enthielten (www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/Hilfe/Hilfe_Betroffene_node.html). In den folgenden Wochen und Monaten nach Bekanntwerden des „Doxing“-Vorfalls wurden weitere Sensibilisierungsmaßnahmen für Bürgerinnen und Bürger ergriffen, wie z. B. der Versand eines themenbezogenen Sonder-Newsletters, Sensibilisierungsmaßnahmen in sozialen Medien (u. a. Bereitstellung von Videos, Grafiken und Hinweise zu den Themen „Passwort“ und „Zwei-Faktor-Authentisierung“) und eine Beilage in einer überregionalen Zeitung. Weitere Sensibilisierungsmaßnahmen sind geplant. So wird das BSI z. B. den europäischen Aktionsmonat zur Cyber-Sicherheit (European Cyber Security Month – ECSM) im Oktober 2019 zur Bürgersensibilisierung nutzen. Im Mittelpunkt wird dabei das Thema „Hilfe zur Selbsthilfe“ stehen, wobei sich die vorgestellten Maßnahmen unter anderem auf das Thema „Doxing“ beziehen werden.

Für betroffene Mitglieder des Deutschen Bundestages fanden unter anderem Einzelberatungen vor Ort gemeinsam mit BSI und BKA statt. Auch für diese Zielgruppe hat das BSI Handlungsempfehlungen erarbeitet und zur Verfügung gestellt. Seit Anfang Mai 2019 versendet das BSI auch Warnmeldungen an die Fraktionen des Deutschen Bundestages.

Um die Situation Betroffener besser nachvollziehen zu können und möglichen weiteren Handlungsbedarf zu eruieren, fanden – losgelöst vom konkreten Vorfall im Dezember 2018 – im Bundesministerium der Justiz und für Verbraucherschutz Gespräche mit Personen statt, die Opfer von „Doxing“ wurden oder über Erfahrungen mit „Doxing-Fällen“ berichten können.

Maßnahmen der allgemeinen Gefahrenabwehr zum Schutz von Politikerinnen und Politikern, Prominenten und anderen Nutzerinnen und Nutzern fallen nach der Kompetenzordnung des Grundgesetzes grundsätzlich in die Zuständigkeit der Bundesländer und richten sich nach den jeweiligen Polizeigesetzen.

Durch die Abteilung Sicherungsgruppe des BKA wurden alle von der „Adventskalender“-Veröffentlichung betroffenen „§ 6-BKAG-Personen“ (Mitglieder der Verfassungsorgane des Bundes) über die Tatsache der Nennung ihrer Namen und den Umfang der zu ihrer Person veröffentlichten Daten in Kenntnis gesetzt. Darüber hinaus erfolgten eine individuelle Gefährdungsanalyse sowie das Angebot eines Sicherheitsgespräches (insbesondere in Bezug auf Gefahren in Zusammenhang mit der Nutzung informationstechnischer Systeme) an diesen Personenkreis.

14. In welcher Weise beschäftigt sich das Bundesamt für Sicherheit in der Informationstechnik mit dem Thema „Doxing“, und wurden seit den Vorfällen im Januar 2019 neue oder ergänzende Maßnahmen festgelegt oder geplant, gegebenenfalls welche (bitte jeweils detailliert ausführen)?

Das BSI beschäftigt sich mit dem Thema Doxing im Rahmen seiner Zuständigkeit für Beratungen und Warnungen in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen. In diesem Zusammenhang werden fortlaufend umfangreiche Handlungsempfehlungen und Informationen für An-

wenderinnen und Anwender u. a. zur sicheren Nutzung von Social-Media- und E-Mail-Accounts erarbeitet und der Öffentlichkeit zur Verfügung gestellt.

Zudem wird von BSI und BMI gemeinsam eine nationale Informations- und Sensibilisierungskampagne geplant und beginnend ab 2020 umgesetzt.

Im Übrigen wird auf die Antwort zu Frage 13 verwiesen.

15. Fokussieren sich die genannten Maßnahmen zum „Doxing“ auf im weitesten Sinne Personen des öffentlichen Lebens, und wie wird der Schutz weniger prominenter Nutzerinnen und Nutzer dabei berücksichtigt?

Die Maßnahmen des BSI im Zusammenhang mit dem Phänomen Doxing richten sich grundsätzlich an alle Betroffenen. Das Informations- und Beratungsangebot „BSI für Bürger“ hat dabei insbesondere Privatanwenderinnen und -anwender als Zielgruppe definiert.

16. Definiert die Bundesregierung Doxing als Cybercrime, bzw. unter welchen Umständen definiert sie Doxing als Cybercrime?

Nach der auch vom Bundeskriminalamt verwendeten Definition handelt es sich bei Cybercrime um Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden.

Unter Cybercrime im engeren Sinne fällt „Doxing“, wenn die unberechtigt öffentlich zugänglich gemachten Daten durch Taten erlangt werden, welche sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten, wie beispielsweise durch das Ausspähen von Daten nach § 202a des Strafgesetzbuchs (StGB), durch Datenhehlerei (§ 202d StGB), durch Datenveränderung (§ 303a StGB) oder durch Computersabotage (§ 303b StGB).

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.betrifft-gesetze.de
ISSN 0722-8333