Deutscher Bundestag **Drucksache 19/17546**

19. Wahlperiode 04.03.2020

Kleine Anfrage

der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller und der Fraktion der AfD

Umsetzung der Digitalisierung der Justiz und Cyberangriffe auf Kammergerichte und Oberlandesgerichte

Im Rahmen der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ wurde in der März-2019-Version der Strategie erstmals die Maßnahme „Digitalisierung der Justiz voranbringen“ angekündigt (https://www.bildung-forschung.digital/files/pdf-umsetzungsstrategie-digitalisierung-data.pdf, S. 167). Darin werden als Ziele der „medienbruchfreie Austausch zwischen Polizei und Staatsanwaltschaft von Bund und Ländern“ sowie die „Interoperabilität mit den Gerichten“ definiert. Diese Ziele sollen durch die Schaffung einer, in dem „Pakt für den Rechtsstaat“ vereinbarten „Kommunikationsschnittstelle“ erreicht werden (ebd.).

Ende Januar 2020 wurde der Umfang der Cyberattacke auf das Berliner Kammergericht seit September 2019 bekannt, die zu einem vollständigen Abfluss von Zeugennamen oder von Informationen über verdeckte Ermittler in Terror- und Staatsschutzverfahren geführt haben kann (http://prarchiv.bundestag.btg/PressDok/docview.html;sessionid=6E7773F893E57441D425EDE0?mode=pressarchive&doclist=DBT:PressArchiveResultServlet:result_doclist&n=61&pdf=0).

Nach Auffassung der Fragesteller bestehen durch die beabsichtigte Vernetzung von Polizei, Gerichten und Staatsanwaltschaften von Bund und Ländern erhebliche Gefährdungen für die Funktionsfähigkeit der Justiz und für die Geheimhaltung und Integrität von Prozessdaten im Bereich der organisierten Kriminalität, des internationalen Terrorismus oder anderer schwerer staatsgefährdender Delikte, wenn nicht zuvor ein hinreichendes Maß an IT-Sicherheit insbesondere in den beteiligten Landeseinrichtungen hergestellt wurde.

Wir fragen die Bundesregierung:

1. Aus welchem Grund wurde in der ersten Fassung der Umsetzungsstrategie „Digitalisierung gestalten“ von November 2018 (https://www.bundesfinanzministerium.de/Content/DE/Downloads/Digitalisierung/2018-11-15-Digitalisierung-gestalten.pdf?__blob=publicationFile&v=2) noch keine Maßnahme zur Digitalisierung der Justiz ausgewiesen?
2. Seit wann ist dem Bundesministerium der Justiz und für Verbraucherschutz bekannt, dass das Thema Digitalisierung nicht nur Verbraucherschutzaspekte umfasst, sondern auch die Digitalisierung der Justiz selbst, und auf welchem Wege ist das Bundesministerium der Justiz und für Verbraucherschutz zu dieser Erkenntnis gelangt?
3. Warum beinhaltet die Maßnahme „Digitalisierung der Justiz voranbringen“ (vgl. Vorbemerkung der Fragesteller) keine Ziele im Bereich der IT-Sicherheit der Justiz?

4. Wurden in dem „Pakt für den Rechtsstaat“ (https://www.bmjv.de/SharedDocs/Artikel/DE/2019/020119_Rechtstaat.html) auch weitere Planstellen für IT-Mitarbeiter in der Justiz geschaffen, wenn nein, warum nicht?
5. Aus welchem Grund wurden in dem „Pakt für den Rechtsstaat“ (ebd.) zusätzliche Planstellen für Presse- und Öffentlichkeitsarbeit bei Bundesgerichtshof, Bundesfinanzhof und Bundesverwaltungsgericht geschaffen?
6. Kann aus der Bewilligung von Planstellen eine Priorisierung des Themas Presse- und Öffentlichkeitsarbeit im Vergleich zum Thema IT-Sicherheit abgeleitet werden, wenn nein, warum nicht?
7. Wurde vor der Vereinbarung der Schaffung einer Kommunikationsschnittstelle (vgl. Vorbemerkung der Fragesteller) zwischen Polizei, Staatsanwaltschaft und Gerichten von Bund und Ländern eine IT-Risikoanalyse durchgeführt?
   a) Wenn nein, warum nicht?
   b) Wenn ja, mit welchem Ergebnis und welchen abgeleiteten Handlungsempfehlungen?
   c) Wurden bereits erste Handlungsempfehlungen umgesetzt, wenn ja, welche, wenn nein, warum nicht?
8. Liegen der Bundesregierung Kenntnisse über den Stand der IT-Ausstattung und insbesondere der IT-Sicherheitssysteme von Staatsanwaltschaften und Gerichten in den Ländern vor, z. B. am Kammergericht Berlin oder am Hanseatischen Oberlandesgericht Bremen, und wenn ja, welche?
9. Beinhaltet das in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD auf Bundestagsdrucksache 19/15818, Stand der Umsetzung der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ – Digitalisierung der Justiz voranbringen) angekündigte Proof of Concept der Kommunikationsschnittstelle Maßnahmen der IT-Sicherheit?
   a) Wenn nein, warum nicht?
   b) Wenn ja, um welche Maßnahmen handelt es sich?
10. Was genau versteht die Bundesregierung unter einem Proof of Concept (vgl. Bundestagsdrucksache 19/15818), und welcher Begriff in der offiziellen Landessprache würde sich dafür eignen?
11. Welchen Umfang hat das Proof of Concept (ebd.) im hier vorliegenden Fall der Kommunikationsschnittstelle?
12. Sieht die Bundesregierung das Risiko, dass durch einen Abfluss oder die Manipulation von Daten durch die Cyberattacke auf das Berliner Kammergericht (https://www.rbb24.de/politik/beitrag/2020/01/berlin-kammergericht-arbeitsfaehig-februar-cyberangriff.html) die Arbeit von Bundeskriminalamt, Bundesverfassungsschutz oder anderen Bundesbehörden bei Ermittlungen im Bereich der organisierten Kriminalität, des internationalen Terrorismus oder anderer schwerer staatsgefährdender Delikte beeinträchtigt wird, wenn nein, warum nicht?
13. Hat die Bundesregierung Kenntnis davon, ob im Laufe der Aufarbeitung des Cyberangriffs auf das Berliner Kammergericht die entsprechenden Regelungen der europäischen Datenschutz-Grundverordnung umgesetzt wurden, insbesondere in Bezug auf möglicherweise betroffene Mitarbeiter von Bundessicherheitsbehörden?

14. Hat das Berliner Kammergericht oder haben andere Berliner Landesbehörden ein Amtshilfeersuchen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder an andere Bundesbehörden zur Abwehr der Cyberattacke auf das Berliner Kammergericht von September 2019 gestellt?

    a) Wenn ja, wann, durch wen, in welcher Form, und mit welchem Inhalt?

    b) Wie, und wann wurde das Ersuchen von den entsprechenden Bundesbehörden beschieden?

    c) War das Bundesamt für Sicherheit in der Informationstechnik (BSI) in irgendeiner Art an der Abwehr oder Aufarbeitung der Cyberattacke auf das Berliner Kammergericht von September 2019 beteiligt, und wenn ja, auf welcher Rechtsgrundlage?

15. Hat die Bundesregierung Kenntnisse davon, ob es sich bei den Hackern des Berliner Kammergerichts um dieselbe russische Hackergruppe handelt, die auch bereits der Cyberangriffe auf den Bundestag verdächtigt und geheimhin als „APT 28 Fancy Bear“ bezeichnet wird (https://www.verfassungsschutz.de/de/aktuelles/schlaglicht/schlaglicht-2017-06-die-russische-angriffskampagne-apt-28)?

16. Sieht die Bundesregierung nach wie vor keine Notwendigkeit der Definition eines digitalen Verteidigungsfalls (https://www.bundestag.de/presse/hib/655786-655786), wenn nein, warum nicht?

17. Werden die IT-Systeme an Bundesgerichten nach Kenntnis der Bundesregierung, wie im Fall des Kammergerichts Berlin (vgl. Vorbemerkung der Fragesteller), ebenfalls durch die Gerichte selbst oder durch professionelle Dienstleister betrieben?

18. Werden die IT-Systeme an Bundesgerichten, wie im Fall des Kammergerichts Berlin ausgeblieben, nach Kenntnis der Bundesregierung regelmäßig durch externe Gutachter auditiert, und wenn nein, warum nicht?

19. Sieht die Bundesregierung in der Schaffung einer Kommunikationsschnittstelle (vgl. Vorbemerkung der Fragesteller) mit Staatsanwaltschaften und Gerichten in den Ländern ein IT-Sicherheitsrisiko für Bundesanwaltschaft und Bundesgerichte, wenn nein, warum nicht?

20. Wird der Cyberangriff auf das Berliner Kammergericht die weitere Umsetzung der Maßnahme „Digitalisierung der Justiz voranbringen“ der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ verzögern?

    a) Wenn nein, warum nicht?

    b) Wenn ja, in welchem Ausmaß?

21. Sieht die Bundesregierung durch einen vergleichbaren Cyberangriff auf ein oder mehrere Bundesgerichte den Rechtsstaat gefährdet?

    a) Wenn nein, warum nicht?

    b) Wenn ja, in welchem Ausmaß?

22. Sieht die Bundesregierung die Notwendigkeit, IT-Systeme der Judikative als kritische Infrastruktur einzustufen, und wenn nein, warum nicht?

23. Hält die Bundesregierung eine Meldepflicht von Hackerangriffen auf Gerichte an das Bundesamt für Sicherheit in der Informationstechnik (BSI) für sinnvoll, und wenn nein, warum nicht?

24. Welche Cyberangriffe auf Bundesgerichte gab es nach Kenntnis der Bundesregierung seit Oktober 2017?

Berlin, den 3. März 2020

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion

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