**Deutscher Bundestag** **Drucksache 19/18271**

**19. Wahlperiode** 19.03.2020

# Antwort

## der Bundesregierung

### auf die Kleine Anfrage der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller und der Fraktion der AfD
### – Drucksache 19/17546 –

## Umsetzung der Digitalisierung der Justiz und Cyberangriffe auf Kammergerichte und Oberlandesgerichte

Vorbemerkung der Fragesteller

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.

---

*Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 18. März 2020 übermittelt.*

*Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.*

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?

Die Umsetzungsstrategie „Digitalisierung gestalten“ der Bundesregierung konzentriert sich auf Schwerpunktvorhaben, die die Ministerien identifiziert haben. Weder die erste Auflage aus November 2018 noch die zweite Auflage aus März 2019 ist hierbei als abschließend zu sehen. Die Bundesregierung wird die Strategie vielmehr kontinuierlich weiterentwickeln.

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?

Das Ziel der Digitalisierung verfolgt das Bundesministerium der Justiz und für Verbraucherschutz seit vielen Jahren. Ein Ausdruck hiervon ist die Mitarbeit des Bundes in der Bund-Länder-Kommission für Informationstechnik in der Justiz. Bei allen Bundesgerichten und dem Generalbundesanwalt sind bereits IT-Fachverfahren im Einsatz.

3. Warum beinhaltet die Maßnahme „Digitalisierung der Justiz voranbringen“ (vgl. Vorbemerkung der Fragesteller) keine Ziele im Bereich der IT-Sicherheit der Justiz?

Die Anforderungen der IT-Sicherheit werden bei allen Vorhaben der Digitalisierung der Justiz generell mitberücksichtigt, ohne dass es einer ausdrücklichen Erwähnung dieses Aspektes bedarf.

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?

Die Fragen 4 bis 6 werden gemeinsam beantwortet.

Die zwischen dem Bund und den Ländern vereinbarten Ziele und Maßnahmen des Pakts für den Rechtsstaat zum Personalaufbau und zur Digitalisierung ergeben sich aus dem MPK-Beschluss zum Pakt für den Rechtsstaat vom 31. Januar 2019, der unter der URL https://www.bundesregierung.de/resource/blob/973812/1575742/d2aa4f58e3ee33e96a4a28d1ea98d2f5/2019-01-31-beschluss-pakt-rechtsstaat-data.pdf?download=1 aufrufbar ist.

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?

Die Fragen 7 bis 7c werden gemeinsam beantwortet.

Vor der Vereinbarung der Schaffung einer Kommunikationsschnittstelle zwischen Polizei, Staatsanwaltschaft und Gerichten von Bund und Ländern wurde eine IT-Risikoanalyse nicht durchgeführt. Fragen der IT-Sicherheit werden im Rahmen der auf der Grundlage dieser Vereinbarung durchzuführenden Konzeptions- und Implementierungsprojekte geprüft und entsprechend berücksichtigt.

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?

Die IT-Ausstattung der Gerichte und Staatsanwaltschaften in den Ländern, einschließlich der dort eingesetzten IT-Sicherheitssysteme, liegt in der Verantwortung der Länder. Der Bundesregierung liegen keine über die aus der öffentlichen Berichterstattung bekannten Informationen hinausgehende Erkenntnisse dazu vor.

Die Bund-Länder-Kommission für Informationstechnik in der Justiz stellt einmal im Jahr Berichte der Länder zusammen, aus denen die Entwicklung des Einsatzes der Informationstechnik in der Justiz hervorgeht. Diese Berichte sind unter https://justiz.de/BLK/laenderberichte/index.php abrufbar.

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?

Die Fragen 9 bis 9b werden gemeinsam beantwortet.

Der in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD auf Bundestagsdrucksache 19/15818 erwähnte Proof of Concept beinhaltet keine spezifischen Maßnahmen der IT-Sicherheit. Die zentralen Schutzziele der IT-Sicherheit „Vertraulichkeit, Integrität und Verfügbarkeit“ wurden bei der Konzeption und Realisierung des Proof of Concept aber stets mitgedacht und berücksichtigt. Konkrete Maßnahmen der IT-Sicherheit können erst für ein künftiges Produktivsystem und in Kenntnis der konkreten infrastrukturellen Gegebenheiten ermittelt und umgesetzt werden.

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?

Der Begriff Proof of Concept wird im Projektmanagement üblicherweise als Bezeichnung eines frühen Projektabschnitts verwendet, bei dem die Realisierbarkeit des in einem Konzept konkretisierten Projektvorhabens anhand einer Machbarkeitsstudie oder eines Prototyps überprüft wird. Ein erfolgreicher Proof of Concept ist Beleg dafür, dass ein Vorhaben prinzipiell technisch und/oder wirtschaftlich realisierbar ist. Die Verwendung derartiger Entlehnungen aus der englischen Sprache ist im Projektmanagement wie auch generell im IT-Bereich üblich.

11. Welchen Umfang hat das Proof of Concept (ebd.) im hier vorliegenden Fall der Kommunikationsschnittstelle?

Gegenstand des in der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der AfD auf Bundestagsdrucksache 19/15818 erwähnten Proof of Concept war zum einen die Frage, über welche Kommunikationsinfrastruktur Justiz und Polizei sicher und zuverlässig Daten austauschen können und zum anderen, wie die beiden XÖV-Datenstandards xPolizei und xJustiz so aufeinander abgebildet werden können, dass eine verlustfreie Datenübermittlung in beide Richtungen sichergestellt werden kann. Die Erkenntnisse aus dem Proof of Concept bilden eine der Grundlagen der weiteren Konzeption und Realisierung einer Kommunikationsschnittstelle zwischen Polizei, Staatsanwaltschaft und Gerichten von Bund und Ländern.

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?

Die Bundesregierung sieht den Abfluss oder die Manipulation von Daten im Zuge von erfolgreichen Cyberattacken als mögliches Grundgefährdungsszenario. Hinsichtlich der Cyberattacke auf das Berliner Kammergericht liegen aber keine Hinweise vor, dass die Arbeit von Bundeskriminalamt, Bundesamt für Verfassungsschutz oder anderer Bundesbehörden bei Ermittlungen im Bereich der organisierten Kriminalität, des internationalen Terrorismus oder anderer schwerer staatsgefährdender Delikte beeinträchtigt wird.

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?

Der Bundesregierung liegen hierzu keine Kenntnisse vor.

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?

Die Fragen 14 bis 14c werden gemeinsam beantwortet.

An das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder eine andere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat wurde vom Berliner Kammergericht oder einer Berliner Landesbehörde kein Amtshilfeersuchen zur Abwehr der Cyberattacke von September 2019 übermittelt.

Im Rahmen der Zusammenarbeit von Bund und Ländern im VerwaltungsCERT-Verbund (VCV) hat das BSI das CERT.Berlin auf Grundlage der vom IT-Planungsrat beschlossenen Geschäftsordnung VCV unterstützt.

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)?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

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?

Die Bundesregierung sieht keine Veranlassung den Begriff „digitaler Verteidigungsfall“ zu definieren. Dieser stellt keinen Rechtsbegriff dar und wird durch die Bundesregierung auch nicht verwendet. Alle Voraussetzungen des Verteidigungsfalls sind abschließend und hinreichend in Artikel 115a GG geregelt und im Einzelfall anhand der konkreten Situation zu beurteilen.

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?

Die IT-Systeme in den Bundesgerichten werden durch die Gerichte selbst mit spezialisiertem IT-Personal 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?

Ja. Gemäß des Umsetzungsplans Bund 2017 sind die Behörden/Gerichte in der Bundesverwaltung überdies verpflichtet, regelmäßige Revisionen/Audits durchzuführen.

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?

Jede Schnittstelle stellt grundsätzlich eine abstrakte Gefahr für die IT-Sicherheit dar. Definierte Schnittstellen mit konkreten Austauschformaten erhöhen allerdings typischerweise die IT-Sicherheit gegenüber dem Einsatz unspezifischer Austauschformate wie E-Mail.

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?

Die Fragen 20 bis 20b werden gemeinsam beantwortet.

Der Cyberangriff auf das Berliner Kammergericht wird nach Einschätzung der Bundesregierung die weitere Umsetzung der Maßnahme „Digitalisierung der Justiz voranbringen“ der Umsetzungsstrategie der Bundesregierung „Digitalisierung gestalten“ nicht verzögern. Grundsätzlich wurden und werden Anforderungen der IT-Sicherheit bei allen Maßnahmen zur weiteren Digitalisierung der Justiz umfassend berücksichtig. Die Erfahrungen aus dem Cyberangriff auf das Berliner Kammergericht sind geeignet, die Beteiligten für Aspekte der IT-Sicherheit noch weiter zu sensibilisieren. Projektverzögerungen sind deshalb aber nicht zu erwarten.

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?

Die Fragen 21 bis 21b werden gemeinsam beantwortet.

Die Bundesregierung sieht den Rechtsstaat durch einen vergleichbaren Cyberangriff auf ein oder mehrere Bundesgerichte nicht gefährdet. Die Prinzipien des Rechtsstaats, wie die Achtung der Grundrechte, die Gewaltenteilung und die Bindung staatlichen Handelns an Recht und Gesetz, gelten auch im Falle einer vorübergehenden Einschränkung der Arbeitsfähigkeit einzelner Gerichte unverändert fort.

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

Infrastrukturen gelten dann als „kritisch“, wenn sie für die Funktionsfähigkeit moderner Gesellschaften von wichtiger Bedeutung sind und ihr Ausfall oder ihre Beeinträchtigung nachhaltige Störungen im Gesamtsystem zur Folge hat. Kritische Infrastrukturen können aufgrund ihrer technischen, strukturellen und funktionellen Spezifika in unverzichtbare technische Basisinfrastrukturen und unverzichtbare sozioökonomische Dienstleistungsinfrastrukturen unterschieden werden. Die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) der Bundesregierung stuft Justizeinrichtungen ausdrücklich als unverzichtbare sozioökonomische Dienstleistungsinfrastrukturen ein. Die IT-Systeme der Justizeinrichtungen sind für deren Arbeitsfähigkeit essentiell.

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?

Die Bundesregierung hat eine Meldepflicht von Hackerangriffen auf Bundesgerichte an das BSI bereits in § 4 BSIG i. V. m. der „Allgemeinen Verwaltungsvorschrift über das Meldeverfahren gemäß § 4 Absatz 6 BSIG“ geregelt. Da den Bundesgerichten – der Rechtsprechung – eine besondere verfassungsrechtliche Unabhängigkeit zukommt, sind die Bundesgerichte grundsätzlich von der Meldepflicht ausgenommen, wenn eine Übermittlung dieser besonderen Unabhängigkeit widerspricht. Die Bundesgerichte können auf freiwilliger Basis Informationen übermitteln (vgl. § 3 der Verwaltungsvorschrift).

Für eine Meldepflicht der Gerichte der Länder gegenüber dem BSI sieht die Bundesregierung aufgrund der föderalen Struktur der Bundesrepublik Deutschland keine Grundlage. Derartige Meldepflichten können allenfalls – unter Beachtung der vorgenannten Unabhängigkeit der Rechtsprechung – auf Landesebene umgesetzt werden.

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

Der Bundesregierung sind keine Cyberangriffe auf Bundesgerichte seit Oktober 2017 bekannt.

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