Deutscher Bundestag **Drucksache 19/898**

19. Wahlperiode 23.02.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Katrin Helling-Plahr, Katharina Kloke, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/677 –

Einführung der besonderen elektronischen Anwaltspostfächer

Vorbemerkung der Fragesteller

Gemäß § 176 Absatz 2 der Bundesrechtsanwaltsordnung (BRAO) führt das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) die Rechtsaufsicht über die Bundesrechtsanwaltskammer (BRAK). Die Aufsicht bezieht sich dabei insbesondere darauf, dass die der Bundesrechtsanwaltskammer übertragenen Aufgaben erfüllt werden.

Laut § 177 Absatz 2 Nummer 7 BRAO gehört zu den Aufgaben der BRAK die elektronische Kommunikation der Rechtsanwälte mit Gerichten, Behörden und sonstigen Dritten zu unterstützen.

Mit dem Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013 (BGBl. I S. 3786) wurde das besondere elektronische Anwaltspostfach (beA) eingeführt. Für seine Einrichtung ist gemäß § 31a BRAO die BRAK zuständig.

Am 20. Dezember 2017 wurde in der Software zur Anmeldung zum besonderen elektronischen Anwaltspostfach (beA), im sog. ClientSecurity-System, ein Design- und Konstruktionsfehler aufgedeckt. Ein für die sichere Anmeldung erforderliches Zertifikat liegt inklusive des privaten Schlüssels lokal in der Software vor. Damit bietet eine solche HTTPS-Verbindung keinerlei Schutz etwa vor Umleitungen auf andere Server zwecks Gewinnung der Zugangsdaten. Daraufhin wurde das Zertifikat nach Medienberichten von der zuständigen Zertifizierungsstelle gesperrt.

Bei einem in der Folge durch die BRAK bereitgestellten Ersatzzertifikat handelte es sich um ein selbstsigniertes Wurzelzertifikat, also ein Zertifikat, das seinerseits andere Zertifikate signieren kann. Wiederum ist der private Teil des Schlüssels öffentlich. Mithin waren und sind die mit diesem Zertifikat bestückten Rechner der Rechtsanwaltschaft einem erheblichen Sicherheitsrisiko ausgesetzt.

Nachdem die BRAK das Problem am Nachmittag des 22. Dezember 2017 erkannte (vgl. „beA muss vorerst offline bleiben – Schreiben des BRAK-Präsidenten an die deutsche Anwaltschaft“, abrufbar unter www.brak.de/zur-rechtspolitik/newsletter/bea-newsletter/2018/sondernewsletter-v-03012018.news.html), wurde das beA durch die BRAK offline geschaltet. Sollte diese Phase zunächst noch

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 21. Februar 2018 übermittelt.

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

auf die Weihnachtstage beschränkt sein, entschied die BRAK nach eigener Darstellung am 26. Dezember 2017, das beA bis zu einer Behebung dieser und weiterer Sicherheitsprobleme offline zu lassen, auch über den geplanten Beginn der passiven Nutzungspflicht am 1. Januar 2018 hinaus.

Am 26. Januar 2018 schließlich empfahl die BRAK allen Rechtsanwälten, das ClientSecurity-Modul in seiner aktuellen Version zu Deaktivieren bzw. zu Deinstallieren, da es über die bis dato diskutieren Probleme hinaus auch auf veralteten Java-Bibliotheken basiert und somit in seiner derzeitigen Fassung ein eigenständiges Sicherheitsrisiko für die Rechner der Rechtsanwaltschaft darstellt. Diese können bereits beim Besuch einer Website übernommen werden.

1. Geht das BMJV davon aus, dass die BRAK die ihr übertragenen Aufgaben im Bereich der elektronischen Kommunikation der Rechtsanwälte gegenwärtig erfolgreich wahrnehmen kann?

2. Hat das BMJV die beA-Einführung betreffend aufsichtsrechtliche Maßnahmen gemäß 176 Absatz 2 BRAO ergriffen?

   Wenn ja, welche?

Die Fragen 1 und 2 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Die Staatsaufsicht des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV) über die BRAK beschränkt sich nach § 176 Absatz 2 Satz 2 BRAO darauf, dass Gesetz und Satzung beachtet werden. Nachdem die BRAK das beA am 23. Dezember 2017 vorläufig außer Betrieb genommen hatte, steht das BMJV mit der BRAK in Kontakt, um sicherzustellen, dass das beA entsprechend den gesetzlichen Vorgaben so zügig wie möglich wieder in Betrieb genommen werden kann.

3. Für wann geht das BMJV von einer tatsächlichen Bereitstellung des beA aus?

Der Bundesregierung ist derzeit noch kein konkreter Termin für die Wiederinbetriebnahme des beA bekannt.

4. Plant die Bundesregierung eine Anpassung der Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach (Elektronischer-Rechtsverkehr-Verordnung – ERVV) bis zur tatsächlichen Verfügbarkeit des beA?

   Wird an dem gegenüber bisherigen Regelungen neu aufgenommenen Ausschluss einer Containersignatur gemäß § 4 Absatz 2 ERVV trotz Unverfügbarkeit des beA festgehalten?

Die Bundesregierung sieht momentan keinen Anlass für eine Änderung der ERVV.

5. Ist die Darstellung zutreffend, dass der ursprünglich für die Abschaltung am 14. Februar 2018 vorgesehene „Elektronische Gerichts- und Verwaltungspostfach“-Client (EGVP-Client) angesichts der Nichtverfügbarkeit des beA bis Ende Mai 2018 weitergeführt wird?

   Welche Gründe sprechen aus Sicht der Bundesregierung gegen einen darüber hinaus gehenden Betrieb des EGVP-Client?

Die für diese Frage zuständige Bund-Länder-Kommission für Informationstechnik in der Justiz hatte zunächst die Abschaltung des EGVP-Classic-Clients zum 1. Januar 2018 geplant, hat diese Frist jedoch mittlerweile bis zum Mai 2018 verlängert. Danach wird sie erneut über die Frage der Abschaltung entscheiden.

6. Welche Erkenntnisse liegen der Bundesregierung hinsichtlich in der Öffentlichkeit diskutierten erheblichen Zweifeln an der Darstellung der BRAK, Nachrichten innerhalb des Systems beA würden Ende-zu-Ende verschlüsselt, vor?

   Ist es zutreffend, dass anders als in einem System mit Ende-zu-Ende-Verschlüsselung alle privaten Schlüssel der teilnehmenden Rechtsanwälte zentral in einem sogenannten Hardware Security Module (HSM) vorliegen, sodass eine Umschlüsselung von Nachrichten möglich wird?

   Ist der Bundesregierung insbesondere bekannt, welche Parteien diesbezüglich als sog. Key Custodians fungieren, also gemeinsam Vollzugriff auf den Inhalt des HSM haben?

Der Bundesregierung sind die momentan in der Öffentlichkeit diskutierten Fragen zur Sicherheit des beA und die daraufhin von der BRAK kommunizierten Erläuterungen zur Funktionsweise des beA bekannt. Die Bundesregierung prüft im Rahmen ihrer Staatsaufsicht nach § 176 Absatz 2 BRAO die Einhaltung der rechtlichen Vorgaben zur Sicherheit des beA. Diese Überprüfung ist derzeit noch nicht abgeschlossen.

7. Welche Erkenntnisse liegen der Bundesregierung vor, wie der Betrieb des beA im Falle einer Insolvenz des Dienstleisters Atos Information Technology GmbH gewährleistet werden soll?

Die Bundesregierung sieht aktuell keinen Anlass für eine Prüfung dieser Frage.

8. Betrachtet die Bundesregierung das beA als öffentlich zugänglichen Telekommunikationsdienst i. S. v. § 3 Nummer 17a des Telekommunikationsgesetzes (TKG), findet ihrer Auffassung nach also § 110 TKG Anwendung?

Das beA bietet seine Funktionen zum Senden und Empfangen von Nachrichten lediglich Rechtsanwältinnen und Rechtsanwälten und damit einer geschlossenen Benutzergruppe an. Öffentlich zugänglich im Sinne von § 3 Nummer 17a TKG ist dagegen nur ein Telekommunikationsdienst, der nicht nur einem begrenzten, sondern einem grundsätzlich unbeschränkten Personenkreis zur Verfügung steht. Deshalb ist das beA nach Auffassung der Bundesregierung kein öffentlich zugänglicher Telekommunikationsdienst im Sinne des § 3 Nummer 17a TKG.

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