Deutscher Bundestag **Drucksache 19/25999**

19. Wahlperiode 19.01.2021

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Wieland Schinnenburg, Stephan Thomae, Renata Alt, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/25561 –

Datensicherheit des besonderen elektronischen Anwaltspostfachs

Vorbemerkung der Fragesteller

Die Bundesrechtanwaltskammer (BRAK) hat am 28. November 2016 für jeden Rechtsanwalt in Deutschland ein besonderes elektronisches Anwaltspostfach (beA) eingerichtet (erreichbar über www.bea-brak.de). Nach anfänglichen Startproblemen und gerichtlichen Auseinandersetzungen ist das beA für alle Rechtsanwälte seit 1. Januar 2018 zu nutzen (https://www.lto.de/recht/juristen/b/brak-praesident-bea-anwaelte-rechtsstaat-datenschutz). Auch von Unstimmigkeiten bei der Begutachtung von Sicherheitsrisiken war die Rede (https://www.golem.de/news/bundesrechtsanwaltskammer-originalfassung-von-bea-sicherheitsgutachten-freigeklagt-2010-151190.html). Die Anforderungen an das Sicherheitslevel des beA scheinen mittlerweile geklärt zu sein (https://www.heise.de/newsticker/meldung/Gericht-Durchgehende-Verschluesselung-beim-Anwaltspostfach-nicht-noetig-4586672.html), allerdings wirft der Wechsel vom bisherigen Dienstleister Atos zu Wesroc neue Sicherheitsfragen auf. Es sei nicht auszuschließen, dass der alte Dienstleister noch über Sicherheitsschlüssel verfüge. Darauf hatte ein Sachverständiger in der Sitzung des Rechtsausschusses am 16. November 2020 hingewiesen. Es bestehe die Gefahr, dass die gesamte Kommunikation, die über das beA abgewickelt wird, mitgelesen werden könne. Über eine Ende-zu-Ende-Verschlüsselung, die das verhindern würde, verfüge das beA nicht. Aus Sicht eines Experten sollte deshalb zügig auf die Herstellung neuer Sicherheitsschlüssel hingewirkt werden. Die Frage, ob der rechtmäßige Betrieb des beA eine Ende-zu-Ende-Verschlüsselung erfordert, liegt dem Bundesgerichtshof zur Beantwortung vor (AnwZ (Brfg) 2/20). Durch Unsicherheiten in der Nutzung der elektronischen Infrastruktur leidet das Vertrauen der Bürger in den elektronischen Rechtsverkehr. Das muss nach Ansicht der Fragesteller verhindert werden.

Vorbemerkung der Bundesregierung

Die Bundesregierung weist zu dem Gegenstand der Kleinen Anfrage darauf hin, dass die Einrichtung des besonderen elektronischen Anwaltspostfachs (beA) durch § 31a der Bundesrechtsanwaltsordnung (BRAO) der Bundesrechtsanwaltskammer (BRAK) als Selbstverwaltungsorgan der Rechtsanwaltschaft übertragen wurde. Die BRAK hat dabei insbesondere die in der BRAO und in

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums der Justiz und für Verbraucherschutz vom 19. Januar 2021 übermittelt.
Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

der Rechtsanwaltsverzeichnis- und -postfachverordnung (RAVPV) festgelegten rechtlichen und technischen Anforderungen zu beachten. Dem Bundesministerium der Justiz und für Verbraucherschutz (BMJV) kommt insoweit nach § 176 Absatz 2 BRAO lediglich eine Staatsaufsicht über die BRAK zu, die auf die Beachtung der gesetzlichen und satzungsrechtlichen Vorschriften und insbesondere die Erfüllung der der BRAK übertragenen Aufgaben beschränkt ist.

Anlässlich des in der Vorbemerkung der Fragesteller in Bezug genommenen Wechsels der Betreiberin des beA von der Atos Information Technology GmbH zur Wesroc GbR wurde die Sicherheit des beA im Auftrag der BRAK von der secuvera GmbH unabhängig im Wege einer IT-Sicherheitsprüfung begutachtet. Dies schloss auch die Fragestellung ein, ob der Betriebsübergang ein Risiko für die Sicherheit des beA darstellen würde. Das Abschlussgutachten der secuvera GmbH vom 2. Juli 2020 (im Folgenden: secuvera-Gutachten; abrufbar unter: https://brak.de/w/files/02_fuer_anwaelte/bea/abschlussgutachten_secuvera.pdf) verneint Letzteres (S. 9). Das secuvera-Gutachten konnte dabei auf der von der secunet Security Networks AG durchgeführten grundlegenden IT-Sicherheitsprüfung zum beA aufbauen, deren Ergebnisse im Abschlussgutachten „Technische Analyse und Konzeptprüfung des beA“ vom 18. Juni 2018 niedergelegt sind (im Folgenden: secunet-Gutachten; abrufbar unter: https://www.brak.de/w/files/04_fuer_journalisten/presseerklaerungen/pe-18-anlage1.pdf).

1. Trifft es nach Kenntnis der Bundesregierung zu, dass die BRAK beziehungsweise ihre technischen Dienstleister rein technisch jede Nachricht entschlüsseln können?

   a) Wenn ja, wie ist diese Zugriffsmöglichkeit mit dem Schutz der Vertraulichkeit von Anwalt-Mandanten-Korrespondenz zu vereinbaren?

   b) Wenn nein, warum wurde der Hinweis laut eines Presseberichts im Originalgutachten der Secunet Security Networks AG entfernt (https://www.golem.de/print.php?a=151190)?

   c) Liegen die Daten während der Umschlüsselung unverschlüsselt vor und könnten diese Daten von Dritten oder von der BRAK gelesen werden?

3. Wie wird der Verzicht auf eine Ende-zu-Ende-Verschlüsselung beim beA nach Kenntnis der Bundesregierung begründet?

Die Fragen 1 und 3 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Im Zuge der von der BRAK durchgeführten technischen Konzeption und Umsetzung des beA hat sich ergeben, dass eine Ende-zu-Ende-Verschlüsselung im arbeitsteilig organisierten Kanzleibetrieb der Rechtsanwältinnen und Rechtsanwälte nicht hinreichend praktikabel wäre. Daher wurde für das beA das Konzept einer Umverschlüsselung in einem Hardware-Sicherheitsmodul (HSM) gewählt (vergleiche dazu auch S. 11 und 72 des secunet-Gutachtens).

Bei der im HSM erfolgenden Umverschlüsselung werden die für den jeweiligen Kommunikationsvorgang benötigten Schlüssel zum Teil im HSM gebildet, entschlüsselt und verschlüsselt (vergleiche im Einzelnen S. 75 ff. des secunet-Gutachtens). Hierfür sind Master-Schlüssel (Arbeitsschlüssel) im HSM gespeichert, die von der beA-Betreiberin unter den im secunet-Gutachten auf S. 78 und 86 dargestellten Hochsicherheitsbedingungen erzeugt, verschlüsselt, samt des zur Verschlüsselung verwendeten Schlüssels (key encryption key – KEK) an die BRAK übergeben und von dieser verwahrt werden. Die Arbeitsschlüssel liegen damit zwar auch außerhalb des HSM vor. Zur Sicherheit des KEK sind jedoch physisch-organisatorische Maßnahmen (Schlüsselteilung, getrennte phy-

sische Verwahrung der Schlüsselteile und nur beschränkter Zugriff spezifischer BRAK-Mitarbeiter) getroffen. Zudem erfolgt ein regelmäßiger Wechsel in den vorhandenen Varianten der Master-Schlüssel (vergleiche secunet-Gutachten S. 78).

Das aus der Konzeption des beA folgende Risiko einer Entschlüsselung der über das beA laufenden Kommunikation ist in Anbetracht der im Übrigen getroffenen Sicherheitsmaßnahmen aus Sicht der Bundesregierung in Übereinstimmung mit der Einschätzung des secunet-Gutachtens (dort S. 86) als akzeptabel anzusehen. Die Entschlüsselung der Kommunikation im laufenden Betrieb würde ein kollusives Zusammenwirken mehrerer Personen erfordern, da jeweils mehrere Mitarbeitende der Betreiberin und der BRAK bei der Zusammenführung von Schlüssel und Nachrichten gemeinsam agieren müssten. Das Konzept einer Umverschlüsselung im HSM unter Einsatz von auch außerhalb des HSM gespeicherten Masterschlüsseln ist daher auch in anderen sicherheitssensiblen Bereichen üblich (vergleiche secunet-Gutachten S. 86).

2. Wie wird ein „sicherer Übermittlungsweg“ im Sinne des § 130a der Zivilprozessordnung (ZPO) sichergestellt?

Die rechtlichen Anforderungen an das beA sind in § 31a BRAO und den auf der Grundlage des § 31c Nummer 3 BRAO ergangenen Bestimmungen des Teils 4 der RAVPV festgelegt.

4. Wie wird bzw. ist ausgeschlossen, dass Dritte einen Zugriff auf den „privaten Schlüssel“ erhalten?

   a) Wie wurde sichergestellt, dass durch den Wechsel der Dienstleister keine Kopien der „privaten Schlüssel“ erstellt wurden?

   b) Wären (rein theoretisch) Konstellationen denkbar, in denen es möglich wäre, auf die „privaten Schlüssel“ Zugriff zu erhalten?

   c) Trifft es zu, dass die „privaten Schlüssel“ ohne Aufsicht der BRAK erstellt wurden?

5. Ist aus der Sicht der Bundesregierung erforderlich, dass auf die Herstellung neuer Schlüssel hingewirkt wird?

   a) Wenn ja, welche Schritte unternimmt sie?

   b) Wenn nein, warum nicht?

   c) Wie oft werden die jeweilig verwendeten Schlüssel und Zertifikate jeweils erneuert?

6. Welche Schwachstellen beim beA sind nach Freischaltung aufgedeckt und beseitigt worden (bitte anhand Zeitstrahl detailliert auflisten)?

7. Gibt es aktuell Sicherheitslücken, an deren Behebung nach Kenntnis der Bundesregierung aktuell gearbeitet wird?

   a) Wenn ja, welche sind das, und bis wann werden sie behoben?

   b) Wenn nein, wie werden Sicherheitslücken ausgeschlossen, bzw. woran kann man das Nichtbestehen solcher Lücken festmachen?

8. Wie wird das aktuelle Sicherheitsregelwerk beschrieben?

9. Wie und durch wen werden Störungen der IT-Sicherheitsarchitektur nach Kenntnis der Bundesregierung behoben?

   a) Gibt es einen Notfallplan, und wie sieht er aus?

   b) Wenn nein, warum nicht?

10. Welche Sicherheitstests und Sicherheitsanalysen des beA hat es nach Kenntnis der Bundesregierung bisher gegeben, und was waren jeweils die Ergebnisse?

11. Auf welcher Serverarchitektur wird das beA nach Kenntnis der Bundesregierung betrieben?

    a) Welche Betriebssysteme in welcher Version werden verwendet?

    b) Welche Webserver-Software in welcher Version wird verwendet?

    c) Welche Webserver-Module und Erweiterungen in welchen Versionen werden verwendet?

Die Fragen 4 bis 11c werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen zu diesen Fragen keine Informationen vor, die über diejenigen hinausgehen, die sich aus den Gutachten von secunet und secuvera ergeben. Auf die Ausführungen in der Vorbemerkung zum Gegenstand der Staatsaufsicht wird verwiesen.

12. Ist es nach Kenntnis der Bundesregierung geplant, die Authentifizierung beim beA zu vereinfachen und etwa auch eine App-basierte Authentifizierung oder weitere Verfahren einzuführen?

13. Ist nach Kenntnis der Bundesregierung eine Offenlegung des beA-Quellcodes geplant?

    a) Sollten Lizenzrechte Dritter einer vollständigen Offenlegung entgegenstehen, ist eine teilweise Offenlegung der übrigen Teile des Quellcodes geplant?

    b) Falls nein, warum nicht?

14. Hat die Bundesregierung Kenntnis über Pläne die Weiterentwicklung hin zu einem sogenannten beA 2.0 betreffend, welches konzeptionelle Schwächen der aktuellen Version, insbesondere den Verzicht auf durchgehende Ende-zu-Ende-Verschlüsselung, angeht?

Die Fragen 12 bis 14 werden wegen des Sachzusammenhangs gemeinsam beantwortet.

Zur Vorbereitung der 112. Sitzung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestags am 18. November 2020 (TOP 17: Antrag der Fraktion der FDP „Bericht der Bundesregierung zur Nutzungsakzeptanz und der geplanten Weiterentwicklung des besonderen elektronischen Anwaltspostfachs“) hat die BRAK das BMJV darüber informiert, dass die Betreiberin des beA mit Weiterentwicklungen und Überarbeitungen insbesondere der beA-Oberfläche beauftragt wurde. Folgende Themen werden nach Auskunft der BRAK analysiert und zum Teil bereits umgesetzt:

- automatisierte Wiederholung bei fehlerhaftem Nachrichtenversand
- technische Umsetzung der Regeln für Dateinamen von Anhängen zur Nachricht

- Verbesserungen der Kanzleisoftware-Schnittstelle und des Kanzleisoftware-Tool-Kits sowie verbesserte Bereitstellung von Software und Dokumentation für Hersteller von Kanzleisoftware
- Verbesserung der Nachrichtenübertragung an den Intermediär
- vereinfachte Auswahl von Authentifizierungstoken
- technische Einbindung der Erstellung von Fernsignaturen, um das mobile Arbeiten mit dem System zu erleichtern
- Überarbeitung der Benutzeroberfläche.

Weitere Erkenntnisse zu den Gegenständen der Frage liegen der Bundesregierung nicht vor.

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