Antrag zu TOP 6

Entsprechend § 8 Nr. 7 Geschäftsordnung der RAK Sachsen werden zum Tagesordnungspunkt 6 der Versammlung der RAK Sachsen am 23.03.2018 folgende **zwei** Anträge gestellt:

I. **Die RAK Sachsen wirkt nachhaltig auf allen Ebenen darauf hin, dass die BRAK**
   - **die Quelltexte der beA-Software (Clients und Server) unter einer gängigen Open-Source- / Freie-Software-Lizenz zur Verfügung stellt und**
   - **unabhängige externe Sachverständige mit Audits des gesamten Programmcodes (d.h. neben black-box-Tests auch white-box-Tests der Clients und Server) zur Sicherheit des beA-Systems sowie der absolut vertraulichen Ende-zu-Ende-Verschlüsselung der Kommunikation im herkömmlichen Sinn beauftragt und die Audit-Berichte sowie aktuelle Fehlerlisten, offene Schnittstellen und historisierte Störungsmeldungen veröffentlicht sowie**
   - **die beA-Software (Clients) zu allen aktuellen Betriebssystemen (u.a. GNU/Linux, Windows, macOS) ausnahmslos gleichermaßen kompatibel hält, dokumentiert und supportet.**

II. **Weiterhin wirkt die RAK Sachsen nachhaltig auf allen Ebenen darauf hin, dass die BRAK das beA kurzfristig in ein dezentrales einheitliches System umstellt.**

Über die **Anträge** soll **getrennt abgestimmt werden**. Die **Begründung** erfolgt mündlich in der Versammlung und für das Protokoll schriftlich wie folgt:

Das von der BRAK in Auftrag gegebene, entwickelte und zu verantwortende besondere elektronische Anwaltspostfach (beA) hat zu einer Gefährdung der IT-Sicherheit der gesamten Anwaltschaft geführt und zugleich den Ruf der Anwaltschaft nachhaltig beschädigt. In der gegenwärtigen bekannten Ausgestaltung stellt das beA auch für die Zukunft ein Risiko für das Anwaltsgeheimnis in Bezug auf die Korrespondenz mit Gerichten, Behörden und Kollegen dar. Die Unabhängigkeit der Anwaltschaft und die Funktionsfähigkeit der Rechtspflege als solche sind gefährdet.

Zu I.

Ein funktionierender Betrieb erfordert die Offenlegung des Quellcodes, regelmäßige unabhängige Sicherheits-Überprüfungen (Audits), eine echte Ende-zu-Ende-Verschlüsselung sowie die positive Unterstützung und den Support aktueller Betriebssysteme.

a) Die Offenlegung des vollständigen Quellcodes ist ein wesentlicher Baustein für den nachhaltigen Betrieb und die Möglichkeit einer kompetenten Selbstverwaltung der Anwaltschaft. Mit der Offenlegung des Codes kann dem Grundsatz der *security-by-transparency* Rechnung getragen werden. Eine jederzeitige Kontrolle des Codes auf Fehler und Hintertüren ist damit möglich. Dies fördert die Qualität und die Sicherheit des Codes, denn jeder kann potentiell Fehler oder Hintertüren melden. Bei nicht freier Software ist der Code nicht einsehbar. Das damit einhergehende Modell der *security-by-obscurity* bietet nur eine scheinbare Sicherheit. Zwar ist nicht jedem der Code bekannt. Aber nur der, der den Code

kennt, kann ihn verbessern. Die Qualität des Codes hängt damit von der Leistung einzelner weniger ab.

b) Daher sind regelmäßige Sicherheitsaudits zwingend notwendig. Die Veröffentlichung des Ergebnisses fördert wiederum die Qualität des Audits und des Codes. Jeder Dritte mit den entsprechenden Kenntnissen kann so bei Fehlern im Audit oder im Code helfen. Sicherheitsaudits können viel schneller und unkomplizierter durchgeführt werden, da Geheimhaltungsvereinbarungen entfallen. Wegen des intransparenten Vorgehens und der zögerlichen Kommunikation der Verantwortlichen der BRAK ist das notwendige Vertrauen verloren gegangen. Nur ein transparentes Vorgehen, einschließlich einer transparenten Überprüfung der Software können das notwendige Vertrauen wieder herstellen.

c) Eine echte Ende-zu-Ende-Verschlüsselung ist unabdingbar. Dies nicht nur wegen der gegenwärtig passiven und zukünftig auch aktiven **Nutzungspflicht** des beA. Ohne echte Ende-zu-Ende-Verschlüsselung werden die Anwälte gezwungen sein, für einen wesentlichen Teil ihrer Kommunikation einen potentiell unsicheren, nicht dem Stand der Verschlüsselungstechnik entsprechenden Kommunikationsweg nutzen zu müssen. Dies ist mit dem Anwaltsgeheimnis nicht zu vereinbaren. Dies ist aber insbesondere nicht mit Blick auf das informelle Selbstbestimmungsrecht unserer Mandanten vereinbar. Jeder Mandant hat ein Recht auf vertrauliche Kommunikation. Wenn er dies einfordert, muss der Anwalt – und die Justiz – ihm das bieten. Der Verweis auf ein potentiell unsicheres Zwangskommunikationsmittel wie das aktuelle beA schädigt das Vertrauen in die Anwaltschaft und in die Rechtsordnung als solche nachhaltig.

d) Das beA muss aktuelle Betriebssysteme wie GNU/Linux, Windows, macOS vollständig und umfangreich unterstützen. Kein Anwalt darf über das beA gezwungen sein, eine bestimmte IT vorzuhalten. Ihm kann nur auferlegt werden, überhaupt IT-Systeme zur elektronischen Datenverarbeitung (EDV) und als Schnittstelle zum elektronischen Rechtsverkehr (ERV) vorzuhalten. Ein auf bestimmte Betriebssysteme begrenztes beA stellt damit einen Eingriff in die Grundrechte des Anwalts dar. Wenn der Anwalt zwecks Nutzung des beA zur Nutzung eines bestimmten Betriebssystems gezwungen wird, stellt dies einen Eingriff in die Berufsausübungsfreiheit aus Art. 12 GG und die informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Hinzukommt das Problem der Datensicherheit, zu dem der Rechtsanwalt über das Anwaltsgeheimnis verpflichtet ist. Er selbst muss wählen dürfen, welches Betriebssystem er hierfür nutzt.

> Die Offenlegung des Quellcodes wird u.a. von der Arbeitsgemeinschaft IT-Recht des DAV unterstützt[1].
>
> Ein vergleichbarer Antrag wurde in der Kammerversammlung des RAK Berlin mit 96,89 % angenommen. Die RAK Berlin hat einen Aufruf zum Anschluss an diesen Auftrag veröffentlicht[2]. Dieser liegt als **Anlage** bei.

Zu II.

Die von der BRAK für das beA gewählte Architektur mit dem zentralen Hardware-Security-Mudule (HSM) stellt – unabhängig der bekannten Problematik der Umschlüsselung – ein hohes Sicherheitsrisiko für die Anwaltschaft und den geordneten Rechtsverkehr dar. Das

1http://www.davit.de/aktuelles/artikel/mehr-transparenz-arbeitsgemeinschaft-it-recht-des-dav-fordert-open-source-loesung-fuer-das-besondere
2https://www.rak-berlin.de/rak-berlin/aktuelles/2018/180322_Aufruf.php

HSM stellt einen single-point-of-entry und zugleich einen single-point-of-failure dar. Das heißt, ein erfolgreicher Angriff auf das HSM kann zum Abgreifen sämtlicher Kommunikation die darüber läuft führen. Jedenfalls solange keine echte End-zu-End-Verschlüsselung implementiert ist, besteht diese Gefahr. Da es sich um ein zentralisiertes System handelt, kann ein Angriff sich aber auch auf dessen Beschädigung beschränken. Ergebnis wäre eine unvorhersehbare Unterbrechung der Anwaltskommunikation über das beA. Spätestens bei vollständiger Nutzungspflicht könnte ein Angreifer mit einem Schlag einen wesentlichen Teil des elektronischen Rechtsverkehrs jedenfalls zeitweise behindern. Nur eine dezentrale Lösung kann einen solchen Komplettausfall mit all den negativen Folgen verhindern.

Anlage(n): wie benannt