# beA Update:

# Wie geht es weiter mit dem beA?

Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ., BRAK, Berlin

***Wie geht es weiter mit dem besonderen elektronischen Anwaltspostfach (beA) – und vor allem: wann? Das fragen sich derzeit nicht wenige. Indes, das „Wie" ist zum jetzigen Zeitpunkt deutlich leichter zu beantworten als das „Wann".***

## Der Fahrplan ...

Das „Wie" ist klar. Denn einen Fahrplan zur Wiederinbetriebnahme des beA hat die BRAK-Präsidentenkonferenz in mehreren Sitzungen seit Anfang dieses Jahres aufgestellt und konkretisiert, darüber wurde an dieser Stelle laufend berichtet (zuletzt *Beyrich*, BRAK-Magazin 2/2018, 9):

Die BRAK trat im „beAthon" mit kritischen IT-Experten in Dialog und nahm deren Hinweise dankbar auf. Eine vom Bundesamt für Sicherheit in der Informationstechnologie empfohlene IT-Sicherheitsspezialistin, die Firma secunet Security Networks AG, prüfte im Auftrag der BRAK das beA-System. Die BRAK-Präsidentenkonferenz wird – nachdem die Präsidentinnen und Präsidenten der regionalen Rechtsanwaltskammern die Möglichkeit hatten, den abschließenden Bericht von secunet zu prüfen und sich dazu auch in ihren Kammervorständen zu beraten – über die weiteren Schritte zur Wiederinbetriebnahme entscheiden.

## ... und wie er erledigt wird

Was im Hintergrund geschah, seit die BRAK-Präsidentenkonferenz den Fahrplan zur Wiederinbetriebnahme festgelegt hat, lässt sich ganz einfach resümieren: Der Fahrplan wird Schritt für Schritt abgearbeitet.

Secunet nahm eine technische Analyse der beA Client Security und eine konzeptionelle Prüfung der Gesamtlösung des beA inklusive Hardware Security Modul (HSM) vor. Dabei wurden auch die im „beAthon" gewonnenen Hinweise berücksichtigt. In einem Zwischenbericht bestätigte secunet Mitte April, dass sie nach aktuellem Untersuchungsstand nichts gefunden haben, was den grundlegenden Aufbau des beA-Systems in Frage stellt. Die bisher festgestellten Schwachstellen des beA-Systems seien behebbar. Parallel arbeitete die Entwicklerin des beA-Systems, die Firma Atos, an der Behebung der Schwachstellen, die zur Abschaltung des Systems Ende Dezember letzten Jahres geführt hatten, sowie weiterer, die in der Zwischenzeit gemeldet worden waren. Umgehend behoben hat Atos insbesondere eine Schwachstelle, die das bundesweite amtliche Anwaltsregister (BRAV) betraf. Nachdem dort eine Sicherheitslücke gemeldet worden war, hatte die BRAK das Verzeichnis, das ein Bestandteil des beA-Systems ist, vorsorglich vorübergehend vom Netz genommen. Die Befunde des secunet-Zwischenberichts hat Atos berücksichtigt. secunet hat insoweit Nachtests vorgenommen und auch die von Atos vorgenommenen Reparaturen am System einer Sicherheitsprüfung unterzogen.

## Haushalts- und andere Fragen

Mit Spannung war die BRAK-Hauptversammlung Ende April erwartet worden, hatte sie doch unter anderem den Haushalt, auch für den elektronischen Rechtsverkehr zum Gegenstand. Verbunden mit einem Antrag zum Haushalt hatte eine Kammer einen Misstrauensantrag gegen zwei Mitglieder des BRAK-Präsidiums, verbunden mit Rücktrittsforderungen, gestellt. Mit überwältigender Mehrheit, bei nur einer Ja-Stimme, wurde dieser Antrag abgelehnt. Und obwohl es – sowohl zum Haushalt als auch zum beA – kritische Nachfragen und kontroverse Diskussionen gab, stärkte die Hauptversammlung dem BRAK-Präsidium in Sachen beA den Rücken:

Zum Haushalt – auch für den elektronischen Rechtsverkehr – für das Jahr 2017 wurde Präsidium und Geschäftsführung mit großer Mehrheit Entlastung erteilt. Einen Nachtragshaushalt zum Titel elektronischer Rechtsverkehr beschloss die Hauptversammlung ebenfalls mit großer Mehrheit. Und auch die Diskussion um die in den Medien und aus Teilen der Anwaltschaft seit dem Ausfall des beA in der Kritik stehenden beA-Beiträge für das kommende Haushaltsjahr (dazu Nitschke, BRAK-Magazin 2/2018, 10) zeigte, dass die Kammern hinter der BRAK stehen: Einrichtung und Betrieb des beA seien eine gesetzliche Aufgabe der BRAK, und diese müsse auch in finanzieller Hinsicht erfüllbar bleiben, betonten die Kammern. Daher müssen die Beiträge auch weiterhin an die BRAK entrichtet werden. Der Beitrag für 2019 wurde auf 52 Euro pro Mitglied festgesetzt – eine Reduzierung um 6 Euro gegenüber dem Beitrag für 2018.

## Weitere Fragen zum beA

In mehreren Kammerversammlungen und auch in den Medien wurden weitere Fragen rund um das beA diskutiert, darunter die Forderung, den Quellcode des beA-Systems zu veröffentlichen. Mit diesem Antrag befasste sich die BRAK-Präsidentenkonferenz in ihrer Sitzung am 28.5.2018 – und stand ihm durchaus aufgeschlossen gegenüber.

Allerdings will sie zunächst einmal eruiert wissen, welche Sach- und Personalkosten damit für die BRAK (also über den beA-Beitrag letztlich: für die gesamte Anwaltschaft) verbunden wären und in welcher Gestalt dies sinnvoll umsetzbar wäre – denn „Open Source" gibt es in verschiedenen lizenzrechtlichen Ausgestaltungen, deren Umsetzung auch auf technischer Seite unterschiedlichen (Kosten-)Aufwand bedeuten würde. Endgültig wird die Präsidentenkonferenz diese Frage erst entscheiden, wenn das beA wieder in Betrieb ist; denn dass die Wiederinbetriebnahme des beA Priorität hat, darüber war man sich einig.

Einen für die anwaltliche Praxis wichtigen Punkt hat die Präsidentenkonferenz in ihrer Sitzung am 28.5.2018 ebenfalls diskutiert: die Dokumentation von Störungsmeldungen des beA-Systems für etwaige Wiedereinsetzungsanträge. Der entsprechende Antrag einer Kammer wurde indes zurückgenommen, denn bereits jetzt publiziert die BRAK Störungen des beA-Systems auf einer zentralen Seite der Justiz (https://egvp.justiz.de/meldungen/), auf der auch Störungen z.B. von Gerichtsservern gemeldet werden. Selbstverständlich wird es eine Störungsdokumentation auch weiterhin geben.

## Und wann geht es weiter?

Wann das beA wieder online geht hängt vor allem davon ab, wie die BRAK-Präsidentenkonferenz entscheidet, mit den Ergebnissen des secunet-Gutachtens umzugehen. Eine Entscheidung darüber wird voraussichtlich noch nicht gefallen sein, wenn Sie diesen Beitrag druckfrisch in Händen halten. Die Präsidentenkonferenz wird aber so bald wie möglich einberufen werden. Die BRAK wird darüber ganz aktuell über ihre Online-Medien berichten und das Gutachten dann selbstverständlich veröffentlichen.

# Verschlüsselung im beA

Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ., BRAK, Berlin

Über die Verschlüsselung der Nachrichten im beA wurde und wird viel diskutiert; auch der BRAK-Hauptversammlung am 27.4.2018 lag ein (mit großer Mehrheit abgelehnter) Antrag vor, das beA auf „echte Ende-zu-Ende-Verschlüsselung" umzustellen. Das steckt hinter dieser Diskussion:

Von Ende-zu-Ende-verschlüsselter Übermittlung spricht man, wenn eine Nachricht auf dem Rechner des Absenders verschlüsselt wird und erst auf dem Rechner des Empfängers wieder entschlüsselt werden kann. Im ganz strengen Sinne des technischen Fachjargons nutzt das beA dies nicht, auch wenn die Nachrichten im beA durchgehend verschlüsselt sind:

Ein technischer Zwischenschritt – in einem Hardware Security Module (HSM), dessen Einsatz übrigens Industriestandard u.a. im Online-Banking ist – ist nötig, um eine wichtige berufsrechtliche Anforderung zu erfüllen: § 31a III 2 BRAO verlangt, dass auch Vertreter, Abwickler und Zustellungsbevollmächtigte Zugriff auf das Postfach eines Anwalts haben. Und um den normalen Arbeitsablauf in Kanzleien abzubilden, sollten Anwälte zudem ihrem Büropersonal Zugriff auf ihr Postfach gewähren können. Vereinfacht gesagt prüft das HSM, ob für diese Nutzer eine Berechtigung hinterlegt ist, und schlüsselt dann für sie den (seinerseits verschlüsselten) Schlüssel zum Öffnen der Nachricht um; die Nachricht selbst bleibt verschlüsselt.

Weshalb nutzt man für die Kommunikation zwischen Anwalt und Gericht nicht einfach De-Mail, wie manche Kritiker fordern? Dort kann Abwicklern, Vertretern u.a. kein Zugriff auf Nachrichten ermöglicht werden, ohne dass der Anwalt jede Nachricht manuell weiterleitet (oder entgegen § 26 I RAVPV seine Zugangsdaten herausgibt). De-Mail ist zudem, anders als das beA, nicht an die Anwaltszulassung gekoppelt. Und Ende-zu-Ende-verschlüsselt versendet De-Mail Nachrichten auch nicht, sie werden vielmehr entschlüsselt, um die Inhalte auf Viren zu prüfen. Der Versand Ende-zu-Ende-verschlüsselter E-Mails (oder zusätzlich verschlüsselter De-Mails) kommt aus denselben Gründen nicht in Frage.