BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

An die Vorsitzende der
Arbeitsgemeinschaft IT-Recht
im Deutschen Anwaltverein (DAV) e.V.
Frau Rechtsanwältin
Dr. Astrid Auer-Reinsdorff
Littenstraße 11
10179 Berlin

per Mail

Berlin 16.03.2018

Status des besonderen elektronischen Anwaltspostfachs (beA) und digitale Anwaltschaft
Ihr Schr. v. 15.02.2018

Sehr geehrte Frau Kollegin Dr. Auer-Reinsdorff,

die in Ihrem Schreiben vom 15.02.2018 aufgeworfenen Fragen möchte ich Ihnen wie folgt beantworten und Sie ergänzend auf die Seite www.bea.brak.de verweisen. Dort sind die meisten Ihrer Fragen bereits ausführlich beantwortet.

Wiederinbetriebnahme des beA-Systems

Fragen 1, 2, 7, 8 und 9

Derzeit findet eine Sicherheitsprüfung des beA durch eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zertifizierte Gutachterfirma, die secunet Security Networks AG aus Essen, statt. Die Beauftragung der secunet Security Networks AG mit der Erstellung eines Sicherheitsgutachtens wurde von den Präsidentinnen und Präsidenten der Rechtsanwaltskammern in der Präsidentenkonferenz am 18.01.2018 beschlossen (http://www.brak.de/fuer-journalisten/pressemitteilungen-archiv/2018/presseerklaerung-02-2018/). Das Sicherheitsgutachten soll sich dabei insbesondere auf die Frage fokussieren, ob es weiterhin mögliche Sicherheitsrisiken in der Verbindung zwischen Browser und Client Security des beA-Systems gibt.

Erste Ergebnisse dieser Prüfung sollen Ende März vorliegen. Nach Abschluss der vollständigen Prüfung des beA-Systems wird die BRAK das Gutachten veröffentlichen. Der Verlauf des weiteren Verfahrens zur Wiederinbetriebnahme des beA hängt von den Ergebnissen der Sicherheitstests ab.

Derzeit können wir deshalb noch keinen definitiven Zeitpunkt nennen, wann das beA wieder verfügbar sein wird.

HSM / Verschlüsselung von Nachrichten

Fragen 3 bis 5

Hinsichtlich der Fragen zur Verwendung des Hardware Security Moduls (HSM) und zur Verschlüsselung von Nachrichten erlaube ich mir, Sie zunächst auf die Übersicht der Firma Atos zu verweisen, die die BRAK auf der Seite www.bea.brak.de veröffentlicht hat.

Die funktionalen – berufsrechtlich vorgegebenen - Anforderungen, die den Einsatz der HSM begründen, sind insbesondere mögliche Zugriffsrechte gewillkürter Vertreter und Mitarbeiterinnen bzw. Mitarbeiter in den Rechtsanwaltskanzleien. Darüber hinaus soll insbesondere vor dem Hintergrund der Wiedereinsetzungsrechtsprechung arbeitsteiliges Arbeiten in der Kanzlei und die Postbearbeitung über ein „virtuelles Kanzleipostfach“ möglich sein. Die gesetzliche Grundlage für die Vertreterbestellung durch den Rechtsanwalt selbst ist in § 53 Abs. 2 BRAO geregelt. Dass Mitarbeitern der Zugriff auf das Postfach des Rechtsanwalts möglich sein muss, setzte der Gesetzgeber voraus. § 31a Abs. 3 Satz 3 regelt, dass die Bundesrechtsanwaltskammer die Zugriffsrechte für Kammermitglieder und andere Personen unterschiedlich ausgestalten kann.

Kein Nutzer hat im normalen Betrieb des HSM Zugriff auf Schlüsselmaterial. Die Schutzmechanismen des HSM stellen sicher, dass kein Anwender im Falle eines Angriffs auf das HSM (etwa das gewaltsame Öffnen und der Versuch des Auslesens des Speichers) Zugriff auf das Klartext-Schlüsselmaterial erhalten kann. Über das beA versandte und empfangene Nachrichten sind durchgängig verschlüsselt. Das bedeutet, dass sie auf dem Computer des Absenders verschlüsselt und erst auf dem Computer des Empfängers entschlüsselt werden. Während der Übertragung sind sie durchgehend verschlüsselt. Niemand außer dem vorgesehenen Empfänger (oder einer von diesem berechtigten Person) kann von dem Inhalt der Nachricht Kenntnis nehmen. Dies gilt auch nach der Übertragung; auch bereits gelesene Nachrichten im Posteingang können nur von dem Empfänger (oder einer von diesem berechtigten Person) gelesen werden. Die Vergabe sowie der Entzug von Rechten und Rollen in Bezug auf ein bestimmtes Postfach werden in dem jeweiligen Postfachjournal vermerkt und können hierüber von dem Postfachbesitzer nachvollzogen bzw. kontrolliert werden.

Die DataCenter von Atos haben an beiden Standorten ein mehrschichtiges Sicherheitskonzept in Bezug auf den physischen Zugang: Geländeumzäunung und Videoüberwachung, Gebäudeüberwachung mit Videokameras an den Haupteingängen, extra gesicherter DC Kernbereich mit Vereinzelungsanlage und speziellen Ausweisen, DC Käfige für verschiedene Kunden. Für die BRAK sind sämtliche beA-Komponenten in dedizierten, abgeschlossenen Käfigen und zusätzlich durch abgeschlossene Racks (mit RFID-Schlüsseln) gesichert untergebracht. Der Empfang und das Einbringen von Komponenten in das DC oder in Käfige erfolgt nur über Netz und DC Services (NDCS), DC Operations Personal oder begleitete Hersteller-Mitarbeiter. Der Zugang wird nur gestattet, wenn ein entsprechender Antrag/Change avisiert und genehmigt wurde. Für kurzfristig notwendige Wartungsarbeiten (z. B. Plattenaustausch) sind Techniker durchgehend vor Ort. Im normalen Betrieb und für Monitoring-Zwecke ist kein physischer Zugang notwendig. Der Versuch, ein HSM-Modul physisch zu öffnen, führt zur kompletten Löschung der im Modul gespeicherten Daten. Eine Wartung eines HSM Moduls kann nicht vor Ort erfolgen. Dies kann nur in den gesicherten Herstellerräumen von Atos Worldline erfolgen. Um bei einer Wartung eine Betriebsunterbrechung zu vermeiden, werden dabei erst neue Geräte vor Ort gebracht, in das System eingebunden und synchronisiert, danach die alten Geräte herausgenommen und an Atos Worldline zurückgeschickt. Bei der Umsetzung des beA sind alle technischen und organisatorischen Maßnahmen erfüllt.

Abnahme der beA-Anwendung

Frage 6

Bei der BRAK bestand und besteht ein Testteam aus externen IT-Beratern und Rechtsanwälten, das funktionale Tests der jeweils bereitgestellten Software-Version – teilweise automatisiert – durchführt. Die festgestellten Fehler werden in enger Abstimmung mit Atos geprüft, behoben und anschließend die Fehlerbehebung nachgetestet. Sodann erfolgt eine Empfehlung an das Präsidium der Bundesrechtsanwaltskammer, ob die Version abnahmereif ist oder nicht. Dabei werden die vertraglichen Vorgaben zur Abnahmefähigkeit beachtet. Darüber hinaus lässt die BRAK externe Sicherheitstests durchführen.

Für die Version 0.9, mit der die BRAK das System am 28.11.2016 in Betrieb nahm, erklärte das Präsidium der BRAK die Teilabnahme am 07.11.2016, für die Version 1.0 am 23.03.2017 und für die Version 1.1. am 18.08.2017.

Das Update zur Behebung der bekannt gemachten Sicherheitslücken wird wie beschrieben derzeit weiteren Sicherheitstests unterzogen. Von deren Ergebnis hängt die Abnahme durch das Präsidium ab.

Kapazität des beA-Systems

Frage 10

Die BRAK ermittelte die Anforderungen an die Kapazität des Systems in Workshops, anhand der Justizstatistik und über online-Umfragen in den Anwaltskanzleien. Bei 2,3 Mio. Gerichtsverfahren ergaben die Umfrageergebnisse, dass jährlich mindestens 67 Mio. elektronische Dokumente alleine im gerichtlichen Verfahren über das beA-System versandt werden müssen. Gemeinsam mit der außergerichtlichen Kommunikation rechnete die BRAK mit ca. acht Schriftsätzen pro Sekunde. Entsprechend sind die Systeme ausgelegt.

Die Atos GmbH führt im Auftrag der BRAK ein System-Monitoring durch, so dass rechtzeitig vor dem Erreichen von Kapazitätsgrenzen geeignete Maßnahmen eingeleitet werden können.

Atos führte als Teil ihrer vertraglichen Pflicht Lasttests durch, die regelmäßig wiederholt werden.

Vertragliche Vereinbarungen

Fragen 11 bis 13

Die BRAK hat im September 2014 mit der Atos IT Solutions and Services GmbH (Atos) einen „Vertrag über die Erstellung beziehungsweise Anpassung von Software“ (EVB IT-Erstellungsvertrag) geschlossen. Gegenstand des Vertrags ist die Entwicklung der Software für besondere elektronische Anwaltspostfächer (beA) sowie die laufende Wartung und Pflege der Software. Ferner hat die Bundesrechtsanwaltskammer im April 2015 mit Atos einen „Vertrag über den Betrieb des besonderen elektronischen Anwaltspostfachs" (Betriebsvertrag) geschlossen. Gegenstand dieses Vertrags ist der Betrieb des von demselben Unternehmen entwickelten beA-Zentralsystems im Rahmen eines Dienstleistungsvertrags.

Die Anwendungen werden in Rechenzentren in Deutschland gehostet. Im Übrigen verweise ich auf die Sicherheitskonzepte der Rechenzentren, die ich oben bei der Beantwortung der Fragen 3 bis 5 beschrieben habe.

Ich bitte um Verständnis, dass ich Ihnen die Einzelheiten der Service-Level-Agreements, die Teil des Betriebsvertrags sind, aufgrund der vergaberechtlichen Verschwiegenheitsverpflichtung der Bundesrechtsanwaltskammer nicht nennen kann.

Vertraglich vereinbart ist aber die Bereitstellung und der 24/7-Betrieb eines hochverfügbaren georedundanten Rechenzentrums in Deutschland mit einer Mindestverfügbarkeit in der Kernzeit täglich von 6.00 Uhr bis 24.00 Uhr von 99,9 % im Monat für die Anwendung des beA-Zentralsystems.

Downtimes sollen nach Möglichkeit ganz ausgeschlossen sein. Etwaige Wartungsfenster werden nach Möglichkeit in der Randzeit zwischen 0.00 Uhr und 6.00 Uhr eingerichtet. Sie werden mit der BRAK abgestimmt und allen Nutzern rechtzeitig angekündigt. Bislang hat die BRAK es so gehandhabt, dass Wartungsfenster auf der beA-Startseite angekündigt und auf egvp.de veröffentlicht wurden. Dieses System hat sich bewährt.

Datenschutzgrundverordnung und berufsrechtliche Anforderungen

Frage 14

Da die bereichsspezifischen Vorschriften der §§ 31a, 31c BRAO, 22 Abs. 2 Satz 1 RAVPV das Verhältnis zwischen den an der Datenverarbeitung beteiligten Stellen vorrangig regeln, liegt ein gesetzlicher Erlaubnistatbestand für die Datenübermittlung an das beA und die Datenverarbeitung durch das beA vor. Es müssen daher keine Verträge zur Auftragsdatenverarbeitung zwischen BRAK und den das beA nutzenden Rechtsanwälten abgeschlossen werden, um (u. a.) die Speicherung personenbezogener Daten im beA datenschutzrechtlich zu erlauben. Auch die ab dem 25.05.2018 geltende EU-Datenschutz-Grundverordnung (DSGVO) führt zu keiner anderen Bewertung. Die Datenverarbeitung ist auf der Grundlage von Art. 6 Abs. 1 e), Abs. 3 DSGVO in Verbindung mit §§ 31a, 31c BRAO, 22 Abs. 2 Satz 1 RAVPV zulässig. Der Abschluss von Vereinbarungen über die Auftragsverarbeitung im Sinne von Art. 28 DSGVO ist nicht erforderlich.

Quellcode und Veröffentlichung unter einer Open Source Software Lizenz

Frage 15

Ob es zielführend ist, den Quellcode der beA-Software zukünftig vollständig offen zu legen, werden wir sorgfältig prüfen und uns dabei auch von Sicherheitsexperten beraten lassen. Soweit die BRAK Standard-Software-Komponenten einsetzt, ist allerdings die Veröffentlichung des Quellcodes nicht möglich, da die BRAK darauf keinen Zugriff hat.

Ich hoffe, Ihre Fragen umfassend beantwortet zu haben. Falls Sie Rückfragen haben sollten, sprechen Sie mich bitte an.

Mit freundlichen kollegialen Grüßen

Ekkehart Schäfer
Rechtsanwalt