ANWALTSKANZLEI DIERCKS

Anwaltskanzlei Diercks | Heußweg 25 | 20255 Hamburg

Bundesrechtsanwaltskammer (BRAK)
Präsidium der BRAK
Littenstraße 9
10179 Berlin

Unser Zeichen: 110-17

Datum: 07.01.2018

Offener Brief im Hinblick auf die außerordentliche Präsidentenkonferenz am 09.01.2018

Fragenkatalog im Hinblick auf die IT-Projektleitung für das besondere elektronische Postfach (beA)

Sehr geehrte Damen und Herren Kollegen,

wie Sie wissen, steht das beA seit Beginn in der Kritik von IT-Sicherheitsexperten und Datenschützern. Dies unter anderem deswegen, weil eine Konstruktion gewählt wurde, bei der die gesamte, höchst vertrauliche, nationale Kommunikation zwischen Anwälten und Gerichten sowie Behörden und zentral über eine Plattform abgewickelt werden soll. Daneben war von Beginn an festzustellen, dass die lokal zu installierende Softwarekomponente (Client Security) Java einsetzt. Zentralisierung und Java – zwei Faktoren, die dem der Technik nicht ungeneigten Anwalt den Kopf wenigstens fragend schütteln lassen. Dies insbesondere auch deswegen, weil längst wirkungsvolle wie unkomplizierte Standards für eine sichere Kommunikation und Authentifizierung im Internet existieren, mit denen auch alternative dezentrale Szenarien denkbar gewesen wären.

Doch selbstverständlich kann auch eine zentrale Plattform sicher sein. Und natürlich auch eine solche, die Java-Komponenten einsetzt. Das ist beim beA jedoch leider nicht der Fall.

Inzwischen wissen Sie auch, dass im Zusammenhang mit dem beA nicht mehr nur Kritik im Raum steht, sondern dass nunmehr nachweislich konkre-

ANWALTSKANZLEI DIERCKS
Nina Diercks Rechtsanwältin
M.Litt (University of Aberdeen)
Beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein anerkannte Sachverständige für IT-Produkte (rechtlich)
Heußweg 25
20255 Hamburg
Tel 040 28 47 04 75
Fax 040 28 47 04 76
kontakt@anwaltskanzlei-diercks.de
www.anwaltskanzlei-diercks.de
USt-IdNr. DE278457208

te, zum Teil äußerst schwere, Sicherheitslücken aufgefunden und beschrieben worden sind.

Die Sicherheitslücken sind dergestalt, dass sich nicht nur drängende Fragen in Bezug auf die gesamte Sicherheitsarchitektonik stellen, sondern vor allem in Bezug auf die Verantwortlichkeiten der IT-Projektleitung, welche nun einmal bei Ihnen, wertes Präsidium der BRAK, liegt.

Soweit bekannt wurde, wollen Sie, wertes Präsidium, zusammen mit den Präsidenten der regionalen Kammern, diese Fragestellungen in der von Ihnen für den 09.01.2018 anberaumten Sondersitzung eruieren. Dies ist gut und richtig. Die bisherige Reaktion und Kommunikation der BRAK in dieser Angelegenheit erweckt jedoch leider den Eindruck, dass den zuständigen Verantwortlichen die aus dem Zustand des beA resultierenden sicherheitstechnischen wie IT- und datenschutzrechtlichen resultierenden Problemstellungen und Auswirkungen in ihrer Tragweite weder hinreichend bewusst sind noch dass – bei allem Respekt – überhaupt ein grundlegendes Verständnis für IT-technische Fragestellungen herrschen würde. Anders sind jedenfalls der Umgang mit dem beA-Projekt und die diesbezügliche Kommunikation der BRAK kaum zu erklären. Reaktionen wie die des pfälzischen Kammerpräsidenten (RAK Zweibrücken), der am 02.01.2018 in einem Mitgliederschreiben die folgende Einschätzung mitteilte

„*Meine Einschätzung: Den Gegnern der BRAK ist es erneut gelungen, eine Verschiebung des beA zu erreichen. Teile der Anwaltschaft begrüßen dies, da man sich ggfls. schwertut, mit der digitalen Entwicklung Schritt zu halten. Diese nachvollzienbaren Ängste vor dem Neuen werden jedoch von einigen Wenigen genutzt, um die anwaltliche Selbstverwaltung massiv anzugreifen*."

untermauern den diesseitig vorhanden Eindruck – auch wenn der Präsident der RAK Zweibrücken nicht Mitglied des verantwortlichen BRAK-Präsidiums ist - leider immens. Denn diese Aussage lässt nur darauf schließen, dass das Ausmaß der sicherheitstechnischen Lücken nicht nachvollzogen und dass vor allem nicht erkannt wird, dass die aktuelle Diskussion nicht durch „Ängste vor Neuem" von „Gegnern" des beA, sondern von Menschen getrieben wird, die höchst gerne mit digitalen Werkzeugen arbeiten würden, aber dies ganz sicher nicht um den sicherheitstechnischen Preis, der dafür derzeit zu zahlen wäre. Die Kollegen, die aus „Angst vor Neuem" beA entgegenstehen, haben im Zweifel die ganze (technische) Diskussion der letzten Tage noch nicht einmal nachverfolgt.

Das beaA ist ein Desaster. Anders lässt sich der Fall, in dem die passive Nutzung einer Software-Anwendung gesetzlich verpflichtend vorgeschrieben und eben diese Software-Anwendung zum Zeitpunkt der eintretenden gesetzlichen Verpflichtung trotz jahrelanger Entwicklungszeit und Betaphase sowie Investments von 38 Millionen EUR aufgrund von erheblichen Sicherheits- und Kapazitätsmängeln als funktionsunfähig darstellt, nicht beschreiben.

Die BRAK, die dieses Projekt im Rahmen der Selbstverwaltung für die Anwaltschaft umsetzt, steht hierfür in der vollen Verantwortung.

Vielen Kollegen und Kolleginnen stellen sich bezüglich der IT-Projektdurchführung und –leitung, den geschlossenen Vertragswerken, der IT- und Datensicherheit des beA, etwaigen Krisenplänen sowie vor allem im Hinblick auf das weitere Vorgehen in Sachen beA drängende Fragen.

Auch mir. In Folge dessen habe ich diese Fragen hier offen formuliert. Ich bitte Sie an dieser Stelle herzlich, in Ihrem eigenen Interesse und im Interesse des beA-Projektes, die Ausführungen und die Frage-

stellungen sowohl binnen Ihrer Sitzung, als auch in der weitere Projektplanung zu berücksichtigen als auch mir diese, sei es persönlich oder öffentlich zu beantworten.

Natürlich könnte ich Ihnen diese Fragen, wie es einige Kollegen bezüglich der einen oder anderen Fragestellung auch schon getan haben, im Rahmen eines IFG-Antrags stellen. Und wie Sie wissen, wären Sie dann im Rahmen des IFG gezwungen, diese Fragen soweit zu beantworten.

Wie Sie wohl bemerkt haben, ist das Vertrauen der Anwaltschaft, jedenfalls von Teilen der Anwaltschaft in das Organ der BRAK gerade aufgrund der bisher von Ihnen erfolgten Reaktion und Kommunikation in Sachen beA zutiefst erschüttert. Eine Zugehen auf die Anwaltschaft selbst, das Beantworten von Fragen und eine transparente Kommunikation sowie die Einführung einer Kultur, in der Fehler offen angesprochen und eingestanden werden, wird für die BRAK voraussichtlich der einzige Weg sein, dieses zutiefst erschütterte Vertrauen der Anwaltschaft wieder herzustellen.

Vor diesem Hintergrund bin ich guter Hoffnung, dass auch Sie, wertes Präsidium, ein starkes Interesse daran haben, dieses Vertrauen wieder herzustellen und in Folge dessen die hier gestellten Fragen nicht nur zur Kenntnis, sondern ebenso mit in Ihre Beratungen nehmen wie Sie sie im Anschluss beantworten werden.

Bevor ich zu den eigentlichen Fragestellungen komme, finden Sie hier noch einmal die in der Diskussion stehenden bislang bekannten sicherheitstechnischen Mängel des beA in der gebotenen Kürze sowie der Verständlichkeit halber vereinfacht dargestellt zusammengefasst. Wenn Ihnen diese alle geläufig sein sollten, können Sie sich gerne direkt zu den Fragen auf Seite 10 begeben.

1. Zusammenfassung der bekannten Sicherheitstechnische Mängel des beA

Nachfolgend finden Sie kurze, so verständlich als möglich gehaltene, Ausführungen und Erläuterungen zu den folgenden Punkten:

- Grundlegende Problematik: Verschlüsselungstechnologie der Nachrichten im beA und Zentralisierung
- Webinterface torpediert Ende zu Ende Verschlüsselung
- Lokale beA-Software – Java
- Verwendung veralteter Libaries
- beA-Anwendung unterstützt keine aktuellen Betriebssysteme
- Gefahr des Cross-Site-Sciptings (XXS)
- Suboptimale https-Konfiguration der beA-Webanwendung
- beA-Client verteilte private Keys
- Neues Sicherheitszertifikat öffnet vollständig die IT-Sicherheit der Anwender
- Sendebeschränkungen als „Sicherheitsfeature“ / Serverlast

1.1. Grundlegende Problematik: Verschlüsselungstechnologie der Nachrichten im beA und Zentralisierung

Das beA soll – vereinfacht ausgedrückt – wie folgt für eine Sicherheit bei der Übertragung von Nachrichten nebst Schriftsätzen etc. pp. sorgen:

Eine Nachricht wird seitens des Absenders mit einem sog. „private Key" verschlüsselt. Diesen „private Key" darf nur der Absender selbst kennen (sonst wäre er auch nicht „private"). Dieser private Key wird wiederum mit einem „public key" des Empfängers verschlüsselt („public key" deswegen, weil dieser Schlüsselteil eben zwingend öffentlich zur Verfügung gestellt wird). In Folge dessen ist der vom Versender bestimmte Empfänger der Einzige, der die für ihn bestimmte Nachricht entschlüsseln kann.

Soweit so gewöhnlich.

Das beA wirbt mit eben einer solchen sicheren Ende-zu-Ende-Verschlüsselung. In den beA FAQ heißt es unter Punkt c) Technische Fragen bis heute:

„Über das beA versandte und empfangene Nachrichten sind Ende-zu-Ende 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."[1]

Diese Aussage ist jedoch schlicht falsch. Eine derartige Ende-zu-Ende Verschlüsselung findet beim beA nicht statt. Vielmehr verfügt das beA über eine Funktion, die die eigene Sicherheitsarchitektonik an dieser Stelle aushebelt. Es sollte eine Weiterleitungsfunktion des Empfängers existieren, d.h. der Empfänger und Nutzer eines Postfaches sollte definieren können, dass an ihn versandte Nachrichten auch von anderen durch ihn berechtigten Nutzern gelesen können werden sollten. So weit so verständlich.

Allerdings wird zu diesem Zweck jede Nachricht zwar beim Empfänger verschlüsselt, innerhalb des HSM aber „umgeschlüsselt" und so dann an den oder die Empfänger weitergeleitet. Um diese „Umschlüsselung" durchführen zu können, ist es notwendig, dass sich die privaten Keys eines jeden Anwalts im Zugriff des HSM befinden.

Dies bedeutet wiederum, dass die Aussage *„Niemand außer dem vorgesehenen Empfänger (oder einer von diesem berechtigten Person) kann von dem Inhalt der Nachricht Kenntnis nehmen"* ebenso falsch ist wie die Behauptung, es existiere eine Ende-zu-Ende-Verschlüsselung.

Die BRAK und der zuständige Dienstleister können jederzeit Zugriff auf die Nachrichten nehmen. Zwar ist die Information auf der Seite der BRAK *„Die Nachricht selbst liegt bei diesem Verfahren zu keiner Zeit unverschlüsselt vor. Der Nachrichtenschlüssel liegt außerhalb des HSM ebenfalls zu keiner Zeit unverschlüsselt vor*."[2] richtig, aber die dafür notwendigen Schlüssel liegen – sinnbildlich gesprochen – eben

[1] http://bea.brak.de/fragen-und-antworten/c-technische-fragen/, Abruf am 05.01.2018.
[2] http://bea.brak.de/technische-informationen-zum-verschluesselungsverfahren-beim-bea/, Abruf am 05.01.2018.

direkt daneben im Zugriff des HSM. Folglich können die BRAK, der Dienstleister - oder jeder unbefugte Dritte, der sich Zugang zum System verschafft – diese Nachrichten sehr wohl zur Kenntnis nehmen.[3]

Damit wird deutlich, dass die Vertraulichkeit der gesamten Kommunikation der deutschen Anwaltschaft von zweierlei abhängt: Zum einen davon, dass der Dienstleister einschließlich seiner Mitarbeiter absolut vertrauenswürdig ist. Zum anderen davon, dass das HSM und die sonstigen beA-Infrastruktur nach dem jeweils aktuellsten Stand der Technik vor Angriffen, Eingriffen und sonstigen Manipulationen bestmöglich geschützt sein muss. Dabei muss auch sichergestellt sein, dass die IT von Anwälten, die über keine nennenswerten Sicherheitskonfigurationen in ihrer IT-Struktur verfügen, keine Einfallstore für Hacker in das beA darstellen können. Dabei geht es nicht nur darum, dass die Nachrichten direkt ausgelesen werden, sondern auch darum, dass z.B. sichergestellt wird, dass die Nachrichten nicht unbefugt weitergeleitet werden, d.h. die Empfänger manipuliert werden.[4]

Wie eingangs bereits erwähnt, ist eine IT-Infrastruktur, die die gesamte Kommunikation der deutschen Anwaltschaft untereinander sowie mit Gerichten und Behörden abwickelt, selbstverständlich ein hochinteressantes Ziel für Cyberangriffe. Sei es von Hackern, die sich finanzielle Vorteile erhoffen, sei es von in- und ausländischen Diensten oder schlicht von sog „Script-Kiddies“, die aus Spaß an der Freude oder als Mutprobe versuchen, in die Systeme einzudringen und Schäden anzurichten.

In Folge dessen muss nicht nur ein bestmöglicher Schutz nach dem aktuellsten Stand der Technik vorhanden sein, sondern es muss ein Notfall-Maßnahmenplan im Fall von Angriffen vorliegen. Sie alle wissen, was es bedeuten würde, wenn die Plattform, über die der gesamte elektronische Schriftverkehr der deutschen Anwaltschaft abgewickelt wird, korrumpiert würde. (Und hier liegt im Übrigen auch ein entscheidender Unterschied zur postalischen Übertragung oder per Telefax. Selbstverständlich ist es faktisch relatives leicht Briefe abzufangen oder Telefonleitung zur Faxübertragung zu manipulieren – hier handelt es sich jedoch um dezentrale Kommunikation, so dass eben ein zentraler Ein-/Angriff nicht möglich ist.)

Hinsichtlich der Sicherheit des HSM heißt es bloß: „*Dabei handelt es sich um spezielle Hardwarekomponenten, die unter Einsatz kryptographischer Schlüssel bestimmte vordefinierte Funktionen ausführen. Sie sind dabei gegen jede Art von Manipulation geschützt*.“

Dies ist erstaunlich. Keine IT-Einrichtung ist 100%ig geschützt. Gerade seriöse IT-Anbieter würden dies nicht behaupten. Es ist immer nur ein bestmöglicher Schutz nach dem aktuellen Stand der Technik zu versichern. Dieser Satz ist nicht vertrauensbildend. Der Satz ist verstörend.

Dass ein bestmöglicher Schutz nach dem jeweils aktuellen Stand der Technik vor Manipulationen gegeben ist, lassen die weiteren Ausführungen zu den bislang bekannten Sicherheitslücken mehr als bezweifeln.

---

[3] Ausführlich hierzu u.a.: Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html; Borchers - 34C3: Das besondere Anwaltspostfach beA als besondere Stümperei, heise, 28.12.2017 https://www.heise.de/newsticker/meldung/34C3-Das-besondere-Anwaltspostfach-beA-als-besondere-Stuemperei-3928474.html.

[4] Lt. Drenger einer der ersten Angriffspunkte, wie er in einer Diskussion auf Twitter mitteilte.

1.2. Webinterface torpediert Ende zu Ende Verschlüsselung

Die Nutzer der BeA-Anwendung kommunizieren mit dieser generell über ein Webinterface. Ein Webinterface verträgt sich jedoch nicht mit einer Ende-zu-Ende-Verschlüsselung, da der Server jederzeit anderen Javascript-Code schicken kann, der die Verschlüsselung aushebelt oder Nachrichten unverschlüsselt an Dritte weiterleitet.[5]

1.3. Lokale beA-Software – Java

Die lokal zu installierende Software (beA Client) verwendet ebenfalls Java. Java ist eine Programmiersprache, welche zunehmend weniger Verwendung findet. Dies unter anderem, weil immer wieder unbekannte Sicherheitslücken im Code bzw. in Bibliotheken auftreten. Java-Applikationen werden auch genutzt, um Schadsoftware auf Rechnern zu platzieren. [6] Viele Nutzer haben Java bzw. das notwendige Envionment, um Java ausspielen zu können, aus diesem Grunde nicht mehr auf den Rechnern installiert" und/oder den Computer so konfiguriert, dass Java-Applikationen bzw. Content nur dann verarbeitet werden darf, wenn entsprechende Sicherheitszertifikate hinterlegt sind (bekanntermaßen hat es hier auch mehr als ein Problem gegeben, dazu so gleich).

1.4. Verwendung veralteter Libaries

Doch nicht nur, dass Java verwendet wurde. Es wurden bei der Programmierung veraltete Programmbibliotheken verwendet. Hierbei handelt es sich nicht um eigenständige, lauffähige Software, sondern um Hilfsmodule, die „Unterprogramme" oder Routinen, also Lösungswege für thematisch gleiche Programmfragen anbieten. Es sind sozusagen vorgefertigte Hilfsbausteine, die bei der Programmierung helfen.

Die bei der Programmierung des bea Clients verwendeten Bibliotheken sind jedoch veraltet und verfügen über bekannte (!) Sicherheitslücken. Eine der verwendeten Bibliotheken wird seit Oktober 2015 nicht mehr unterstützt. Nutzer sind schon lange aufgefordert, entsprechend neuere Bibliotheken zu verwenden.[7]

---

[5] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;

[6] https://www.heise.de/download/blog/Wie-sicher-ist-Java-3632920

[7] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html; Hinweis, dass Version 1.1 der in Rede stehenden Bibliothek nicht mehr unterstützt wird: https://logging.apache.org/log4j/1.2/.

1.5. beA-Anwendung unterstützt keine aktuellen Betriebssysteme

Erschreckenderweise unterstützt die beA-Anwendung laut den offiziellen Anwenderhinweisen keine aktuellen Betriebssysteme.[8] An Linuxsystemen wird offiziell nur OpenSUSE 13.2 unterstützt - dessen Support endete im Januar 2017;[9] Windows wird demnach von Vista bis 8.1 unterstützt, Windows 10 findet man nicht, und auch von OS X wird nur die schon etwas ältere Version El Capitan unterstützt. [10]

1.6. Gefahr des Cross-Site-Sciptings (XXS)

Cross-Site-Scripting bzw. webseitenübergreifendes Skripting bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen. Dabei werden Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen Kontext eingefügt werden, der als vertrauenswürdig eingestuft wird. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden. Ziel ist es meist, an sensible Daten des Benutzers zu gelangen. Die Bezeichnung „Cross-Site" bezieht sich darauf, dass der Angriff zwischen verschiedenen Aufrufen einer Seite stattfindet, in der Regel jedoch nicht darauf, dass unterschiedliche Websites beteiligt sind. Meist werden für diese Angriffsart aufgrund ihrer weiten Verbreitung Script-Sprachen – insbesondere JavaScript – genutzt: daher „Scripting". [11]

Im Hinblick auf das beA gibt es eine Informationsseite der BRAK zum bea (bea.brak.de). Diese ist nur mittels einer (unsicheren) http-Verbindung erreichbar. Damit sind Cross-Site-Scripting-Angriffe denkbar, in dem Anwender zunächst die Informationsseite aufrufen und sich von dort zum beA-Login begeben.[12]

1.7. Suboptimale https-Konfiguration der beA-Webanwendung

Auch die HTTPS-Konfiguration der eigentlichen beA-Webanwendung ist nicht optimal, so kommt kein HSTS zum Einsatz.[13] HSTS (HTTP Strict Transport Security) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen, der vor Aushebelung der Verbindungsverschlüsselung schützen soll. Hierzu kann ein Server dem Browser des Anwenders mitteilen, in Zukunft für eine definierte Zeit ausschließlich verschlüsselte Verbindungen für diese Domain zu nutzen. Hierdurch wird die Anwendung von sogenannten

---

[8] Anwenderhinweise zum beA seitens der BRAK https://www.bea-brak.de/xwiki/bin/view/BRAK/%2300002., abgerufen am 06.01.2018.
[9] Hinweis zum Ablauf des Supports: https://en.opensuse.org/Lifetime, abgerufen am 06.01.2018.
[10] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html; Hinweis, dass Version 1.1 der in Rede stehenden Bibliothek nicht mehr unterstützt wird: https://logging.apache.org/log4j/1.2/.
[11] Vgl vorstehender Absatz mwH https://de.wikipedia.org/wiki/Cross-Site-Scripting.
[12] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;
[13] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;

„Man-in-the-Midddle-Angriffen besser geschützt, die sich ansonsten bereits vor dem Zustandekommen einer verschlüsselten Verbindung dazwischen schalten können.[14]

1.8. beA-Client verteilte private Keys

Wird der beA-Client lokal installiert wird, wird damit ein lokaler https-Server betrieben (auch „localhost" genannt). Ein lokaler Server ist ein Server, der auf einem Arbeitsplatzrechner (eben lokal) eingerichtet ist. Damit Verbindungen zwischen beA und diesem lokalen https-Server nicht zu einer Sicherheitszertifikatswarnung führen, wurde dafür ursprünglich ein echtes, von Browsern akzeptiertes signiertes Zertifikat genutzt. Sicherheitszertifikate dienen im Internet – wieder einmal sehr vereinfacht ausgedrückt - der Beurteilung, ob es sich bei einer Website, einem Server oder einer Anwendung, die Sie gerade besuchen oder nutzen, auch um diejenige handelt, für die sie sich ausgibt. Dies dient natürlich insbesondere dazu „Man-in-the-Middle-Angriffe" zu unterbinden. D.h., Vorsorge dafür zu tragen, dass sich nicht Dritte für eine vertrauenswürdige Stelle ausgeben können und z.B. nur so tun als seien sie die beA-Anwendung.[15]

Für das vorgenannte Zertifikat wurde die Domain bealocalhost.de registriert. Die Domain verweist (natürlich) jedoch auf keine Adresse im Netz, sondern auf die Localhost-Adresse (127.0.0.1).[16]

Das Problem im beA-Fall war zum einen, dass die Software, d.h. der beA-Client, die https-Verbindung zu bealocalhost.de selbst durchführt. Damit bietet aber eine solche HTTPS-Verbindung keinerlei Schutz. Ein Man-in-the-Middle-Angreifer hätte durch manipulierte DNS-Antworten Anfragen nach bealocalhost.de auf seinen eigenen Server umleiten und dort eine falsche Version der beA-Software präsentieren können.[17]

Und zum anderen wurde mit dem Sicherheitszertifikat auch der private Key als Teil der Software übermittelt. Ein Sicherheitszertifikat, das einen privaten Key mit sich führt (das darf nun einmal nicht passieren, dieser muss privat bleiben!) verstößt jedoch gegen die grundlegenden Regeln der Zertifizierungsstellen. In Folge dessen musste das Sicherheitszertifikat des Clients binnen 24 Stunden nach Kenntnis vom Herausgeber für ungültig erklärt werden. [18]

Darauf aufmerksam wurde Markus Drenger, der entsprechend diesen Verstoß meldete.

---

[14] Vgl. auch und weiterführende Informationen:
https://de.wikipedia.org/wiki/HTTP_Strict_Transport_Security.
[15] Vgl. vorstehender Absatz auch: https://de.wikipedia.org/wiki/Lokaler_Server und
https://de.wikipedia.org/wiki/Localhost.
[16] Per Internetstandard (RFC 2606 und RFC 6761) sind einem lokalen Server immer die IP-Adresse 127.0.0.1 und der korrespondierende Domainname localhost zugewiesen.
[17] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018,
https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html;
Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017
https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;
[18] Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018,
https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html;
Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017
https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;

[Auf die Peinlichkeit, dass die BRAK dann zunächst mitteilte, das Zertifikat „abgelaufen“ und so dann erklärte, es sei durch eine „nicht nur Anwaltschaft zugelassenen Person“ „kompromittiert“ worden, was mit an Sicherheit grenzender Wahrscheinlichkeit bei einer Vielzahl von technisch nicht zu sehr versierten Kollegen den Eindruck erweckte, ein Dritter habe das Zertifikat von außen angegriffen und zerstört, soll jetzt an dieser Stelle nicht weiter eingegangen werden.]

Als Glück im Unglück kann man hier nur beschreiben, dass wir alle hiervon von Markus Drenger aufmerksam gemacht wurden.

1.9. Neues Sicherheitszertifikat öffnet vollständig die IT-Sicherheit der Anwender

Der von der BRAK beauftragte Dienstleister Atos Information Technology GmbH reagierte und stellte ein neues Zertifikat zur Verfügung. Bekanntermaßen rief die BRAK dann auch noch vor Weihnachten umgehend dazu auf, ein neues „Sicherheitszertifikat“ zu installieren.

Hierbei handelte es sich zum einen um ein sogenanntes Root-Zertifikat. Also ein Grund- oder Wurzel-Zertifikat. Solche Zertifikate sind vom Herausgeber selbstzertifiziert. Die beA-Anwender sollten dieses Zertifikat ausdrücklich installieren.

Dieses Zertifikat wird nun wieder für den lokalen https-Server genutzt. Doch am grundlegenden Problem änderte sich nichts: Wieder ist der private Key Teil der Software. Und wieder können Man-in-the-Middle-Angriffe wie zuvor beschrieben stattfinden. Doch nun können diese noch ganz andere Auswirkungen haben. Denn mit einem Root- oder Stammzertifikat und dem vorhandenen private Key könnten Angreifer beliebige Zertifikate auf Basis des Root-Zertifikats signieren – also etwa für amazon.de, facebook.de oder für die von Ihnen sonst bevorzugten Online-Seiten. [19]

Die Installation dieses Zertifikats für die beA-Software reißt also ein offenes Scheunentor in die IT-Infrastruktur der Anwaltsbüros ohne gleichen.

Vor der Installation eines solchen Root-Zertifikats warnen Browser wie Betriebssystem ausdrücklich – eben weil es ein immens hohes Sicherheitsrisiko darstellt. Das Eingehen eines solchen Sicherheitsrisikos würde keine seriöse Bank oder ein seriöses Handelsunternehmen mittels eines Zertifikats verlangen.

Die BRAK jedoch, die angeblich ein sicheres System zur Kommunikation schaffen wollte, verlangte von Ihren Mitgliedern eben dies. Und zwar ausdrücklich. In der Anweisung zur Installation des Zertifikats wurde ausdrücklich darauf gedrungen, die Sicherheitswarnungen zu ignorieren.

Es ist vollkommen unverständlich, wie die BRAK dies von Ihren Mitgliedern verlangen konnte und erst auf Drängen von IT-Sicherheitsexperten und Stimmen aus Anwaltschaft wie Medien zur Deinstallation riet.

---

[19] Vgl. Böck - Noch mehr Sicherheitslücken im Anwaltspostfach, golem, 04.01.2018, https://www.golem.de/news/bea-noch-mehr-sicherheitsluecken-im-anwaltspostfach-1801-131942.html; Drenger/Rohrbach – Talk auf dem 34C3 zum beA vom 28.12.2017 https://video.golem.de/security/20355/talk-von-markus-drenger-auf-dem-34c3-zum-bea.html;

1.10. Sendebeschränkungen als „Sicherheitsfeature“ / Serverlast

Als „Sicherheitsfeature“ wird weiter erwähnt, dass nur Anhänge von 30 MB versendet werden können. Und dass nur alle 15 Minuten Nachrichten versendete werden können. Das gilt auch für Terminalserver über die beA in größeren Kanzleien betrieben werden.

In wie weit dies mit der täglichen Praxis von Anwälten und Kanzleien vereinbar sein soll, die täglich ein hohes Aufkommen an Anwalts- und Gerichtskorrespondenz zu bewältigen haben, ist nicht erklärlich.

Weiter ist nicht erklärlich, warum offensichtlich die Serverkapazitäten nicht ausreichend sind. Bislang sind gerade einmal 65.000 von 165.000 Anwälten im beA registriert – und trotzdem gab es bereits jetzt Instabilitäten, weil die Server den Anfragen nicht standhielten.

1.11. Zusammenfassung - Sicherheitslücken

Aus dem Vorstehenden ergibt sich, dass vorliegend nicht nach Inbetriebnahme eine oder zwei unentdeckte Softwarefehler, die mit ein oder zwei Patches beseitigt werden können, bestehen, sondern dass an sich nicht zu erklärende strukturelle Fehler in der Anlage des Systems und in der Programmierung vorliegen.

Hinzu kommt, dass bislang nur recht oberflächlich nach Fehlern gesehen wurde, da tiefer gehende Informationen und Zugänge seitens der BRAK und dem ausführenden Dienstleister bis heute verhindert werden. Hier wurde wohl der Grundsatz „Security by Obscurity“, also „Sicherheit durch Unklarheit“ ausgegeben. Das Problem an diesem „Sicherheitsprinzip“ ist jedoch, dass Geheimnissen zu eigen ist, dass diese kein Geheimnis bleiben. Der Nachteil dieses Prinzips folgt damit auf dem Fuße: Vermeintliche Sicherheitsmethoden können nicht hinreichend auf ihre Wirksamkeit extern überprüft und gegebenenfalls unwirksame Sicherheitsverfahren aufgedeckt, verbessert und/oder ersetzt werden können.

Mit dem Inkrafttreten der DSGVO wird diese Sicherheitsmethode darüber hinaus weiter erschüttert. Schließlich sind spätestens ab diesem Zeitpunkt Zweifel technisch und organisatorische Maßnahmen zur Datensicherheit nachzuweisen Der allgemeine Verweis auf eine „sichere Handhabung“ wird dann so nicht mehr genügen.

Es drängt sich vorliegend – leider – der Verdacht auf, dass unter dem Schlagwort „Security by Obscurity“ der Auftraggeber vom Auftragnehmer in einer (falsche) Sicherheit gewiegt werden sollte.

Denn wenn schon an der Oberfläche derartige Fehlkonstruktionen, wie hier geschildert wurden, zu Tage treten, ist nicht davon auszugehen, dass die sonstigen Programmierleistungen mit der gebotenen Sorgfalt und nach dem Stand der Technik durchgeführt wurden. Dies gilt ganz besonders für das HSM. Dass dieses tatsächlich vor „jeglichen Manipulationen sicher ist“, darf angesichts der bereits bei einer oberflächlichen Betrachtung zu Tage getretenen technischen Mängel begründet bezweifelt werden.

2. Fragen an die Verantwortlichen des beA

Aus dem Vorstehenden und der damit verbundenen Tatsache, dass derzeit eine nicht funktionsfähige Software zum Preis von 38 Millionen EUR vorliegt, ergeben sich eine Vielzahl von Fragen im Hinblick auf das beA-Projekt an die Verantwortlichen der BRAK.

2.1. Art der Auftragsvergabe

Warum ist der Auftrag zur Erstellung des beA im Rahmen eines freien Vergabeverfahrens erfolgt, obwohl üblicherweise Projekte dieser Größenordnung nur im Rahmen von öffentlichen Ausschreibungen vergeben werden (und zwar unabhängig von der Fragestellung, ob der Auftraggeber gesetzlich hierzu verpflichtet ist oder nicht)?

Was waren die Gründe, die zur Vergabe des Auftrags an die Atos Information Technology GmbH führten.

2.2. Zentralisierung des Systems

Warum ist eine Lösung präferiert worden, bei der zwingend die gesamte nationale Anwalts- und Gerichtskorrespondenz zentral über ein System verarbeitet wird?

Obwohl damit die Funktionsfähigkeit der Rechtspflege in Deutschland von diesem einen zentralen System abhängig ist?

2.3. Dezentrale Alternativen

Wurde überhaupt über dezentrale Alternative, wie z.B. verschlüsselte Nachrichten und Authentifizierungen der Beteiligten nachgedacht?

Warum wurden nicht dezentrale Alternativen basierend auf E-Mail-Lösungen entwickelt? Hier existieren standardisierte ausgereifte Verschlüsselungs- und Authentifizierungsmethoden, die entsprechend weiterentwickelt und modifiziert hätten werden können, um einen sicheren elektronischen und praktikablen Rechtsverkehr der Anwälte ermöglicht hätten.

Warum musste für die Anwaltschaft zwingend eine „neue, eigene“ Lösung aufgebaut werden?

2.4. Vertreterversand über HSM-Lösung

Und wenn eine zentrale Lösung gewählt werden musste, warum eine Lösung gewählt, bei der es zwingend notwendig ist, die Nachricht derart umzuschlüsseln?

Warum war keine Lösung wie die Folgende denkbar: Der Empfänger (Herr Özgür) von Nachrichten, meldet dem System, dass Nachrichten sogleich an Partnerin Müller und ReFa Herrn Meier zu senden sind. Diese „Meldung“ ist dann als Information unmittelbar mit der Adresse des Empfängers verknüpft. Will ein Anwalt oder ein Gericht an Herrn Kollegen Özgür eine Nachricht senden, taucht unmittelbar der Hinweis/die Information auf, dass diese Nachricht sogleich an Partnerin Müller und ReFa Herrn Meier zu senden ist. In solch einem Fall hätte der Versender die Nachrichten sogleich entsprechend versenden können, bzw. er wäre verpflichtet, sie an die angegebenen Personen zu senden. Eine Umschlüsselung in einer ominösen Blackbox wäre nicht notwendig.

2.5. Anwaltspostfächer und Anwenderfreundlichkeit

Einer der maßgeblichen Kritikpunkte der BRAK am EGVP war die vorgebliche Anwenderunfreundlichkeit. Der elektronische Rechtsverkehr müsse so einfach wie E-Mail funktionieren.20

Hierbei fragt sich dann, warum eine der E-Mail-Anwendung ähnliche Webanwendung geschaffen wurde, die nicht nur die E2E-Verschlüsselung konterkariert, sondern auch noch hochgradig benutzerunfreundlich ist (z.B. hochgeladene Anlagen müssen erneut benannt werden).

Mit der Praxis verträgt sich auch nicht, der totale Zuschnitt des Anwaltspostfachs auf den Anwalt nicht. Weder ist dabei bedacht worden, dass in der täglichen Sekretariatspraxis natürlich ständiger Zugriff auf Briefe und Faxe herrscht und die/der ReFa sich nicht jeweils als zum Empfang oder Versand der Dokumente gesondert berechtigt ausweisen muss. Noch wurde daran gedacht, dass Anwälte natürlich durchaus auch den Arbeitsplatz wechseln. Der Hinweise diese Fälle bitte von Beginn an (arbeits-)vertraglich zu regeln, ist wohl möglich, aber wohl nicht im Sinne einer „einfachen“ Lösung.

Vor diesem Hintergrund stellt sich die Frage, in wie weit bei der Bestimmung des Anforderungskatalogs/der Leistungsumfänge der Software-Anwendung praktische Anwendungsszenarien eine Rolle spielten?

2.6. Vertragliche Regelungen zwischen der BRAK und atos GmbH in Bezug auf die Software-Entwicklung und - Pflege

Hinsichtlich des Vertragswerkes stellen sich vor dem Hintergrund des derzeitigen Ist-Zustandes und des Umgangs viele Einzelfragen, von denen an dieser Stelle jedenfalls die folgenden sehr grundlegenden genannt werden sollen:

2.6.1. Lastenheft

Welche Anforderungen wurden seitens des Auftraggebers (BRAK) im Lastenheft oder einer vergleichbaren Auftragsbeschreibung festgelegt.

2.6.2. Pflichtenheft

Welche Leistungen wurden im Pflichtenheft oder einem vergleichbaren Dokument als vertragsgegenständlich zu erbringende Leistungen festgehalten? Welche Gegenleistungen sind für welche Leistungen vereinbart?

2.6.3. Agile Projektabwicklung

Wenn eine agile Projektabwicklung vereinbart und in Folge dessen auf klassische Lasten- und Pflichtenhefte verzichtet wurde, welche zu erfüllenden Grundkriterien und welche Form der Projektkoordinierung zur Überprüfung und Nachhaltung des Projektfortschritts wurden festgelegt?

Welche Leistungserbringungen lösen/lösten hier jeweils Ansprüche auf die Gegenleistung aus?

Waren Kostendeckelungen für Sprints vorgesehen?

---

[20] http://www.brak.de/w/files/stellungnahmen/Vorschlaege_Akzeptanz_ERV.pdf

Waren Kostendeckelungen für die Gesamterstellung der beA-Software vorgesehen?

2.6.4. Verantwortlicher Ansprechpartner

Ausweislich des Organigramms der BRAK ist Hannes Müller für die Projektleitung des BRAK verantwortlich.

a) Ist Hannes Müller auch im IT-Vertrag als weisungsbefugter Ansprechpartner auf Seiten des Auftraggebers benannt?

b) Wenn nicht, wer wurde als weisungsbefugter Ansprechpartner auf Seiten des Auftraggebers im Vertrag benannt?

2.6.5. Abnahmen/Milestones

Sind Abnahmen/Milestones für konkrete Leistungen vereinbarten worden? Wenn ja, welche?

Gab es eine Gesamtabnahme vor Inbetriebnahme der Anwendung? Was wurde im Abnahmeprotokoll vermerkt?

2.6.6. Durchführung von Abnahmen

Wer hatte auf Seiten des Auftraggebers, also der BRAK, die Software oder Teile der Software nach den jeweiligen Projektabschnitten endgültig abgenommen bzw. freigegeben?

2.6.7. Regelung in Bezug auf Unterauftragnehmer

Wie sehen die Regelungen im Hinblick auf die Einschaltung von Unterauftragnehmern aus? Welche Kontrollmöglichkeiten hat der Auftraggeber (die BRAK)? Wie wurden diese Kontrollmöglichkeiten ausgeübt?

2.6.8. Festlegung von Prozessen zur Feststellung der Funktionsfähigkeit und Sicherheit der gesamten Software-Anwendung

Welche Prozesse sind festgelegt worden, um die Funktionsfähigkeit und Sicherheit der Anwendung vor der Inbetriebnahme und während der Inbetriebnahme zu sichern? (Pen-Tests, Sicherheitsprüfungen, Audits etc. pp.)

Gibt es festgelegte Prozesse für technische Krisenfälle, wie etwa die seit den Weihnachtstagen vorliegenden?

2.6.9. Regelung zur Nicht- oder Schlechtleistung

Welche Regelungen im Falle von Nicht- oder Schlechtleistungen seitens des Auftragnehmers sind getroffen worden?

Sind – wie in Software-Erstellungs- und IT-Entwicklungsverträgen üblich – Formen der Nicht- und Schlechtleistung definiert worden?

2.6.10. Pflicht zur Unterhalt von Versicherungen

Wurde eine Pflicht zur Unterhaltung einer Versicherung vom Auftragnehmer für den Fall von Schäden auf Seiten des Auftraggebers bzw. der Endnutzer des Auftraggebers, die auf Schlechtleistungen des Auftragnehmers beruhen, festgeschrieben?

2.6.11. Software-Pflegevertrag

Wurde neben dem Software-Entwicklungsvertrag ein Software-Pflegevertrag geschlossen?

Für welche Leistungen wird ein jährlicher Betrag von 10 Millionen EUR berechnet?

2.6.12. Auditierung, Sicherheitsprüfung

Wenn eine Auditierung des beA-Anwendung durch die Firma SEC Consult durchgeführt wurde, warum wurden die offen liegenden Lücken nicht gefunden oder wenn diese gefunden wurden, warum wurden diese nicht behoben?

Warum wurde das letzte Audit im Jahr 2015 durchgeführt?

Wieso ist keine erneute Auditierung/Sicherheitsprüfung angesetzt worden, bevor die Software zu einer gesetzlich verpflichtenden Anwendung wird, d.h. im vierten Quartal 2017?

Wieso ist nicht das BSI als unabhängige Prüfstelle angerufen worden, wenn es doch um die Funktionalität der Rechtspflege in Deutschland mit dem beA geht? Auch diese Frage ist bitte unabhängig von der Tatsache der „Selbstverwaltung“ zu betrachten.

2.7. Kenntnis von Sicherheitslücken

Der bei der BRAK verantwortliche Leiter des Projekts muss von den bestehenden Sicherheitslücken bzw. IT-technischen Mängeln Kenntnis gehabt haben.

Entweder aufgrund des Audits und/oder aufgrund der Abstimmungen im Projektverlauf.

Warum hat der verantwortliche Leiter auf Seiten der BRAK diese IT-sicherheitstechnischen Mängel nicht beanstandet? Warum wäre die Anwendung so online gegangen?

2.8. Verteilen eines Root-Zertifikats

Ein Großteil der Anwälte ist – auch heute noch – technisch relativ unbedarft. Das muss ein Anwalt auch nicht zwingend sein. Ein Anwalt muss nicht wissen, was ein Root-Zertifikat ist und was dieses mit einem private Key für Auswirkungen haben kann.

Aber wie kann die BRAK denn ihren Mitgliedern ernsthaft empfehlen, ein solches Root-Zertifikat zu installieren? Und in die Anleitung dazu auch noch zu schreiben, die Sicherheitswarnungen müssen ignoriert werden?

Wer zeichnet dafür bei der BRAK verantwortlich?

War dem Verantwortlichen bei der BRAK bewusst, welche Gefährdung der IT-Sicherheit jedes einzelnen Kanzlei-Rechners, auf dem dieses Zertifikat, installiert wird, einhergeht?

Wenn es dem Verantwortlichen bei der BRAK nicht bewusst war, wieso war diese Person mit der Leitung eines IT-Projekts wie beA betraut? Jedenfalls, warum war diese Person ohne zusätzliche, dann dringend notwendige, externe Expertise mit der Leitung dieses Projekts betraut?

2.9. Hinzuziehung von sachverständigen Experten zur Unterstützung der BRAK

Warum hat sich die BRAK bis jetzt keine sachverständigen Experten auf ihrer Seite beigezogen und sich (scheinbar) stets auf die Aussagen des Dienstleisters verlassen?

Wird die BRAK nun mehr eigene Sachverständige beiziehen?

Wer werden diese Sachverständigen sein?

2.10. DSGVO (Datenschutzgrundverordnung)

Es scheint nicht so, als sei die Anwendung DSGVO-konform ausgestaltet und/oder als seien die Beteiligten auf die DSGVO vorbereitet. Doch mit dem besonderen elektronischen Anwaltspostfach werden personenbezogene Daten und in Teilen sogar besonders sensible personenbezogene Daten im Sinne von Art. 9 DSGVO verarbeitet – mit der Verarbeitung personenbezogener Daten unterliegt diese Anwendung der DSGVO. Die Datenschutzgrundverordnung tritt am 25. Mai 2018 in Kraft.

Die Verarbeitung der eigenen personenbezogenen Daten, der Mitarbeiterarbeiterdaten sowie der Mandantendaten erfolgt im Auftrag des jeweiligen Anwalts/der jeweiligen Anwältin. Der Verantwortliche für die Datenverarbeitung (also der Anwalt) ist nach Art. 28 DSGVO verpflichtet „nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“ zusammenzuarbeiten. Der Verantwortliche muss sich die ordnungsgemäße Verarbeitung durch den Auftragsverarbeiter zu sichern und sich umfassende Aufsichts- und Kontrollrechte hierfür vom Auftragsverarbeiter einräumen lassen. Es müssen Auftragsverarbeitungsverträge nach Art. 28 DSGVO abgeschlossen werden.21

Kommen der Verantwortliche (der Anwalt/die Anwältin) und der Auftragsverarbeiter den u.a. aus Art. 28 DSGVO resultierenden Verpflichtungen nicht nach, so drohen nach Art. 83 Abs. 4 DSGVO Bußgelder von bis zu 10.000.000 EUR.

Es stellt sich die Frage mit wem diese abzuschließen sind. Mit der BRAK als Auftragsverarbeiter? Wenn dies der Fall ist, dann müsste die BRAK entsprechenden Unterauftragsverarbeitungsverträge mit der Atos GmbH abschließen. Diese Verträge könnten aufgrund der Kontrollrechte des Verantwortlichen (der Anwälte und Anwältinnen) ebenfalls nicht unter Verschluss gehalten werden. Und Anlage von Auftragsverarbeitungsverträgen ist regelmäßig ein Verzeichnis von Verarbeitungsübersichten sowie ein Übersicht zu den technisch und organisatorischen Maßnahmen.

Vor diesem Hintergrund sollte deutlich sein, warum die Sicherheitsmethode „Security by Obscurity“ schon keine geeignete Methode sein kann. Denn es muss im Rahmen der DSGVO Rechenschaft über die Maßnahmen zur Daten- und IT-Sicherheit abgelegt werden.

2.11. Weiteres Vorgehen

Wie plant die BRAK nun weiter vorzugehen?

---

[21] Nach der DSGVO findet keine Unterscheidung mehr zwischen Auftragsdatenverarbeitung und Funktionsübertragung statt.

Wie will die BRAK Sorge dafür tragen, dass die Situation rund um die Entwicklung des beA umfassend und transparent aufgeklärt und Verantwortung für das Vorliegen einer nicht funktionsfähigen Software übernommen wird?

Prüft die BRAK die Möglichkeit, nach den bestehenden Verträgen Schadensersatz vom Dienstleister wegen der nicht funktionsfähigen Software zu erlangen?

Werden unabhängige Sachverständige zur Beurteilung der IT-sicherheitstechnischen Lage sowie ggf der IT- und datenschutzrechtlichen Situation hinzugezogen?

Werden Szenarien durchdacht, in denen externe Sachverständige zu dem Ergebnis kommen, dass die beA-Anwendung im vorliegenden Konstrukt nicht sicher oder nur mit unverhältnismäßigen Kosten sicher in einen funktionsfähigen Zustand zu bekommen ist? Bereitet sich die BRAK auf ein solches Szenario vor?

Hat die BRAK bereits Szenarien durchdacht, in denen Anwälte Schadensersatz wegen Nichtleistung verlangen? Bereitet sich die BRAK auf solche Szenarien vor?

Wie will die BRAK künftig sicherstellen, dass sie als Auftraggeber Ihren Aufsichts- und Kontrollpflichten nachkommt und vor allem nachkommen kann?

Wertes Präsidium, ich hoffe, Sie verstehen, dass die Fragen weder von einem Gegner des digitalen Rechtsverkehrs noch der BRAK formuliert sind. Im Gegenteil. Nicht nur, dass ich digitalen Rechtsverkehr für sinnvoll und notwendig halte, ich halte auch die Selbstverwaltung der Anwälte für ein achtenswertes Gut.

Diese Selbstverwaltung der Anwälte kann jedoch nur dann (wieder) erfolgreich und wird nur dann (wieder) mit dem notwendigen Vertrauen der Anwaltschaft ausgestattet sein, wenn sie sich der Kritik stellt, zu Selbstkritik fähig ist, sich lernfähig zeigt und anerkennt, dass Selbstverwaltung nicht heißt, dass die ausschließlich eigene Verwaltung von Angelegenheiten immer die zielführendste und beste Verwaltung ist.

Mit freundlichen kollegialen Grüßen

Diercks
Rechtsanwältin
M.Litt., University of Aberdeen