Rechtsanwaltskammer München

DER FALL „BEA“

Knapp drei Monate sind vergangen, nachdem das besondere elektronische Anwaltspostfach (beA) vom Netz genommen wurde. Was folgte waren Fragen, Spekulationen und die Aussage der BRAK, dass die Rückkehr des beA erst nach vollständiger Klärung aller Sicherheitsrisiken erfolgen wird.

„Postfach-Pleite“, „Peinliche Panne“ oder der Hashtag „beAgate“ sind nur wenige Stichworte, mit denen das besondere elektronische Anwaltspostfach in den letzten Wochen in die Schlagzeilen geriet. Sowohl in der Anwaltschaft als auch in der Presse und der Online-Welt überschlugen sich die Reaktionen auf den beA-Ausfall. Mehr und mehr Informationen zu sicherheitstechnischen Problemen wurden veröffentlicht und auch die Zahl der Fragen stieg. Was bedeutet der Ausfall für die passive Nutzungspflicht, die eigentlich seit dem 01.01.2018 gilt? Wie konnten die Sicherheitsrisiken so lange unbemerkt bleiben? Und wie geht es nun weiter mit dem beA? Der vorliegende Artikel schafft einen Überblick.

MITGLIEDERBRIEF DES PRÄSIDENTEN

In Form eines Briefes informiert(e) Präsident Michael Then die Mitglieder der Rechtsanwaltskammer München über die Hintergründe des beA-Ausfalls sowie über die Ergebnisse des am 26.01.2018 stattgefundenen beAthons. In diesem Schreiben, das auch als Newsletter versendet wurde, geht er außerdem auf technische Details ein und gibt einen Überblick zu aktuellen Informationsmaterialien.

Liebe Kolleginnen und Kollegen,

nach einem turbulenten Jahreswechsel, zumindest im Hinblick auf das besondere elektronische Anwaltspostfach (beA), darf ich Sie mit diesem Schreiben über die aktuellen Entwicklungen des beA und die ersten Ergebnisse des „beAthon“ informieren.

Aus dem gemeinsamen Austausch am 26.01.2018 zwischen der BRAK, den beauftragten Gutachtern sowie IT-Experten und Kritikern, die sich mit dem beA sowohl in der Entwicklungs- und Realisierungsphase als auch in der jetzigen Situation besonders auseinandergesetzt haben, ging unter anderem die Empfehlung an alle Rechtsanwältinnen und Rechtsanwälte hervor, die gegenwärtig installierte beA Client Security zu deaktivieren. Der Grund dafür ist der Zugriff der bisherigen Client Security auf veraltete JAVA-Bibliotheken. Damit könnte die Client Security eine Lücke für externe Angreifer darstellen. Wir bitten Sie daher, die Software entweder zu deinstallieren oder sie auf dem Rechner zu schließen und aus dem Autostart des Rechners zu entfernen. Die BRAK hat hierzu technische Hinweise für Windows-Computer und MacOS erarbeitet, die Sie auch auf unserer Website einsehen können.

Der für die technische Umsetzung des beA beauftragte Dienstleister, die Firma Atos, hat bereits eine neue Version der Client Security entwickelt, die u.a. auf aktuelle JAVA-Bibliotheken zugreift. Diese wird zunächst noch geprüft. Auch

sobald es hierzu Neuigkeiten gibt, werden wir Sie umgehend informieren. Ich möchte dieses Schreiben aber auch zum Anlass nehmen, um Ihnen die Hintergründe für die Offline-Stellung des beA noch einmal ausführlich darzulegen. Am 20.12.2017 wurde seitens des Chaos Computer Clubs (CCC) ein Schwachpunkt im Sicherheitszertifikat des Client Security Systems gemeldet. Der technische Dienstleister, die Firma Atos, hielt am 22.12.2017 eine Ersatzlösung mit einem neuen Zertifikat bereit, das die bekannten Probleme nicht mehr aufweisen sollte. Nachdem das neue Zertifikat bereits allen Anwälten zum Download zur Verfügung gestellt wurde, erkannte Atos jedoch eine neu entstandene Sicherheitsproblematik, die insbesondere Risiken für die IT-Infrastruktur der nutzenden Anwälte enthielt. Das Anwaltspostfach wurde daraufhin vom Netz genommen.

Vor dem Start des beA am 28.11.2016 wurden bereits umfangreiche Sicherheitstests durchgeführt. So erstellte die Firma Atos auf Grundlage des Umsetzungsfeinkonzepts eine Teststrategie und wurde zugleich damit beauftragt, diese Tests durchzuführen. Nach Übergabe der Testberichte im Mai 2016 ließ die BRAK diese zusätzlich von der Firma CapGemini, die für den Bereich Qualitätsmanagement hinzugezogen worden war, prüfen. Auch die Mitarbeiter von CapGemini sahen keinen Anlass, die Vollständigkeit und Ergebnisse der Tests zu bezweifeln. Weitere Sicherheitstests durch die Firma SEC Consult – um mögliche Schwachstellen der beA-Architektur, des Authentifizierungskonzepts und der Signaturmechanismen aufzudecken – kamen zu dem Ergebnis, dass das beA-System ein hohes Sicherheitsniveau aufweist und damit an den Start gehen konnte. Auch hatte sich die BRAK im Vorfeld an den Chaos Computer Club (CCC) gewandt, um das beA von den dortigen Experten testen zu lassen. Nachdem es seitens des Clubs jedoch keine verbindliche Zusage darüber gab, dass die Ergebnisse der BRAK vollumfänglich zur Verfügung gestellt werden können, kam es insofern nicht zur Zusammenarbeit.

Während Atos in den letzten Wochen an einer neuen Lösung gearbeitet hat, um das beA baldmöglichst wieder in Betrieb nehmen zu können, rückt derzeit immer mehr die Frage in den öffentlichen Fokus, ob die Kommunikation über das Postfach wirklich sicher und ausreichend verschlüsselt war bzw. ist. Die BRAK weist daraufhin, dass alle sich im beA befindlichen Nachrichten

durchgehend verschlüsselt sind. Das liegt insbesondere am sogenannten Hardware Security Modul (HSM) – einer speziellen Hardware-Komponente, die den Zugriff auf das beA für mehrere Nutzer (Kanzleimitarbeiter etc.) ermöglicht sowie die Verschlüsselung, Entschlüsselung, Authentifizierung und digitale Signierung gewährleistet. In ihren beA-FAQs erklärt die BRAK, dass das HSM die einzige zur Verfügung stehende Lösung sei, um die Sicherheitsanforderungen an das beA-System umzusetzen. Wie diese Ende-zu-Ende-Verschlüsselung genau funktioniert, können Sie auf der Website der BRAK (http://bea.brak.de/wie-sicher-ist-das-bea/sichere-nachrichtenuebermittlung/) nachlesen.

Was das weitere Vorgehen betrifft, informierte die BRAK in einer Presseerklärung vom 18.01.2018, dass sich die Präsidentinnen und Präsidenten der 28 Rechtsanwaltskammern und das Präsidium der BRAK darüber einig seien, das beA erst wieder in Betrieb zu nehmen, wenn alle relevanten Fragen zur Sicherheit des Systems zweifelsfrei geklärt seien. In diesem Zuge wird die Bundesrechtsanwaltskammer die vom BSI empfohlene Gesellschaft secunet Security Networks AG mit der Erstellung eines Sicherheitsgutachtens beauftragen.

Ergänzend darf ich darauf hinweisen, dass seit dem 10.01.2018 das mit dem beA-System verbundene, auf derselben Datenbank basierende bundesweite amtliche Anwaltsverzeichnis (BRAV) sowie der europaweite Anwaltssuchdienst Find a Lawyer wieder zugänglich sind.

"Nicht verwunderlich ist es, dass sich seit Abschaltung des beA die Reaktionen in der Anwaltschaft, der Justiz, aber auch in der Presse und den Social Media Kanälen überschlagen."

Nicht verwunderlich ist es, dass sich seit Abschaltung des beA die Reaktionen in der Anwaltschaft, der Justiz, aber auch in der Presse und den Social Media Kanälen überschlagen. Die BRAK nimmt die sachlich geübte Kritik sehr ernst. Aus diesem Grund bat sie institutionell nicht gebundene Experten und Gutachter am vergangenen Freitag zum oben erwähnten „beAthon“, um den

Lösungsweg des Dienstleisters zu diskutieren und diesem anschließend die erörterten Fragestellungen und Vorgehensweisen vorzulegen. Auf Grundlage der erstatteten Gutachten sowie der im beAthon niedergelegten Ergebnisse wird die BRAK dann über das weitere Vorgehen entscheiden können.

Geplant ist bereits, dass es eine angemessene Übergangszeit zwischen Ankündigung und Wiederinbetriebnahme des beA geben wird. Dies ermöglicht allen Nutzern, sich selbst wieder auf den beA-Prozess einzulassen und die eigenen etwaig notwendigen Anpassungen durchzuführen oder nachzuholen.

Gestatten Sie mir an dieser Stelle noch folgenden Hinweis: Die Aussage, der Versand von Schriftstücken über das beA sei nur im 15-Minuten-Rhythmus möglich, ist eine Falschmeldung. Dass eine Nachricht hingegen nicht größer als 60 MB sein und nicht mehr als 100 Anhänge haben darf, ist nicht Folge der beA-Konstruktion, sondern eine Anforderung der Bekanntmachung zu § 5 der Elektronischen-Rechtsverkehr-Verordnung.

Verehrte Kolleginnen und Kollegen,

ich möchte Sie mit diesem Schreiben auch auf die verschiedenen Informationsmaterialien zur aktuellen Entwicklung des beA hinweisen. Auf der Website der Rechtsanwaltskammer München haben wir wichtige Fragen und Antworten zum beA und zur Offline-Stellung zusammengestellt (www.rak-muenchen.de). Alle dortigen Informationen werden regelmäßig aktualisiert. Wichtige Neuigkeiten in der aktuellen beA-Entwicklung versenden wir außerdem als Rundschreiben an unsere Mitglieder. Die Bundesrechtsanwaltskammer informiert auf ihrer Website (www.brak.de) in Pressemeldungen und Newslettern zum beA. Hier können Sie beispielsweise die Pressemeldung und den Sondernewsletter zum beAthon, beides vom 26.01.2018, sowie den Sondernewsletter vom 03.01.2018 einsehen, in dem sich der Präsident der BRAK an alle Kolleginnen und Kollegen wendet und für die entstandene Situation um Entschuldigung bittet. Bitte beachten Sie in diesem Zusammenhang auch die aktualisierten beA FAQs der BRAK, die Sie unter www.bea.brak.de abrufen können. Hier finden Sie auch zahlreiche technische

Fragen beantwortet. Darüber hinaus verweisen wir auf die Stellungnahme der Firma Atos zum beA vom 26.01.2018.

Wir hoffen, dass die jetzige Situation bald geklärt ist und wir möglichst zeitnah wieder alle sicher und reibungslos mit dem Anwaltspostfach arbeiten können. Der Vorstand der Rechtsanwaltskammer München weist der Vollständigkeit halber auch darauf hin, dass dort, wo durch die Vorgänge vom 22./23.12.2017 nutzloser Aufwand entstanden sein sollte, etwaige Ansprüche an die Bundesrechtsanwaltskammer zu richten sind, die diese im Zweifel an den Dienstleister weiterreicht.

Mit freundlichen kollegialen Grüßen

Rechtsanwalt Michael Then
Präsident

AKTUELLE INFORMATIONEN ZUM BEA

Welches Sicherheitsproblem nun konkret ausschlaggebend für den Trubel in den vergangenen Wochen war und wie der aktuelle Stand zu den Entwicklungen des Postfachs aussieht, darüber berichtet im Weiteren Rechtsanwältin Dr. Tanja Nitschke von der Bundesrechtsanwaltskammer (BRAK):

Worin die Sicherheitslücke liegt

Um die Frage, welche Sicherheitsrisiken beim beA bestehen, gibt es von berufener und weniger berufener Seite die heißesten Diskussionen und Spekulationen. Dabei gerät leicht einmal aus dem Blick, wo überhaupt die aufgetretene Sicherheitslücke liegt.

Sie liegt erstens in der Verbindung zwischen der lokalen beA Client Security und der beA-Webanwendung. Diese Verbindung hat keinerlei Auswirkungen auf die Sicherheit der im beA versandten Nachrichten, sondern verschafft dem Nutzer Zugang zum beA-System. Mit Hilfe des dafür notwendigen Zertifikats, das Atos am 22.12.2017 zur Verfügung stellte, konnten Angreifer theoretisch eigene Webseiten als vertrauenswürdig präsentieren und danach einen weiteren Angriff (sog. DNS-Spoofing oder Cache Positioning) durchführen. So hätte ein Angreifer schließlich Nutzer des beA auf eigene Webseiten umleiten und im äußersten Fall den Rechner mit Schadsoftware infizieren können. Das Zertifikat konnte zudem nach Installation zu Sicherheitsrisiken für die PC-Umgebung des Nutzers führen.

Zweitens soll die Client Security von einer sog. Java- Deserialisierungslücke betroffen sein. Durch eine trickreiche Konstruktion könnte ein Angreifer die Client Security dazu bringen, Code auszuführen; damit kann der Angreifer z.B. (Schad-)Software auf dem PC starten. Vertreter des Chaos Computer Clubs wiesen beim beAthon auf diese weitere Schwachstelle hin. Die BRAK reagierte umgehend und riet allen Anwältinnen und Anwälten noch am gleichen Tag, die beA Client Security auf den eigenen Rechnern zu deaktivieren (vgl. BRAK-PE Nr. 4/2018 v. 26.1.2018).

Keine halben Sachen

Erste Priorität hat für die BRAK weiterhin, die Sicherheit des beA-Systems zu gewährleisten. Die BRAK und der IT-Dienstleister Atos arbeiten mit Hochdruck daran, die aufgeworfenen (potenziellen) Sicherheitsrisiken zu beheben und so schnell wie möglich alle sicherheitsrelevanten Fragen zu klären. Teil dessen ist die Prüfung durch die vom BSI empfohlene Firma secunet. Dieses Gutachten wird die BRAK veröffentlichen. Wenn alle sicherheitsrelevanten Fragen geklärt sind und das beA-System wieder online ist, wird die BRAK – auf Grundlage der Gutachten und der Ergebnisse des beAthon – in aller Ruhe diskutieren und entscheiden, welche weiteren Instrumente der Qualitätssicherung zusätzlich eingesetzt werden.

Klar ist für die BRAK, dass sie keine halben Lösungen akzeptieren und auf die Klärung aller sicherheitsrelevanten Fragen bestehen wird. Deshalb lässt sich aus heutiger Perspektive noch kein definitiver Zeitpunkt benennen, wann das beA-System wieder vollumfänglich verfügbar sein wird. Klar ist aber, dass es eine angemessene Frist zwischen Ankündigung und Wiederinbetriebnahme der beA-Plattform geben wird – damit aus „beAGate“ eine beA-Erfolgsgeschichte wird.

Autorin: Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ.

BRAK, Berlin / Auszug aus dem Beitrag „Mythen und Fakten – aktuelle Entwicklungen beim beA“ (Erst-Veröffentlichung aus dem BRAK-Magazin Heft 1/2018)

INTERVIEW MIT DR. MARTIN ABEND, VIZEPRÄSIDENT DER BRAK, ZUM THEMA „WIE STEHT ES UM DAS BEA?“

„Kurz vor Weihnachten musste die BRAK das besondere elektronische Anwaltspostfach vom Netz nehmen, nachdem ein Sicherheitsrisiko in der beA Client Security entdeckt wurde, dem Programm, das u.a. den Zugang zur beA-Webanwendung ermöglicht. Welche Lehren zieht die BRAK daraus und wie geht sie mit der Situation um? Darüber hat sich das BRAK-Magazin mit Dr. Martin Abend, 1. Vizepräsident der BRAK und verantwortlich für den Bereich elektronischer Rechtsverkehr, unterhalten.

Herr Dr. Abend, das dürfte einer der turbulenteren Jahreswechsel in Ihrem Berufsleben gewesen sein.

So ist es. Wir erwarteten beim Betrieb des beA den reibungslosen Übergang in die Phase der flächendeckenden Eröffnung des elektronischen Rechtsverkehrs und der „passiven Nutzungspflicht“ für die Anwaltschaft ab Januar 2018. Kurz vor Weihnachten galt es dann aber wegen des von der Entwicklerin des beA

verursachten Ausfalls der beA Client Security ohne zu zögern die richtigen Entscheidungen zu treffen, um die Sicherheit der anwaltlichen Komponenten des ERV in Deutschland zu wahren. Nun setzen wir alles daran, beA so schnell wie möglich wieder in Betrieb nehmen zu können und zuvor alle relevanten Fragen zur angemessenen Sicherheit des beA vollständig zu beantworten; gleichwohl: Sicherheit geht vor Geschwindigkeit.

Welche Erfahrungen haben Sie dabei in den vergangenen Wochen gemacht?

Die Entwicklung und der Betrieb der Unternehmung beA sind nur in einem Team zu leisten, in dem sich alle Beteiligten die Erfüllung dieser wichtigen Aufgabe selbst zu eigen machen. Das beA musste wegen der besonderen gesetzlichen Anforderungen komplett neu entwickelt werden – für über 165.000 Nutzer mit diversen komplexen Schnittstellen an verschiedene schon existierende Systeme. Darauf kann die Anwaltschaft schon stolz sein. Negativ überrascht war ich über die Heftigkeit und Tonalität so manch eines Kollegen. Diejenigen, die beA schon seit November 2016 intensiv nutzen, sind von seinen Vorzügen überzeugt. Deshalb wollen wir es so schnell wie möglich fit für die Wiederinbetriebnahme machen.

Warum hat die BRAK überhaupt die Einführung des beA verantwortet?

Der Bundestag hat der BRAK als Dachorganisation der 28 Rechtsanwaltskammern die Aufgabe übertragen, das beA zu entwickeln. Dieser Herausforderung haben wir uns gerne gestellt. Denn das entspricht auch unserem Selbstverständnis als unabhängige anwaltliche Selbstverwaltung.

Wäre es nicht angesichts der Kritik an mehreren Teilen des beA das Beste, es komplett neu aufzusetzen?

Das beA-System, seine Gesamtarchitektur, die einzelnen Software- und Hardware-Komponenten sind ja sicher, die dahinter stehenden hochkomplexen hybriden Verschlüsselungsverfahren mit symmetrischen und asymmetrischen Schlüsseln waren und sind nicht Teil der zuweilen hitzig geführten Debatte.

Deshalb gibt es gar keinen Anlass, das beA als solches in Frage zu stellen. Sicher, die identifizierten Sicherheitsrisiken der Client Security sind ernst zu nehmen und müssen abgestellt werden. Aber das Verschlüsselungsverfahren und das beA selbst sind angemessen sicher.

Wie wollen Sie Akzeptanz und Vertrauen der Rechtsanwälte für das beA, aber auch für die Arbeit der BRAK zurückgewinnen?

Die BRAK hat in dieser herausfordernden Situation zwei Dinge unter Beweis gestellt: Sie ist handlungsfähig. Und sie ist diskursfähig, d.h. sie ist bereit zu einer breiten fachlichen und öffentlichen Debatte. Das haben wir mit unserem sofortigen konsequenten Vorgehen nach Bekanntwerden der Sicherheitsprobleme demonstriert. Und wir haben uns schließlich auch der Diskussion mit unseren Kritikern gestellt – mit Rechtsanwälten, Rechtsanwaltskammern, Fachpresse und auch mit den Akteuren des Chaos Computer Clubs. Auch das Sicherheitsgutachten, das wir gerade erstellen lassen, beabsichtigen wir, zu veröffentlichen. Ich bin davon überzeugt, dass wir damit Akzeptanz und Vertrauen in das beA zurückgewinnen werden und auch diejenigen von der Sicherheit und den Vorzügen des beA für die anwaltliche Praxis überzeugen werden, die sich auch schon vor dem Ausfall des beA gegen die Digitalisierung der forensischen Kommunikation aussprachen.

Autorin: Rechtsanwältin Dr. Tanja Nitschke, Mag. rer. publ.

BRAK, Berlin / Erst-Veröffentlichung aus dem BRAK-Magazin Heft 1/2018

FAQ'S

Die wichtigsten Fragen und Antworten zur Offline-Stellung des beA hat die Rechtsanwaltskammer München in einem Infokatalog zusammengestellt. Darin finden sich u.a. Informationen zum Umgang mit der passiven Nutzungspflicht ab 01.01.2018, zur Deinstallation der beA Client Security, dem Einreichen von Anträgen im Zentralen Schutzschriftenregister sowie zur erweiterten Nutzungsverpflichtung im automatisierten Mahnverfahren. Auch geben die

FAQs Aufschluss über die aktuelle bzw. vorübergehende Nutzung von EGVP-Postfächern und die Sicherheitslage der sich im beA befindlichen Nachrichten.

Die FAQs zur Offline-Stellung des beA werden regelmäßig aktualisiert und sind auf der Website der Rechtsanwaltskammer München im Bereich „Aktuelles“ sowie unter Rechtsanwälte / Mitgliederservice / Elektronischer Rechtsverkehr veröffentlicht. Sie können den Infokatalog außerdem direkt hier abrufen.

HINWEIS ZUM KAMMERBEITRAG

Mit der Abschaltung des beA rückte in den vergangenen Wochen zunehmend die Frage nach etwaigen Entschädigungsansprüchen sowie der Erstattung der im Kammerbeitrag enthaltenen „Umlage“ für das beA in den Raum.

Was hat es mit der „Umlage“ für das beA auf sich?

Die Rechtsanwaltskammer München muss jährlich einen Betrag in Höhe von 58 Euro pro Mitglied an die Bundesrechtsanwaltskammer für die Entwicklung und den Betrieb des beA abführen. Die Höhe dieses Betrages wird durch die Hauptversammlung der Bundesrechtsanwaltskammer, also alle Präsidentinnen und Präsidenten der Regionalkammern, jährlich festgelegt und beschlossen. Über die Höhe des Beitrags für das Jahr 2018 hat die Hauptversammlung bereits im Jahr 2017 entschieden. Dieser Beschluss wurde aktuell auch nicht abgeändert. Dies bedeutet, dass die Rechtsanwaltskammer München auch im Jahr 2018 diese Kosten zu tragen hat.

Im Gegensatz zu vielen anderen Regionalkammern erhebt die Rechtsanwaltskammer München diese Kosten nicht in Form einer Umlage. Vielmehr wurde dieser Betrag bei der Berechnung des jährlich zu zahlenden Kammerbeitrags als Verwaltungsaufwand berücksichtigt. Die Höhe des Kammerbeitrags wiederum wird von der Kammerversammlung für die jeweiligen Folgejahre bestimmt. Der für das Jahr 2018 maßgebliche Kammerbeitrag in Höhe von 285 EUR wurde bereits im Rahmen der Kammerversammlung 2017 beschlossen.

Können sich Rechtsanwältinnen und Rechtsanwälten den Betrag in Höhe von 58,- Euro zurückerstatten lassen?

Eine kurzfristige Reduzierung des Kammerbeitrags ist aus mehreren Gründen nicht möglich:

Zum einen dient der Kammerbeitrag der Deckung des bei der Kammer entstehenden Aufwands einschließlich des Betrages, der an die BRAK abzuführen ist, also auch der Anteil für das beA. Dieser fällt jedoch auch unabhängig des technischen beA-Ausfalls an, u.a. für den Unterhalt der Rechenzentren und den Support sowie für externe Beratung und den Einsatz der Mitarbeiter. Zum anderen wird der von den Regionalkammern zu zahlende Beitrag an die BRAK einschließlich des beA im Rahmen der BRAK-Hauptversammlung entschieden – und zwar immer für das Folgejahr. Wie sich die Fortentwicklungen des beA auf die zukünftigen Beiträge konkret auswirken, kann erst nach endgültiger Klärung der Situation und nach Durchsetzung der zustehenden Ansprüche der BRAK gegenüber dem Dienstleister Atos festgestellt werden.