BUNDESRECHTSANWALTSKAMMER

beA Digital. Einfach. Sicher.

Mythen und Fakten – aktuelle Entwicklungen beim beA

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

Berlin, 15.2.2018 (Veröffentlichung aus dem BRAK-Magazin Heft 1/2018)

„beAGate", „Postfach-Pleite", „Fataler Konstruktionsfehler", „Noch mehr Sicherheitslücken im Anwaltspostfach" – so und ähnlich berichteten Medien und Internet-Communities, seit das besondere elektronische Anwaltspostfach (beA) Ende Dezember 2017 offline gehen musste. Die seitdem geführte öffentliche Diskussion zum beA ist geprägt von – zuweilen für die Anwaltschaft überraschend heftiger – Emotionalität, mitunter Spott, aber auch von Fehlinformationen und Spekulationen. Bei allem berechtigten Ärger über die vorübergehende Abschaltung des beA: Es ist an der Zeit für einen unaufgeregten Blick auf die Fakten.

Warum das beA offline ging

Was genau ist passiert, dass die BRAK das beA-System offline schalten und alle Rechtsanwältinnen und Rechtsanwälte dazu auffordern musste, die lokal installierte beA Client Security zu deaktivieren? 15 Monate lief das beA-System schließlich bereits und hat seitdem viele Nutzer von den Vorteilen des elektronischen Rechtsverkehrs überzeugt.

Ein Mitglied des Chaos Computer Clubs informierte am 20.12.2017 die BRAK und das Bundesamt für Sicherheit in der Informationstechnik (BSI), dass er Sicherheitsprobleme beim beA sehe. Die BRAK handelte nach diesem Hinweis sofort und informierte ihren IT-Dienstleister, die Atos GmbH. Am Folgetag ging Atos davon aus, dass zur Behebung der Probleme der Austausch eines Zertifikats ausreiche. Denn dieses sichere lediglich auf dem PC des Nutzers die lokale Verbindung zwischen der Client Security und dem Browser ab und habe keine weiteren sicherheitsrelevanten Funktionen. Außerdem riet Atos dazu, über Nacht das neue Zertifikat zum Download zur Verfügung zu stellen, damit die beA-Plattform möglichst rasch wieder funktioniere.

Am Vormittag des 22.12.2017 stand das aktualisierte Zertifikat allen Nutzern samt Installationsanleitung zur Verfügung. Zu diesem Zeitpunkt konnte die BRAK selbstverständlich nicht davon ausgehen, dass die Installation des neuen Zertifikats Sicherheitsrisiken für die PC-Umgebung der Rechtsanwältinnen und Rechtsanwälte mit sich bringt. Erst am Mittag desselben Tages informierte

Atos die BRAK darüber, dass das neue Zertifikat wegen Sicherheitsbedenken erneut aktualisiert werden müsse. Die BRAK wies Atos daraufhin an, den Download des neuen Zertifikats unverzüglich zu unterbinden und empfahl allen beA-Nutzern, das neue Zertifikat wieder zu deinstallieren.

Noch am 22.12.2017 forderte die BRAK schließlich Atos auf, das beA-System komplett offline zu schalten, was am 23.12.2017 gegen 10 Uhr auch geschah. Da nicht alle Zweifel an der Beseitigung der Sicherheitslücke ausgeräumt werden konnten, beschloss das BRAK-Präsidium am 26.12.2017, das beA-System so lang offline zu lassen, bis alle sicherheitsrelevanten Fragestellungen zweifelsfrei geklärt sind.

Aufklärungsarbeiten

Diese Entscheidung bekräftigte auch die BRAK-Präsidentenkonferenz, bestehend aus den Präsidentinnen und Präsidenten aller 28 Rechtsanwaltskammern und dem BRAK-Präsidium, die sich am 9.1. und 18.1. in zwei Sitzungen eingehend mit der beA-Problematik befasste. Und sie beschloss, dass ein vom BSI empfohlener Gutachter, die Firma secunet Security Networks AG, die von Atos entwickelte neue Lösung prüfen wird, bevor das beA wieder ans Netz gehen darf. Auch Atos hat einen Gutachter beauftragt.

Außerdem steht die BRAK mit kritischen IT-Experten und IT-Anwälten im Dialog, um die von ihnen geäußerten Bedenken berücksichtigen zu können. Hierzu fand am 26.1.2018 der „beAthon" statt, bei dem die von Atos zur Verfügung gestellte neue Lösung und mögliche weitere Sicherheitsrisiken konstruktiv diskutiert wurden. An weiterem Austausch ist die BRAK durchaus interessiert.

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).

Mythen rund um das beA

Die öffentliche Diskussion rund um die Abschaltung des beA-Systems haben aber nicht nur (mögliche) Sicherheitsrisiken bestimmt, sondern auch nicht wenige Fehlinformationen. Zum einen betreffen diese die Funktionalität des beA-Postfachs als solches. So entspricht es nicht der Realität, dass bei jedem Login nur jeweils eine einzelne Nachricht abgerufen werden kann oder dass der Abruf einer Nachricht 15 Minuten dauert. Bei jedem Login können selbstverständlich alle Nachrichten aus dem beA abgerufen werden; dass das System sonst überlastet wäre, ist ein bloßes Gerücht. Es ist auch nicht etwa Vorgabe der BRAK, sondern der Justiz, dass Einzelnachrichten derzeit nicht größer als 60 MB sein dürfen. Auch die Beschränkung auf 100 Anhänge ist eine Vorgabe der Justiz und gilt für das gesamte EGVP-System, in dem auch Justiz, Verwaltung und Notare kommunizieren; das beA ist der anwaltliche Bestandteil dieses Systems und muss sich hier einfügen.

Andere Fehlinformationen betreffen die Datensicherheit des beA-Systems im Grundsatz. Dazu im Klartext: Die Kommunikation war stets durchgängig verschlüsselt; ob man dabei im strengen Sinne von „Ende-zu- Ende-Verschlüsselung" sprechen kann, daran scheiden sich freilich die Geister der Techniker. Deshalb konnte auch die BRAK zu keiner Zeit auf die Nachrichten zugreifen oder sie gar entschlüsseln. Es stimmt auch nicht, dass die BRAK oder Dritte Zugriff auf die im beA-System hinterlegten privaten Schlüssel haben. Bei den verwendeten Hardware Security Modulen stellen die eingesetzten Schutzmechanismen sicher, dass kein Angreifer – etwa durch gewaltsames Öffnen und den Versuch, den Speicher auszulesen – Zugriff auf das Klartext-Schlüsselmaterial erhalten kann. Die hier eingesetzte Lösung entspricht, auch das ergab der beAthon, dem Stand der Technik.

Keine halben Lösungen

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.