BUNDESRECHTSANWALTSKAMMER

Der Vizepräsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

Anbieter von beA-Schulungen

Berlin, 27.12.2017

beA - besonderes elektronisches Anwaltspostfach

Anlage: Presseerklärung Nr. 15 v. 27.12.2017

Sehr geehrte Damen und Herren,

in der Anlage füge ich eine Kopie der Presseerklärung der Bundesrechtsanwaltskammer Nr. 15 vom heutigen Tage bei.

Am Abend des 26. Dezember 2017 beschloss das Präsidium der Bundesrechtsanwaltskammer, beA vorerst weiter offline zu lassen. Dem ging Folgendes voraus:

1. beA fiel nach dem letzten großen Update mehrfach für Zeiträume zwischen 20 und 150 Minuten aus. Inzwischen modifizierte Atos sowohl die Software als auch Hardware in den Rechenzentren. Das beA-System sollte seit Mittwoch, 20. Dezember 2017, wieder in der Lage gewesen sein, kontinuierlich 24h/7d im Dauerbetrieb zu funktionieren.

2. Am Donnerstag, 21. Dezember 2017, zeigte eine nicht zur Rechtsanwaltschaft zugelassene Person an, dass sie in der Client-Security, dem Zugangsinstrument, um auf das beA-System zu gelangen, ein Zertifikat kompromittiert habe. Daraufhin sperrte die Zertifizierungsstelle dieses Zertifikat. Bis Freitagvormittag, 22. Dezember 2017, entwickelte Atos ein neues Zertifikat sowie eine Anleitung zu dessen Integration in die Client-Security auf den Computern der Nutzer. Die BRAK stellte dann diese Anleitung auf der Webseite als PDF und Atos die Software den Nutzern zur Verfügung.

   In der zweiten Tageshälfte des Freitag, 22. Dezember 2017, mussten wir zur Kenntnis nehmen, dass die Client-Security in der dann vorliegenden Version die Möglichkeit eröffnete,

Programme und Ausführungen auf Computern der Nutzer, die unter dieser Client-Security an das Internet angeschlossen sind, zu manipulieren. Daraufhin nahmen wir das beA-System vom Netz. Die Bundesrechtsanwaltskammer forderte Atos auf, unverzüglich den vertraglich geschuldeten Zustand herzustellen. Atos kündigte an, bis zum 26. Dezember 2017 eine neue Version der Client-Security zu entwickeln und einzusetzen, die sicher sei. Allerdings, so Atos, sei in einem zweiten Schritt zu einem späteren Zeitpunkt die Client-Security nochmals zu überarbeiten.

3. Bei der Vorstellung der nun abermals revidierten Version der Client-Security am Nachmittag des 26. Dezember 2017 war Atos nicht in der Lage, Zweifel an der Schließung der vor wenigen Tagen aufgetretenen Sicherheitslücke der Client-Security auszuräumen. Daher beschloss das Präsidium der Bundesrechtsanwaltskammer, beA so lange offline zu lassen, bis Atos eine Lösung präsentieren und einen sicheren Zugang zum beA gewährleisten kann.

Bei der Client-Security handelt es sich um eine für den Zugang zum beA erforderliche Software, die auf den Computern der Nutzer installiert sein muss. Von der entdeckten Sicherheitslücke in der Client-Security waren die beA-Plattform selbst und die über die Plattform versandten Nachrichten nie betroffen. Da die Bundesrechtsanwaltskammer der EDV-Sicherheit für alle Anwältinnen und Anwälte, die das beA einsetzen, und dem Schutz vor möglichen Hackerangriffen absoluten Vorrang einräumt, werden wir daher im Interesse des Elektronischen Rechtsverkehrs und zum Schutze der Anwaltschaft das beA erst wieder zur Verfügung stellen, sobald Atos eine Lösung gefunden hat.

Was die ab 01. Januar 2018 eintretende passive Nutzungspflicht der Anwälte betrifft, bedeutet dies, dass diese Nutzungspflicht, solange beA vom Netz ist, nicht erfüllt werden kann. Es können auch keinerlei Nachrichten in das beA der Anwälte gesandt oder von dort abgeholt werden. Gerichte sind daher auch nicht in der Lage, in diesem Zeitraum Nachrichten an Anwälte zu senden.

Auch die Schulungs- und Partnertestumgebung ist aufgrund der Zweifel an der ausreichenden Sicherheit derzeit über die webbasierte Oberfläche nicht mehr erreichbar.

Wir können Ihnen den Zugang wieder gewähren, wenn Sie ein dafür erstelltes Zertifikat herunterladen und installieren. Hierbei besteht allerdings folgendes Risiko, auf das wir ausdrücklich hinweisen: Mit Hilfe dieses Zertifikat könnte ein Angreifer eigene Webseiten als vertrauenswürdig präsentieren. Derselbe Angreifer könnte anschließend einen weiteren IT-Sicherheitsangriff (sogenanntes DNS-Spoofing oder Cache poisoning) durchführen. Schließlich könnte er Anwenderinnen und Anwendern auf seine eigene Webseite umleiten und ihre Rechner über diese Webseiten mit Schadsoftware infizieren. Falls Sie sich trotz dieses Risikos für die Installation des Zertifikats entscheiden sollten, wenden Sie sich bitte an die Bundesrechtsanwaltskammer unter kneer@brak.de.

Die an der Entwicklung des beA-Systems, insbesondere der Client-Security, Beteiligten setzen alles daran, die entstandene Sicherheitslücke zu schließen, so dass das beA-System schnellstens wieder einsetzbar ist.

Sobald uns der Zeitpunkt der Wiederinbetriebnahme des beA-Systems bekannt ist, werden wir Sie unaufgefordert unterrichten.

Mit freundlichen Grüßen

Dr. Martin Abend