BUNDESRECHTSANWALTSKAMMER

Der Vizepräsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

An die
Präsidentinnen und Präsidenten
der Rechtsanwaltskammern

BRAK-Nr. 039/2018
Az. beA-ERV

Berlin, 30.01.2018

vorab per E-Mail

beAthon am 26. Januar 2018

Anlagen:
1. Atos Stellungnahme zum beA v. 26.01.2018
2. Deinstallationsanleitung der beA Client Security für Windows
3. Deinstallationsanleitung der beA Client Security für MAC-Systeme

Sehr geehrte Präsidentinnen und Präsidenten,
sehr geehrte Damen und Herren Kolleginnen und Kollegen,

am vergangenen Freitag fand der sogenannte beAthon in Berlin statt. Im Anschluss daran hatten wir zunächst ad hoc von einem bei dieser Veranstaltung diskutierten, möglichen Sicherheitsrisiko berichtet. Hier folgt nun ein ausführlicher Bericht über den beAthon.

Ziel des beAthon war es, mit unabhängigen Experten und Journalisten ins Gespräch zu kommen, um die Behebung aktueller Schwachstellen im technischen System des beA konstruktiv zu diskutieren. Teilnehmer des beAthon waren neben der BRAK deshalb auch vorrangig IT-Experten, zum Beispiel Herr Drenger und zwei weitere Mitglieder des Chaos Computer Clubs (CCC), Vertreter der secunet Security Networks AG, die von der BRAK beauftragt ist, ein technisches Gutachten zur Sicherheit des beA zu erstellen, sowie Vertreter des EDV-Gerichtstags e. V., des DAV, des BMJV und zwei Fachjournalisten. Rechtsanwalt Professor Dr. Ory, Vorsitzender des EDV-Gerichtstags e.V., moderierte die Veranstaltung.

Atos hatte eine Teilnahme leider einige Tage zuvor abgesagt, obwohl es ursprünglich eine mündliche Zusage gab. Atos gab wenige Stunden vor dem beAthon gegenüber der Presse eine Stellungnahme ab, die als Anlage beigefügt ist. Darin erläuterte Atos die der BRAK zur Verfügung gestellte beA-Software in der neuen Version 2.0.9. Demnach wird die neue beA Client Security bei der Installation auf den Rechner der Nutzer ein individuelles, lokales Zertifikat erstellen. Dieses Zertifikat soll die sichere Verbindung zwischen beA Client Security und beA-Webanwendung ermöglichen und nur mit

eingeschränkten Rechten ausgestattet sein. Hintergrund dieser Aktualisierung sind vor Weihnachten durch den Chaos Computer Club gemeldete Sicherheitsrisiken, die auf Schwachpunkte in eben dieser Verbindung fokussieren. Die beA Client Security ist ein zentrales Programm der beA-Anwendung, das die Anwältinnen und Anwälte zur Nutzung des elektronischen Anwaltspostfachs auf ihrem jeweiligen PC installieren.

Die anwesenden Experten waren sich einig, dass die von Atos vorgeschlagene Lösung zur Behebung dieses Problems prinzipiell geeignet ist. Nun komme es darauf an, die Lösung auch operativ fehlerfrei umzusetzen. Die BRAK hat secunet deshalb damit beauftragt, die durch Atos umgesetzte Lösung zu begutachten.

Fazit: Wenn die nun skizzierte Lösung einer veränderten beA Client Security gut umgesetzt wird und die von der BRAK eingesetzten Gutachter sie als angemessen sicher bewerten, können wir beA unverzüglich wieder zur Verfügung stellen.

Ein wesentliches Ergebnis des beAthon war überdies die klare Aussage der großen Mehrheit der anwesenden IT-Experten (darunter alle Vertreter des Chaos Computer Clubs), dass sie es grundsätzlich für möglich erachten, die hohen Sicherheitsanforderung an das System innerhalb der bestehenden Konstruktion umzusetzen. Dabei erkennen sie an, dass die Nutzung eines sogenannten Hardware Security Moduls (HSM) Industriestandard darstellt und ein hohes Sicherheitsniveau gewährleistet, sofern es auch entsprechende Verhaltensregeln für den Betreiber der Infrastruktur des beA-Systems gibt. Das beA-HSM ist eine spezielle Hardware-Komponente des beA-Systems. Hier findet die kryptografische Umschlüsselung des Schlüsselmaterials statt, mit dem die im beA versendeten Nachrichten verschlüsselt sind. Diese Umschlüsselung gewährleistet, dass es verschiedene Zugangsberechtigungen für den Nachrichtenabruf gibt, so wie es der Gesetzgeber vorgeschrieben hat. Dazu erörterten die Teilnehmer auch die Frage, inwieweit das derzeitige System aufgrund der Umschlüsselung terminologisch als ein Ende-zu-Ende verschlüsseltes System bezeichnet werden könne.

In der unter den teilnehmenden Experten kontroversen Diskussion über weitere Schritte nach einer Wiederinbetriebnahme des beA erörterten die Teilnehmer die technischen und rechtlichen Rahmenbedingungen des beA-Systems als Kommunikationsplattform zur Justiz und die damit für das beA-System einhergehenden Vorgaben. Diese Diskussion drehte sich insbesondere um den Punkt, wie mittels neuester Krypto-Technologien unter Verzicht auf die HSM eine Verschlüsselung unter Wahrung der gesetzlichen Vorgaben möglich ist. Es herrschte aber weitgehend Einigkeit, dass Modifikationen an der Sicherheitsarchitektur, respektive bei der Frage Umschlüsselung in den HSM oder nicht, bei der Fortentwicklung des beA und der justizseitigen Systeme berücksichtigt werden sollten. Die Teilnehmer diskutierten unter dem Stichwort einer Weiterentwicklung des beA weitere technische Einzelheiten. Dabei ging es unter anderem um die Wahrscheinlichkeit der Ausnutzung von Cross-Site-Scripting-Lücken und um die Anbindung des beA an das Elektronische Gerichts- und Verwaltungspostfach (EGVP).

Der Chaos Computer Club wies im Verlauf des beAthon auf eine in seinen Augen wesentliche Sicherheitsproblematik hin. Herr Drenger bemängelte nochmals die Nutzung veralteter Software-Bibliotheken bei der Programmierung der beA Client Security. Atos hatte bereits mitgeteilt, dass in der neuen, aktualisierten Version des beA der Zugriff auf aktuelle Software-Bibliotheken sichergestellt sei, nachdem Herr Drenger diesen Sachverhalt bereits am 20. Dezember gemeldet hatte.

Auf dem beAthon führte der Chaos Computer Club nun erstmals aus, weshalb er diesen Sachverhalt für so wichtig erachtet: Denn durch die Verwendung veralteter Software-Bibliotheken sei die beA Client Security ihrer Ansicht nach von einer sogenannten Java-Deserialisierungslücke betroffen. Das bedeutet, dass – sollte der beA-Nutzer mit seinem Rechner infizierte Webseiten besuchen und zuvor auf den Startknopf der alten, auf dem Rechner noch vorhandenen beA Client Security gedrückt haben – Unberechtigte die Java-Deserialisierungslücke nutzen könnten, um Programmcodes auszuführen. Ein Angreifer könne also im äußersten Fall Software auf dem Rechner des Anwalts starten. Die anwesenden Experten waren gemeinschaftlich der Auffassung, dass diese Java-Deserialisierungslücke auch dann auftritt, wenn, wie es aktuell der Fall ist, das beA gar nicht in Betrieb ist. Es genüge, so der CCC, dass sich die alte beA Client Security auf dem Rechner des Anwalts oder der Anwältin im Autostart des Rechners befinde und dann nicht korrekt abgebrochen werde, sondern im Hintergrund aktiv bleibe. Atos hatte bisher immer die Auffassung vertreten, dass ältere Java-Bibliotheken kein Sicherheitsrisiko darstellen.

Nachdem Atos sich kurzfristig auf Nachfrage während des beAthon nicht abschließend zu den Hinweisen des CCC äußerte, hat sich die BRAK dazu entschlossen, höchst fürsorglich alle Rechtsanwältinnen und Rechtsanwälte unverzüglich über die Einschätzung der Experten des beAthon zu informieren und sie dazu aufzufordern, die beA Client Security im Autostart zu deaktivieren. Eine Anleitung zur Deaktivierung bzw. zur Deinstallation der beA Client Security für Windows- und MAC-Systeme erhalten Sie anbei.

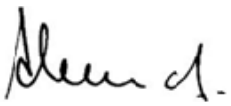
Schließlich diskutierten die Teilnehmer des beAthon auch über die Veröffentlichung des Quellcodes der Client Security. Es gibt Initiativen, die die Veröffentlichung des Quellcodes fordern. Die BRAK hat in der Diskussion klargestellt, dass ihr die Freigabe des Quellcodes aufgrund der Verwendung von Programmcodes von Dritten im Moment nicht möglich ist. Die BRAK hat sich mit dieser Frage bereits in der Vergangenheit beschäftigt und wird sie bei der Weiterentwicklung des beA auch unter Berücksichtigung der Anforderungen der Justiz für die Zukunft erneut prüfen.

Der beAthon hat weitere, gute Erkenntnisse gebracht, welche die BRAK als Anregungen für die Fortentwicklung des beA nutzen wird. Daher ist sie auch an einem weiteren Dialog mit den Netzexperten interessiert.

Der nächste Schritt zur raschen Wiederinbetriebnahme des beA-Systems ist nun die Erstellung des Gutachtens durch die secunet AG. Sollte das Gutachten ein angemessen hohes Sicherheitsniveau attestieren, wird die BRAK der Präsidentenkonferenz vorschlagen, das beA dann unverzüglich wieder in Betrieb zu nehmen. Die BRAK beabsichtigt, das Gutachten danach zu veröffentlichen.

Wir halten Sie unterrichtet.

Mit freundlichen kollegialen Grüßen



Dr. Martin Abend