

Stellungnahme der Firma Atos vom 26.01.2018

Stellungnahme zum besonderen elektronischen Anwaltspostfach (beA)

München, 26. Januar 2018 - Atos, ein führender Anbieter für die digitale Transformation, ist von der Bundesrechtsanwaltskammer (BRAK) mit der Entwicklung, der Implementierung und dem Betrieb des "besonderen elektronischen Anwaltspostfachs (beA)" beauftragt worden. Die Lösung besteht aus einer zentralen Anwendung, die sich in deutschen Atos-Rechenzentren befindet, einer Browserbasierten Web-Anwendung und einer lokal installierten Client-Anwendung. Darüber hinaus gibt es Schnittstellen zu den entsprechenden Systemen der Justiz, der Rechtsanwaltskammern sowie Kanzleisoftware-Anwendungen. Der Vertragsbeginn war Oktober 2014. Seit Projektbeginn Ende 2014 wurden in mehreren Zwischenschritten Entwicklungsstufen der Lösung eingeführt und Elemente weiterentwickelt. Die Umsetzung des beA erfolgte gemäß konzeptioneller Vorgabe der BRAK und berücksichtigte jeweils gültige gesetzliche Vorgaben. Am 28. November 2016 hat die BRAK als Auftraggeber die Lösung den Rechtsanwälten zur Verfügung gestellt.

Am 21. Dezember 2017 wurde durch externe IT-Experten eine Sicherheitslücke bei der sicheren Kommunikation zwischen Browser und Client-Anwendung festgestellt. Ein Zertifikat war zusammen mit dem zugehörigen privaten Schlüssel Bestandteil der installierten Client-Anwendung und wurde damit öffentlich gemacht. Hierdurch war die Sicherheit des Zertifikates nicht mehr gewährleistet und es wurde durch den Anbieter gesperrt. Es handelte sich allein um ein Problem in der Kommunikation des lokalen Browsers mit der Client-Anwendung auf dem Client des Anwalts - die Sicherheit der zentralen Anwendung in den Rechenzentren sowie der Schnittstelle zu den Kanzleisoftware-Anwendungen war hiervon nicht betroffen. Die sichere Kommunikation zwischen den beA-Postfächern war zu jedem Zeitpunkt gewährleistet.

Um sicherzustellen, dass das beA schnellstmöglich wieder verfügbar ist, hat Atos kurzfristig ein neues Zertifikat zur Verfügung gestellt. Am 22. Dezember 2017 hat Atos allerdings festgestellt, dass dieses neue Zertifikat mit zu weitreichenden Rechten ausgestattet war. Angreifer wären mit diesem Zertifikat in der Lage gewesen, Identitäten zu fälschen (Man-in-the-middle Attacken). Atos informierte den Kunden BRAK umgehend. Am gleichen Tag hat die BRAK das beA offline genommen.

Mittlerweile hat Atos dem Kunden BRAK eine neue Version der beA Client-Anwendung zur Verfügung gestellt. Diese Version ist wie folgt überarbeitet:

Die Client-Anwendung erstellt bei der Installation ein individuelles, lokales Zertifikat auf dem Rechner des Anwalts, welches die sichere Kommunikation zwischen Client-Anwendung und Browser ermöglicht. Dieses Zertifikat ist nur in der lokalen Installation bekannt und mit eingeschränkten Rechten ausgestattet. Hierdurch wird der Schutz gegen den missbräuchlichen Einsatz des Zertifikats massiv erhöht. Die Funktionstüchtigkeit und die Sicherheit der Lösung soll durch ein von Atos beauftragtes externes Security-Gutachten bestätigt werden.

Aus Sicht von Atos war mit der Bereitstellung der neuen Lösung die potenzielle

Sicherheitslücke in der beA Browser-Anwendung geschlossen. Die Entscheidung über die erneute Inbetriebnahme des Systems liegt bei der BRAK. Die Rechte an dem Quellcode liegen ebenfalls bei der BRAK beziehungsweise bei den Herstellern der genutzten Standardsoftware-Komponenten.

Die identifizierten Sicherheitsprobleme betrafen ausschließlich die lokale Kommunikation zwischen dem Browser und der Client-Anwendung - weder die zentralen Anwendungen noch die Schnittstelle zu Fachanwendungen waren hiervon direkt betroffen.

Die Sicherheit und Integrität sind wiederhergestellt und das System ist in der aktuell vorliegenden Ausbaustufe voll einsatzfähig.

Über Atos

Atos ist ein weltweit führender Anbieter für die digitale Transformation mit circa 100.000 Mitarbeitern in 72 Ländern und einem Jahresumsatz von rund 12 Milliarden Euro. Als europäischer Marktführer für Big Data, Cybersecurity, High Performance Computing und Digital Workplace unterstützt Atos Unternehmen mit Cloud Services, Infrastruktur- und Datenmanagement sowie Business- und Plattform-Lösungen. Hinzu kommen Services der Tochtergesellschaft Worldline, dem europäischen Marktführer für Zahlungsverkehrs- und Transaktionsdienste. Mit innovativen Technologien, umfassender digitaler Kompetenz und tiefgreifendem Branchenwissen begleitet Atos die digitale Transformation von Kunden aus unterschiedlichen Marktsegmenten: Banken, Bildung, Chemie, Energie und Versorgung, Gesundheit, Handel, Medien und Verlage, Öffentlicher Sektor, Produktion, Telekommunikation, Transport und Logistik, Versicherungen und Verteidigung. Der Konzern ist der weltweite IT-Partner der Olympischen und Paralympischen Spiele. Atos firmiert unter den Marken Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify und Worldline. Atos SE (Societas Europaea) ist an der Pariser Börse als eine der 40 führenden französischen Aktiengesellschaften (CAC40) notiert.

www.atos.net