Besonderes elektronisches Anwaltspostfach: Schadenersatzforderung und Vertröstungen

23.02.2018 08:05 Uhr – Martin Weigel vorlesen

Die Kontroversen rund um das besondere elektronische Anwaltspostfach (beA) reißen nicht ab. Das von Sicherheitslücken belastete System sollte eigentlich seit 01.01. als verbindlicher digitaler Korrespondenzkanal für Rechtsanwälte und Gerichte dienen.

Selten zuvor hat ein Thema des elektronischen Rechtsverkehrs auch unter Nichtjuristen so leidenschaftliche Diskussionen ausgelöst wie das besondere elektronische Anwaltspostfach (beA). Das Spektrum der Positionen ist breit.

Manche Rechtsanwälte klagen: "Der Staat bürdet den Kanzleien damit auf unausgegorene Weise Belastungen auf, nur um selbst Geld zu sparen."

Die Bundesrechtsanwaltskammer (BRAK) sieht sich selbst als Geschädigte, findet aber offenbar, das von ihr in gesetzlichem Auftrag initiierte System sei doch funktionsfähig und könne nach erfolgter Überprüfung im Prinzip ohne grundsätzliche Änderungen starten.

Ekkehard Schäfer, seit September 2015 Präsident der Bundesrechtsanwaltskammer (BRAK), will von der Atos GmbH Schadenersatz für deren Fehlleistungen im Zusammenhang mit dem beA verlangen.

Etliche IT-Fachleute hingegen finden angesichts der ans Licht gekommenen Schwächen des beA, das technische Konzept sei vor die Wand gefahren!

-- Das Beste wäre nach Meinung mancher, ein völlig neues System auf Open-Source-Grundlage zu schaffen --.

Sorgfalt

In dieser Situation hatte der Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestags für Mittwoch, den 21. Februar, zu seiner zweiten Sitzung geladen. Die Moderation der nichtöffentlichen Sitzung lag in den Händen des neuen Ausschussvorsitzenden Stephan Brandner (AfD).

Auf die Berichte der Bundesregierung und der Bundesrechtsanwaltskammer (BRAK) zu den Ursachen der Sicherheitsmängel beim beA hin hatten die Ausschussmitglieder viele Fragen – zu deren Beantwortung waren Staatssekretär Christian Lange vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV), BRAK-Präsident Ekkehard Schäfer und Martin Schaffhausen, Mitglied im Vorstand des Deutschen Anwaltsvereins (DAV) anwesend.

Der BRAK-Präsident wollte offenbar jede Vermutung zerstreuen, die Kammer habe es bei der Auswahl ihrer Vertragspartner zur Entwicklung und zum Implementieren des beA an Sorgfalt fehlen lassen.

So habe sie sich etwa von der adesso AG bei der Verwirklichung des komplizierten Projekts beraten lassen. Das Vergabeverfahren und die Entwicklung des beA selbst habe die Capgemini SE begleitet – so eine Presseerklärung der BRAK vom Mittwoch.

Besonderes elektronisches Anwaltspostfach

Das besondere Anwaltspostfach sollte eigentlich ab dem **1. Januar 2018** zur Kommunikation zwischen Rechtsanwälten und Gerichten mit einer Nachsichtspflicht gestartet werden. Eine Analyse ergab jedoch erhebliche Mängel, die Vetraulichkeit und Sicherheit der Anwalts-Post in Frage stellten.

"Kein gesetzgeberischer Handlungsbedarf"

Staatssekretär Lange sprang der BRAK bei. In seinem der Aussprache vorausgehenden Bericht betonte er, dass das Ministerium der BRAK vertraue und keinen gesetzgeberischen Handlungsbedarf sehe. Damit wurde klar, dass das Ministerium nicht beabsichtigt, gegenüber der Kammer aufsichtsrechtliche Maßnahmen zu ergreifen.

Schäfer teilte mit, dass die gegenwärtige Prüfung des von der Atos Information Technology GmbH entwickelten beA durch die **secunet Security Networks AG** aus **Essen** derzeit noch andauere. Mit ersten Ergebnissen sei erst Ende März zu rechnen. Ein endgültiges Ergebnis ist damit wohl frühestens im Sommer zu erwarten. Von der eigenen Prüfung des BMJV sind keine Ergebnisse bekannt; nicht einmal Zwischenergebnisse haben bislang den Weg an die Öffentlichkeit gefunden.

Keine grundlegenden Änderungen

Das Online-Magazin Legal Tribune Online (LTO) weiß zu berichten, dass die BRAK grundlegende Änderungen an der Technik des Systems nicht für nötig halte und diese Überzeugung schon vor Vollendung des Gutachtens gewonnen habe.

Die Kammer halte auch an der umstrittenen Nutzung des Hardware-Sicherheitsmoduls (HSM) für die Umschlüsselung der elektronischen Nachrichten fest, so LTO.

In ihren offiziellen Verlautbarungen hat die BRAK jedoch wiederholt erklärt, den Verlauf des weiteren Verfahrens sowie der Inbetriebnahme des beA von den Ergebnissen des Sicherheitstests der secunet AG abhängig machen zu wollen.

Zweifel

Währenddessen weht der Wind den beA-Verantwortlichen auch noch aus ganz anderen Richtungen ins Gesicht. Unbeantwortet blieb bislang eine kleine Anfrage der FDP-Bundestagsfraktion vom 31. Januar zum Thema. Zweifel an der grundsätzlichen Sicherheit des beA sind geblieben.

Neben anderen hat etwa die Rechtsanwaltskammer Berlin gefordert, den Quellcode der fürs beA verwendeten Software der Atos GmbH offenzulegen und beim beA ausschließlich freie Software zu verwenden.

Während die BRAK immer wieder betont hat, das beA so schnell wie möglich an das Netz bringen zu wollen, hatte der deutsche Anwaltsverein (DAV) einen weiteren Testzeitraum von zwei Monaten gefordert.

Rechtsstreit

Zusätzlichen Zündstoff bekommt das Projekt durch einen drohenden Rechtsstreit zwischen den Vertragspartnern.

Auf mehrfache Anfrage hat der BRAK-Präsident mitgeteilt, dass die Kammer gegenüber der Atos GmbH Schadenersatzforderungen geltend machen will.

Einerseits ist ein zerrüttetes Verhältnis zu den hauptsächlichen Entwicklern des Konzepts so ziemlich das Letzte, was die BRAK gegenwärtig gebrauchen kann. Andererseits werden die Rechtsanwälte, die bereits Millionen für ein nicht funktionierendes System bezahlt haben, darauf bestehen, dass die Atos GmbH für ihre Fehlleistungen geradestehen muss. (*Martin Weigel*) / (psz)

Fataler Konstruktionsfehler im besonderen elektronischen Anwaltspostfach Update

Volker Weber

Markus Drenger und Felix Rohrbach vom **Chaos Darmstadt** haben ihre Erkenntnisse zum beA am Dienstagabend an der TU Darmstadt erneut präsentiert.

Und es sieht ganz danach aus, dass die Client-Software einen irreparablen Konstruktionsfehler hat.

Der Hörsaal im Piloty-Gebäude der Technischen Universität Darmstadt war bis auf den letzten Platz gefüllt: Die Bugs und Sicherheitslücken im besonderen elektronischen Anwaltspostfach (beA) stoßen offensichtlich auf großes Interesse. Verwunderlich war der rege Publikumszuspruch auch angesichts der Vortragenden nicht: Markus Drenger und Felix Rohrbach vom Chaos Darmstadt e.V. präsentierten ihre Erkenntnisse zum beA der interessierten Öffentlichkeit.

Drenger und Rohrbach haben keinen vollständigen Security Review des beA-Systems durchgeführt. Sie hatten weder Zugriff auf Sourcen noch zum Server. Sie hatten auch keine Benutzer-ID im System, keine Smartcard oder irgendwelche privilegierten Informationen. Sie haben lediglich die Linux-Version des öffentlich verfügbaren Clients heruntergeladen und diese installiert. Dabei zieht die Software zahlreiche weitere Bibliotheken aus dem Netz nach und installiert diese.

Ein erster Blick auf diese Komponenten ergab bereits, dass einige davon seit Jahren veraltet sind und ungepatchte dokumentierte Sicherheitslücken aufweisen. Das ist ein lösbares Problem.

Keine Sicherheit auf unsicherem Grund

Schwerwiegender ist ein grundsätzliches Problem. beA versucht eine sichere Lösung auf unsicherem Untergrund aufzubauen. Die Software lädt einen Webserver als Hintergrundprozess und präsentiert die Benutzerschnittstelle in einem Browser. Da sie Verbindungen zum öffentlichen beA-Server per TLS unterhält, muss sie mit dem Hintergrundprozess ebenfalls per TLS kommunizieren, da sonst der Browser wegen unsicherer Seitenbestandteile Alarm schlägt. Und daraus folgt, dass dieser Hintergrundprozess ein gültiges Zertifikat vorweisen muss, das vom Browser akzeptiert wird.

Dieses Zertifikat mit öffentlichem und privaten Schlüssel war zusammen mit dem verschleierten Passwort in der Client-Software gespeichert. Da diese Lösung aus Sicherheitsgründen ausdrücklich verboten ist, zog die Zertifizierungsstelle das Zertifikat zurück, sobald diese Tatsache bekannt wurde. Die BRAK (Bundesrechtsanwaltskammer) sprach davon, das Zertifikat sei "abgelaufen", was nach einem Flüchtigkeitsfehler klang, und gab ein neues Zertifikat aus. Dieses neue Zertifikat war nicht von einer dem Browser bekannten Zertifizierungsstelle signiert, sondern von einer selbst erstellten eigenen Certificate Authority.

Das Problem hatte sich damit verdoppelt. Nicht nur war das Zertifikat unsicher gespeichert, sondern jetzt musste diese CA noch im Browser installiert werden. Auch hier wurde wieder das Zertifikat vollständig ausgeliefert und kompromittierte damit die Sicherheit des Browsers komplett. Nach Bekanntwerden wurde diese scheinbare Lösung umgehend zurückgezogen.

Der gesetzlich vorgeschriebene Start des beA zum 1. Januar 2018 war gescheitert.

Spitze des Eisbergs?

Das grundlegende Problem liegt darin, dass der Client sowohl das Zertifikat als auch das Kennwort dazu kennt. Der Schlüssel liegt sozusagen unter der Fußmatte. Es spielt keine Rolle, unter welcher Ecke der Fußmatte man ihn versteckt, denn er ist stets präsent. Das lässt sich nur heilen, indem man den Client anders konzipiert. Unklar ist, wie diese Konstruktion überhaupt als sicher zertifiziert werden konnte.

Hinter diesem bekannten Problem lauert ein viel größeres. Drenger und Rohrbach haben diesen Fehler nur zufällig gefunden, weil man den Client einfach herunterladen konnte. Die Frage ist, wie viele andere eGovernment-Lösungen ähnlich angreifbar sind und nur noch nicht entdeckt wurden. Man denke etwa an das Notariatspostfach. Wegschauen dürfte keine Lösung sein.

Update 20.1.2018: Chaos Darmstadt hat einen Mitschnitt des Vortrags online gestellt.

Besonderes elektronisches Anwaltspostfach: Zur Sicherheit sollen Rechtsanwälte die beA Client Security deaktivieren

Volker Weber 27.01.2018 09:37 Uhr

Die Bundesrechtsanwaltskammer hat die erste Lehre aus ihrem beAthon gezogen. Die gar nicht sichere Client Security der beA-Software soll nun von den Anwältinnen und Anwälten umgehend deaktiviert werden.

Beim besonderen elektronischen Anwaltspostfach überschlagen sich die Ereignisse. Während der technische Dienstleister Atos als Entwickler und Betreiber der beA-Plattform gestern noch mitteilen ließ, die Sicherheitsprobleme der Client Security seien nun durch neue Zertifikate wiederhergestellt, konnten sich die Juristen der Bundesrechtsanwaltskammer (BRAK) bei ihrem beAthon gestern vorführen lassen, dass dies nicht die einzige Sicherheitslücke ist. So hatte man zwar am 22. Dezember letzten Jahres das beA serverseitig abgeschaltet und den Anwälten empfohlen, das von der Atos verteilte Zertifikat zu deinstallieren, hatte dabei aber vermisst, auch die Client Software still zu legen. Und so lief dort weiterhin die sogenannte Client Security als lokaler Webserver mit sämtlichen veralteten Java-Bibliotheken, die Markus Drenger und Felix Rohrbach vom Chaos Darmstadt e.V. bereits moniert hatten.

Besonderes elektronisches Anwaltspostfach

Das besondere Anwaltspostfach sollte eigentlich ab dem 1. Januar 2018 zur Kommunikation zwischen Rechtsanwälten und Gerichten mit einer Nachsichtspflicht gestartet werden. Eine Analyse ergab jedoch erhebliche Mängel, die Vetraulichkeit und Sicherheit der Anwalts-Post in Frage stellten.

Client Security umgehend deaktivieren

Gestern Abend verschickte die BRAK daraufhin einen Newsletter und gab eine Pressemitteilung heraus: "Die gegenwärtig bei den Anwältinnen und Anwälten installierte Client Security kann eine Lücke für einen externen Angriff darstellen. Aus diesem Grund empfiehlt die BRAK allen Anwältinnen und Anwälten, ihre bisherige Client Security zu deaktivieren." Am sichersten erscheint es, die gesamte SoftwareinsDie Bundesrechtsanwaltskammer hat die erste Lehre aus ihrem beAthon gezogen. Die gar nicht sichere Client Security der beA-Software soll nun von den Anwältinnen und Anwälten umgehend deaktiviert werden.

Beim besonderen elektronischen Anwaltspostfach überschlagen sich die Ereignisse. Während der technische Dienstleister Atos als Entwickler und Betreiber der beA-Plattform gestern noch mitteilen ließ, die Sicherheitsprobleme der Client Security seien nun durch neue Zertifikate wiederhergestellt, konnten sich die Juristen der Bundesrechtsanwaltskammer (BRAK) bei ihrem beAthon gestern vorführen lassen, dass dies nicht die einzige Sicherheitslücke ist. So hatte man zwar am 22. Dezember letzten Jahres das beA serverseitig abgeschaltet und den Anwälten empfohlen, das von der Atos verteilte Zertifikat zu deinstallieren, hatte dabei aber vermisst, auch die Client Software still zu legen. Und so lief dort weiterhin die sogenannte Client Security als lokaler Webserver mit sämtlichen veralteten Java-Bibliotheken, die Markus Drenger und Felix Rohrbach vom Chaos Darmstadt e.V. bereits moniert hatten.

Besonderes elektronisches Anwaltspostfach

Das besondere Anwaltspostfach sollte eigentlich ab dem 1. Januar 2018 zur Kommunikation zwischen Rechtsanwälten und Gerichten mit einer Nachsichtspflicht gestartet werden. Eine Analyse ergab jedoch erhebliche Mängel, die Vetraulichkeit und Sicherheit der Anwalts-Post in Frage stellten.

Client Security umgehend deaktivieren

Gestern Abend verschickte die BRAK daraufhin einen Newsletter und gab eine Pressemitteilung heraus: "Die gegenwärtig bei den Anwältinnen und Anwälten installierte Client Security kann eine Lücke für einen externen Angriff darstellen. Aus diesem Grund empfiehlt die BRAK allen Anwältinnen und Anwälten, ihre bisherige Client Security zu deaktivieren." Am sichersten erscheint es, die gesamte Softwareinstallation zu entfernen, da beA ohnehin erst nach der Prüfung einer neuen Client Security wieder in Betrieb genommen werden kann.

Die BRAK führt aus, dass sie "ihren Entwickler bereits 2017 auf seine Verpflichtung hingewiesen (hat), diese Sicherheitslücken zu schließen. Atos hat nach eigenen Angaben in der neuen Version der Client Security sichergestellt, dass der Zugriff auf aktuelle JAVA-Bibliotheken erfolgt." Dabei ist den Juristen wohl entgangen, dass diese Lücke auf allen Anwalts-PC mit der alten beA-Software weiterhin besteht. Vor dem beAthon hat sie jedenfalls nicht dafür Sorge getragen, das Problem auch zu lösen.

beAthon nur ein Auftakt

Während des beAthon war es auf Twitter merkwürdig still. Nach dem Event meldete sich Drenger dann zurück: "zeitlich kurz, fühlt sich aber wie marathon an. #beA". Gut zwei Stunden später schob er mit etwas mehr Abstand nach: "Hab ich viel erwartet? Nein. Fand ich, dass es gut lief? Ja. Es lief sehr produktiv, ich habe quasi alle Dinge auf dem Zettel in den Bugtracker geworfen. Ich hoffe, der beAthon war ein Auftakt, Dinge besser zu machen."

Die BRAK akzeptierte in ihrer Meldung die von Atos bereitgestellte neue beA-Version wohl etwas voreilig "als sichere Basis". Das war die alte Version schließlich auch, bis der CCC den Anwälten den Spiegel vorhielt. Die Sicherheitslücken, welche die BRAK gestern erst zur Kenntnis nahmen, bestanden von Anfang an und wurden bereits vor Wochen durch Drenger und Rohrbach gemeldet. Nun muss durch qualifizierte und unabhängige Sicherheitsfachleute gründlich und umfassend geprüft werden. Sonst stolpert das beA von einem Schlagloch zum nächsten.

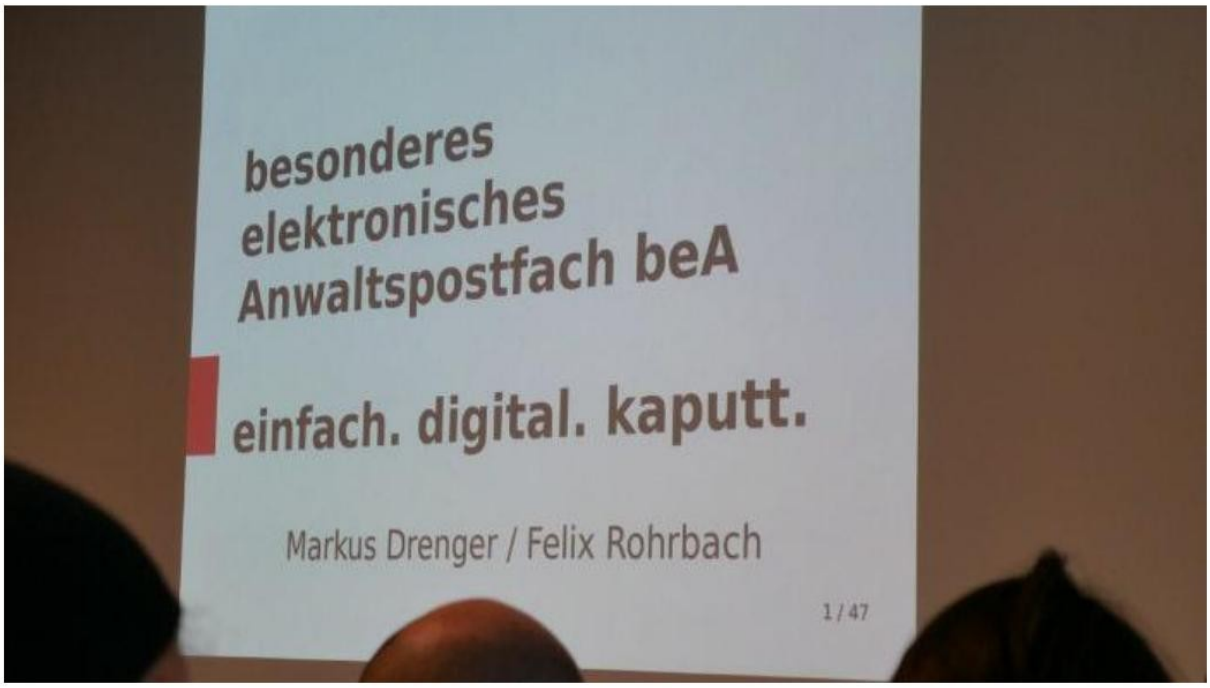
(*Volker Weber*) / (vowe)

beAthon nur ein Auftakt

Während des beAthon war es auf Twitter merkwürdig still. Nach dem Event meldete sich Drenger dann zurück: "zeitlich kurz, fühlt sich aber wie marathon an. #beA". Gut zwei Stunden später schob er mit etwas mehr Abstand nach: "Hab ich viel erwartet? Nein. Fand ich, dass es gut lief? Ja. Es lief sehr produktiv, ich habe quasi alle Dinge auf dem Zettel in den Bugtracker geworfen. Ich hoffe, der beAthon war ein Auftakt, Dinge besser zu machen."

34C3: Das besondere Anwaltspostfach beA als besondere Stümperei

28.12.2017 16:09 Uhr – Detlef Borchers vorlesen



Darmstädter Hacker zeigen, dass das besondere elektronische Anwaltspostfach, kurz beA, mit veralteter Software und einem veralteten Anwendungskonzept entwickelt wurde.

Atos[*)], der technische Dienstleister, der beA entwickelt und für die Bundesrechtsanwaltskammer (BRAK) betreibt, hat heute Fehler eingeräumt. 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. Um sicherzustellen, dass das beA schnellstmöglich wieder verfügbar ist, habe Atos kurzfristig ein neues Zertifikat zur Verfügung gestellt. Am **22. Dezember 2017** habe Atos allerdings festgestellt, dass dieses neue Zertifikat mit zu weitreichenden Rechten ausgestattet sei und die BRAK habe das beA deshalb am gleichen Tag **offine** genommen.

Besonderes elektronisches Anwaltspostfach

Das besondere Anwaltspostfach sollte eigentlich ab dem 1. Januar 2018 zur Kommunikation zwischen Rechtsanwälten und Gerichten mit einer **Nachsichtspflicht** gestartet werden. Eine Analyse ergab jedoch erhebliche Mängel, die Vetraulichkeit und Sicherheit der Anwalts-Post in Frage stellten.

Mittlerweile hat Atos der BRAK eine neue Version der beA Client-Security zur Verfügung gestellt. Diese Software 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."

Probleme behoben?

Atos hält die Sicherheitsprobleme damit für behoben; das Unternehmen will sich die Funktionstüchtigkeit und die Sicherheit der Lösung durch ein von Atos beauftragtes externes Security-Gutachten bestätigt lassen. Die BRAK will wiederum selbst ein Gutachten von der vom BSI empfohlenen secunet beauftragen.

Weiterhin stellt Atos fest, dass die Rechte an dem Quellcode von beA bei der BRAK lägen mit der Einschränkung der genutzten Standardsoftware-Komponenten, an denen die jeweiligen Hersteller die Rechte haben. 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 läge nun bei der BRAK.

Zertifikats-Wirrwarr

Die Stellungnahme von Atos geht ganz spezifisch nur auf das Zertifikatsproblem ein. Andere Bedenken zur Sicherheit der Lösung werden nicht adressiert. Es handele 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 seien hiervon nicht betroffen. Die sichere Kommunikation zwischen den beA-Postfächern sei zu jedem Zeitpunkt gewährleistet.

Die BRAK will am heutigen Freitagnachmittag den so genannten beAthon veranstalten, bei dem externe Experten einen Fragenkatalog an Atos entwickeln sollen. (*Volker Weber*) / (vowe)

---

*) Nach eigener Darstellung: … Ein Weg führt zu Atos, einem der zehn größten IT-Unternehmen der Welt mit rund 100.000 Mitarbeitern in 72 Ländern. ...

Zum 1. Januar 2018 wird das besondere elektronische Anwaltspostfach (beA) "passiv nutzungspflichtig". Ab diesem Zeitpunkt muss jeder Rechtsanwalt nachsehen, ob ihm auf diesem Wege Schriftstücke zugeschickt wurden. Wenige Tage vor diesem Datum müssen alle Anwälte nach einer Eilmitteilung der Bundesrechtsanwaltskammer nun ein neues elektronisches Zertifikat installieren, weil das ausgestellte Zertifikat zum heutigen 22. Dezember ungültig wurde.
Einem IT-Dienstleister war nämlich aufgefallen, dass der beA-Client nicht den Public Key, sondern den Private Key des von T-Systems signierten Zertifikates verteilte. Nach den allgemeinen Regeln für Sicherheitszertifikate musste dieser Key für ungültig erklärt werden.

Zur eiligen Installation des neuen Zertifikates veröffentlichte die Kammer eine Anleitung. Sie enthält die Empfehlung, die dringlichen Installationswarnungen von Microsofts Explorer und Mozillas Firefox zu ignorieren. Besonders harsch fällt diese Warnung für Firefox aus: "Seriöse Banken, Geschäfte und andere öffentliche Seiten werden Sie nicht bitten, derartiges zu tun." Entsprechend verunsichert dürfte sich jetzt mancher Anwalt die Frage stellen, ob es sich bei der Bundesrechtsanwaltskammer um eine seriöse Vereinigung handelt.

beAthon zum Anwaltspostfach

Es ist noch schlimmer. Aber es wird besser.

von Jörn Erbguth 28.01.2018

© maxsim - stock.adobe.com

Statt einem offenen Hackathon zum Anwaltspostfach gab es eine geschlossene Diskussion mit 20 handverlesenen Gästen, aber ohne die Softwarehersteller. Die Skepsis gegenüber der BRAK-Veranstaltung war groß. *Jörn Erbguth* war dabei.

Vorweg: Die Skepsis erwies sich als unbegründet. Ohne Softwarehersteller konnte man zügig durch die lange Liste von Sicherheitsproblemen des besonderen elektronischen Anwaltspostfachs (beA) gehen, die Markus Drenger und seine Kollegen Justus Hoffmann und Felix Rohrbach vom CCC Darmstadt vorbereitet hatten.

Souverän moderiert wurde der beAthon von Prof. Dr. Stephan Ory, dem Vorstandsvorsitzenden des EDV-Gerichtstags. Der Verein für IT in Rechtspflege und Verwaltung war daneben noch durch Christoph Sorge und meine Person vertreten. Ory schichtete die Probleme ab: Was ist eine Minimalbedingung für eine Wiederinbetriebnahme und in welche Richtung sollte das beA weiterentwickelt werden? Letzteres wurde unter dem Stichpunkt "beA+" gefasst und wird am 5. März vom EDV-Gerichtstag in Berlin diskutiert.

Anhang 1

Die BRAK wurde in der Krisensitzung zum Postfach-Desaster vertreten durch den Vizepräsidenten Dr. Martin Abend, die Geschäftsführerinnen Julia von Seltmann und Stephanie Beyrich sowie den Projektleiter Hannes Müller. Positiv wurde allseits aufgenommen, dass die Begutachtung durch die Firma Secunet alle Komponenten des beA – also auch Server und HSM umfassen soll. Sie soll schrittweise geschehen und zumindest der BRAK-Präsidentenkonferenz zugänglich gemacht werden.

Der Gastgeberin wurde mitgegeben, mehr Offenheit zu wagen und nach Möglichkeit den Quellcode offen zu legen. Obwohl die vorgetragene Liste der Sicherheitsmängel lang war, ist es unwahrscheinlich, dass ohne den Zugriff auf diesen alle Schwachstellen gefunden werden.

Massive Sicherheitslücke: beA-Client trotz abgeschalteten Postfachs gefährlich

Auf technischer Seite stellten sich noch mehr Probleme heraus, als bisher bereits bekannt waren. So führt die Verwendung veralteter Java-Bibliotheken zu einer sehr konkreten Gefährdung der Anwaltsrechner. Anwaltsrechner können bereits beim Besuch einer Website angegriffen und übernommen werden.

ATOS war auf diese Sicherheitslücke hingewiesen worden, wiegelte aber ab: Es bestehe wegen des abgeschalteten beA-Servers aktuell keine konkrete Gefährdung. Die beim beAthon anwesenden Experten sahen dies jedoch anders. Nach kurzer Diskussion schuf ein Test Klarheit: Das Problem der Java-Deserialisierungslücke war selbst bei dem aktuell abgeschalteten beA-Server vorhanden. Surft ein Anwalt, der die beA-Software installiert und aktiviert hat, im Internet, setzt er seinen Rechner einer akuten Gefahr aus. Ähnlich wie vor Weihnachten musste konstatiert werden: Das beA-System macht Anwaltsrechner unsicher.

Die BRAK reagierte umgehend und gab noch am selben Abend eine Presseerklärung heraus, mit der sie die Nutzer zur Deinstallation aufforderte. Darüber hinaus ist ein Update geplant, wodurch die bis dahin noch nicht deaktivierten Client-Security-Installationen automatisch deaktiviert werden.

Vorgestellt wurde auch die neue Lösung von Atos für die https-Anbindung der Client-Security. Bei der Installation wird ein selbst signiertes Client-Zertifikat generiert und installiert. Nach ein paar Rückfragen war klar: In der gegebenen Architektur ist das der richtige Weg. Der BRAK war kurz vor dem beAthon eine überarbeitete Version der Client-Security zur Verfügung gestellt worden, die ATOS öffentlich anpries: "Sicherheit und Integrität sind wieder hergestellt". Ungeprüft glauben wollte das beim beAthon jedoch niemand mehr. Von daher wird die BRAK diese vor einer ausführlichen Begutachtung nicht ausliefern.

Generalschlüssel statt Ende-zu-Ende-Verschlüsselung

Kontrovers war die Diskussion um die Ende-zu-Ende-Verschlüsselung (E2EE). Die BRAK nutzt diesen Begriff seit Jahren, um die Sicherheit des Anwaltspostfachs zu beschreiben.

Anhang 2

Die fachsprachliche, allgemeine Definition von E2EE ist, dass niemand außer den kommunizierenden Parteien Zugriff auf die Schlüssel zur Entschlüsselung hat. Damit kann auch ein böswilliger "man in the middle" nicht auf die Inhalte der Nachrichten zugreifen. Es sollte also durch eine Verschlüsselung außerhalb des Servers von vorneherein technisch ausgeschlossen sein, im beA-Server die Nachrichten zu entschlüsseln.

Im vorliegenden beA-System könnte der Server die Nachrichten aber sehr wohl entschlüsseln. Nur die korrekte Implementierung von Sicherheitsmaßnahmen sowie der sichere Betrieb des Servers gewährleisten, dass dies nicht geschieht.

Als falsch erwies sich auch die bisherige Darstellung der BRAK, dass es keinen Generalschlüssel für das Hardware Security Module (HSM) gäbe. Vielmehr wurde deutlich, dass es für die Übertragung von einem HSM auf ein neues HSM einen Schlüssel gibt, der auf mehrere Parteien – sogenannte Key-Custodians – verteilt ist. Würde man ein neues, manipuliertes HSM aufbauen, könnte man mit diesem Schlüssel die privaten Postfachschlüssel in das manipulierte HSM übertragen und von diesem dann auslesen.

Auf welche Personen ist nun dieser Generalschlüssel aufgeteilt? Das ist geheim. Zumindest soll ihn nicht ATOS haben und ohne Mitwirkung der BRAK ist der Schlüssel nicht komplett. Aus dem Kreis der anwesenden Kryptoexperten wurde bestätgt, dass diese Art der Absicherung ein Standardverfahren für HSM ist. Einig war man sich auch, dass die Implementierung via HSM – wenn sie richtig gemacht wird – ein hohes Sicherheitsniveau erreicht, die z.B. deutlich über der Sicherheit des Fax-Versands liegt.

Da eine Entschlüsselung bei der BRAK nicht völlig ausgeschlossen werden kann, wurde aber auch andiskutiert, ob die BRAK deshalb als Auftragsdatenverarbeiter im Sinne der DS-GVO angesehen werden muss.

Ein intensiver Austausch fand in der Folge darüber statt, warum diese Umschlüsselung durch das HSM gewählt wurde. Am Ende waren fast alle davon überzeugt, dass es keine gesetzlichen oder sonstigen triftigen Gründe gegen eine echte E2EE der Nachrichteninhalte gibt. Das wird sicher bei der Diskussion über die Weiterentwicklung auf der Tagesordnung stehen. Aus dem Kreis der anwesenden Anwälte mit fundiertem IT-Know How wie Matthias Bergt sowie Dr. Marcus Werner und Sebastian Reiling vom Deutschen Anwaltverein wurde betont, wie wichtig eine E2EE für die Akzeptanz sei – das habe man bei Whatsapp gesehen und es gelte noch viel mehr für die Anwaltschaft.

Überwachung durch staatliche Stellen?

Gefragt, aber nicht beantwortet wurde, ob BRAK und das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) bestätigen können, dass sie das beA nicht als öffentlich zugänglichen Telekommunikationsdienst i.S.v. § 3 Nr. 17a Telekommunikationsgesetz (TKG) sehen. Wichtig ist das deshalb, weil für öffentlich zugängliche Kommunikationsdienste die Vorschrift des § 110 TKG gilt: Ihr Betreiber muss Einrichtungen zur Überwachung vorhalten. Zwar ist das beA nur einem beschränkten Nutzerkreis zugänglich. Allerdings ist es mit dem öffentlich zugänglichen Elektronischen Gerichts- und Verwaltungspostfach (EGVP) verbunden.

Anhang 3

Nach einer Mindermeinung in der Literatur reiche das aus, um das Anwaltspostfach selbst zum öffentlich zugänglichen Kommunikationsdienst zu machen.

Kontrovers wurde debattiert, wie gravierend es ist, dass beliebige Websites erkennen können, dass sie von einem Anwalt besucht werden. Demonstriert hatte diese Möglichkeit bereits im März 2017 Ralph Hecksteden . Atos hat in Aussicht gestellt, die Software umzubauen, um diese Erkennung zu unterbinden. Ob und wie dies bei der gegebenen Architektur möglich ist, blieb am Freitag offen.

Es ging schließlich auch um eine Reihe von Schwachstellen beim EGVP, die dessen Betrieb empfindlich störten könnten. Die BRAK, die den Betrieb des EGVP nicht verantwortet, kann dabei nur indirekt aktiv werden. Umso mehr dürfte die Debatte den Vertreter des BMJV, Oliver Sabel, interessiert haben, der ebenfalls anwesend war.

Der beAthon war nur ein Anfang

Allen Beteiligten war klar, dass es mit einem beAthon nicht getan ist. Um den elektronischen Rechtsverkehr zum Fliegen zu bringen, braucht die BRAK Unterstützung. Positiv ist, dass sie inzwischen bereit ist, diese anzunehmen. Ebenfalls positiv ist die zunehmende Offenheit und die Bereitschaft der BRAK, dazu zu lernen. Dies ist denn auch der Grund, trotz der erschütternden Nachrichten über den technischen Zustand des beA vorsichtig optimistisch zu sein.

Darüber hinaus müssen grundsätzliche Fragen noch diskutiert werden. Denn eines ist klar: Ein repariertes beA in der aktuellen Konzeption ist eher Notlösung als Ideallösung für den elektronischen Rechtsverkehr.

Organisiert wurde der beAthon von der stark vertretenen Kommunikationsagentur Johanssen + Kretschmer. Auch wenn deren Kommunikation zum beAthon im Vorfeld auf Kritik gestoßen ist, war die Durchführung der Veranstaltung sicherlich ein Erfolg und ein wichtiger Schritt für den elektronischen Rechtsverkehr in Deutschland.

Der Autor Jörn Erbguth ist Legal-Tech-Berater zu Blockchain und Smart Contracts in Genf. Er ist zertifizierter Datenschutzbeauftragter und lehrt an der Geneva School of Diplomacy. Zusätzliche Hintergründe und weitere Details zum beA wird das Vorstandsmitglied des EDV-Gerichtstags in der Online-Zeitschrift jurPC veröffentlichen.