beA – Fragen und Antworten

1. Frühere Sicherheitstests des beA-Systems?

Auf der Grundlage der Leistungsbeschreibung und des Umsetzungskonzeptes von Atos erstellte Atos eine Teststrategie als Teil des Umsetzungsfeinkonzepts, deren Aufgabe die Definition und Beschreibung aller Tests ist, die im Rahmen der Realisierungsphase des Projekts geplant und realisiert werden sollten. Diese Teststrategie sieht je nach Testziel unterschiedliche Methoden vor. Die Sicherheitstests sollten als Blackbox-Tests durchgeführt werden. Mit der Durchführung des Tests beauftragte die BRAK im Rahmen des Realisierungsprojekts die Firma Atos.

Die abgestimmten Tests führte Atos vor der Inbetriebnahme des Systems Ende 2015/Anfang 2016 durch. Nach Durchführung der Tests übergab Atos der BRAK den Testbericht mit dem Stand 09.05.2016. Die BRAK hat keine Anhaltspunkte dafür, dass die Tests nicht vollständig durchgeführt wurden. Extern für den Bereich des Qualitätsmanagements hinzugezogene Mitarbeiter der Firma Capgemini sahen ebenfalls keinen Anlass, die Testergebnisse zu bezweifeln.

Über die Entwicklungstests hinaus beauftragte Atos die Firma SEC Consult mit der Durchführung weiterer Sicherheitstests, in die die vom Frontend erreichbaren Server sowie die Client Security einbezogen wurden. Die Prüfungen zielten darauf, Schwachstellen in der HW/SW-Architektur, des Authentifizierungskonzepts, der Signaturmechanismen und der sog. Ende-zu-Ende-Verschlüsselung auszumachen. Die Tests sind in Form von Black-Box-Tests durchgeführt worden. Die Tests der SEC Consult wurden nach dem Timebox-Verfahren durchgeführt. Die Testergebnisse sind der BRAK von Atos zur Verfügung gestellt worden. Ergebnis der Tests war, dass das beA-System ein hohes Sicherheitsniveau aufweist.

Das Gutachten der Firma SEC Consult ist als „streng vertraulich“ gekennzeichnet. Es kann daher nicht überlassen werden, solange nicht die ausdrückliche Freigabe vorliegt.

Im Jahr 2015 wurden Überlegungen angestellt, das beA-System im Rahmen eines Chaos Communication Camps, das vom Chaos Computer Club (CCC) organisiert wird, testen zu lassen. Entgegen der Darstellung in den Medien ist die BRAK mit dieser Idee an den CCC herangetreten. Die Zusammenarbeit wurde nicht wie behauptet von der BRAK abgelehnt. Allerdings erhielt die BRAK vom CCC keine verbindliche Zusage dahingehend, dass ihr die Testergebnisse vollumfänglich zur Verfügung gestellt werden. Aus diesem Grund entschied das Präsidium der BRAK, dass das beA-System dem CCC nicht zum Testen im Rahmen des Chaos Communication Camps zur Verfügung gestellt wird.

2. Ende-zu-Ende-Verschlüsselung?

Gemäß § 31a Abs. 3 Satz 2 BRAO hat die Bundesrechtsanwaltskammer (BRAK) auch Vertretern, Abwicklern und Zustellungsbevollmächtigten die Nutzung des besonderen elektronischen Anwaltspostfachs (beA) zu ermöglichen. Sie kann nach § 31a Abs. 3 Satz 3 BRAO unterschiedlich ausgestaltete Zugangsberechtigungen für Kammermitglieder und andere Personen vorsehen. Da das Berufsrecht vorgibt, dass auch andere Personen als der Rechtsanwalt und damit der Postfachinhaber selbst Zugriff auf dessen Postfach haben müssen, musste die BRAK eine Lösung suchen, die den Zugriff anderer – berechtigter – Personen auf die Nachrichten zulässt. Sie musste dabei berücksichtigen, dass sowohl der von der Kammer eingesetzte Abwickler oder Vertreter als auch der vom Rechtsanwalt selbst bestimmte Vertreter den Zugriff erhalten können muss. Die Umsetzung dieser Anforderungen war bei gleichzeitiger Einhaltung der Ende-zu-Ende-Verschlüsselung der Nachricht selber nur mit der Entwicklung einer eigenen Lösung, nämlich des beA-HSM, möglich.

Hinsichtlich der Fragen zur Verwendung des Hardware Security Moduls (HSM) und zur sog. Ende-zu-Ende-Verschlüsselung wird im Übrigen auf die Übersicht zur technischen Funktionsweise des beA-Systems verwiesen.

Die Implementierung des HSM enthält keinerlei Funktionalität, die diesen (oder andere) Schlüssel im Klartext exportieren kann. Somit hat kein Nutzer im normalen Betrieb des HSM Zugriff auf diesen Schlüssel. Die Schutzmechanismen der Hardware des HSM stellen sicher, dass kein Anwender im Falle eines Angriffs auf das HSM (etwa das gewaltsame Öffnen und der Versuch des Auslesens des Speichers) Zugriff auf das Klartext-Schlüsselmaterial erhalten kann.

Die DataCenter von Atos haben an beiden Standorten ein mehrschichtiges Sicherheitskonzept in Bezug auf den physischen Zugang: Geländeumzäunung und Videoüberwachung, Gebäudeüberwachung mit Videokameras an den Haupteingängen, extra gesicherter DC Kernbereich mit Vereinzelungsanlage und speziellen Ausweisen, DC Käfige für verschiedene Kunden. Für die BRAK sind sämtliche beA-Komponenten in dedizierten, abgeschlossenen Käfigen und zusätzlich durch abgeschlossene Racks (mit RFID-Schlüsseln) gesichert untergebracht. Der Empfang und das Einbringen von Komponenten in das DC oder in Käfige erfolgt nur über Netz und DC Services (NDCS) DC Operations Personal oder begleitete Hersteller-Mitarbeiter. Der Zugang wird nur gestattet, wenn ein entsprechender An-trag/Change avisiert und genehmigt wurde. Für kurzfristig notwendige Wartungsarbeiten (z.B. Plattenaustausch) sind Techniker durchgehend vor Ort. Im normalen Betrieb und für Monitoring Zwecke ist kein physischer Zugang notwendig. Der Versuch ein HSM-Modul physisch zu öffnen führt zur kompletten Löschung der im Modul gespeicherten Daten. Eine Wartung eines HSM Moduls kann nicht vor Ort erfolgen. Dies kann nur in den gesicherten Herstellerräumen von Atos Worldline erfolgen. Um bei einer Wartung eine Betriebsunterbrechung zu vermeiden, werden dabei erst neue Geräte vor Ort gebracht, in das System eingebunden und synchronisiert, danach die alten Geräte herausgenommen und an Atos Worldline zurückgeschickt.

Der im HSM hinterlegte Schlüssel erfüllt verschiedene Funktionen: Der Schlüssel wird für die Authentifizierung, die Verschlüsselung und für die Anmeldung verwendet. Bei dem privaten Schlüssel auf der beA-Karte (privater Benutzerschlüssel) und dem im HSM hinterlegten Schlüssel (privater Postfachschlüssel) handelt es sich um zwei verschiedene Schlüssel. Die privaten Schlüssel der Postfächer und die zugehörigen öffentlichen Schlüssel werden beim Anlegen des Postfaches im HSM erstellt. Der private Schlüssel wird von der BNotK bei Generierung der beA-Karte erstellt. Der private Schlüssel im HSM wird im Rahmen der Postfachgenerierung erzeugt und verlässt dieses nie unverschlüsselt. Es wird sichergestellt, dass ein Sicherheitstoken einem System-Benutzer eindeutig zugeordnet wird. Nach § 26 Abs. 1 RAVPV dürfen die Inhaber eines für sie erzeugten Zertifikats dieses keiner weiteren Person überlassen und haben die dem Zertifikat zugehörigen Zertifikats-PIN geheim zu halten. Nach § 26 Abs. 2 RAVPV hat der Postfachinhaber unverzüglich alle erforderlichen Maßnahmen zu ergreifen, um einen unbefugten Zugriff auf sein Postfach zu verhindern. Den Fall, dass mehrere Personen über denselben Schlüssel verfügen, sieht das beA-System nicht vor.

3. Geplante Prüfung des Systems

In der Präsidentenkonferenz wurde festgehalten, dass die BRAK einen durch das BSI empfohlenen Experten beauftragen wird, um die Sicherheit des beA-Systems vor Zurverfügungstellung für die Rechtsanwaltschaft zu testen. Das Gutachten der BRAK wird den Rechtsanwaltskammern zur Verfügung gestellt. Darüber hinaus ist von Atos bereits ein externer Gutachter zur Überprüfung der sicherheitsrelevanten Bereiche des beA-Systems hinzugezogen worden.

Ferner plant die BRAK, verschiedene kritische Experten, die sich in den letzten Tagen verstärkt zu den möglichen Risiken der bestehenden Plattform und der erforderlichen Sicherheitsarchitektur äußerten, in den Prozess zur Klärung sicherheitsrelevanter Fragestellungen einzubinden. Dazu soll ein sogenannter beAthon am 26.01.2018 stattfinden. Beim beAthon sollen institutionell nicht gebundene Experten den Lösungsweg des Dienstleisters zusammen mit den Gutachtern und den technischen Dienstleistern erörtern.

4. Sicherheits-/Kapazitätsprobleme des beA-Systems?

a. Bug Cross-Site-Scripting

Es wurden und es werden fortlaufend Filter in der beA-Anwendung eingesetzt, um neuen Bedrohungssituationen zu begegnen. Zu betonen ist, dass Angriffe durch Cross-Site-Scripting nicht speziell Web-Anwendungen immanent sind, sondern grundsätzlich ein Angriffsszenario für jede Software-Anwendung darstellen. Der Projektleiter der Firma Atos, Herr Busch, hatte in der Präsidentenkonferenz erläutert, dass das beA-System vorsieht, dass nur maximal zehn zusätzliche Zeichen eingegeben werden können. Damit sind Angriffsmöglichkeiten durch Cross-Site-Scripting extrem eingeschränkt.

b. Verwendung abgelaufener Java-Libraries?
Zwischenzeitlich sind alle verwendeten Libraries nochmals überprüft und z.T. ausgetauscht worden. Die Libraries werden zudem bei jeder neuen beA-Software-Lieferung überprüft und ggf. aktualisiert werden.

c. Anfälligkeit gegen ROBOT-Attacken?
Eine der beiden Anwendungsfirewalls hat verspätet ein Sicherheitsupdate erhalten. Dieses wurde inzwischen nachgeholt. In Zukunft werden beide Systeme jeweils auf dem aktuellen Stand gehalten. Zutreffend ist, dass der NetScaler Citrix Systems eingesetzt wird. Dieses System ist im Eigentum sowie in der Verantwortung des IT-Dienstleisters der BRAK. Er ist vertraglich verpflichtet, die Hard- und Software auf dem aktuellen Stand zu halten.

d. Zugriff auf Kartenlesegeräte
Die Ansteuerung von Kartenlesegeräten ist eine der Funktionen, die zu der Entscheidung geführt haben, die Client Security einzubinden. Moderne Browser erlauben es auch heute noch nicht, die Verschlüsselung vorzunehmen.

Als ursprüngliche Variante war eine Plugin Schnittstelle (NSAPI) vorgesehen worden. Die Kryptografie -Funktionalitäten und die Kartenansteuerung sollten in Form eines Java-Applets bereitgestellt werden. Java-Applets können im Kontext einer Webseite ausgeführt werden und erlauben eine Javascript-basierende Kommunikation zwischen der Webseite und dem Applet. Voraussetzung für die Nutzung von Applets ist es, dass der Browser eine Schnittstelle für Plug-Ins, in diesem Fall für ein Java-Plug-In, bereitstellt. Dies war zum Zeitpunkt des Angebots Standard und ist aktuell auch noch bei allen Browsern am Markt der Fall. Allerdings wurde der Support der Plug-In-Schnittstelle (NPAPI) von den Schnittstellenunterstützern (u.a. Google) abgekündigt. Als Lösung wählte daraufhin die BRAK die Realisierung der Web-Anwendung in der zur Verfügung gestellten Form.

e. Software nicht codesigned/von zertifiziertem Entwickler
Die macOS-Installationsdatei stammt nicht von einem verifizierten Entwickler – sie ist nicht codesigned, d.h. es handelt sich um eine nicht signierte Installationsdatei. Nutzer sollten durch den Download auf der Startseite von beA die Client Security-Installationsdatei laden. Eine Weitergabe der Installationsdatei an Dritte ist nicht vorgesehen. Die zu ladenden Installationsdateien sind mit einem Hashwert versehen und können entsprechend auf ihre Integrität überprüft werden.

f. Update mit einem abgelaufenen Zertifikat?
Der BRAK ist dieser Sachverhalt nicht bekannt. Sie hat Atos um Prüfung gebeten.

g. https-Konfiguration der beA-Anwendung
HTTP Strict Transport Security (HSTS) wurde bislang bei der beA-Webanwendung nicht eingesetzt. Vor Wiederinbetriebnahme des beA-Systems wird dies umgesetzt werden.

h. weitere Mängel?
Der BRAK liegen über die bereits diskutierten Mängel hinaus keine Kenntnisse über relevante Sicherheitslücken des beA-Systems vor. Ihr sind keine weiteren Fehler der Software bekannt, die betriebsverhindernd sind. Die genannten Mängel werden von Atos im Rahmen des etablierten Fehlerbehebungsprozesses behoben.

Nach dem Einspielen der Version 2.0 am 25./26.11.2017 traten zwischen dem 01.12.2017 und dem 15.12.2017 Verbindungsprobleme zum beA auf, die an fünf Tagen zu einer Nichterreichbarkeit des Systems für eine Zeitdauer zwischen 30 Minuten und 2,5 Stunden führten.

Zur Lösung der aufgetretenen Probleme nahm Atos Konfigurationsanpassungen vor. Zudem wurden Systemressourcen den Arbeitsprozessen in größerem Umfang zur Verfügung gestellt. Insbesondere sind Anpassungen der Cookie-Verarbeitung in der Client-Security vorgenommen worden. Eine Veränderung der Software erfolgte dabei nicht, sondern nur eine Ressourcenzuordnung bei der Hardware. Die vorgenommenen Änderungen waren nicht sicherheitsrelevant. Diese waren nur auf die Verfügbarkeit des beA-Systems ausgerichtet, nicht auf die Integrität und die Vertraulichkeit der Daten oder der Kommunikation.

Die Prüfungs- und Analyseergebnisse der Ausfälle zeigen, dass ein Index in der Cookie-Verarbeitung zu einer Blockierung der Anwendungsfirewall geführt hat. Darüberhinaus bestanden Probleme in einem System der Justiz, das allein innerhalb von zwei Tagen über 20.000 Nachrichten schickte.

Die Einhaltung der Sicherheitsanforderungen des von Atos angebotenen Systems sind von einem IT-Sicherheitsexperten von Capgemini überprüft worden. Ergebnis der Überprüfung war, dass die erkannten Fehlerpunkte im Rahmen der Finalisierung von Atos beantwortet und behoben wurden. Zudem erfolgte ein Review der Konzepte in Bezug auf die Umsetzung der Sicherheitsanforderungen.

Die von Atos angebotene HSM-Lösung ist ebenfalls von dem IT-Sicherheitsexperten von Capgemini überprüft worden, da das Konzept zum HSM Bestandteil der Prüfung war. Die Ergebnisse der Überprüfung sind in die weitere Verhandlung der Konzeption des Systems eingeflossen. Das HSM war Teil der Abnahme der Funktionsüberprüfung (Version 0.9) vom 07.11.2016 durch die BRAK.

Im Übrigen werden regelmäßig sowie nach Bedarf Audits und Evaluierungen bei Worldline in verschiedenen Bereichen durchgeführt.

Regelmäßige Audits finden im Rahmen der Zertifizierungen ISO 27001, PCI DSS und PCI PA-DSS statt. Hier liegt der Fokus aber nicht auf der Worldline Atos Security Modul (ASM) Entwicklung und Produktion selbst, sondern auf den durch die jeweiligen Zertifizierungen

vorgegebenen Kernthemen. Allerdings sind auch die Entwicklungsumgebungen und -bedingungen bei Worldline Bestandteil der Audits, wozu auch die ASM-Entwicklung gehört.

Evaluierungen der ASM-Software (und damit auch deren Entwicklungsumgebung sowie der Produktionsumgebung) werden von Atos in unregelmäßigen Abständen gemäß den Anforderungen der Kunden durchgeführt.

5. Zeitsperre/Einschränkung der Nutzbarkeit?

Es ist nicht zutreffend, dass Anwender nur alle 15 Minuten eine Nachricht über das beA versenden können. Eine derartige Beschränkung sieht das beA nicht vor. Auch ist es unzutreffend, dass pro Anmeldevorgang und Rechtsanwalt nur eine Nachricht heruntergeladen werden darf.

Auf Nachrichten und Schriftstücke in den beA-Postfächern kann wegen der Abschaltung des beA-Systems im Moment nicht zugegriffen werden. Durch das Verschlüsselungsverfahren im beA-System ist es weder der BRAK noch Atos möglich, die Nachrichten einzusehen oder diese in irgendeiner Weise zu kopieren oder den betroffenen Rechtsanwälten in anderer Weise zur Verfügung zu stellen. Die im beA gesendeten Nachrichten sind stets vertraulich und verschlüsselt und nur für den Empfänger bestimmt.

Die Entwicklung einer Client Security für eine Terminalserver-Infrastruktur ist bei Atos beauftragt. Die zurzeit stattfindenden Modifikationen der Client Security zur Entfernung von Sicherheitsrisiken werden auch in die Terminal-Server-Version einfließen. Bislang konnte der BRAK noch kein verbindlicher Bereitstellungstermin genannt werden. Die BRAK geht davon aus, dass bis Mitte 2018 eine Bereitstellung erfolgen kann.

6. Subunternehmer/Zugriff Dritter

Atos als beauftragter Dienstleister zur Entwicklung des beA-Systems der BRAK ist berechtigt, Subunternehmer einzubinden. Insofern wurden von Atos die Worldline S.A. sowie die Governikus GmbH & Co.KG jeweils als Subunternehmer beauftragt.

Alleinige Vertragspartnerin und damit für die Sicherheit der BRAK gegenüber verantwortlich ist aber Atos.

7. Kommunikation der Schnittstellen an Softwarehersteller

Die gesamte Dokumentation zur KSW-Schnittstelle wurde den interessierten Herstellern im Vorfeld bereitgestellt. Darüber hinaus wurden diverse Informationsveranstaltungen von der BRAK durchgeführt, in denen Fragen von Herstellern zur Dokumentation geklärt worden sind. Zudem beantwortete die BRAK Fragen zur Implementierung der Schnittstelle durch einen erfahren Softwareentwickler. Die Dokumentation wird im Rahmen der Weiterentwicklung

entsprechend gepflegt und den KSW-Herstellern zur Verfügung gestellt. Die KSW-Schnittstelle ist ein integraler Bestandteil des beA-Systems.

8. BRAV/regionale Verzeichnisse

Die BRAK richtet gem. § 31a Abs. 1 Satz 1 BRAO für jedes im Gesamtverzeichnis (Bundesweites Amtliches Anwaltsverzeichnis (BRAV), § 31 BRAO, § 9 RAVPV)eingetragene Mitglied einer Rechtsanwaltskammer ein beA empfangsbereit ein. Nach § 21 Abs. 1 RAVPV unterrichten die Rechtsanwaltskammern die BRAK über die bevorstehende Eintragung einer Person in das Gesamtverzeichnis. Die BRAK richtet unverzüglich nach der Eintragung einer Person in das Gesamtverzeichnis für diese ein beA empfangsbereit ein.

Aufgrund dieser rechtlichen Rahmenbedingungen basieren das beA-System und das BRAV auf derselben Datenbank. Denn im BRAV ist jeder in Deutschland zugelassene Rechtsanwalt aufgeführt und für jeden in Deutschland zugelassenen Rechtsanwalt ist ein beA einzurichten. Nach der gesetzlichen Regelung werden die beA-Postfächer auf der Basis des BRAV errichtet. In rechtlicher Hinsicht sind das beA und das BRAV also direkt voneinander abhängig. Deshalb ist eine Verknüpfung der Daten realisiert worden.

Aus diesem Grund ging bislang automatisch das BRAV offline, sobald das beA-System ausgeschaltet wurde.

Zwischenzeitlich ist eine Logik aufgebaut worden, die der BRAK netzwerktechnisch ermöglicht, die Bestandteile des Systems einzeln zur Verfügung zu stellen. Damit können in Zukunft das beA und das BRAV unabhängig voneinander bereitgestellt werden, obwohl beide Systeme auf derselben Datenbank basieren. Deshalb ist das BRAV ebenso wie die Find-A-Lawyer-Suchfunktion seit dem 10.01.2018 wieder online.

9. Erweiterung des Zugangskreises zum beA

Das beA-System sieht keine Beschränkungen vor, wie viele Nachrichten der Nutzer pro Zeiteinheit verschicken darf. Es ist daher nicht zutreffend, dass Anwender nur alle 15 Minuten eine Nachricht über das beA-System versenden können. Ebenso kann der Nutzer natürlich pro Login alle im beA sich befindenden Nachrichten abrufen.

Die Nachrichtengröße beruht auf Vorgaben der Justiz. Nach der Bekanntmachung zu § 5 ERVV (Elektronischer-Rechtsverkehr-Bekanntmachung 2018, ERVB 2018) vom 19.12.2017 wird gemäß § 5 Abs. 1 Nr. 3 ERVV bis mindestens 31.12.2018 die Anzahl elektronischer Dokumente in einer Nachricht auf höchstens 100 Dateien und das Volumen elektronischer Dokumente in einer Nachricht auf höchstens 60 Megabyte begrenzt.

Im Übrigen kann das beA gem. § 19 Abs. 2 RAVPV auch der elektronischen Kommunikation mit anderen Personen oder Stellen dienen. Insofern erfüllte die BRAK durch die Erweiterung des Zugangs des beA für „jedermann“ die Vorgaben des § 19 Abs. 2 RAVPV.

10. weitere Fragen

Die BRAK wurde zu der Verfassungsbeschwerde den anwaltlichen elektronischen Rechtsverkehr betreffend (BVerfG, Beschl. v. 20.12.2017 – 1 BvR 2233/17) nicht zur Stellungnahme aufgefordert. Die Verfassungsbeschwerde ist vom BVerfG bereits als unzulässig verworfen worden. Grundsätzlich stellt das BVerfG nur Verfassungsbeschwerden zur Stellungnahme, wenn diese zulässig erhoben sind, um sich dann die inhaltlichen Positionen anzuhören.

Etwaige Schadensersatzansprüche wird die BRAK zu gegebener Zeit geltend machen. Sie geht derzeit davon aus, dass eine gütliche Einigung mit Atos erfolgen kann. Die Auswirkungen der Stilllegung von beA auf den Beitrag werden in der Hauptversammlung erörtert.

(Stand: 17.01.2018)