RAK | Rechtsanwaltskammer Berlin
Der Präsident

Rechtsanwaltskammer Berlin · Littenstraße 9 · 10179 Berlin

Bundesrechtsanwaltskammer
Littenstraße 9
10179 Berlin

- nachrichtlich an alle RAKn im Bundesgebiet -

Berlin, 08. Januar 2018/mtr

Vorbereitung der außerordentlichen Hauptversammlung am 09.01.2018

Sehr geehrte Damen und Herren,

ich verweise zuerst auf das anliegende Schreiben von GT Restructuring vom 05.01.2018 an die RAK Berlin. Ich bitte um Beantwortung der darin aufgeworfenen Fragestellungen.

Zusätzlich stellen sich derzeit (eine Ergänzung bleibt vorbehalten) folgende Fragen:

A) Frühere Sicherheitstests des beA-Systems

- Wurden Sicherheitstest und wenn ja, wann durchgeführt?
- Von wem wurden diese Tests in wessen Auftrag durchgeführt?
- Welchen konkreten Inhalt hatte der jeweilige Auftrag?
- Handelte es sich um black-box-tests oder white-box-tests?
- Wurde lediglich der www-server resp. sonstige Teilbereiche des beA-Systems (welche?) oder das Gesamtsystem getestet?
- Was wurde den Testern für die Durchführung des jeweiligen Tests zur Verfügung gestellt?
- Gab es Vorgaben für die Testdauer?
- Wem wurden die Ergebnisse des Tests von den Testern mitgeteilt?
- Sind der BRAK die Testergebnisse (vollständig?) bekannt?
- Welche Ergebnisse hatten die Tests?

RAK Berlin · Littenstraße 9 · 10179 Berlin · Tel. 030 306931-0 · Fax 030 306931-99 · info@rak-berlin.org · www.rak-berlin.de
Deutsche Kreditbank AG · BLZ 120 300 00 · Kto. 1 550 219 · BIC BYLADEM1001 · IBAN DE74 1203 0000 0001 5502 19

Ich bitte um Übergabe vollständiger Kopien sämtlicher Testergebnisse und –berichte.

Nach Medienberichten soll der BRAK vorgeschlagen worden sein, eine Überprüfung des beA-Systems durch den CCC durchführen zu lassen. Konkret sei vorgeschlagen worden, auf einem CCC-Camp 2015 das beA zur Verfügung zu stellen, damit der CCC eine Überprüfung durchführen kann. Die BRAK soll dies abgelehnt haben.

- Sind diese Medienberichte (wenn teilweise, in welchem Teil?) zutreffend?

Wenn ja:

- Wer war in der Geschäftsführung und / oder im Präsidium der BRAK über den Vorschlag informiert und wer hat diesen Vorschlag abgelehnt?
- Mit welcher Begründung wurde der Vorschlag abgelehnt?

B) HSM / Ende-zu-Ende-Verschlüsselung

Offenbar wird im/mittels des HSM eine verschlüsselt übersandte Nachricht so „aufbereitet", dass auch mit dem privaten Schlüssel der übrigen für den Zugang zum Empfängerpostfach berechtigten Nutzer (z.B. Kanzleimitarbeiter) diese Nachricht abgerufen und gelesen werden kann. Ebenso muss das wohl geschehen, wenn eine Nachricht zeitgleich an mehrere beA-Postfächer oder andere Postfachinhaber (Vertreter) gesandt wird.

- Wie erfolgt diese „Aufbereitung" für andere/weitere private Schlüssel im HSM?
- Wie wird bei der Aufhebung der asymmetrischen Verschlüsselung des Nachrichtenschlüssels sichergestellt, dass die damit symmetrisch verschlüsselte (und mit diesem einen Schlüssel als Klartext lesbare) Nachricht nicht zeitgleich mit entschlüsselt wird?
- Wie ist das HSM gegen (unberechtigte) Zugriffe von außen gesichert?
- Wer konkret hat (berechtigten) Zugriff auf das HSM und für welche konkreten Fälle?
- Wer überwacht wie die Einhaltung von etwaigen Zugriffsberechtigungen?
- Ist das HSM eine wartungsfreie Hardware, die niemals ausgetauscht oder auch nur aktualisiert werden muss?
- Liegen die/der Schlüssel eines Postfachinhabers auf dem HSM? Wenn ja: welche?
- Welche Schlüssel liegen auf der beA-Karte?
- Gibt es für unterschiedliche Funktionen (Anmeldung, Authentifizierung, Signierung) unterschiedliche Schlüssel oder wird derselbe Schlüssel für mehrere Funktionen genutzt? Wenn ja, welche Funktionen werden mit demselben Schlüssel durchgeführt?

- Ist gewährleistet, dass jede natürliche Person, die eine Zugangsberechtigung zu einem Postfach hat, über einen individuellen, also nur ihr zugeordneten Schlüssel verfügt?
- Liegen Fallvarianten vor, bei denen mehrere Personen über denselben Schlüssel verfügen? Wenn ja, welche Varianten sind das?
- Wie werden die privaten Schlüssel der Postfachinhaber erstellt? Wenn es sich auf dem HSM und der beA-Karte um denselben privaten Schlüssel handelt, wie gelangt dieser auf HSM und beA-Karte?

C) Geplante Prüfung des Systems

Es soll nunmehr ein externer Sachverständiger eine Prüfung des Systems durchführen.

Die RAK Berlin erwartet, dass sie im Vorfeld in die Auswahl sowie in die Formulierung des konkreten Auftrages an den Sachverständigen einbezogen wird und mitentscheiden kann. Dies muss eine Entscheidung der Hauptversammlung der BRAK sein.

Vorsorglich zu diesem Thema:

- Wurde, wenn ja an wen, bereits ein Auftrag erteilt?
- Welchen konkreten Inhalt hat der Auftrag?
- Wer erhält die Testergebnisse?
- Wird die BRAK die Testergebnisse vollständig und ohne Verschwiegenheitsverpflichtung gegenüber sonstigen Dritten gegenüber den Rechtsanwaltskammern offenlegen?
- Wird es über diese singuläre Prüfung hinaus dauerhafte Tests durch externe Dritte geben?
- Wird die BRAK von Kammern beauftragten Dritten die Möglichkeit geben, zeitlich und im Umfang unbeschränkte white-box-tests durchzuführen?

D) Kapazitätsprobleme des beA-Systems

Nach dem Update vom 27.11.2017 ("beA 2.0") waren Ausfälle, Verbindungs- und Übertragungsschwierigkeiten zu verzeichnen. Die Kammern wurden darüber erstmals einen Monat später mit Schreiben vom 27.12.2017 informiert.

Die Lösung dieser Probleme soll (vgl. das Schreiben) durch eine Modifikation der Software und der Hardware in den Rechenzentren erfolgt sein.

- Was ist unter dem Begriff „Modifikation" zu verstehen?
- Welche konkreten Arbeiten / Veränderungen wurden durchgeführt?
- Erfolgte eine Veränderung der Software und / oder der Hardware?
- Wenn ja, welche?

- Wurden die Änderungen auf Sicherheitsrelevanz geprüft, wenn ja, wie, durch wen, mit welchem Ergebnis? Wenn ja, bitte ich um Übergabe einer vollständigen Abschrift.

Das beA wurde ursprünglich mit zwei georedundanten Rechenzentren in Deutschland geplant, in denen sich jeweils eine Serverlinie befinden sollte. Mit der Dopplung der Rechenzentren sollte gewährleistet werden, dass selbst bei einem Komplettausfall eines Zentrums über das andere Zentrum das System funktionsfähig aufrechterhalten werden kann. Mithin gehe ich von einer geplant vorzuhaltenden System-Kapazität von 200 % aus.

Auf der 148. HV am 18.09.2015 (Protokoll HV 18.09.2015, S. 16) wurde erklärt, dass die BRAK mit Atos intensive Diskussionen zur Ausfallsicherheit und der Dimensionierung des Systems geführt habe. Im Ergebnis wurde die Hardware-Kapazität verdoppelt, indem beide Rechenzentren mit jeweils einer zusätzlichen Serverlinie ausgestattet wurden. Es müsste sich also nach meinem Verständnis um eine Kapazitätserweiterung auf 400 % handeln.

- Welche Ursachen hat der Ausfall des Systems nach dem Update auf beA 2.0, wenn doch eine Kapazität von 400 % vorgehalten wurde und bis dato lediglich ca. 65.000 Rechtsanwältinnen und Rechtsanwälte registriert waren?

Die Kammern wurden über die Auftragserteilung an die Atos IT-Solution & Services GmbH erst nach Abschluss eines „freihändigen Vergabeverfahrens" informiert. Wesentlicher Ausschlagpunkt für die Auftragsvergabe an Atos sei – so wurde mitgeteilt – ie Sicherheit des von Atos angebotenen Systems. Angesichts der Bedeutung der Sicherheitsanforderungen seien die angebotenen Systeme im Bereich Sicherheit „von besonders qualifizierten Sicherheitsexperten" überprüft worden (Protokoll HV 26.09.2014, S. 14).

- Wer wurde von wem mit der Prüfung der angebotenen Systeme beauftragt?
- Welchen konkreten Inhalt hatte der Auftrag?
- Welche Ergebnisse hatte die Prüfung?
- Liegen die Stellungnahmen / Prüfergebnisse der Sicherheitsexperten vor?

Wenn ja, bitte ich um Übergabe einer vollständigen Abschrift.

In dem Angebot von Atos war bereits das Hardware Security Module (HSM) enthalten.

- Erfolgte eine Prüfung der angebotenen HSM-Lösung durch die besonders qualifizierten Sicherheitsexperten?
- Wurden von Atos die HSM in der angebotenen und überprüften (?) Angebotsvariante tatsächlich erstellt?

- Erfolgte, und wenn ja, wann und durch wen, eine Überprüfung der Identität von Angebot und Werkerstellung?
- Wurden die bis zur Abnahme des HSM erfolgten Weiterentwicklungen von Technik und Standards berücksichtigt?
- Gab es eine Verpflichtung von Atos, etwaige Fortentwicklungen von Technik und Standards zu berücksichtigen?
- Wurden jegliche Veränderungen an HSM/Software auf Auswirkungen bzgl. der Sicherheit geprüft? Wenn ja, wie, durch wen, mit welchem Ergebnis? Wenn ja, bitte ich um Übergabe einer vollständigen Abschrift der Prüfergebnisse.

E) BRAV / regionale Verzeichnisse

Gemäß § 31 Abs. 1 Satz 1 BRAO ist jede Kammer verpflichtet, ein elektronisches Verzeichnis der in ihrem Bezirk zugelassenen RAe zu führen. Die BRAK hat ein entsprechendes Gesamtverzeichnis zu führen. Die RAK Berlin führt ihr Verzeichnis gemäß § 31 Abs. 1 Satz 2 als Teil des BRAK-Gesamtverzeichnisses.

Mit dem beA-update vom 27.11.2017 erfolgte (vermutlich) eine Verknüpfung des beA mit dem BRAV dergestalt, dass – wenn das beA offline ist – auch das BRAV offline geht. Über diese Folge wurde die RAK Berlin nicht informiert.

Das BRAV ist mit dem find a lawyer-System verknüpft, so dass derzeit auch über dieses europäische System die Zulassung eines RA nicht geprüft werden kann.

- Hat die erfolgte Verknüpfung zur Folge, dass auch umgekehrt bei einem offline des BRAV automatisch das beA-System offline geht?
- Gibt es andere technische Möglichkeiten, die ein offline des BRAV bei offline des beA (und eventuell umgekehrt) ausschließen?
- Welche Gründe sprachen für die derart erfolgte Verknüpfung von BRAV und beA?

Ich bitte um Übergabe einer Haftungsfreistellungserklärung der BRAK gegenüber der RAK Berlin bzgl. sämtlicher Haftungsrisiken der RAK Berlin aus dem offline des BRAV und damit des Teilverzeichnisses der RAK Berlin.

F) Erweiterung des Zugangskreises zum beA

Am 6. Juni 2017 gab es ein „kleines Update" der beA-Anwendung. Damit wurde, ohne vorherige Information der Kammern resp. deren Entscheidung, der Zugang zu den beA-Postfächern auf „jedermann" erweitert.

Anwaltspostfächer sind seitdem nicht nur für Rechtsanwälte (beA-Postfachinhaber) und den institutionellen Teilnehmerkreis des EGVP (Gerichte, Gerichtsvollzieher, einzelne Behörden) erreichbar. Seit Pfingsten 2017 kann

jedermann, der sich ein eigenes EGVP-Postfach zulegt, auch jedes beA-Postfach und jedes institutionelle EGVP-Postfach anschreiben. Für die Einrichtung eines eigenen EGVP-Postfachs ist keine Identitätsprüfung erforderlich. Jedermann kann sich eine frei verfügbare Software ("EGVP-Communicator") herunterladen und sich unter beliebigem (Pseudo-)Namen ein eigenes EGVP-Postfach einrichten.

- Treffen die Medienberichte zu, wonach zwischen Nachrichtenübersendungen durch einen beA-Postfachinhaber oder dessen Mitarbeiter eine Unterbrechung von mindestens 15 Minuten liegen muss?
- Ist die BRAK bereit, den Zugang durch „jedermann" zum beA wieder abzuschaffen?

G) Allgemein

- Liegen der BRAK heute Kenntnisse über weitere Fehler oder Sicherheitslücken des beA-Systems vor? Wenn ja: welche?
- Wurde die BRAK durch Dritte auf mögliche weitere Fehler oder Sicherheitslücken hingewiesen? Wenn ja, auf welche, wann und von wem?
- Wann wurde die BRAK über die jetzt bekannten Fehler und Sicherheitslücken von wem informiert? Wer innerhalb des Präsidiums und / oder der Geschäftsstelle wurde wann von wem informiert?
- Lt. Medieninformationen (der RAK Berlin liegt dazu bisher keine Information durch die BRAK vor), soll sich das BMJV an die BRAK nach dem 27.12.2017 mit Fragen und Forderungen bezgl. des beA gewandt haben. Ich bitte um Übergabe einer vollständigen Kopie dieses Schreibens.
- Stimmt die BRAK der Forderung der RAK Berlin zu, den Quellcode für die beA-Software zukünftig vollständig offenzulegen?
- Stimmt die BRAK der Forderung der RAK Berlin zu, für das beA ausschließlich open source-Software zu verwenden bzw. die selbst erstellte Software als open source-Software zu definieren?

Mit freundlichen kollegialen Grüßen

gez. Dr. jur. Mollnau
Präsident