rakko

Rechtsanwaltskammer für den
Oberlandesgerichtsbezirk Koblenz

Körperschaft des öffentlichen Rechts

rakko · Rheinstraße 24 · 56068 Koblenz

**An alle Mitglieder der
Rechtsanwaltskammer
für den Oberlandesgerichtsbezirk Koblenz**

Telefon: 0261 30335-0
Durchwahl: -
Telefax: 0261 30335-66 und -22

Datum: 10.01.2018/L

AZ.:

Störungen bei beA

Liebe Kolleginnen,
liebe Kollegen,

am gestrigen Tage fand in Berlin eine außerordentliche Hauptversammlung der Bundesrechtsanwaltskammer (BRAK) statt, deren einziges Thema die allgemein bekannten Probleme des besonderen elektronischen Anwaltspostfaches (beA), die zu dessen vollständiger Abschaltung führten, war. Hierzu hat die BRAK eine Presseerklärung abgegeben, die Sie auf deren Homepage finden können. Darüber hinaus hat die NJW in ihrem Onlineauftritt inzwischen einen Bericht veröffentlicht, der den Gang und die Ergebnisse der rund sechsstündigen Konferenz stark verkürzt und aus meiner Sicht teilweise irreführend wiedergibt. Ich möchte Ihnen daher die Ereignisse, wie sie sich aus meiner Sicht zugetragen haben, nachfolgend darstellen.

1. Die verantwortlichen Präsidiumsmitglieder der BRAK schilderten eingangs noch einmal die Historie des beA einschließlich der Ereignisse seit dem 20.12.2017, die letztlich zur Abschaltung des Systems führten. An diesem Tag hat bekanntlich ein Mitglied des Chaos Computerclubs (CCC) die BRAK über von ihm festgestellte Sicherheitsrisiken des Systems informiert. Die missglückten Versuche des Systementwicklers, der Firma Atos, diese Risiken zu beseitigen, zwangen die BRAK letztlich zur Abschaltung des Systems.

   Erwähnenswert ist aus meiner Sicht insbesondere der Umstand, dass das System vor seiner erstmaligen Freischaltung schon im Jahre 2015 durch eine von Atos beauftragte Drittfirma, die SEC Securities auf seine Sicherheit hin überprüft wurde. Ein der BRAK vorliegender Bericht dieser Firma hat die Sicherheit uneingeschränkt bestätigt. Die BRAK wurde zu dieser Zeit fachlich durch die IT Consultingfirma Capgemini Deutschland GmbH beraten, die diesen Bericht ihrerseits geprüft und inhaltlich nicht beanstandet hat. Eine Offenlegung dieses Berichtes scheitert im Moment noch daran, dass zwischen Atos und SEC insoweit Vertraulichkeit vereinbart wurde. Die im weiteren Verlauf der Veranstaltung zeitweise anwesenden Vertreter der Firma Atos sagten zu, sich bei SEC für eine Freigabe des Berichts einzusetzen.

Wie es dazu kam, dass zwei Fachfirmen die Sicherheit des Systems bestätigt haben, wird nach der Offenlegung des Berichts kritisch zu prüfen sein.

2. Die sodann hinzugebetenen Vertreter der Firma Atos wie auch eines Subunternehmers erläuterten im Rahmen einer knapp zweistündigen kritischen Befragung, dass die durch das Mitglied des CCC vorgenommenen Manipulationen die grundsätzliche Sicherheit des Systems, also die Verschlüsselung versandter Nachrichten und damit deren Vertraulichkeit nicht gefährdet hätten. Die Manipulationen hätten „nur" dazu geführt, dass das für die Nutzung des Systems erforderliche Zertifikat nach Offenlegung der Manipulationen durch die Zertifizierungsstelle gesperrt wurde, so dass der Zugang zum System nicht mehr möglich war. Ich habe den Vertretern beider Firmen das im Internet kursierende Video über den Vortrag des Mitgliedes des CCC auf dessen Jahreskongress im Dezember vorgehalten. In diesem Vortrag wird bekanntlich behauptet, dass die Verschlüsselung von Nachrichten im Bereich des sogenannten High Security Modules (HSM) angreifbar sei. Auch auf Nachfrage blieben die Vertreter der Firmen bei ihrer Einschätzung, dass die Verschlüsselung von Nachrichten auch in diesem Bereich sicher sei. Diese Auskunft kann ich mangels eigener Sachkunde nur unkommentiert weiterreichen. Auch sie wird im weiteren Verlauf der Ereignisse zu überprüfen sein.

   Dass es bei der Erstellung des neuen Zertifikates zu gravierenden Fehlern gekommen ist, räumten die Vertreter der Firmen uneingeschränkt ein und teilten mit, dass derzeit an einer weiteren Version des Zertifikates gearbeitet wird. Auf Nachfrage bekräftigten sie, dass das System als solches sicher und dauerhaft funktionsfähig sei, also keine grundlegende Überarbeitung erforderlich ist. Auch hierbei setzten sie sich mit den Äußerungen des CCC auseinander und erläuterten ihre gegenteilige Auffassung. Wiederum gilt, dass ich diese Ausführungen mangels eigener Sachkunde nur unkommentiert weitergeben kann.

3. Im Anschluss an die Befragung wurde die Versammlung in Abwesenheit der Firmenvertreter fortgesetzt. Die Präsidenten der Regionalkammern kritisierten die BRAK heftig dafür, dass sie nach Bekanntwerden der Sicherheitsrisiken, die durch die Installationen des neuen Zertifikats drohten, keine entsprechende Warnmeldung an die Regionalkammern versandt hat, was dazu führte, dass die Regionalkammern in guten Glauben die Installation des neuen Zertifikates noch unmittelbar vor den Weihnachtsfeiertagen empfahlen, obwohl die Gefahren bei der BRAK bereits bekannt waren. Die verantwortlichen Präsidiumsmitglieder der BRAK verwiesen auf Personalengpässe im Vorfeld der Weihnachtsfeiertage, was angesichts der Möglichkeiten, Informationen heute auch kurzfristig per E-Mail weiterzuleiten, nicht wirklich überzeugte. Ich muss allerdings einräumen, dass das „timing" des CCC, so sehr ich dessen Beitrag zur Aufdeckung von Schwachstellen schätze, für mich Fragen aufwirft. Die Überprüfung hätte ohne Weiteres schon Monate vorher stattfinden können. Ob die zeitliche Nähe des öffentlichkeitswirksamen Vorganges zum Jahreskongress des CCC eine Rolle gespielt hat, kann man nur vermuten.

   Sehr eingehend wurde dann das weitere Vorgehen erörtert. Die Firma Atos wird das von ihr zu erstellende neue Zertifikat wiederum durch einen Dritten – angedacht wird offenbar das Fraunhofer Institut – überprüfen lassen. Auch die BRAK wird eine solche Überprüfung vornehmen lassen und hat beim Bundesamt für Sicherheit in der Informationstechnik (BSI) um Benennung geeigneter Fachfirmen gebeten. Darüber hinaus soll das gesamte System in einem offenen Prozess umfassend geprüft werden. Zu dieser Prüfung wird man auch dritte Personen und Institutionen einladen, die in den letzten Wochen bei der Aufdeckung der Mängel wie auch der sich anschließenden fachlichen Diskussion aufgetreten sind. Ich möchte die in diesem Zusammenhang kursierenden Namen – sie liegen auf der Hand – nicht veröffentlichen, bevor die BRAK formale Anfragen gestellt hat. Anregungen für die Beteiligung weiterer Personen und Institutionen sind willkommen und können der BRAK übermittelt werden, sobald diese ihre eigenen Vorschläge

bekanntgegeben hat. Im Anschluss an diesen Prozess und abhängig von seinem Ausgang wird sodann noch einmal eine weitere förmliche Sicherheitsprüfung stattfinden. Erst nach einem zufriedenstellenden Ergebnis dieser Prozesse und seiner Offenlegung wird das System dann mit ausreichender zeitlicher Vorankündigung wieder in Gang gesetzt. Zeitliche Prognosen sind angesichts der absehbaren Komplexität dieser Prozesse kaum möglich und wurden von allen Verantwortlichen auch vermieden. Mein Eindruck ist, dass hierfür mehrere Monate benötigt werden.

4. Vor dem Hintergrund der geschilderten Situation leistet die BRAK derzeit keine Zahlungen an Atos. Dies betrifft namentlich die ganz erheblichen Kosten für die Vorhaltung der Infrastruktur für den Betrieb des Systems. Die rechtlichen Möglichkeiten der BRAK gegenüber Atos und möglicherweise auch gegenüber Dritten werden derzeit durch einen auf IT-Recht spezialisierten Anwalt von „avocado rechtsanwälte" geprüft.

   Weitere Schritte werden im Rahmen einer schon vor längerer Zeit routinemäßig für den 18.01.2018 anberaumten Konferenz der Präsidenten der Regionalkammern erörtert. Abschließend darf ich festhalten, dass personelle Konsequenzen – insofern in dem Bericht der NJW zutreffend geschildert – nicht erörtert wurden. Angesichts der Tatsache, dass die Sachverhaltsaufklärung weiter andauert, fehlte es hierfür derzeit an einer seriösen Grundlage. Dass in der gegebenen Situation niemand gesteigertes Interesse daran hat, in die Verantwortung einzutreten, liegt im Übrigen auf der Hand.

   Über den weiteren Gang der Dinge werde ich Sie zu gegebener Zeit unterrichten. Dass meine Berichte nicht in derselben Geschwindigkeit veröffentlicht werden, wie dies durch einschlägige Publikationsorgane erfolgt, wollen Sie mir im Hinblick auf meine ehrenamtliche Tätigkeit nachsehen. Ich habe allerdings den Eindruck, dass ein gewisser zeitlicher Abstand auch für die Qualität der Berichterstattung hilfreich ist.

Mit freundlichen kollegialen Grüßen

JR Gerhard Leverkinck
Präsident