BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

Bundesministerium der Justiz und für
Verbraucherschutz
Herrn Ministerialdirigent
Dr. Matthias Korte
Mohrenstraße 37
10117 Berlin

Berlin, 17.01.2018

besonderes elektronisches Anwaltspostfach – Nichtverfügbarkeit seit dem 22.12.2017

Sehr geehrter Herr Dr. Korte,

in vorbezeichneter Angelegenheit danke ich für Ihr Schreiben vom 29.12.2017. Die darin gestellten Fragen beantworte ich gerne wie folgt:

1. Welche Sicherheitsprobleme haben die Bundesrechtsanwaltskammer (BRAK) dazu bewogen, das beA-System nicht mehr weiter zu betreiben?

Nicht Sicherheitsprobleme haben die BRAK dazu bewogen, das beA-System ab dem 22.12.2017 zunächst nicht mehr weiter zu betreiben, sondern ein Dritter hatte den privaten Schlüssel eines von der TeleSec erstellten und auf allen Clients installierten Schlüsselpaares gefunden und dies der TeleSec gemeldet. Aufgrund der Kompromittierung des Zertifikats sperrte die TeleSec dieses umgehend. Damit war die lokale Kommunikation zwischen der beA-Browseranwendung und der beA-Komponente „Client Security“ nicht mehr möglich. Zu keiner Zeit bestand ein Sicherheitsproblem wegen der Veröffentlichung dieses Zertifikats, denn die Verschlüsselung der von der Anwaltschaft zu sendenden bzw. die Entschlüsselung der an sie gesandten Nachrichten erfolgt mit einem gänzlich anderen Schlüsselmaterial, nämlich den auf den beA-Karten enthaltenen Zertifikaten.

In dem Bemühen, die drohende Nichtverfügbarkeit des beA-Systems so schnell wie möglich zu überwinden und das beA-System so schnell wie möglich wieder funktionsfähig zu machen, stellte der technische Dienstleister der BRAK am 22.12.2017 gegen 1:00 Uhr nachts ein neues Zertifikat bereit, das die BRAK der Anwaltschaft gegen 11:30 Uhr am 22.12.2017 zum Download zur Verfügung stellte. Der technische Dienstleister der BRAK übersah dabei jedoch aufgrund mangelhafter Kontrolle, dass dieses neue Zertifikat ein Gefährdungspotential für jeden Computer enthielt,

auf dem es installiert wurde, denn der Einsatzzweck des Schlüsselmaterials wurde nicht ausreichend eingeschränkt. Darüber informierte der technische Dienstleister die BRAK unmittelbar, nachdem ihm dieser Fehler bekannt geworden war. Die BRAK sorgte daraufhin unverzüglich dafür, dass dieses fehlerhafte Zertifikat nicht mehr heruntergeladen werden konnte und entschied am Abend des 22.12.2017 nach Rücksprache mit dem Dienstleister, beA zunächst komplett vom Netz zu nehmen. Dies diente dem Zweck, einerseits die Weiterverbreitung des zwischenzeitlich zur Verfügung gestellten Zertifikats zuverlässig zu verhindern und andererseits mit der gebotenen Gründlichkeit eine tragfähige Lösung für die technischen Probleme der Anbindung der Browseranwendung zu prüfen.

2. Welche Sicherheitsrisiken haben für die elektronische Kommunikation der Rechtsanwälte bestanden? Über welchen Zeitraum haben diese Sicherheitsrisiken bestanden?

Das kompromittierte Zertifikat dient der Verbindung zwischen dem Browser und der lokalen Software-Komponente „Client Security“. Für Anwender, die beA nicht über eine Integration in einer Kanzleisoftware verwenden, entwickelte die Dienstleisterin der BRAK eine über einen Browser bedienbare Anwendung. Der Browser kommuniziert dabei sowohl mit dem im Internet stehenden beA-Server, aber auch mit der lokal installierten beA-Komponente „Client Security“. Die Kommunikation der Browser-Anwendung mit dem beA-Server erfolgt aus Sicherheitsgründen über eine SSL-Verbindung. Da die aktuellen Browser unterschiedliche Kommunikationsarten innerhalb des Browsers gleichzeitig (sog. Mixed Content) nicht zulassen, muss die Kommunikation zur lokalen Komponente „Client Security“ ebenfalls mittels SSL erfolgen. Allein dieser Umstand ist Grund für die SSL-Verwendung bei der Client Security, ein dahinter stehendes bzw. benötigtes Schutzziel gibt es nicht. Nach Informationen der BRAK waren und sind die beA-Plattform selbst, die sog. Ende-zu-Ende-Verschlüsselung der Nachrichten, die Sicherheit der Nachrichtenübermittlung und Speicherung im beA-System von dem festgestellten Problem nicht betroffen. Die Vertraulichkeit der Datenübertragungen der über die beA-Plattform gesendeten und empfangenen Dokumente war zu jedem Zeitpunkt gesichert. Kein Dokument, das über das beA versendet wurde, war öffentlich, die Kommunikation war stets vertraulich und verschlüsselt.

Die Risiken, die aus dem am 22.12.2017 zur Verfügung gestellten „neuen“ Zertifikat nach Installation für die Sicherheit des PC-Nutzers resultieren, stellen sich wie folgt dar:

Das neue, private Zertifikat war als sog. Stammzertifikat ausgestaltet. Das bedeutet, dass es nicht nur die Authentizität zum lokalen beA-Server verbürgt, sondern dass mit Hilfe dieses Zertifikats auch beliebige weitere Zertifikate für weitere Seiten erstellt werden können.

Mit Hilfe des genannten Zertifikats kann ein Angreifer deshalb eigene Webseiten als vertrauenswürdig präsentieren. Der Angreifer kann anschließend einen weiteren IT-Sicherheitsangriff (sog. DNS-Spoofing oder Cache Positioning) durchführen. Dies würde den Angreifer in die Lage versetzen, Anwenderinnen und Anwender auf eigene Webseiten umzuleiten und im äußersten Fall den Rechner mit Schadsoftware zu infizieren. Der über die Webseite des Angreifers getätigte Datenverkehr wäre in diesem Fall für den Angreifer einsehbar.

Das Zertifikat konnte am 22.12.2017 von ca. 11:30 Uhr bis ca. 13:30 Uhr über den von der BRAK zur Verfügung gestellten Link heruntergeladen werden. Danach stellte die BRAK den Link offline.

Im Übrigen ist die beA-Plattform seit 28.11.2016 online. Schon vor Inbetriebnahme des Systems haben Experten 2015 bis Anfang 2016 die Funktionsfähigkeit und Sicherheit des Systems umfassend geprüft. Durchgeführte Tests waren u. a. Atos Pentests, SecConsult Pentests, Qualys SSL

Labs Tests sowie diverse Herstellertests. Die Prüfungen zielten darauf, Schwachstellen in der HW/SW-Architektur, des Authentifizierungskonzepts, der Signaturmechanismen und der Ende-zu-Ende-Verschlüsselung auszumachen. Dabei waren auch IT-Sicherheitsunternehmen beteiligt, die nicht an der Entwicklung der beA-Plattform beteiligt waren. Ergebnis der Tests war, dass die beA-Plattform problemlos online gehen kann.

3. Wie werden die Sicherheitsprobleme gelöst und findet auch eine rückwirkende Überprüfung der Systeme statt?

Die technische Dienstleisterin der BRAK arbeitet derzeit an einer neuen Version der Verbindung zwischen Browser und Client Security. Diese Lösung befindet sich derzeit im Test. Atos hat bereits eine gutachterliche Überprüfung veranlasst.

Darüber hinaus hat die BRAK beschlossen, einen durch das BSI empfohlenen Experten zu beauftragen, die von Atos zur Verfügung gestellte Lösung gutachterlich zu überprüfen und darüber hinaus Sicherheitstests des gesamten beA-Systems zu veranlassen.

Ferner plant die BRAK verschiedene kritische IT-Experten in den Prozess zur Klärung sicherheitsrelevanter Fragestellungen einzubinden. Dazu soll ein sog. beAthon am 26.01.2018 stattfinden. Dabei sollen die Experten den Lösungsweg des Dienstleisters zusammen mit den Gutachtern und den technischen Dienstleistern erörtern.

Auf der Grundlage der erstatteten Gutachten sowie der Ergebnisse des beAthon wird die BRAK dann die Entscheidung über das weitere Vorgehen treffen.

4. Wann kann das beA-System voraussichtlich wieder in Betrieb genommen werden?

Einen Termin der Wiederinbetriebnahme des beA-Systems kann ich zum jetzigen Zeitpunkt noch nicht nennen. Es werden – wie bereits dargelegt – verschiedene technische Varianten für eine sichere Lösung auf ihre Machbarkeit geprüft. Die BRAK hat deutlich gemacht, dass sie keine halben Lösungen akzeptieren wird, sondern auch künftig sowohl die Sicherheit der beA-Webanwendung, als auch die Sicherheit der individuellen PC-Umgebung der Anwälte gewährleisten will. Die beA-Plattform wird erst dann wieder ans Netz gehen, wenn alle Fragen zu den Sicherheitsproblematiken zweifelsfrei geklärt sind.

Derzeit geht die BRAK davon aus, dass das beA auch im Januar nicht erreichbar und nicht adressierbar sein wird, auch nicht für Gerichte oder andere nichtanwaltliche Teilnehmer am elektronischen Rechtsverkehr.

Dies insbesondere auch unter dem Aspekt, dass die BRAK für die Wiederinbetriebnahme des beA derzeit einen zweiphasigen Prozess beabsichtigt: Zuerst soll die neue Client Security zum Herunterladen bereitgestellt werden und erst nach einer angemessenen Frist soll das beA wieder aktiv geschaltet werden.

5. Warum wurde zur Behebung der Sicherheitsprobleme zunächst ein neues Sicherheitszertifikat angeboten, das sich kurz darauf ebenfalls als unsicher erwiesen hat? Für eine Erläuterung, auf der Grundlage welcher Informationen diese Entscheidung getroffen wurde, wäre ich dankbar.

In der Nacht vom 21. auf den 22.12.2017 stellte die technische Dienstleisterin der BRAK kurzfristig ein neues Zertifikat zur Verfügung, um den drohenden Ausfall des produktiven Systems zu verhindern. Dieser Ausfall drohte deshalb, weil die Zertifizierungsstelle des ursprünglichen Zertifikats mitgeteilt hatte, das kompromittierte Zertifikat am 22.12.2017, 5:00 Uhr, zu sperren. Stattdessen wurde das von der TeleSec herausgegebene Zertifikat durch ein selbst erstelltes und selbst signiertes Zertifikat ausgestellt. Dieses Zertifikat hat allerdings zu o. g. Problematik geführt, da der Einsatzzweck des Schlüsselmaterials nicht ausreichend eingeschränkt wurde.

Die Dienstleisterin der BRAK informierte die BRAK am Abend des 21.12.2017, dass sie beabsichtige, das kompromittierte Zertifikat durch ein eigenes zu ersetzen und dass dies keinerlei Sicherheitsprobleme mit sich bringe. Dass übersehen worden war, den Einsatzzweck des Schlüsselmaterials einzuschränken, war den Gesprächspartnern der BRAK selbst nicht bekannt, so dass sie auch die Vertreter der BRAK nicht entsprechend aufklärten.

6. Wie ist das Krisenmanagement bei technischen Störungen des beA-Systems organisiert? Bitte beschreiben sie insbesondere die Zusammenarbeit mit dem technischen Dienstleister.

Das Krisenmanagement bei technischen Störungen ergibt sich aus internen Regelungen der Informationsweitergabe bzw. Kommunikation und der Dienstleistersteuerung entsprechend dem Vertrag und mit dem Dienstleister abgestimmten ITIL-Prozessen:

Kommunikationsmatrix

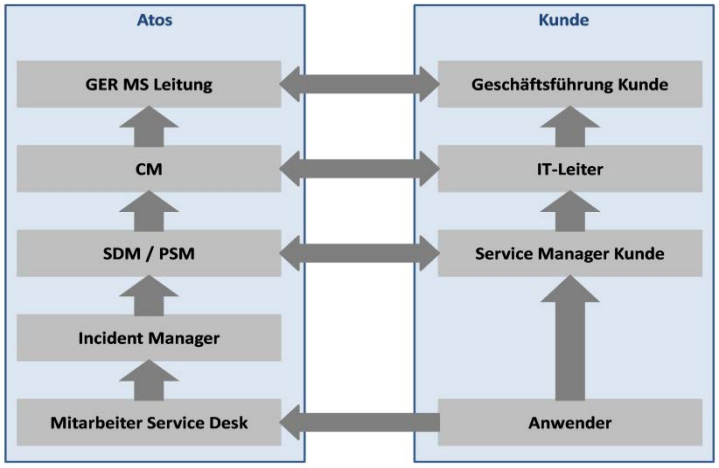
Intern existiert eine Kommunikationsmatrix, welche bei betriebswichtigen Situationen innerhalb der BRAK über die Bereiche:

- Präsidium
- Management
- Öffentlichkeitsarbeit
- Content-Management Portale
- regionale Kammern
- Kanzlei-Software- und Schulungs-Anbieter
- Verbundteilnehmer (EGVP-Projektbüro, BNotK)
- Dienstleister

die Weitergabe/Verteilung relevanter Informationen regelt. Zudem ist hier der Alarmierungsablauf für kritische Situationen geregelt.

Eskalationsebenen

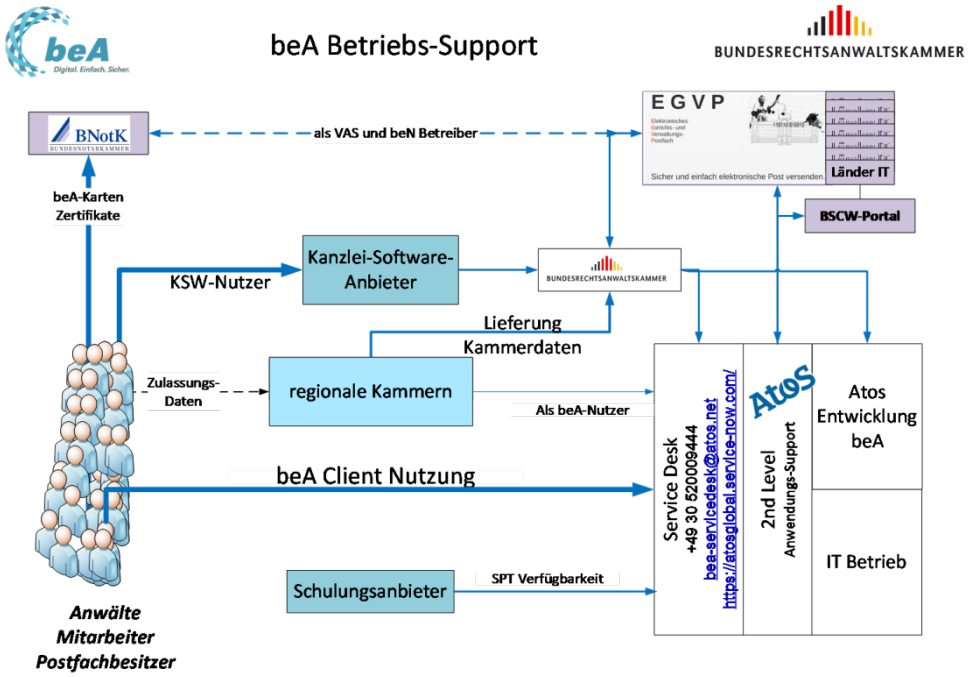
Die Eskalationsebenen des Dienstleister, der Firma Atos, spiegeln sich auch bei der BRAK wider. Dort sind, entsprechend der Aufgabenverteilung, die Geschäftsführung und die IT-Leitung zusammengefasst.



Schnittstelle zum Dienstleister

Neben dem Service Desk für die Nutzer von beA steht bei der Firma Atos ein b2b-Service Desk 7/24 zur Verfügung. Priorität 1-Incidents werden über ein Major Incident Verfahren innerhalb der Firma Atos behandelt, um in kritischen Situationen kurzfristig alle notwendigen Ressourcen erreichen zu können bzw. Entscheidungen zu treffen. Die BRAK wird über die eingeleiteten Maßnahmen informiert, um die Service-Wiederherstellung zu erreichen.

Übergreifendes Supportkonzept



Prozessmodell

Das Modell basiert auf dem ITIL-Framework V3, welches entsprechend der vertraglichen Regelung konkretisiert wurde.

Regelungen bestehen für folgende Prozesse

- Service Design
    - Availability Management
    - Capacity Management
    - IT Service Continuity Management
    - Service Level Management
    - Information Security Management
- Service Transition
    - Change Management
    - Knowledge Management
- Service Operations
    - Incident Management
    - Problem Management
    - Request Fulfillment
    - Event Management

Dokumentation der Prozesse der Zusammenarbeit zwischen der Bundesrechtsanwalts-kammer und dem Dienstleister

Die Prozesse der Zusammenarbeit sind primär dokumentiert im Prozess-Handbuch und im Service Organisations-Handbuch.

Kurzdarstellung Service Oranisations-Handbuch

Das Service Organisations-Handbuch (SOHB) stellt eine Ergänzung des Vertrages zum Betrieb des besonderen elektronischen Anwaltspostpachs (beA) mit der BRAK dar und umfasst alle Servicebelange für die Vertragserfüllung betriebsübergreifend über alle zur Leistungserbringung für diesen Vertrag erforderlichen Service Lines und Delivery-Einheiten der Atos IT GmbH (nachfolgend „Atos“ genannt) hinweg. Alle Dienstleistungen werden dabei entsprechend den Atos-Prozessen (gemäß Prozess-Handbuch) erbracht, die an die besonderen Erfordernisse der BRAK angepasst sind.

Der Service Delivery Manager (SDM) erstellt das SOHB in Abstimmung mit dem Kunden und hält es bei Änderungen aktuell.

Der Inhalt des SOHB bzw. des mitgeltenden Prozess-Handbuchs (PHB) spezifiziert Organisationen und Prozesse zur Betriebsführung der IT-Infrastruktur für den beA-Betrieb mit dem Fokus auf die Zusammenarbeit der Vertragspartner.

Wesentliche Bestandteile der Betriebsführung sind:

- Überwachung der notwendigen IT-Infrastruktur
- Entstörung und Problemlösung an der IT-Infrastruktur
- Änderung und Erweiterung der IT-Infrastruktur gemäß dem Änderungs-prozess aufgrund von Anforderungen der BRAK oder aus dem Atos IT-Betrieb
- Verfügbarkeits-, Kapazitäts- und Performanceüberwachung und -anpassung der IT-Infrastruktur entsprechend dem Bedarf
- Reporting über die erreichte Service Qualität gemäß der SLA’s und Durchsprachen mit den Verantwortlichen der BRAK

- Verhalten bei Ausnahmesituationen, wie z. B. Major Incident, durch ein abgestimmtes Eskalationsverfahren

Das SOHB beschreibt die Vorgänge an den Kontaktstellen der Prozessaktivitäten, bei denen die BRAK und Atos in eine gemeinsame Interaktion treten. Die technische Durchführung des „Betriebs“ ist in den entsprechenden Betriebshandbüchern zur Infrastruktur dokumentiert.

Kurzdarstellung Prozess-Handbuch

Das Prozess-Handbuch (PHB) beinhaltet die Beschreibung der betriebsspezifischen Prozesse bei der Leistungserbringung für die BRAK. Das PHB ist Teil der Gesamtdokumentation der IT-Dienstleistungen und Prozesse, die Atos für die Endkunden erbringt. Es dient zur internen Information und der Festlegung interner Abläufe in Abstimmung mit der BRAK.

Ziel dieses PHB ist die Darstellung der operativen Prozesse mit ihren Schnittstellen und Verantwortlichkeiten im Rahmen der Zusammenarbeit zwischen BRAK und Atos.

Ich hoffe, Ihre Fragen mit diesen Informationen beantwortet zu haben. Bei Rückfragen setzen Sie sich bitte gerne mit mir in Verbindung.

Mit freundlichen Grüßen

Ekkehart Schäfer
Rechtsanwalt