BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

An die
Präsidentinnen und Präsidenten
aller Rechtsanwaltskammern

BRAK-Nr. 259/2018

Berlin, 20.06.2018

besonderes elektronisches Anwaltspostfach (beA)
Hier: Abschlussgutachten der secunet Security Networks AG

Anlage: Gutachten secunet AG

Sehr geehrte Präsidentinnen und Präsidenten,
liebe Kolleginnen und Kollegen,

wir sind auf der Zielgeraden unseres Entscheidungsprozesses angekommen, ob wir unser beA-System wieder in Betrieb nehmen.

Ich lade Sie daher herzlich zu einer außerordentlichen Präsidentenkonferenz am

27. Juni 2018
11:00 Uhr bis 16:00 Uhr
in die Geschäftsstelle der Bundesrechtsanwaltskammer, Littenstraße 9, 10179 Berlin,

ein. Einziger Tagesordnungspunkt wird die Diskussion und Beschlussfassung über die Wiederinbetriebnahme des beA sein.

Als Grundlage für diese Entscheidung soll uns, wie in der Präsidentenkonferenz beschlossen, das beigefügte technische Gutachten der secunet AG dienen, das wir am Abend des 18.06.2018 erhalten haben. Das Präsidium hat sich in seiner gestrigen Sitzung eingehend mit dem Gutachten, insbesondere mit den darin beschriebenen Risiken befasst und dazu auch Rückfragen an Atos gerichtet, die zur Bewertung von Aussagen des Gutachtens erforderlich waren.

Das Präsidium empfiehlt auf der Grundlage dieses Gutachtens die – gestufte – Wiederinbetriebnahme des beA-Systems. Diese Empfehlung möchte ich Ihnen im Folgenden erläutern und begründen.

I.

Ich zitiere aus dem Gutachten (S. 13 des Gutachtens):

> *„Grundsätzlich ist das beA ein geeignetes System zur vertraulichen Kommunikation im elektronischen Rechtsverkehr. Das Verschlüsselungskonzept bietet technisch gesehen einen hinreichenden Schutz für die Vertraulichkeit der vom beA übermittelten Nachrichten. Nicht tragbare Risiken, die noch bestehen, können beseitigt werden und sind teilweise auch schon beseitigt worden. Die erneute Inbetriebnahme ist bei Beachtung der folgenden Empfehlungen aus sicherheitstechnischer Sicht möglich.*
>
> *Für die noch nicht behobenen betriebsverhindernden Schwachstellen wird empfohlen, die beA-Anwendung erst nach deren vollständiger Beseitigung wieder in Betrieb zu nehmen.*
>
> *Darüber hinaus empfehlen wir ebenfalls, die als „betriebsbehindernd" eingestuften Schwachstellen baldmöglichst zu beheben."*

Weiter heißt es in dem Gutachten (S. 10 des Gutachtens):

> *„Im Rahmen der Quelltext-Analyse (teilweise unterstützt durch die Penetrationstests) wurden auch die vom Chaos Computer Club e. V. (CCC) bemängelten Schwachstellen überprüft, die in der zum Stichtag vorliegenden Fassung von beA-Client-Security und beA-Anwendung fast alle nicht mehr vorhanden sind. Die Unterstützung von aktuellen Betriebssystemen konnte noch nicht bestätigt werden."*

Diesen Bewertungen und Empfehlungen folgend, schlägt das Präsidium Ihnen die folgenden Schritte zur Wiederinbetriebnahme des beA-Systems vor:

1. Bereitstellung der Client Security zum Download und zur Installation ab dem 04.07.2018

In dieser ersten Phase können die Rechtsanwältinnen und Rechtsanwälte die neue Client Security installieren und sich – falls noch nicht geschehen – erstregistrieren.[1] Ein Zugriff auf die Postfächer ist in dieser ersten Phase noch nicht möglich, sie bleiben gesperrt.

2. Freigabe der Postfächer ab dem 03.09.2018

Ab dem 03.09.2018 wird das Senden und Empfangen von Nachrichten wieder möglich sein. Damit wird die passive Nutzungspflicht der Postfächer für die Rechtsanwältinnen und Rechtsanwälte wieder aufleben.

Begleitet wird der Restart unseres beA-Systems durch umfangreiche Maßnahmen zur Information der Rechtsanwältinnen und Rechtsanwälte (Anleitungen auf der Homepage, Newsletter, Pressebegleitung). Alle Materialien werden Sie so schnell wie möglich erhalten.

[1] Da die in der Vergangenheit eröffneten Postfächer bestehen bleiben, ist eine nochmalige Registrierung der Rechtsanwältinnen und Rechtsanwälte, deren Postfächer bereits freigeschaltet sind, nicht erforderlich.

II. Risikobewertung

Das Präsidium hat, wie von secunet empfohlen, eine eigene Risikobewertung vorgenommen. Ich zitiere (S. 9 des Gutachtens):

> *„Die Risikobewertung wurde aus technischer Sicht vorgenommen. Dabei gingen die Menge der potentiellen Angreifer, die Komplexität des Angriffs und die Schäden durch einen erfolgreichen Angriff in die Risikobewertung ein. Die mögliche Motivation der Angreifer (ihre Bereitschaft, die erforderlichen Mittel für einen Angriff aufzubringen und die erforderlichen Risiken einzugehen) wurde mangels Schätzbarkeit nur sehr grob berücksichtigt. Sie ist allerdings ein Faktor, der die Eintrittswahrscheinlichkeit eines erfolgreichen Angriffs beeinflusst und bei genauerer Berücksichtigung die Risikobewertung verändern kann. Eine fachliche Sicht (z. B. Bewertung der Bedeutung eines Verlustes von Vertraulichkeit aus juristischer Sicht) von beA-Betreiber und -Anwenderseite kann mögliche Schäden oder ihre Eintrittswahrscheinlichkeit und damit das Risiko ebenfalls anders bewerten."*

Ich zitiere weiter aus dem Gutachten (S. 14):

> *„Das Ausnutzen einzelner identifizierter Schwachstellen kann eventuell durch geeignete technische und organisatorische Maßnahmen – seitens des Auftraggebers oder des Betreibers – deutlich erschwert oder sogar vereitelt werden."*

Bei seiner Risikobewertung hat das Präsidium die Kategorisierung der Schwachstellen aus dem Gutachten (vgl. Abschnitt 2.3.3, S. 21) übernommen.

1. Keine Wiederinbetriebnahme mit Risiken der Kategorie A

Die Empfehlung des Präsidiums steht unter dem Vorbehalt, dass bis zu den genannten Stichtagen die Bestätigung von secunet vorliegt, dass die im Gutachten als noch nicht behoben beschriebenen Risiken der Kategorie A beseitigt sind. Dies bedeutet, dass bis zum 03.07.2018 die auf die Client Security bezogenen Schwachstellen der Kategorie A, die Auswirkungen auf die Sicherheit und Integrität des Computersystems der Rechtsanwältin oder des Rechtsanwalts haben können, als behoben gemeldet werden müssen. Bis zum 02.09.2018 müssen die übrigen Risiken der Kategorie A als behoben von secunet bestätigt sein. Atos hat die fristgerechte Erledigung zugesagt, secunet auch.

2. Wiederinbetriebnahme trotz einzelner noch bestehender Risiken der Kategorie B

Secunet empfiehlt, Risiken der Kategorie B so bald wie möglich zu beheben, macht aber die Wiederinbetriebnahme nicht von der Beseitigung abhängig (vgl. Kapitel 2.3.3, S. 21). Bezogen auf die Client Security weist das Gutachten noch zwei Schwachstellen der Kategorie B auf, bezogen auf die Anwendung (inkl. der Kammerschnittstelle) sind es – einschließlich der Betrachtung der Hardware Security Module (HSM) – 14. Von diesen Schwachstellen sind vier bereits behoben, aber von secunet noch nicht als behoben bestätigt. Weitere drei dieser Risiken werden bis zum 02.09.2018 behoben und nachgetestet sein. Sieben der aufgezeigten Schwachstellen befinden sich derzeit in Prüfung bei Atos und werden bis zum 02.09.2018 beseitigt und von secunet nachgetestet sein. Aus den im Weiteren noch darzustellenden Gründen hält das Präsidium die Wiederinbetriebnahme trotz dann teilweise noch bestehender weniger Risiken der Kategorie B für vertretbar.

3. Wiederinbetriebnahme trotz noch bestehender Risiken der Kategorie C

Risiken der Kategorie C lassen lediglich unerhebliche Auswirkungen auf den Betrieb erwarten. Secunet (vgl. Kapitel 2.3.3, S. 21) empfiehlt ihre Behebung, sobald dies mit verhältnismäßigem Aufwand möglich ist. Wir werden diese Punkte mit Atos im Rahmen der Wartung und Pflege unseres Systems erörtern und bei Bedarf beseitigen lassen.

III. Betrachtung der Client Security

Wie bereits dargestellt, sind alle vom Chaos Computer Club (CCC) gemeldeten Fehler beseitigt. Allerdings empfiehlt das Gutachten mit Blick auf zwei vom CCC gemeldete Schwachstellen Weiterentwicklungen (vgl. Kapitel 4.7.2 und 4.7.4, S. 71). Die vorgeschlagenen Weiterentwicklungen werden in Absprache mit Atos bei Bedarf im Rahmen der Wartung und Pflege umgesetzt werden.

1. Risiken der Kategorie A

Das Gutachten benennt vier noch bestehende Schwachstellen der Kategorie A. Sie finden die Beschreibungen dieser Schwachstellen in folgenden Kapiteln des Gutachtens:

- Kapitel 3.5.3, S. 35 - Modifikation von signierten Nachrichten
- Kapitel 3.5.4, S. 36 - Veraltete Softwareelemente
- Kapitel 5.4.1, S. 80 - Verwendung von Javascript beim beA-Client
- Kapitel 5.4.2, S. 81 - Client prüft Postfachzertifikate nicht

Die in den Kapiteln 3.5.3 und 5.4.2 beschriebenen funktionalen, nicht technischen Risiken können erst mit der Wiedereröffnung der Postfächer eintreten, weil sie den Nachrichtenversand betreffen. Die Modifikation bereits signierter Nachrichten (Kapitel 3.5.3) auf dem Versandweg betrifft die Verlässlichkeit der Signatur aus der Sicht des Empfängers. Das Manko, dass die Client Security das Zertifikat des empfangenden Postfachs vor Versand nicht prüft (Kapitel 5.3.2), betrifft die Verlässlichkeit des elektronischen Rechtsverkehrs insgesamt, stellt aber kein Risiko für die Sicherheit und Integrität des Computersystems dar, auf dem die Client Security installiert ist. Diese beiden Risiken müssen – und werden – daher erst am 03.09.2018 beseitigt sein; sie spielen für die Installation der Client Security und die Erstregistrierung keine Rolle.

Atos hat sämtliche notwendigen Updates der in Kapitel 3.5.4 genannten Softwareelemente vorgenommen. Es wurden alle potentiell angreifbaren Bibliotheken aktualisiert. Die Bestätigung durch secunet wird kurzfristig, noch vor dem 04.07.2018 erfolgen. Ein Monitoring als Frühwarnsystem für neu entdeckte Sicherheitslücken ist bei Atos aufgesetzt. Das Monitoring der Client Security am 18.06.2018, 03:56 Uhr, meldete keine Sicherheitslücken in den verwendeten Bibliotheken.

Zur Lösung des in Kapitel 5.4.1 dargestellten Risikos schlägt das Gutachten vor, das ausgelieferte Javascript regelmäßig in kurzen Abständen von einem separaten System, z. B. durch Checksummen, auf Unversehrtheit zu prüfen. Atos hat diesen Vorschlag aufgegriffen und die Checksummenbildung und -prüfung umgesetzt; das neue Verfahren befindet sich derzeit im Test. Bei einer ungewollten Änderung des Javascripts wird eine Nachricht generiert. Die Prüfung des aufgesetzten Prozesses durch secunet wird kurzfristig noch vor dem 04.07.2018 erfolgen.

2. Risiken der Kategorie B

Das Gutachten benennt zwei noch bestehende Risiken der Kategorie B. Sie finden die Beschreibungen dieser Risiken in folgenden Kapiteln des Gutachtens:

- Kapitel 3.6.3, S. 40 - Session-ID als GET Parameter in der URL
- Kapitel 3.6.12, S. 48 - Logdaten: Detaillierte Struktur der REST-Endpunkte

Das in Kapitel 3.6.3 beschriebene Risiko – Auslesen der Sitzungsinformationen – kann erst mit der Wiedereröffnung der Postfächer eintreten, weil eine „Sitzung“ im technischen Sinne mit der Anmeldung am Postfach identisch ist, die in der ersten Stufe der Wiederinbetriebnahme des beA-Systems nicht möglich sein wird. Atos wird die Schwachstelle mit der Version 2.1.2 vor dem 03.09.2018 beheben. Für die Installation der Client Security in der ersten Stufe der Wiederinbetriebnahme ergeben sich aus der Schwachstelle keine Risiken.

Aus der in Kapitel 3.6.12 beschriebenen Schwachstelle ergeben sich für die Installation der Client Security in der ersten Stufe der Wiederinbetriebnahme ebenfalls keine Risiken, weil die bei der Erstregistrierung geschriebenen Logdateien keine sensiblen Inhalte im Sinne des Gutachtens enthalten. Sensible Daten zur Kommunikation fallen in dieser Stufe der Wiederinbetriebnahme des beA-Systems (noch) nicht an.

3. Zwischenergebnis

Die noch nicht behobenen Schwachstellen der Kategorien A und B stellen für die Installation der Client Security in der ersten Stufe der Wiederinbetriebnahme kein Risiko dar. Das Präsidium empfiehlt daher die Wiederinbetriebnahme des beA-Systems in der Stufe 1 – Bereitstellung der Client Security zur Installation – zum 04.07.2018.

IV. Betrachtung der beA-Anwendung und der Schnittstellen

1. Risiken der Kategorie A

Das Gutachten benennt keine noch bestehende Schwachstelle der Kategorie A.

2. Risiken der Kategorie B

Das Gutachten benennt 12 noch bestehende Risiken der Kategorie B bezogen auf die beA-Anwendung und die Schnittstellen (ohne HSM). Sie finden die Beschreibungen dieser Risiken in folgenden Kapiteln des Gutachtens:

- Kapitel 3.6.1, S. 38 - Veraltete Javascript-Bibliotheken in der beA-Anwendung
- Kapitel 3.6.2, S. 39 - Überschreiben von Dateien
- Kapitel 3.6.3, S. 40 - Session-ID als GET Parameter in der URL
- Kapitel 3.6.7, S. 43 - Detaillierte Fehlermeldungen der Webapplikationsfirewall
- Kapitel 3.6.9, S. 45 - Qualität der genutzten Session-Cookies
- Kapitel 3.6.10, S. 46 - Automatisches Ausführen und Öffnen von Dateien

- Kapitel 3.6.11, S. 48 - Modifikation von signierten XML-Nachrichten
- Kapitel 3.6.12, S. 48 - Logdaten: Detaillierte Struktur der REST-Endpunkte
- Kapitel 3.6.13, S. 49 - Nicht konsistente Zertifikatsprüfung
- Kapitel 4.5.1, S. 64 - beA-Anwendung: SQL-Injection
- Kapitel 4.5.2, S. 66 - Initialisierungs-Vector
- Kapitel 4.5.3, S. 67 - Unsicheres Auffüllen von Daten bei Verschlüsselung
- Kapitel 5.5.2, S. 84 - EGVP-Bürger-Verzeichniseinträge im SAFE können irreführend sein

Hierzu im Einzelnen:

Die veralteten Javascript-Bibliotheken in der beA-Anwendung (Kapitel 3.6.1) wurden nach Mitteilung von Atos ausgetauscht. Zusätzlich hat Atos in Absprache mit uns einen Prozess aufgesetzt, der regelmäßig einen Dependency-Check-Report (Schwachstellen-Report) erzeugt und auf neue Sicherheitslücken hin überprüft. In Abhängigkeit von einer anschließenden Risikobetrachtung gemeinsam mit der Bundesrechtsanwaltskammer werden ab sofort die Bibliotheken im Rahmen des normalen Releases-Managements ersetzt. Dies geht mit einer generellen Aktualisierung der verwendeten Bibliotheken einher. Die Bestätigung durch secunet steht noch aus, wird aber bis zum 02.09.2018 vorliegen.

Die in Kapitel 3.6.2 beschriebene Schwachstelle betrifft die bei den Rechtsanwaltskammern eingesetzten IT-Systeme. Die Schwachstelle wird derzeit geprüft und gegebenenfalls mit der Version 2.1.2 unserer Software vor dem 03.09.2018 behoben. Vor einer Behebung der Schwachstelle sind weitere Analysen erforderlich, da secunet ausweislich des Gutachtens eine serverseitige Schwachstelle nur vermutet *(„Bei einem Upload der CSV-Datei schien es während der Analyse auch serverseitig möglich, den Speicherort zu manipulieren“).* Dies konnte secunet während der Analyse allerdings nicht final verifizieren.

Zu der in Kapitel 3.6.3 beschriebenen Schwachstelle verweise ich auf meine Ausführungen auf Seite 5, wonach das beschriebene Risiko – Auslesen der Sitzungsinformationen – erst mit der Wiedereröffnung der Postfächer eintreten kann und vorher behoben sein wird.

Das in Kapitel 3.6.7 erörterte Thema im Zusammenhang mit der Firewall ist laut Aussage von Atos behoben; die Bestätigung durch secunet steht noch aus. Sie wird bis zum 02.09.2018 erfolgen.

Das in Kapitel 3.6.9 erörterte Risiko hinsichtlich der Schutztiefe der Session-Cookies ist behoben; die endgültige Bestätigung durch secunet steht noch aus. Sie wird bis zum 02.09.2018 erfolgen.

Kapitel 3.6.10 betrifft den Schutz vor gefährlichen Dateiformaten. Daher soll die Liste der für das automatische Öffnen von Dateien in der beA-Webanwendung erlaubten Dateiformate ergänzt werden. Diese Liste stimmen wir derzeit mit Atos ab; die Umsetzung wird bis zum 02.09.2018 erfolgen und von secunet bestätigt werden.

Das in Kapitel 3.6.11 beschriebene Risiko betrifft den derzeitigen OSCI-Standard und damit das gesamte EGVP-System. Eine Klärung der Kritikalität und möglicher Abhilfen ist mit der Justiz herbeizuführen. Die Bundesrechtsanwaltskammer kann diese Schwachstelle nicht alleine beheben. Im Übrigen erfüllt die Bundesrechtsanwaltskammer mit der Verwendung des OSCI-Standards die Voraussetzungen nach § 20 Abs. 1 RAVPV. Die Bundesrechtsanwaltskammer hat nach § 20 Abs. 2 Satz 2 RAVPV fortlaufend zu gewährleisten, dass die am Elektronischen Rechtsverkehr beteiligten Personen und Stellen miteinander sicher kommunizieren können. Sie darf daher den Standard nicht einseitig ändern.

Über eine Behebung der Schwachstelle im EGVP-Verbund hat die Bundesrechtsanwaltskammer bereits Gespräche mit der Justiz aufgenommen, um kurzfristig eine gemeinsame Lösung zu erreichen.

Kapitel 3.6.12 habe ich bereits oben auf Seite 5 beleuchtet. Bezogen auf die beA-Webanwendung und die Schnittstellen wird eine Logdatei nach Aussage von Atos nur noch an einer Schnittstelle geschrieben, an der Tickets im Support verarbeitet werden. Auch dieses Mitschreiben von Informationen wird bis zum 02.09.2018 abgestellt und die Behebung der Schwachstelle von secunet bestätigt sein.

Die in Kapitel 3.6.13 beschriebene Schwachstelle mit Bezug zu der bei den Rechtsanwaltskammern eingesetzten Software wird bis zum 02.09.2018 behoben und die Behebung durch secunet bestätigt sein.

Die Behebung der in Kapitel 4.5.1 dargestellten Schwachstelle erfordert laut Gutachten, dass *„alle SQL-Statements vor ihrem Einsatz korrekt maskiert werden“*. Atos hat dies zugesichert; das Gutachten führt dazu aus (S. 65):

> *„Von Entwickler-Seite wurde zugesichert, dass, bedingt durch die Software-Architektur, die Maskierung an vorgelagerten Stellen stattfindet. Eine Überprüfung der Aussage konnte aufgrund des Quelltext-Umfangs nicht durchgeführt werden.“*

Diese Aussage von secunet haben wir erstmals mit Vorlage des Gutachtens zur Kenntnis nehmen müssen. Wir haben daher secunet beauftragt, das entsprechende Quelltext-Audit vorzunehmen. Das Ergebnis wird uns bis zum 02.09.2018 vorliegen.

Die in Kapitel 4.5.2 beschriebene Schwachstelle des Quellcodes geht nach der Vermutung des Gutachters darauf zurück, dass versehentlich Testsequenzen im Code nicht gelöscht worden sind. Ob das so ist, wird derzeit durch Atos geprüft. Die Schwachstelle wird bis zum 02.09.208 von Atos behoben und die Behebung von secunet bestätigt sein.

Das in Kapitel 4.5.3 beschriebene Risiko wird derzeit durch Atos untersucht. Die Schwachstelle wird bis zum 02.09.208 von Atos behoben und die Behebung von secunet bestätigt sein.

Das in Kapitel 5.4.2 beschriebene Risiko einer Irreführung des Elektronischen Rechtsverkehrs durch „Fake-Postfächer“ betrifft den gesamten Elektronischen Rechtsverkehr im EGVP-System. Wir werden deshalb das beA-System ohne die Anbindung der Bürgerpostfächer wieder in Betrieb nehmen. Dabei bleibt es zumindest solange, wie sich der EGVP-Verbund nicht auf ein Identifizierungsverfahren für Bürgerpostfächer geeinigt hat. Wir sind in diese Diskussionen bereits eingebunden.

3. Zwischenergebnis

Bezogen auf die beA-Anwendung und die Schnittstellen (ohne HSM, dazu sogleich) sind derzeit nur noch fünf Schwachstellen der Kategorie B in Prüfung. Die übrigen Schwachstellen wurden behoben oder werden bis zur Wiederinbetriebnahme in der zweiten Stufe am 03.09.2018 behoben sein. Das Präsidium bewertet die bislang noch nicht erledigten Schwachstellen weder jeweils für sich noch in ihrer Gesamtheit als so kritisch, als dass die Postfächer nicht am 03.09.2018 wieder freigeschaltet werden könnten. Im Übrigen geht das Präsidium davon aus, dass voraussichtlich auch die noch in der Prüfung befindlichen Schwachstellen der Kategorie B bis dahin abgestellt sein werden. Atos hat im Übrigen zugesichert, innerhalb der oben jeweils angegebenen Zeitfenster die notwendigen Prüfungen vorzunehmen und Abhilfemaßnahmen zu treffen. Secunet hat bestätigt, dass sie deren Wirksamkeit zeitlich – wie angegeben – prüfen wird.

V. Einsatz von HSM / Umverschlüsselung

Wie wir alle wissen, wird – verbundenen mit der Forderung nach einer „echten“ Ende-zu-Ende-Verschlüsselung – die Umverschlüsselung der Postfachschlüssel im HSM öffentlich besonders kritisch diskutiert. Bei der Umverschlüsselung muss es dennoch bleiben, damit wir unseren gesetzlichen Auftrag erfüllen und in unseren Kanzleien weiterhin arbeitsteilig tätig sein können. Auch die Etablierung von Kanzleipostfächern wäre ohne die Umschlüsselung nicht möglich. Dies gilt zumindest dann, wenn man vermeiden möchte, dass ein Postfachschlüssel in viele Hände gelangt.

Das Gutachten legt daher ein besonderes Augenmerk auf Konzeption und Einsatz der HSM.

Ich zitiere (S. 11 des Gutachtens):

> *„Grundsätzlich ist das dem beA zugrundeliegende Verschlüsselungskonzept geeignet, die Vertraulichkeit der Nachrichten während der Übertragung und Speicherung von Nachrichten durch das beA zu gewährleisten, auch gegenüber dem Betreiber des beA. Nachrichteninhalte liegen unverschlüsselt nur bei den Kommunikationspartnern vor. Die Umverschlüsselung ist in einem HSM gekapselt, schützt daher dort vorübergehend entstehende Schlüsselinformationen in einer besonderen manipulations- und ausspähsicheren Umgebung. Das erkennbare Ziel, die Sicherheit der Nachrichten ausschließlich durch Kryptographie zu schützen, ist aber nicht in vollem Umfang erreicht worden. An einigen Stellen verlässt sich das beA in seiner dem Gutachten zugrunde liegenden Realisierung auf organisatorisch-physikalischen Schutz wichtiger Systemkomponenten (HSM-Schlüssel, SAFE BRAK), was bei voller Ausnutzung der kryptographischen Möglichkeiten, die das Konzept und die eingesetzte Technik bieten, nicht notwendig wäre. […] Fast allen konzeptionellen Schwachstellen ist allerdings auch gemeinsam, dass sie nur durch oder mit Hilfe von Innentätern, darunter auch Personen mit besonderer Vertrauensstellung, durchgeführt werden können, die dabei physikalisch-organisatorische Schutzmaßnahmen unterlaufen müssen.“*

Das Gutachten identifiziert bezogen auf die HSM zwei Schwachstellen der Kategorie B (und zwei Schwachstellen der Kategorie C).

1. Schwachstellen der Kategorie B

- Kapitel 5.5.1, S. 83 - BNotK kann Ursprung der Zertifikatsanträge aus HSM nicht erkennen
- Kapitel 5.5.3, S. 85 - HSM-Schlüssel existieren außerhalb des HSM

Secunet hat in Kapitel 5.5.1 festgestellt, dass die Zertifikatsanträge für Postfachschlüssel, die insbesondere bei Neuzulassungen automatisiert an die BNotK gerichtet werden, keine Authentisierung des sie signierenden HSM enthalten. Dadurch könne ein Innentäter oder ein erfolgreicher Angreifer neue oder bestehende einzelne Postfächer unbemerkt unter seiner Kontrolle halten und Inhalte mitlesen oder verändern.

Secunet empfiehlt dafür zu sorgen, dass die BNotK erkennen kann, dass der Zertifikatsantrag im HSM der BRAK signiert wurde und Schlüssel enthält, die im HSM erzeugt wurden. Dies ist technisch durch eine elektronische Gerätesignatur realisierbar.

Das Präsidium hat das aufgezeigte Risiko eingehend bewertet. Es hält die Eintrittswahrscheinlichkeit aus fachlicher Sicht für gering. Denn ein Täter würde mit deutlich geringerem Aufwand eine Kanzlei direkt angreifen, um Kenntnis von Nachrichteninhalten zu erlangen.

Hinzu kommt, dass Voraussetzung für die Ausstellung neuer Zertifikate eine SAFE-ID ist. Dazu bedarf es entsprechend den Regeln einer bereits erfolgten oder einer beantragten Zulassung zur Anwaltschaft. Der Angreifer müsste also die Identität eines Bewerbers übernehmen oder sich Zugriff auf das SAFE-Verzeichnis verschaffen und sich eine eigene Identität anlegen sowie eine SAFE-ID selbst erstellen. Im Fall der noch nicht erfolgten Zulassung zur Anwaltschaft schickt die BNotK indes Karte und PIN an die zuständige Rechtsanwaltskammer, damit diese sie dem Bewerber bei seiner Vereidigung aushändigt. Ein potentieller Angreifer erhielte keinen Zugriff darauf. Schließlich bezweifelt secunet selbst, dass der Angreifer unentdeckt bleibt.

In Kapitel 5.5.3 des Gutachtens geht es um das grundsätzliche Vertrauen in die Bundesrechtsanwaltskammer und ihre Mitarbeiterinnen und Mitarbeiter in der Funktion der „Schlüsselwächter".

Ich zitiere erneut aus dem Gutachten (S. 86 unten):

> *„Die Verwahrung der Schlüssel außerhalb der HSM dient der Inbetriebnahme neuer HSM. Diese Praxis ist nicht unüblich und findet z. B. im Bankwesen oft Anwendung. Damit sie für das beA geeignet ist, ist es erforderlich, dass die beA-Anwender als potentiell vom Bruch der Vertraulichkeit Bedrohte dem Auftraggeber und dem Betreiber des beA ausreichend vertrauen. Ob dies der Fall ist, kann im Rahmen dieses Gutachtens nicht beurteilt werden. Ist ausreichendes Vertrauen vorhanden, kann die hier aus technischer Sicht (Möglichkeit und Umfang des Schadens) als betriebsbehindernd riskant bewertete Praxis fortgesetzt werden."*

An der Notwendigkeit zu vertrauen ändert nach der Überzeugung des Präsidiums auch der technische Vorschlag von secunet nichts, das Schlüsselmaterial verschlüsselt in einem gesonderten HSM oder auf einer Chipkarte vorzuhalten. Denn auch diese „Token" müssten der Bundesrechtsanwaltskammer als verantwortlicher Betreiberin des beA-Systems zur Verfügung gestellt werden, um die Inbetriebnahme neuer HSM, gegebenenfalls auch bei einem anderen Dienstleister, sicherzustellen. Denn andernfalls müssten sämtliche Postfächer neu angelegt und Rechtsanwältinnen und Rechtsanwälte sowie ihre Mitarbeiterinnen und Mitarbeiter mit neuen Sicherheitstoken ausgestattet werden.

2. Bewertung des technischen Lösungsvorschlags von secunet

Die von secunet vorgeschlagene technische Lösung mittels Verschlüsselung des Schlüsselmaterials im HSM und Hinterlegung auf einem Sicherheitstoken (ein weiteres HSM oder eine Chipkarte) wäre technisch umsetzbar. Die Umsetzung ist inhaltlich zwischen der BRAK, Atos und secunet besprochen und könnte mit einem neuen Release Anfang 2019 erfolgen. Indes müssten für die Umsetzung alle fünf derzeit betriebenen HSM ausgetauscht werden, weil die in den HSM eingesetzte Software in einem aufwendigen Prozess auf die neuen Anforderungen angepasst werden müsste. Der zu erwartende Kostenaufwand wäre erheblich; die Aufwandsschätzung erwarten wir bis zur Präsidentenkonferenz.

3. Zwischenergebnis

Das Präsidium sieht keine Veranlassung, an dem Konzept der Umverschlüsselung der Postfachschlüssel im HSM etwas zu ändern. Es greift die Feststellung der secunet auf, dass bei vorhandenem Vertrauen die bisherige Praxis fortgesetzt werden kann.

VI. Betriebs- und Sicherheitskonzepte

In Kapitel 5.7 (Seite 89) fordert secunet die Optimierung der Betriebs- und Sicherheitskonzepte. Für das Gutachten hat Atos Konzepte bereitgestellt, angepasst bzw. neu erstellt. Dieser Prozess war zum Zeitpunkt der Übergabe des Gutachtens noch nicht abgeschlossen, so dass secunet weiteren Handlungsbedarf sieht. Selbstverständlich setzt Atos den Prozess der Konsolidierung der Konzepte fort.

In diesem Zusammenhang werden wir – dem Vorschlag des Gutachtens folgend – regelmäßige Audits des Betriebs unseres Systems durchführen. Dies hatten wir aber, wie Sie wissen, ohnehin schon geplant.

Das Präsidium, aber auch ich persönlich, sind der Überzeugung, dass unser beA-System wie vorgeschlagen wieder in Betrieb gehen kann. Voraussetzung dafür ist Ihre Zustimmung, die Zustimmung der Präsidentenkonferenz der Bundesrechtsanwaltskammer.

Mit freundlichen kollegialen Grüßen

Rechtsanwalt Ekkehart Schäfer