DeutscherAnwaltVerein

Initiativstellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Elektronischer Rechtsverkehr

zum besonderen elektronischen Anwaltspostfach

Stellungnahme Nr.: 28/2018 Berlin, im Juni 2018

Mitglieder des Ausschusses

- Rechtsanwalt Martin Schafhausen, Frankfurt am Main (Vorsitzender)
- Rechtsanwalt Dr. Markus Burianski LL.M., Frankfurt am Main
- Rechtsanwalt Dr. Helmut Redeker, Bonn
- Rechtsanwältin Ulrike Silbermann, Berlin
- Rechtsanwalt und Notar Ulrich Volk, Wiesbaden
- Rechtsanwalt Dipl.-Inform. Dr. jur. Marcus Werner, Köln
- Rechtsanwalt Dr. Markus Wollweber, Köln

unter Mitwirkung von

- Markus Drenger, Darmstadt
- Prof. Dr. Christoph Sorge, Saarbrücken

Zuständig in der DAV-Geschäftsführung

- Referentin Ina Kitzmann, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

- Bundesministerium des Innern
- Bundesministerium der Justiz und für Verbraucherschutz
- Ausschuss Recht und Verbraucherschutz des Deutschen Bundestages
- SPD-Fraktion im Deutschen Bundestag
- CDU/CSU-Fraktion des Deutschen Bundestages, Arbeitsgruppe Recht
- Fraktionen BÜNDNIS 90/DIE GRÜNEN im Deutschen Bundestag
- Fraktion DIE LINKE im Deutschen Bundestag
- Fraktion der ALTERNATIVE FÜR DEUTSCHLAND im Deutschen Bundestag
- Die Datenschutzbeauftragten des Bundes und der Länder

- Vorstand und Geschäftsführung des Deutschen Anwaltvereins
- Vorsitzende der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Vorsitzende des FORUMs Junge Anwaltschaft

- Deutscher Richterbund
- Bund Deutscher Verwaltungsrichter
- Deutscher Steuerberaterverband
- GRUR
- BITKOM
- DGRI
- Bundesverband der Freien Berufe
- EDV-Gerichtstag
- Gemeinsame Kommission elektronischer Rechtsverkehr des Deutschen EDV-Gerichtstages
- Europäische Kommission - Vertretung in Deutschland
- ver.di Bundesverwaltung, Fachbereich Bund und Länder, Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte

- Bundesrechtsanwaltskammer
- Bundesnotarkammer
- Deutscher Notarverein e. V.
- Vorstand und Geschäftsführer der Rechtsanwaltskammern

- Redaktion NJW
- JUVE-Verlag
- Redaktion heise online
- Redaktion Legal Tribune Online
- Redaktion golem.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit rund 64.500 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Zusammenfassung und Vorbemerkung

Der DAV begrüßt ausdrücklich die Veröffentlichung des Gutachtens der secunet Security Networks AG (secunet) durch die Bundesrechtsanwaltskammer (BRAK). Das Gutachten lässt Fragen offen, die wichtige Punkte der IT-Sicherheit des beA-Systems betreffen. Mit dieser Initiativ-Stellungnahme soll eine erste Einschätzung des Gutachtens vor der Konferenz der Präsidenten der örtlichen Rechtsanwaltskammern am 27.06.2018 veröffentlicht werden, um die dort erforderliche sachliche Analyse der Situation zu unterstützen. Der DAV erwartet, dass vor der Wiederinbetriebnahme des beA-Systems nicht nur die von secunet beschriebenen Schwachstellen der Kategorie A (betriebsverhindernde Fehler), sondern auch solche der Kategorie B (betriebsbehindernde Fehler) behoben werden. Ergänzend müssen die von secunet geforderten Maßnahmen zur IT-Sicherheit (insbesondere ein umfassendes Sicherheitskonzept) umgesetzt und überprüft werden, bevor das System wieder in Betrieb genommen wird. Der DAV fordert die BRAK zudem auf, den Zeitplan den tatsächlichen Notwendigkeiten anzupassen. Nach der Beseitigung der betriebsver- und behindernden Fehler sollte zunächst durch secunet überprüft und sichergestellt werden, dass diese Fehler beseitigt worden sind. Das beA-System sollte daher erst einen Monat nach der Mitteilung von secunet, dass alle betriebsver- und behindernden Fehler beseitigt worden sind, wieder online gehen.

Anforderungen an die IT-Sicherheit von beA

Aus dem Gutachten ergibt sich, dass vor einer Wiederinbetriebnahme des beA folgende Anforderungen an die IT-Sicherheit des beA realisiert werden sollten:

a) Es muss (entsprechend den Forderungen von secunet) ein umfassendes Sicherheitskonzept für beA erstellt werden, welches in wesentlichen Teilen veröffentlicht wird. Es mag Teile geben, deren Veröffentlichung problematisch sein könnte. Dies gilt aber nicht für die zu Grunde liegende Kryptographie, denn nach dem Kerckhoffs-Prinzip gilt, dass Verschlüsselungsverfahren nicht geheim gehalten werden sollten. Der DAV vermutet, dass dieses Sicherheitskonzept, welches auch die „Schnittstellen" zu den Rechtsanwaltskammern erfassen muss, nicht vor September 2018 erstellt und veröffentlicht werden kann.

b) Bezüglich des Client sollten nicht nur Schwachstellen der Kategorie A, sondern auch solche der Kategorie B beseitigt werden.

c) Nach dem Grundsatz „Sicherheit vor Schnelligkeit", den auch die BRAK propagiert, muss sichergestellt werden, dass auch Schwachstellen, die mit einer gewissen Wahrscheinlichkeit den Betrieb der Postfächer nicht verhindern, aber behindern können, beseitigt worden sind, bevor das Postfach wieder in Betrieb genommen wird. Auch die übrigen Systembestandteile dürfen erst wieder in Betrieb genommen werden, wenn alle Fehler, die betriebsverhindernd oder -behindernd sind, beseitigt worden sind.

d) Die Beseitigung aller Fehler der Kategorie A und B sollte durch eine erneute Begutachtung der secunet bestätigt wurden.

Zeitplan

Der im Schreiben des Präsidenten der BRAK vom 20. Juni 2018 vorgestellte, nicht realisierbare, Zeitplan muss den tatsächlichen Notwendigkeiten angepasst werden.

Es mag sinnvolle Gründe geben, den beA-Security-Client bald nach der geplanten Veröffentlichung am 4. Juli 2018 zu installieren, wenn bis dahin alle den Client betreffende Schwachstellen der Kategorie A beseitigt wurden; der DAV erwartet aber, dass mit Betrieb der beA-Postfächer zugewartet wird, bis die weitere Entwicklung sicher abgeschätzt werden kann. Auch für „Early Adopter", Verantwortlichen in Rechtsabteilungen

oder größeren Kanzleien, die eine Vielzahl von Postfächern einrichten müssen, und für die Justiz muss gewährleistet sein, dass der weitere Zeitplan der BRAK nachvollziehbar, realistisch und zuverlässig ist. Der vorgestellte Zeitplan hat eine wesentliche Schwäche, denn die BRAK kündigt an, dass secunet bis zum 02.09.2018 die Möglichkeit hat, der BRAK mitzuteilen, dass die im Gutachten bezeichneten Fehler beseitigt worden sind. Die BRAK kündigt aber nicht an, wie sie verfahren wird, wenn am 02.09.2018 die Bestätigung der secunet nicht oder nicht vollständig vorliegt. Der DAV fordert daher, dass das beA-System erst einen Monat nach der Mitteilung von secunet, dass alle betriebsver- und behinderten Fehler beseitigt worden sind, wieder online gehen sollte. So hat die BRAK die Möglichkeit, die Wiederinbetriebnahme des beA aus nachvollziehbaren sachlichen und transparenten Gründen möglicherweise zu verschieben, ohne das die weiteren Beteiligten des ERV weitere verlorene Investitionen tätigen müssen, denn es würde immer ein sicherer Ankündigungszeitraum von einem Monat verbleiben. Hinzu kommt, dass die von secunet aufgestellten konkreten Forderungen an die IT-Sicherheit von beA umgesetzt und deren Einhaltung überprüft werden müssen. Dies wird vermutlich nicht vor dem September 2018 abgeschlossen sein.

Konkretisierung des Gutachtens, Fragen

Der DAV bittet die BRAK folgende Fragen, die sich aus dem vorgelegten Gutachten von secunet ergeben, zeitnah zu beantworten:

a. Was bedeutet der letzte Satz auf S. 10 des Gutachtens („Die Unterstützung von aktuellen Betriebssystemen konnten noch nicht bestätigt werden.“)?
b. Wieso nahm der Gutachter die konzeptionelle Analyse nur auf der Grundlage von Dokumenten (S. 11 Abs. 3 des Gutachtens) vor?
c. Setzt die BRAK die Empfehlungen auf S. 11 Abs. 4 letzter Satz des Gutachtens (volle Ausnutzung der kryptographischen Möglichkeiten) um?
d. Wieso begrenzte sich der Auftrag des Gutachtens auf eine stichprobenartige Überprüfung (S. 14, 1. Spiegelstrich des Gutachtens)? Wann erfolgt eine vollständige uneingeschränkte Sicherheitsüberprüfung?

e. Bis wann wird die BRAK das (S. 14, 4. Spiegelstrich S. 4 des Gutachtens) dringend empfohlene geschlossene Sicherheitskonzept erstellen (lassen)?
f. Wieso folgt die BRAK nicht dem Vorschlag der secunet und etabliert einen Fat Client, sondern verlässt sich allein auf die regelmäßig durchzuführende Kontrolle der zur Anwendung kommenden Java-Script-Version auf ihre Unversehrtheit? Hat die BRAK in Erwägung gezogen, diese Kontrolle auch lokal (beim einzelnen Nutzer) durch ein Browser-Plugin möglich zu machen?
g. Bis wann werden die unter Ziffer 5.7 Abs. 2 S. 1 des Gutachtens (S. 89) genannten Arbeiten an den Konzepten vom Betreiber abgeschlossen sein? Werden diese erneut von secunet geprüft werden?
h. Bis wann werden die auf S. 90 Abs. 2 S. 1 des Gutachtens genannten Arbeiten (dokumentierte Analyse der Bedrohungen und schutzbedürftigen Assets) abgeschlossen sein? Werden diese erneut von secunet geprüft werden?
i. Wird dem Gutachter die Möglichkeit gegeben, die ihm fehlenden Untersuchungsobjekte (auf S. 90 Abs. 3 S. 3 des Gutachtens) ergänzend zur Verfügung zu stellen und ergänzend Stellung zu nehmen?
j. Bis wann wird das vom Gutachter empfohlene spezifische „Information Security Management“ (auf S. 90 Abs. 7 S. 1 des Gutachtens) zwischen BRAK und dem Betreiber vereinbart und etabliert?
k. Bis wann wird das vom Gutachter empfohlene regelmäßige Sicherheits-Audit von beA (auf S. 91 Abs. 4 des Gutachtens) etabliert?
l. Bis wann wird der vom Gutachter empfohlene nachhaltige Patchmanagement-Prozess (auf S. 91 Abs. 5 des Gutachtens) etabliert?

Sonstige Forderungen

Das Gutachten hält es für unerlässlich, das beA-System auch zukünftig regelmäßig einem Sicherheits-Audit zu unterziehen. Es ist daher selbstverständlich, dass auch ein jetzt erreichtes Sicherheitsniveau (nach der Beseitigung der Schwachstellen nach den Kategorien A und B) regelmäßiger Kontrolle unterzogen werden muss. Die erforderlichen Audits sollen dem noch zu schaffenden Fachbeirat übertragen werden, an dem nicht nur Rechtsanwältinnen und Rechtsanwälte beteiligt werden sollten.

Der DAV unterstützt zudem die Forderung der BRAK, den beA-Postfächern die Rolle „buerger-rueck“ solange wieder zu entziehen, bis eine Authentifizierung der Inhaber der EGVP-Postfachinhaber etabliert wurde.