DeutscherAnwaltVerein

Initiativstellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Elektronischer Rechtsverkehr

zum besonderen elektronischen Anwaltspostfach

Stellungnahme Nr.: 37/2018 Berlin, im August 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
- AfD-Fraktion im Deutschen Bundestag
- 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
- 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
- Präsidentinnen und Präsidenten der örtlichen Rechtsanwaltskammern
- Geschäftsführerinnen und Geschäftsführer der örtlichen Rechtsanwaltskammern
- Bundesnotarkammer
- Deutscher Notarverein e. V.

- 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.

Mit Schreiben vom 27. Juli 2018 hat der Präsident der Bundesrechtsanwaltskammer, Herr Rechtsanwalt Ekkehart Schäfer, die Präsidentinnen und Präsidenten der Rechtsanwaltskammern davon in Kenntnis gesetzt, dass eine Schwachstelle, die den Zugriff auf sämtliche über das beA versandte Nachrichten möglich machen soll, nicht bis zum 3. September 2018 behoben werden soll. Da das neu zu implementierende Verfahren, mit dem die zur Verschlüsselung erforderliche Mindestlänge von Nachrichten oder die erforderliche Länge von Datenblöcken erreicht wird (OAEP-Verfahren), nicht so rechtzeitig eingeführt werden kann, dass das EGVP-Projektbüro die justizinterne Frist von sechs bis acht Wochen zum Testen der neuen EGVP-Version vor der verpflichtenden Inbetriebnahme einhalten kann.

Das Schreiben, das auch dem Deutschen Anwaltverein (DAV) vorliegt, schlägt den Präsidentinnen und Präsidenten der Rechtsanwaltskammern vor, den Beschluss vom 27. Juni 2018 abzuändern und das beA trotz des angreifbaren Verschlüsselungsverfahrens am 3. September 2018 wieder in Betrieb zu nehmen. Widersprechen fünf oder mehr Rechtsanwaltskammern diesem Vorschlag, soll am 13. August 2018 eine außerordentliche Präsidentenkonferenz stattfinden.

In dem secunet-Gutachten heißt es zu dieser B-Schwachstelle, also zu einem betriebsbehindernden Fehler:

> „4.5.3 Unsicheres Auffüllen von Daten bei Verschlüsselung
> …
> Im Quelltext wurden Stellen gefunden, an denen im Zusammenhang mit Verschlüsselungsoperationen unsichere Padding-Algorithmen (gemäß BSI-Vorgaben) verwendet werden. Das gefährdet die Vertraulichkeit der so verschlüsselten Daten, die dann ggf. ohne Kenntnis geheimer Schlüssel

entschlüsselt werden können. Die Ausnutzbarkeit ist niedrig, die Bedrohung der Vertraulichkeit allerdings hoch.

{S26} Es werden unsichere Padding-Algorithmen verwendet, die Angriffe auf damit verschlüsselten Daten erlauben.

{R26} Risikobewertung: B-Betriebsbehindernd

Ausnutzbarkeit der Schwachstelle:

Die Ausnutzbarkeit wird niedrig bewertet, da die betroffenen Kryptodaten nur Innentätern zugänglich sind und die Schwachstelle nicht zuverlässig das Entschlüsseln der Daten erlaubt.

Ausnutzbarkeit: **niedrig**

Bewertung der Bedrohung:

Ein erfolgreicher Angriff kann zur Offenlegung von Nachrichteninhalten führen. Hier sind potentiell alle im beA gespeicherten Nachrichten betroffen. Die Bedrohung der Vertraulichkeit ist daher hoch.

Bedrohung Integrität: **niedrig**

Bedrohung Verfügbarkeit: **niedrig**

Bedrohung Vertraulichkeit:**hoch**

Die Kombination aus niedriger Ausnutzbarkeit und hoher Bedrohung der Vertraulichkeit ergibt eine Bewertung der Schwachstelle als betriebsbehindernd.
{M26} Unsichere Padding-Verfahren durch zurzeit als sicher geltende Verfahren ersetzen“

Das Gutachten beschreibt einerseits bei dieser Schwachstelle eine hohe Bedrohung der Vertraulichkeit der anwaltlichen Kommunikation über das beA, schätzt die Gesamtbedrohung andererseits aber wegen der niedrigen Ausnutzbarkeit des Fehlers, da die Schwachstelle nur von einem Innentäter ausgenutzt werden könne, als betriebsbehindernden ein.

In seiner (Initiativ-) Stellungnahme 28/18 hat der DAV gefordert, dass nach dem Grundsatz „Sicherheit vor Schnelligkeit“ sichergestellt sein muss, dass auch Schwachstellen, die mit einer gewissen Wahrscheinlichkeit den Betrieb der Postfächer nicht verhindern, aber behindern können, beseitigt werden, bevor das Postfach wieder in Betrieb genommen wird. Nach Auffassung des DAV müssen also neben den betriebsverhindernden auch alle betriebsbehindernden Schwachstellen, nicht nur in dem Security Client beseitigt werden.

Die technische Beurteilung der im secunet-Gutachten unter 4.5.3 beschriebenen Schwachstelle bei dem Auffüllen von Daten bei Verschlüsselung mit dem Padding-Algorithmus ist dem DAV zurzeit nicht möglich. Das Gutachten bleibt insoweit vage, unklar ist, was genau dort verschlüsselt wird. Nicht deutlich beschrieben wird auch, warum diese Schwachstelle nur durch einen Innentäter ausgenutzt werden kann. Immerhin ist die Kommunikation mit der EGVP-Infrastruktur betroffen. Der DAV hat aber keine Bedenken, der gutachterlichen Einschätzung zu vertrauen und anzunehmen, dass diese Schwachstelle tatsächlich nur durch einen Innentäter ausgenutzt werden kann.

Auch wenn offenbar der unsichere Padding-Algorithmus nach der Wiederinbetriebnahme der Postfach-Infrastruktur am 3. September 2018 nur kurze Zeit genutzt werden muss, bis der sicherere Optimal Asymmetric Encryption Padding (OAEP) genutzt werden kann, fordert der DAV, die Implementierung des OAEP sowohl beA-seitig als auch nach Abschluss der Tests justizseitig abzuwarten. Nach den Angaben des EGVP-Projektbüros, wie sie in einem Beitrag der F.A.Z. „Einspruch“ vom 28. Juli 2018 wiedergegeben werden, wird die Wiederinbetriebnahme der beA-Infrastruktur nur für kurze Zeit verzögert werden.

Nicht ohne Grund sehen justizinterne Regelungen vor, dass neue Softwareversionen vor ihrer verpflichtenden Verwendung im zeitlichen Umfang von sechs bis acht Wochen getestet werden sollen. Nur durch eine solche Testphase ist sichergestellt, dass die neue Softwareversion tatsächlich funktionsfähig ist. Dies muss gerade im Hinblick darauf gelten, dass mit der Wiederinbetriebnahme der beA-Infrastruktur sicher zu erwarten ist, dass die Systeme des elektronischen Rechtsverkehrs in einem deutlich größeren Umfang als bisher genutzt werden. Jetzt erst mit dem „alten“ Padding-Verfahren zu starten, um dann im laufenden Betrieb nach Abschluss der Testphase auf den OAEP umzustellen, birgt das Risiko, dass es zu Fehlern in der Kommunikation und damit schlussendlich zu einem vorübergehenden Ausfall des elektronischen Rechtsverkehrs kommen kann. Entgegen der Erwartung des EGVP-Projektbüros käme weder die Justiz noch die Bundesrechtsanwaltskammer hinsichtlich des weiteren kurzen Verschiebens der Wiederinbetriebnahme in Erklärungsnot. Angesichts der beschriebenen Schwachstelle, die ein hohes Risiko für die Vertraulichkeit der verschlüsselten Daten darstellt, erwarten wir, dass die Wiederinbetriebnahme des Systems mit dieser Schwachstelle zu einem weiteren Vertrauensverlust in die Systeme des elektronischen Rechtsverkehrs führen kann.

Im Übrigen bleibt es bei den mit der Stellungnahme 28/18 aufgezeigten Forderungen. Der DAV bittet die Bundesrechtsanwaltskammer insoweit auch, die zur Konkretisierung des Gutachtens gestellten Fragen zu beantworten.