BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

Herrn Rechtsanwalt
Michael Schinagl
Kurfürstendamm 188
10707 Berlin

per E-Mail: m.schinagl.kpgnr9bu3h@fragdenstaat.de

Berlin, 09.06.2021

Ihr Antrag auf Informationszugang nach dem IFG vom 18.09.2020

Anlage: Memorandum vom 18.10.2019

Sehr geehrter Herr Kollege Schinagl,

auf Ihren über die Website https://fragdenstaat.de/ gestellten Antrag auf Informationszugang nach § 1 IFG vom 18.09.2020 [#197396] ergeht folgender weiterer

B E S C H E I D

Ihr Antrag wird hinsichtlich des Punkts 2 abgelehnt.

Hinsichtlich des Punkts 3 Ihres Antrages übermitteln wir Ihnen ergänzend zum Teilbescheid vom 18.03.2021 anbei das Memorandum von secunet vom 18.10.2019, wobei personenbezogene Angaben geschwärzt sind.

Im Übrigen wurde Ihr Antrag durch den Teilbescheid vom 18.03.2021 bereits beschieden.

Begründung

Sie beantragten Einsichtgewährung in

1. das secunet-Gutachten vom 30.05.2018, wobei Sie die BRAK dazu aufforderten, Ihnen dieses Gutachten als PDF zur Verfügung zu stellen, das durchsuchbar ist, wie es für Dokumente im elektronischen Rechtsverkehr vorgesehen ist, die Anwälte an Gerichte übersenden

2. die in der öffentlichen Fassung des Gutachtens in der Fassung vom 18.06.2018 genannten "detaillierten technischen Informationen" zu den Schwachstellen

3. das Ergebnis des letzten Audits zum ordnungsgemäßen Betrieb, welches in der öffentlichen Fassung des secunet-Gutachtens in der Fassung vom 18.06.2018 (S. 13) verlangt wird

4. das Sicherheitskonzept, welches in der öffentlichen Fassung des Gutachtens vom 18.06.2018 (S. 13) verlangt wird

5. das Kryptokonzept, welches in der öffentlichen Fassung des Gutachtens vom 18.06.2018 (S. 13) verlangt wird

6. das Konzept für die Behandlung von Sicherheitsvorfällen, welches in der öffentlichen Fassung des Gutachtens vom 18.06.2018 (S. 13) verlangt wird

Dazu im Einzelnen:

I. Anträge zu 1., 3., 4., 5., 6.

Diese Punkte wurden bereits am 18.03.2021 beschieden. Punkt 3 wurde am 18.03.2021 teilbeschieden.

II. Antrag zu 2.

Die auf Seite 15 des secunet-Gutachtens vom 18.06.2018 genannten detaillierten technischen und inhaltlichen Informationen zu den Schwachstellen können nicht offengelegt werden. Die detaillierten technischen und inhaltlichen Informationen, die secunet während der Gutachtenerstattung der BRAK als Auftraggeberin zur Verfügung gestellt hat, dienten dazu, die identifizierten Schwachstellen im Detail nachzuvollziehen und sie zu beseitigen. Die Informationen ermöglichen, dass einzelne identifizierte Schwachstellen von Dritten nachvollzogen und ausgenutzt werden könnten, auch wenn sie bereits behoben wurden. Außerdem könnten durch die Darstellung von detaillierten technischen Informationen Rechte Dritter verletzt werden, zum Beispiel durch die Angabe von Quellcode, oder schützenswerte Informationen aufgedeckt werden, wie zum Beispiel IP-Adressen. Aus diesen Gründen hatte die secunet AG die Schwachstellen in dem zur Veröffentlichung vorgesehenen Gutachten ohne Angabe von detaillierten technischen Informationen dargestellt und die detaillierten technischen und inhaltlichen Informationen zu den einzelnen Schwachstellen der Auftraggeberin nur zu deren gezielter Behebung laufend übermittelt.

1. Der Offenlegung der detaillierten technischen Informationen steht der Ausschlussgrund der Betriebs- und Geschäftsgeheimnisse sowohl von Atos als auch von secunet entgegen (§ 6 S. 2 IFG).

a) Betriebs- und Geschäftsgeheimnisse sind alle auf ein Unternehmen bezogenen Tatsachen, Umstände und Vorgänge, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat (st. Rspr. BVerwG, NVwZ 2009, 1114 ff Rn. 11; NvwZ 2010, 189 ff. Rn. 50). Ein berechtigtes Geheimhaltungsinteresse von Betriebs- und Geschäftsgeheimnissen ist anzunehmen, wenn das Bekanntwerden der Informationen dazu geeignet ist, die Wettbewerbsposition des Unternehmens zu beeinträchtigen (vgl. Brink/Polenz/Blatt, § 6 Rn. 48; Schoch; § 6 Rn. 70, 92; BVerwG Urt. v. 17.03.2016 – 7 C 2.15; vgl. auch OVG Berlin-Brandenburg, Urt. V. 21.02.2019 – 12 B 15.18 –, juris, Rn. 18 ff.).

Diese Voraussetzung ist vorliegend in Bezug auf Atos erfüllt, denn die herausverlangten Unterlagen versetzen einen Angreifer in die Lage, Angriffsszenarien nachzuvollziehen, Schwachstellen auszunutzen und so das beA-System insgesamt anzugreifen.

Die BRAK ist mit dem von Atos konzipierten und umgesetzten beA-System seit 2016 produktiv. Nach der Behebung aufgedeckter Sicherheitsschwachstellen im Jahr 2018 läuft das System stabil. Es sind keine weiteren Sicherheitslücken aufgetreten, die einen Betrieb des beA-Systems gefährdet hätten. Würden nunmehr detaillierte technische und inhaltliche Informationen über die Ausnutzbarkeit von Schwachstellen quasi als Anleitung zum Ausnutzen von Schwachstellen herausgegeben, bestünde die Gefahr, dass Angreifer das System insgesamt korrumpieren und Atos damit erheblichen – auch wirtschaftlichen – Schaden zufügen würden. Denn sie würden die Detailinformationen über die Systemarchitektur nutzen, ggf. offenlegen und dadurch insgesamt die Stabilität des Systems gefährden können. Dies gilt auch nach dem Dienstleisterwechsel, da die Architektur des beA-Systems im Wesentlichen unverändert ist.

Durch die breite mediale Öffentlichkeit, die das beA erfahren hat, verfolgen sowohl die juristische als auch die Fachöffentlichkeit der IT-Branche die EDV-technischen Funktionsgrundlagen des beA seit Jahren, auch hinsichtlich Sicherheitskonzepten. Würden die Details der Sicherheitsarchitektur und mögliche Angriffsszenarien offengelegt, bestünde die Möglichkeit, das System insgesamt zu korrumpieren und eine Außerbetriebnahme zu erzwingen, da ständig mit Angriffsversuchen und Ausnutzung des erlangten Wissens zu rechnen wäre. Die Architekturentscheidungen von Atos würden ausgenutzt werden können, um Atos zu schaden, so dass das Vertrauen in die Systemarchitektur, die secunet als geeignet für den Betrieb eines solchen Systems begutachtet hatte, nachhaltig erschüttert würde. Daraus würden Atos erhebliche wirtschaftliche Nachteile sowohl aufgrund von Schadensersatzansprüchen als auch in der Zukunft wegen verlorenen Renommees erwachsen.

Zudem hat Atos einer Einsichtgewährung im Drittbeteiligungsverfahren nicht zugestimmt. Zugang zu Betriebs- und Geschäftsgeheimnissen kann gemäß § 6 S. 2 IFG nur gewährt werden, falls der Dritte eingewilligt hat. Nach Durchführung des Drittbeteiligungsverfahrens (§ 8 IFG) liegt jedoch keine Einwilligung von Atos in eine Offenbarung der beiden Darstellungen vor. Daraus geht der erforderliche Geheimhaltungswille hervor.

b) Die Detailinformationen stellen überdies auch Betriebs- und Geschäftsgeheimnisse gemäß § 6 S. 2 IFG von secunet dar.

Die Dokumente bilden die Vorgehensweise von secunet bei der Prüfung der Sicherheitsarchitektur von IT-Großprojekten ab. Die secunet Security Networks AG ist ein auf IT-Sicherheit und IT-Hochsicherheit spezialisiertes Unternehmen. Bei einer Veröffentlichung der Unterlagen wäre für Mitbewerber von secunet die Vorgehensweise von secunet bei der Erstellung von IT-Fachgutachten ableitbar. Dies betrifft sowohl die geprüften Fragestellungen wie auch die dargestellten Test- und Analysestrategien. Neben detaillierten Beschreibungen der verwendeten Testmethoden, der eingesetzten Werkzeuge und der Ergebnisse sind in den Unterlagen umfangreiche Informationen zum Hintergrundwissen der Tester vorhanden. Bei künftigen Prüfungsaufträgen könnten Mitbewerber von secunet diese Informationen für ihr eigenes Angebot nutzen.

Auch secunet hat einer Einsichtgewährung in die Dokumente nicht zugestimmt. Daraus geht der erforderliche Geheimhaltungswille hervor.

2. Die Darstellung der Schwachstellen enthält auf insgesamt fast 400 Seiten die nachfolgend beschriebenen Informationen zur alleinigen Verwendung durch die Auftraggeberin:

a) Abschnitt 1 beschreibt die Konventionen im Dokument, insbesondere die Vorgehensweise bei der Beschreibung der identifizierten Schwachstellen.

Daraus wird ersichtlich, auf welche Weise secunet die Überprüfung von IT-Systemen vornimmt, d.h. welche Prüfschritte anhand welcher Kategorien durchgeführt werden.

b) Abschnitt 2 enthält die Detailbeschreibung des Penetrationstests in der Phase 1. Dieser bezieht sich auf die Detailanalyse der beA-Client Security. In dem Dokument wird die Methodik einschließlich der Darstellung von Angreifermodellen detailliert beschrieben. Die Zugriffs- und Kommunikationskanäle werden im Einzelnen dargestellt. Nicht autorisierte Kenner erhielten darüber detaillierte Informationen der durch Atos verwendeten Systemarchitektur und damit Einblicke in Betriebs- und Geschäftsgeheimnisse. Würden sie dies zu Angriffen ausnutzen, entstünde erheblicher Schaden bei Atos.

Im weiteren Verlauf wird dargestellt, wie secunet im Detail die Kommunikationskanäle geprüft hat, welche Methoden zum Aufbrechen der Kanäle angewandt wurden, wie Zertifikate einsetzt werden und welche Schutzmechanismen bestehen.

Das Kapitel 2.6 dokumentiert die Ergebnisse der durchgeführten Detailanalyse nach anerkannten Standards. Dabei werden zunächst die Rahmenbedingungen der Tests erläutert und sodann die identifizierten kritischen Schwachstellen, teilweise unter Beifügung und Auswertung von Log-Dateien und Quellcode-Auszügen, dokumentiert. Das Vorgehen wird sehr detailliert unter Anwendung der eingesetzten Tools beschrieben und lässt Rückschlüsse auf die Vorgehensweise von secunet zu. Die Beschreibung der Schwachstellen unter Beifügung von Log-Dateien und Quellcode-Auszügen lässt detaillierte Schlüsse auf die Architektur des beA-Systems und damit geheimhaltungsbedürftige Details der Programmierung durch Atos zu.

Kapitel 3 befasst sich mit der Detailbeschreibung des Penetrationstests der Phase 2, durch den die externen Schnittstellen des beA-Systems geprüft wurden. In dem Penetrationstest in der Phase 2 wurden der Webservice Kanzleisoftware, der Service SAFE BRAK, der Virtuelle-Attribute-Service, der OSCI-Intermediär, der RAK-Client, das Webportal BRAV-Suche, der Webservice Find a Lawyer, das OCSP-Relay, die Kanzleisoftware-Schnittstelle, das Antragsportal der Bundesnotarkammer sowie die Anwenderhilfe untersucht. In diesem Kapitel werden die durchgeführten Tests im Einzelnen beschrieben, die Angriffsszenarien erläutert und die Prozesse im beA-System im Einzelnen dargelegt. In der darauffolgenden Auswertung der Tests werden die Schwachstellen im Einzelnen unter Beifügung von Log-Dateien und Auszügen aus dem Quellcode beschrieben. Diese detaillierten Beschreibungen ermöglichen zumindest einen Teil-Nachbau des beA-Systems und damit die Nutzung von Entwicklungsdetails der Atos. Zudem ermöglichen sie gezielte Angriffe auf das System, wodurch erheblicher Schaden für Atos, aber auch für secunet entstehen würde, weil sie diese Detailinformationen zum Schaden von Atos nicht vertraulich behandelt hätte.

Die Kapitel 5 bis 9 beschreiben schließlich die durchgeführte Quelltext-Analyse. Dadurch wird einerseits die präzise Vorgehensweise von secunet unter Benennung der konkret eingesetzten Werkzeuge dargestellt. Zum anderen werden die identifizierten Schwachstellen im Einzelnen unter Beifügung von Quelltext-Auszügen dokumentiert und Anleitungen zur Behebung gegeben.

Insbesondere diese Informationen ermöglichten es Angreifern, das System gezielt anzugreifen und ihm damit erheblichen Schaden zuzufügen. Außerdem lässt die detaillierte Beschreibung zu, dass interessierte Kreise eine klare Sicht auf die Architektur des beA-Systems hätten und diese Kenntnisse ausnutzen könnten, um vergleichbare Kommunikationsmittel im Markt einzuführen.

3. Zudem erwachsen der BRAK im Verhältnis zu Atos und zu secunet gemäß § 241 Abs. 2 BGB Rücksichtnahmepflichten aus den ehemaligen Vertragsverhältnissen (vgl. Palandt/Grüneberg, § 241 Rn. 6; vgl. auch OVG Berlin-Brandenburg, Urt. v. 21.02.2019 – 12 B 15.18 –, juris, Rn. 17). Die BRAK ist mithin gehindert, solche Informationen aus den ehemaligen Vertragsverhältnissen zu offenbaren, an denen das beauftragte Unternehmen ein berechtigtes Geheimhaltungsinteresse hat. Dieses ergibt sich sowohl bei Atos als auch bei secunet aus dem Vorliegen von Betriebs- und Geschäftsgeheimnissen nach § 6 S. 2 IFG (s.o.).

Die Informationen aus der Sicherheitsbegutachtung durch die secunet AG, die der Geheimhaltung nicht unterliegen, hat die BRAK durch die veröffentlichte Version des Gutachtens bereits herausgegeben. Die secunet AG hat diese veröffentlichte Version um die geheimhaltungsbedürftigen Detailinformationen bereinigt und eine insgesamt zur Veröffentlichung geeignete Version des Gutachtens zur Verfügung gestellt.

III. Antrag zu 3.

In Ergänzung zu den hinsichtlich Punkt 3 Ihres Antrags am 18.03.2021 gemachten Ausführungen übermitteln wir Ihnen anbei das Memorandum von secunet vom 18.10.2019, wobei personenbezogene Angaben geschwärzt sind. Daraus ergibt sich, dass die zur Prüfung vorgelegten Sicherheitsdokumente ausrechend erscheinen, die wesentlichen Sicherheitsmaßnahmen des beA zu erläutern und den gewünschten Nachweis hinreichender Sicherheit der Funktionen des beA zu liefern. Eine weitere Überprüfung sei nicht notwendig.

Mit freundlichen kollegialen Grüßen

[redacted]
Dr. Ulrich Wessels
Rechtsanwalt und Notar

Rechtsbehelfsbelehrung

Gegen diesen Bescheid kann innerhalb eines Monats nach Bekanntgabe Widerspruch erhoben werden. Der Widerspruch ist bei der Bundesrechtsanwaltskammer, Littenstraße 9, 10179 Berlin schriftlich oder zur Niederschrift einzulegen.