BUNDESRECHTSANWALTSKAMMER

Der Präsident

Bundesrechtsanwaltskammer
Littenstraße 9 | 10179 Berlin

[redacted]

per E-Mail: [redacted]

Berlin, 18.03.2021

Ihr Antrag auf Informationszugang nach dem IFG vom 18.09.2020

Anlage: Gutachten der secunet Security Networks AG v. 30.05.2018

Sehr geehrter Herr Kollege [redacted],

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

B E S C H E I D

Ihrem Antrag wird teilweise stattgegeben.

Auf Ihren Antrag zu 1 wird Ihnen das Gutachten der secunet Security Networks AG vom 30.05.2018 als PDF zur Verfügung gestellt, wobei eine Durchsuchbarkeit nicht gegeben ist.

Hinsichtlich des Punkts 2 Ihres Antrags dauert derzeit noch ein Drittbeteiligungsverfahren an (s. u.). Wir werden diesen Punkt gesondert bescheiden.

Auf Ihren Antrag zu 3 wird auf das Gutachten der Secuvera GmbH verwiesen, das unter folgendem Link abrufbar ist:

https://www.brak.de/w/files/02_fuer_anwaelte/bea/abschlussgutachten_secuvera.pdf

Im Übrigen wird Ihr Antrag abgelehnt.

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

Zu 1. Als Antragsteller eines IFG-Antrags können Sie gemäß § 1 Abs. 1 IFG eine Zugangsvariante ausdrücklich oder konkludent wählen (vgl. Brink/Polenz/Blatt, IFG, § 1 Rn. 105; vgl. Schoch, IFG, § 1 Rn. 247). Diese Wahlmöglichkeit bezieht sich indes auf verschiedene Zugangsarten, etwa „Auskunft“ oder „Akteneinsicht“. Die Anspruchsgrundlage des § 1 IFG beinhaltet demgegenüber keine Formvorgaben, wie Sie etwa in der ERVV bezogen auf den elektronischen Rechtsverkehr enthalten sind. Maßgeblich ist die Lesbarkeit der antragsgegenständlichen Information (vgl. Schoch, IFG, § 1 Rn. 40). Daher übermitteln wir Ihnen das secunet-Gutachten vom 30.05.2018 anbei als PDF, wie es der BRAK vorliegt. Eine weitere Bearbeitung erfolgt nicht.

Zu 2. Hinsichtlich der auf Seite 15 des secunet-Gutachtens vom 18.06.2018 genannten detaillierten technischen und inhaltlichen Informationen der BRAK zu den Schwachstellen führt die BRAK derzeit ein Drittbeteiligungsverfahren durch und wird nach dessen Abschluss eine Bescheidung hinsichtlich der entsprechenden Unterlagen vornehmen.

Zu 3. Auf Seite 13 des secunet-Gutachtens vom 18.06.2018 wird empfohlen, auf der Grundlage der Dokumente, die zum Sicherheitskonzept gehören, ein regelmäßiges Audit durchzuführen. Im Rahmen des Betriebsübergangs von der Atos Information Technology GmbH auf die Wesroc GbR hat die BRAK die Secuvera GmbH mit der Erstellung eines Sicherheitsgutachtens beauftragt. Es sollte unter anderem der Entscheidung dienen, ob die Betriebsaufnahme durch die Wesroc GbR vorgenommen werden kann. Das Gutachten der Secuvera GmbH vom 02.07.2020 bestätigt zudem den sicheren Betrieb des beA. Es ist unter folgendem Link abrufbar:

https://www.brak.de/w/files/02_fuer_anwaelte/bea/abschlussgutachten_secuvera.pdf

Zu 4. Das von der Atos Information Technology GmbH erstellte Sicherheitskonzept Betrieb vom 07.05.2019 kann nicht herausgegeben werden, da es zahlreiche detaillierte Angaben über die IT-technische Architektur des beA-Systems enthält. Im Übrigen hat Atos der Herausgabe des Konzepts nicht zugestimmt.

a) Der Herausgabe steht der Ausschlussgrund der Betriebs- und Geschäftsgeheimnisse von Atos (§ 6 S. 2 IFG) entgegen.

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 liegt vor, wenn das Bekanntwerden der Information 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.).

Der erforderliche Schutz der Betriebs- und Geschäftsgeheimnisse von Atos besteht auch nach Beendigung des Vertrags zwischen der BRAK und der Atos GmbH fort. Zum einen wurden die von Atos erstellten Sicherheitskonzepte insbesondere hinsichtlich der beA-spezifischen Ausführungen von Wesroc zunächst übernommen und dann weiterbearbeitet. Wesentliche Teile gelten somit fort. Zum anderen enthalten die Konzepte Atos-interne Regelwerke, die nicht nur für den Kunden BRAK gelten, sondern für sämtliche Geschäftsvorgänge von Atos. Mit diesen Sicherheitsbestimmungen und deren ständige Überprüfung ist Atos ein im Wettbewerb anerkannter Anbieter von IT-Infrastrukturleistungen, die besonderer Vertraulichkeit unterliegen. Eine Offenlegung der Sicherheitskonzepte würde die Wettbewerbsposition von Atos erheblich verschlechtern.

aa) Das Dokument enthält als Einleitung eine Aufstellung der Bezugsdokumente. Es handelt sich hierbei insbesondere um Atos-interne Regelwerke über Sicherheitsleitlinien und Sicherheitsmaßnahmen sowie Maßnahmen zur Kontrolle des Umgangs mit vertraulichen Dokumenten. Die Offenlegung dieser Angaben würden die betriebsinterne Organisation von Atos offenlegen und Mitbewerber von Atos dazu befähigen, die von Atos mit hohem finanziellem und auch zeitlichem Aufwand aufgebauten Betriebsstrukturen und -abläufe unentgeltlich zu übernehmen sowie Angriffe auf die Atos-interne sowie für diverse Kunden aufgebaute Infrastruktur unter Ausnutzung der Kenntnis interner Sicherheitsmaßnahmen ermöglichen.

bb) In dem Abschnitt über Sicherheitsleitlinien beschreibt Atos die Sicherheitsleitlinien des Unternehmens und deren regelmäßige Überprüfung und stellt einen konkreten Zusammenhang zu den Sicherheitsanforderungen im beA und deren Umsetzung in den Sicherheitsleitlinien von Atos dar.

cc) Der die Organisation der Informationssicherheit behandelnde Abschnitt enthält profunde Angaben zum Management der Informationssicherheit und des Datenschutzes. Es werden die Elemente der Atos-Sicherheitsstrategie im Einzelnen beschrieben. Konkret enthält dieser Abschnitt die Anwendung der Atos-internen Sicherheitsstrategie auf die speziellen Sicherheitsanforderungen des Betriebs des beA-Systems. In dem Abschnitt sind die interne Organisation im Hinblick auf die Informationssicherheit einschließlich der Übertragung des Informationssicherheits-Managementsystems auf den Betrieb des beA-Zentralsystems sowie die Sicherheitsleitlinien im Umgang mit Mobilgeräten und Telearbeit beschrieben.

dd) Im Hinblick auf die Personalsicherheit wird ausgeführt, wie Atos sicherstellt, dass Mitarbeiter und Auftragnehmer ihre Verantwortlichkeiten verstehen und für die für sie vorgesehenen Positionen geeignet sind. Darüber hinaus enthält der Abschnitt Ausführungen zur Überprüfung neuer Atos-Mitarbeiter, zur Durchführung regelmäßiger Schulungen zu verschiedenen, sicherheitsrelevanten Themen einschließlich der Angabe von Lernmaterial sowie zur internen Kommunikation bei aktuellen, die Sicherheit betreffenden Ereignissen. Zudem werden Angaben über arbeitsvertragliche Regelungen,

insbesondere zur Einhaltung und bei Verletzung der Vertraulichkeit auch nach der Beendigung von Arbeitsverhältnissen gemacht.

die Atos gehörenden Werte, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen im Zusammenhang stehen, zu inventarisieren sind. Atos erbringt viele Dienstleistungen für viele Kunden. Aus diesem Grund muss Atos die Kundenumgebung gut kennen, um eine vollständige und korrekte Konfigurationsmanagementdatenbank zu führen. Wie diese Einträge für das beA-Zentralsystem vorgenommen werden, beschreibt dieser Abschnitt ebenfalls. Ferner werden die Regeln beschrieben, die den zulässigen Gebrauch von Informationen und Werten, die mit Informationen und Einrichtungen zur Verarbeitung von Informationen in Zusammenhang stehen, dokumentiert.

Das Kapitel beschreibt ferner die Klassifizierung von Informationen nach ihrem Wert, gesetzlichen Vorschriften, Betriebswichtigkeit und Sensibilität im Hinblick auf unbefugte Offenlegung oder Veränderung mit dem Ziel der Sicherstellung, dass Informationen eine angemessene Schutzstufe entsprechend ihrer Bedeutung für die Organisation zugeteilt bekommen. In diesem Zusammenhang wird insbesondere die Atos-Richtlinie zur Klassifizierung von Informationen einschließlich des Klassifizierungsschemas und der damit verbundenen Schutzvorgaben näher erläutert. Konkret wird die Anwendung dieser Richtlinien auf das beA-Zentralsystem dokumentiert. Schließlich beinhaltet dieses Kapitel einen eigenen Abschnitt zur Handhabung von Speicher- und Aufzeichnungsmedien, insbesondere deren Verwaltung, Entsorgung und Transport.

Die umfassende und sehr detaillierte Darstellung der festgelegten Maßnahmen zum Management organisationseigener Werte lässt eindeutige Rückschlüsse auf die Arbeitsweise von Atos zu, welche für Außenstehende nicht ersichtlich sind und deshalb Betriebs- und Geschäftsgeheimnisse darstellen.

ff) Das Konzept beinhaltet außerdem in dem Abschnitt zur Zugriffskontrolle zahlreiche Informationen über die Beschränkung des Zugriffs auf Informationen und informationsverarbeitende Einrichtungen. Die geschäftlichen Anforderungen in Bezug auf die Zugriffskontrolle bestehen aus Leitlinien zur Zugangskontrolle, die auch den Zugang zu Netzwerken und Netzwerkdiensten regeln. Die Leitlinien sind im Einzelnen beschrieben und deren Anwendung konkret auf das beA-Zentralsystem erläutert.

Die Beschreibung der Benutzerverwaltung, deren Ziel die Sicherstellung des Zugangs ausschließlich für autorisierte Benutzer und die Verhinderung von nicht autorisiertem Zugang zu Systemen und Diensten ist, besteht aus Regelungen zur An- und Abmeldung von Benutzern, zur Zugangsbereitstellung für Benutzer, zur Verwaltung von Sonderzugangsrechten, zur Verwaltung geheimer Authentifizierungsdaten von Benutzern, zur Überprüfung von Benutzerberechtigungen und zur Entziehung oder Anpassung von Zugangsrechten. Die detaillierte Vorgehensweise ist Gegenstand dieses Abschnitts.

Zur Benutzerverantwortung sind detaillierte Informationen zur Verwendung geheimer Authentifizierungsdaten von Benutzern und zur Passworthandhabung niedergelegt.

Schließlich enthält dieses Kapitel einen Abschnitt zur Kontrolle des Zugangs zu Systemen und Anwendungen, Darin ist beschrieben, wie das Ziel, einen nicht autorisierten Zugang zu Systemen und Anwendungen durch die Beschränkung des Zugangs zu Informationen, sichere Anmeldeverfahren, ein Kennwortmanagementsystem, die Verwendung von Systemwerkzeugen sowie einer Kontrolle des Zugriffs von Software-Quellcode sichergestellt wird.

gg) Die Informationen zur Kryptographie und zu den diesbezüglich entwickelten Leitlinien enthalten differenzierte Angaben zu den Schutzmaßnahmen zur Sicherstellung der ordnungsgemäßen und wirksamen Verwendung von Kryptographie zum Schutz der Vertraulichkeit, Authentizität und/oder

Integrität von Informationen. Hinsichtlich der Umsetzung der Anforderungen für das beA-Zentralsystem wird auf das eigens hierfür erstellte Kryptokonzept verwiesen.

hh) Bezüglich der physischen Sicherheitsbereiche werden Ausführungen zum Schutz von Bereichen gemacht, in welchen sich vertrauliche oder betriebswichtige Informationen oder informationsverarbeitende Einrichtungen befinden. Das Sicherheitskonzept enthält hierzu detaillierte Angaben zur Abstufung verschiedener Zonen je nach Geheimhaltungsbedürftigkeit sowie zu den zur Verhinderung unbefugter Zugriffe vorgesehenen Sicherheitsmaßnahmen. Es wird konkret dargestellt, wie der nicht autorisierte physische Zugriff sowie die Beschädigung und Beeinträchtigung von Daten und informationsverarbeitenden Einrichtungen verhindert werden.

Als sicherheitsrelevante Maßnahmen werden abgestufte Vorgaben für die Einrichtung und Durchführung von Zugangskontrollen und für die physische Sicherung von Büros und anderen Räumen dargestellt. Das Konzept beschreibt auch die Risikobewertung im Hinblick auf externe und umweltbedingte Bedrohungen, z.B. vorsätzliche Angriffe von außen.

ii) In dem Abschnitt über die Betriebssicherheit wird dargelegt, welche Verfahren zur Sicherstellung des ordnungsgemäßen und sicheren Betriebs von Einrichtungen zur Informationsverarbeitung eingesetzt werden und wie diese konkret auf das beA-System angewendet werden. In diesem Kapitel werden zudem die Details des Kapazitätsmanagements, des Änderungsmanagements und des Schutzes vor Malware beschrieben. Ein wesentlicher Teil bezieht sich auf die Durchführung von Datensicherungen zum Schutz vor Datenverlust, der Protokollierung und Überwachung von Ereignissen sowie zur Kontrolle von Betriebssoftware. In diesem Kapitel ist ferner das Schwachstellenmanagement von Atos beschrieben.

Für Software-Installationen durch Benutzer sind Regeln festgelegt und implementiert, die in diesem Kapitel detailliert beschrieben sind. Außerdem ist beschrieben, wie die Auswirkungen von Audit-Aktivitäten auf die betrieblichen Systeme minimiert werden können, indem eigene Betriebsabläufe zur Unterstützung und Überwachung entwickelt und eingeführt und fortlaufend weiterentwickelt und verbessert werden.

jj) Der Abschnitt über die Sicherheit in der Kommunikation legt umfassend dar, wie der Schutz von Informationen in den Installationen und Arbeitsmitteln von Atos erfolgen muss. Es wird definiert, wovon die Sicherheit der Netzwerke abhängt und welche Sicherheitsanforderungen zu deren Schutz notwendig sind. Auch die IT-technische Ausgestaltung der Netzwerke, z.B. hinsichtlich der Trennung von Netzwerken, wird erörtert. Die Ausführungen in diesem Abschnitt enthalten u.a. Angaben zu Regelungen, durch die der Schutz klassifizierter Informationen vor unbefugtem Zugriff bezweckt wird. Dies betrifft etwa die Einbeziehung bestimmter Atos-interner Management-Bereiche, falls auf Informationen ab einer bestimmten Klassifizierungsstufe zugegriffen werden soll. Zudem werden Vorgaben zur Übertragung von Informationen dargestellt, um den Schutz der transferierten Daten zu gewährleisten, etwa hinsichtlich der Verwendung von Verschlüsselungstechniken. Es findet sich sodann ein Verweis auf ein Atos-internes Dokument, in dem Vorgaben zur vertraulichen Behandlung von Daten enthalten sind.

kk) Das Sicherheitskonzept enthält in dem Abschnitt über die Anschaffung, Entwicklung und Instandhaltung von Systemen profunde Informationen über ein Analyseverfahren, das dazu dient, die technischen Sicherheitsvorkehrungen gemäß den Atos-internen Standards einzuhalten. Es werden verschiedene Verschlüsselungsschichten und -modelle genannt, durch die die Sicherheit von Diensten auch in öffentlichen Netzen gewährleistet wird. Sodann werden detaillierte Angaben zu dem verwendeten Verschlüsselungsregime gemacht, um die Datensicherheit von beA-Nachrichten zu gewährleisten.

In diesem Abschnitt finden sich auch eingehende Informationen zur Sicherheit in der Entwicklung und deren Kontrolle.

ll) Zu den Lieferantenbeziehungen enthält das Sicherheitskonzept ebenfalls detailreiche Informationen. So werden Maßgaben genannt, mit deren Hilfe die Informationssicherheit im Hinblick auf Risiken im Zusammenhang mit einem eventuellen Zugang von Lieferanten auf die Werte des Unternehmens eingehalten wird. Auch die Änderung von Lieferantenbeziehungen wird thematisiert und die hierfür zu beachtenden Auswahlkriterien genannt.

mm) In dem Abschnitt über das Management von Informationssicherheitsvorfällen wird ausgeführt, welche Schritte beim Eintreten eines Informationssicherheitsereignisses zu befolgen sind. In diesem Kapitel sind die Zuständigkeiten und Verfahren bei der Meldung von Informationssicherheitsereignissen im Detail beschrieben. Ferner behandelt es die Meldung und Bewertung sowie die Entscheidung über Informationssicherheitsschwachstellen, wie auf Informationssicherheitsvorfälle zu reagieren ist sowie welche Erkenntnisse daraus zu ziehen sind. Im Einzelnen beschrieben ist zudem das Sammeln von Beweismaterial.

nn) Die Ausführungen über Informationssicherheitsaspekte des Betriebskontinuitätsmanagements enthält Bestimmungen für die Aufrechterhaltung der Informationssicherheit in einem Krisen- oder Schadensfall. Es wird ausgeführt, welche Strategie für die Sicherheit des Betriebs in einem Notfall Anwendung findet und wie die Kontinuität der IT-Sicherheit aufrechterhalten werden kann. Zudem werden Einzelheiten zur Kommunikation mit Kunden in einem solchen Fall dargelegt. Darüber hinaus wird festgelegt, dass IT-Einrichtungen mit ausreichender Redundanz vorgehalten werden sollen, um die Informationssicherheit auch im Krisenfall zu gewährleisten. In diesem Kapitel wird detailliert beschrieben, wie die Atos-internen Anforderungen an ein Betriebskontinuitätsmanagement auf das beA-System konkret umgesetzt werden.

oo) Das Kapitel über die Richtlinienkonformität beinhaltet u.a. Maßgaben zur Dokumentation der rechtlichen Regelungen, die hinsichtlich des Betriebs der IT-Systeme zu beachten sind. Danach werden Regelwerke und Rechtsgrundsätze bezeichnet, welche im Zusammenhang mit Vertragsverhältnissen mit Kunden besonders zu beachten sind. Um datenschutzrechtliche Anforderungen zu erfüllen, werden sodann Ausführungen etwa zum Schutz von Aufzeichnungen gemacht. Ferner werden die für den Datenschutz Verantwortlichen benannt sowie Einzelheiten zur Anwendung kryptographischer Kontrollmaßnahmen beschrieben. Zudem wird das Erfordernis genannt, dass Informationssysteme regelmäßig auf Übereinstimmung mit den entsprechenden Leitlinien der Organisation geprüft werden.

pp) Das Dokument enthält in einem Kapitel „Anhänge“ detaillierte Regelungen zu Datenbankadministrationsrechten, Firewallsystemen, Datensicherung- und -wiederherstellung, zum Datenschutz, konkret bezogen auf beA zur anwaltlichen Verschwiegenheitsverpflichtung sowie zum Datenschutzaudit. Die Ausführungen sind auf Maßnahmen im Atos-Betrieb und deren konkrete Umsetzung auf das beA-System bezogen.

qq) Diese Informationen legen detailliert die Arbeitsweise von Atos offen und könnten von Mitbewerbern unentgeltlich übernommen werden. Aus den genannten Angaben können Mitbewerber Rückschlüsse auf die Arbeitsorganisation von Atos ziehen und die eigenen Betriebsabläufe entsprechend anpassen und gestalten, ohne das geldwerte Wissen von Atos entweder selbst entwickelt oder von Fachfirmen erworben zu haben.

Die Informationen sind auch nicht öffentlich bekannt. Zugang zu Betriebs- und Geschäftsgeheimnissen kann gem. § 6 S. 2 IFG nur gewährt werden, falls der Dritte eingewilligt hat. Atos hat im Drittbeteiligungsverfahren (§ 8 IFG) keine Einwilligung in eine Einsichtgewährung in das

Sicherheitskonzept erklärt. Daraus geht der erforderliche Geheimhaltungswille hervor. Die Herausgabe von Teilen des Dokuments kommt ebenfalls nicht in Betracht, da jede einzelne darin enthaltene Angabe die Kriterien der Geschäfts- und Betriebsgeheimnisse erfüllt und Rückschlüsse auf nach § 6 S. 2 IFG geschützte Informationen zulässt. 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 Sicherheitstests sowie Betriebskonzepten. Wirtschaftliche Vorteile im Wettbewerb, welche Atos sich durch technische Innovationen und die Entwicklung EDV-technischer und -organisatorischer Vorgehensweisen erarbeitet hat, wären bei Offenlegung der begehrten Informationen gefährdet. Die begehrten Informationen enthalten hinreichende Anhaltspunkte, um für Konkurrenten von Atos einen Vergleich der eigenen Kompetenzen und technischen Konzepte mit denen von Atos zu ermöglichen und geldwertes Wissen von Atos unentgeltlich zu erhalten. Damit wäre ein ungerechtfertigter Wettbewerbsvorteil gegenüber Atos bei der Anbahnung weiterer Verträge hinsichtlich der Erbringung EDV-technischer Leistungen verbunden.

Zudem erwachsen der BRAK im Verhältnis zu Atos sowie zu Wesroc gemäß § 241 Abs. 2 BGB Rücksichtnahmepflichten aus den 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 auch danach gehindert, solche Informationen aus dem Vertragsverhältnis zu offenbaren, an denen das beauftragte Unternehmen ein berechtigtes Geheimhaltungsinteresse hat (s.o).

Zu 5. Eine Informationsgewährung bezüglich des Kryptokonzepts vom 06.09.2019 kann ebenfalls nicht erfolgen, da dieses Dokument detaillierte Angaben über die im beA-System eingesetzte Kryptographie enthält.

a) Es handelt sich auch bei dieser Unterlage um Betriebs- und Geschäftsgeheimnisse von Atos (§ 6 S. 2 IFG).

Der erforderliche Schutz der Betriebs- und Geschäftsgeheimnisse von Atos besteht auch nach Beendigung des Vertrags zwischen der BRAK und der Atos GmbH fort. Zum einen wurden die von Atos erstellten Sicherheitskonzepte insbesondere hinsichtlich der beA-spezifischen Ausführungen von Wesroc zunächst übernommen und dann weiterbearbeitet. Wesentliche Teile gelten somit fort. Zum anderen enthalten die Konzepte Atos-interne Regelwerke, die nicht nur für den Kunden BRAK gelten, sondern für sämtliche Geschäftsvorgänge von Atos. Mit diesen Sicherheitsbestimmungen und deren ständige Überprüfung ist Atos ein im Wettbewerb anerkannter Anbieter von IT-Infrastrukturleistungen, die besonderer Vertraulichkeit unterliegen. Eine Offenlegung der Sicherheitskonzepte würde die Wettbewerbsposition von Atos erheblich verschlechtern.

aa) In dem Dokument wird in Entsprechung einer vom BSI vorgegebenen Gliederung beschrieben, in welcher Weise das beA bei der Übermittlung und Speicherung von Daten Kryptographie verwendet. Es beschreibt die für beA konzipierte spezielle Umsetzung eines hybriden Kryptoverfahrens.

Das Kryptokonzept enthält einen Überblick über das Gesamtsystem. Wesentlicher Teil ist eine Vertraulichkeits-Integritätsanalyse und eine Kryptobedarfsanalyse, in der die Form der Datenerhebung, der Schadensszenarien, des Schutzbedarfs der Daten, des Schutzbedarfs der IT-Systeme inklusive der Netze und der Schutzbedarf der Rollen dargestellt werden. Ein weiterer Abschnitt enthält Angaben zur technischen Sicherheit unter Einbeziehung der kryptografischen Softwareprodukte, der kryptografischen Geräte und des Schlüsselmanagements. Schließlich ist die organisatorische Sicherheit unter Beschreibung der Einsatzumgebungen und -bedingungen der kryptografischen Produkte, die Absicherung der Standorte, der Einsatz und die Bedienung von kryptografischen Produkten und die Dokumentation dargestellt. Sicherheitspolitik und Sicherheitsregeln sind unter

Festlegung der Hauptverantwortlichkeiten, der Kontrolle der Sicherheitsmaßnahmen, der Informationsbeschaffung und der Protokollierung beschrieben.

Das Konzept enthält darüber hinaus einen Abschnitt zur Qualifikation und zur Schulung der Mitarbeiter und stellt in einem weiteren Abschnitt die Reaktion auf mögliche Verletzungen der Sicherheitspolitik dar. In diesem Zusammenhang wird der Ausfall von Kryptogeräten, vorsätzliche Handlungen und Evaluierungen beschrieben. Schließlich befasst sich das Kryptokonzept mit der Ausmusterung von Altgeräten, der Entsorgung von Speichermedien, den Umgang bei Garantiefällen, der regelmäßigen Anpassung an neue kryptografische Algorithmen und Schlüssellängen sowie Informationen für Endanwender.

bb) Das Kryptokonzept stellt das Herzstück des beA-Systems dar, indem es die Details der Kryptografie im Einzelnen beschreibt. Es handelt sich dabei um eine beA-spezifische Kryptografie, die Atos extra für das beA entwickelt hat. Damit liegen Betriebs- und Geschäftsgeheimnisse von Atos vor. Atos hat der Herausgabe des Kryptokonzepts in einem Drittbeteiligungsverfahren nicht zugestimmt.

Zu 6. Das Konzept für die Behandlung von Sicherheitsvorfällen vom 07.05.2019 („Security Incident Management Konzept“) kann wegen der durchgängig darin enthaltenen, spezifischen Informationen zum Procedere bei Eintritt eines Sicherheitsvorfalls nicht herausgegeben werden.

a) Das Konzept bezieht sich auf das Management von Sicherheitsvorfällen, von Datenschutzvorfällen sowie auf das Schwachstellenmanagement. Es liegen aufgrund der darin enthaltenen profunden Informationen Betriebs- und Geschäftsgeheimnisse (§ 6 S. 2 IFG) von Atos vor.

Der erforderliche Schutz der Betriebs- und Geschäftsgeheimnisse von Atos besteht auch nach Beendigung des Vertrags zwischen der BRAK und der Atos GmbH fort. Zum einen wurden die von Atos erstellten Sicherheitskonzepte insbesondere hinsichtlich der beA-spezifischen Ausführungen von Wesroc zunächst übernommen und dann weiterbearbeitet. Wesentliche Teile gelten somit fort. Zum anderen enthalten die Konzepte Atos-interne Regelwerke, die nicht nur für den Kunden BRAK gelten, sondern für sämtliche Geschäftsvorgänge von Atos. Mit diesen Sicherheitsbestimmungen und deren ständige Überprüfung ist Atos ein im Wettbewerb anerkannter Anbieter von IT-Infrastrukturleistungen, die besonderer Vertraulichkeit unterliegen. Eine Offenlegung der Sicherheitskonzepte würde die Wettbewerbsposition von Atos erheblich verschlechtern.

aa) Der Abschnitt „Einleitung“ des Konzepts erläutert den Zweck des Konzepts, nämlich u.a. den Umgang mit Sicherheitsvorfällen, und definiert, in welchem Bereich des Atos-internen Netzwerkes es bereitgestellt wird. Zudem sind in diesem Abschnitt referenzierte Dokumente, z.B. Atos-interne Handbücher zur Betriebsorganisation, genannt.

bb) Das Dokument beinhalt ein eigenes Kapitel mit Definitionen eines Informationssicherheitsvorfalls, einer Prozessübersicht inklusive der Beschreibung und Definition der Prozessschritte sowie der Darstellung der Rollen im Prozess. Auf dieser Grundlage werden die kundenspezifischen Vereinbarungen für Security Incidents beschrieben.

Im Folgenden wird die Schnittstelle zwischen dem Incidentmanagement zum Datenschutzvorfall-Management beschrieben. In diesem Abschnitt wird festgelegt, wie Datenschutzvorfälle zu behandeln sind, es werden Meldepflichten und -fristen statuiert sowie vorgegeben, auf welche Weise die Meldung des Vorfalls an den Auftraggeber zu erfolgen hat.

Der Abschnitt „Schnittstelle Incident Management zu Schwachstellenmanagement“ enthält ferner Ausführungen zur Erkennung von Schwachstellen sowie zur Analyse eröffneter Incidents. Es werden

präzise Regeln für den Fall aufgestellt, dass eine Schwachstelle erkannt wird. Es werden zudem in Tabellenform Beispiele für „Incident Classes“ bezüglich der Sicherheitsvorfälle genannt. Diesbezüglich werden dann Erläuterungen gegeben, welche Angriffe aufgrund des Vorfalles denkbar sind. In einer weiteren Tabelle wird nach Art des Datenschutzvorfalls differenziert und Beispiele für die jeweiligen Vorfälle dargestellt. In einer grafisch dargestellten Prozessübersicht wird die Behandlung von Sicherheitsvorfällen sodann nochmals detailliert beschrieben.

b) Auch für das Konzept zur Behandlung von Sicherheitsvorfällen gilt, dass es insgesamt Betriebs- und Geschäftsgeheimnisse (§ 6 S. 2 IFG) von Atos enthält, die Mitbewerbern und Konkurrenten die Übernahme der Arbeitsweisen und der Organisationsstruktur von Atos sowie die Einschätzung der damit einhergehenden Kosten und Aufwendungen von Atos ermöglichen würde. Atos hat im Drittbeteiligungsverfahren der Offenlegung des Konzepts zur Behandlung von Sicherheitsvorfällen nicht zugestimmt.

Die BRAK beabsichtigt indes, das Ergebnis der Prüfung der Konzepte durch die secunet AG offenzulegen, sobald das diesbezüglich durchgeführte Drittbeteiligungsverfahren abgeschlossen ist.

Mit freundlichen kollegialen Grüßen

[redacted]
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.