HEIDEMANN & DR. NAST

Heidemann & Dr. Nast · Kurfürstendamm 188 · 10707 Berlin

Anwaltsgerichtshof Berlin
Elßholzstraße 30/33
10781 Berlin

MARTIN HEIDEMANN
PATRICK HEIDEMANN
DR. MARCEL MESSERSCHMIDT
DR. ROLAND KÜHNE
NOTARE UND RECHTSANWÄLTE

KURFÜRSTENDAMM 188
10707 BERLIN
www.heidemann-drnast.de

BERLINER VOLKSBANK
IBAN: DE30 1009 0000 2298 0490 00
BIC: BEVODEBB

Berlin, den 18.11.2019
D47/21803

Aktenzeichen
10/18 A01 MH/En
(bitte stets angeben)

Sachbearbeiter/-in
Frau Engemann

Telefon 030 / 88 44 99 - 47
Telefax 030 / 88 25 435
engemann@h-drn.de

In dem Rechtsstreit
Heidemann u.a. ./. Bundesrechtsanwaltskammer
- I AGH 2/18 -

ist uns das Urteil des AGH vom 14.11.2019 (I AGH 6/18) zur Kenntnis gegeben worden. Im Hinblick auf die dortigen Ausführungen des Senates machen wir auf folgendes aufmerksam:

Die uns, der Öffentlichkeit und dem Gericht vorliegende Fassung des secunet-Gutachtens ist nicht die Originalfassung des Gutachtens. Nachdem secunet das Gutachten der Beklagten übergeben hatte, äußerte die Beklagte Änderungswünsche und ließ sie das Gutachten noch einmal umschreiben. Die vorliegende Fassung ist die nach den Wünschen der Beklagten umgeschriebene Fassung. Der Kläger zu 1) hat deshalb um Einsicht in der Originalfassung gebeten. Die Beklagte hat dies abgelehnt. Das Verwaltungsgericht Berlin hat die Beklagte mit dem in Kopie beigefügten **Urteil vom 26.06.2019 (VG 2 K 179/18)** verurteilt, dem Kläger zu 1) Einsicht in den Original-Abschlussbericht zu geben. Dieses Urteil ist noch nicht rechtskräftig. Die Beklagte hat die Zulassung der Berufung beantragt; das OVG hat über diesen Antrag noch nicht entschieden. Nach der Lebenserfahrung ist davon auszugehen, dass die Beklagte die Originalfassung des Gutachtens deshalb umschreiben ließ und sie deshalb geheim hält, weil sie Feststellungen enthält, die für sie nachteilig sind. Im Hinblick auf den Amtsermittlungsgrundsatz regen wir deshalb an, der Beklagten aufzugeben, die Originalfassung des Gutachtens vorzulegen.

Soweit der Senat in dem Urteil vom 14.11.2019 die Auffassung vertrat, dass sich aus dem secunet-Gutachten ergeben würde, dass das beA im Rechtssinne sicher sei, hat er entscheidende Teile des Gutachtens nicht berücksichtigt.

Wir hatten bereits im Schriftsatz vom 31.10.2018 aus dem Gutachten zitiert und weisen besonders auf folgende Punkte hin:

Zuallererst hat secunet gar nicht das real existierende beA und dessen Software und Hardware überprüft, sondern ausdrücklich eine Analyse nach Dokumentenlage durchgeführt (S. 12). Die Kläger müssen aber gegebenenfalls das real existierende beA benutzen, nicht das fiktive nach Dokumentenlage. Solange nicht überprüft wurde, ob das real existierende beA tatsächlich mit der Dokumentenlage übereinstimmt, prüft das Gutachten nur ein fiktives beA, nicht aber das real existierende. Im Hinblick auf das Verhalten von Atos in der Vergangenheit kann auch nicht davon ausgegangen werden, dass das real existierende beA zu 100 % identisch mit dem nach Dokumentenlage geforderten ist. Bekanntlich hat Atos vor dem secunet-Gutachten wiederholt behauptet, dass das beA völlig sicher sei und keine Sicherheitslücken aufweise. Das secunet-Gutachten hat eine Vielzahl fundamentaler und schwerwiegender Fehler aufgezeigt. Dies zeigt, dass ungeprüften Behauptungen von Atos nicht getraut werden kann. Dabei ist es unerheblich, ob dies auf Inkompetenz beruhte oder darauf, dass Atos die Beklagte bewusst getäuscht hatte. In jedem Fall waren die Erklärungen von Atos zur Sicherheit des beA falsch. Ohne Prüfung, dass das real existierende beA mit dem fiktiven der Dokumentenlage übereinstimmt, kann das Gutachten die Sicherheit des real existierenden beA nicht bestätigen.

Sodann hat secunet nur stichprobenartige Überprüfungen durchgeführt, um mit einem vertretbaren Aufwand möglichst viele Schwachstellen innerhalb des Betrachtungsbereichs zu identifizieren (S. 11). Dies bedeutet umgekehrt, dass erhebliche Teile des beA nicht überprüft worden sind und die nicht geprüften Teile noch eine Vielzahl weiterer Sicherheitslücken aufweisen können. Zumindest ist es nach der Lebenserfahrung äußerst unwahrscheinlich, dass wenn in einem komplexen System bei Stichproben Fehler gefunden werden, rein zufällig die Stichproben so ausgewählt waren, dass dort alle Fehler waren und alle nicht überprüften Teile des Systems fehlerfrei sind. Wenn jemand ein Schriftstück von 100 Seiten auf Schreibfehler überprüfen würde, indem er stichprobenartig zwei Seiten liest und auf diesen beiden Seiten mehrere Fehler findet, wäre es weltfremd, daraus abzuleiten, dass die 98 nicht geprüften Seiten fehlerfrei sein müssen oder dass das Gesamtschriftstück nach Korrektur der Fehler auf den zwei gelesenen Seiten insgesamt fehlerfrei sein müsse. Wie groß die Stichproben waren, ergibt sich aus dem Gutachten nicht und hat die Beklagte auch nicht anderweitig offengelegt. Es ist also auch möglich, dass in dem Beispiel nicht von zwei von 100, sondern von zwei von 10.000 Seiten hätte gesprochen werden müssen.

Dann hat secunet darauf hingewiesen, dass ein geschlossenes Sicherheitskonzept fehlt. Secunet hat deshalb ausdrücklich festgestellt:

> „*Dadurch war es nicht möglich, sich von der physikalisch-organisatorischen Sicherheit des beA und der vollständigen Abwehr alle nicht tragbaren Risiken zu überzeugen.*“ (Unterstreichung durch uns)

Entgegen der Auffassung des Senates hat secunet also gerade nicht festgestellt, dass das beA sicher sei, sondern im Gegenteil ausdrücklich festgestellt, dass es nicht möglich gewesen sei, sich von der Sicherheit zu überzeugen.

Secunet hat in dem Gutachten ferner ausgeführt:

> „*Der Missbrauch dieser Schlüssel kann auf zwei Arten geschehen: die Key Custodians des Auftraggebers und ein Helfer beim Betreiber des beA führen den verschlüsselten Nachrichtenbestand und die Schlüssel zusammen und sind dann in der Lage, die Nachrichten zu entschlüsseln. Oder es wurde unberechtigt beim Betreiber des beA nach der Erzeugung der Schlüssel vor der Übergabe an den Auftraggeber an einer Stelle eine Kopie erstellt. Dann kann das Personal des Betreibers alleine die Nachrichten entschlüsseln.*“ (S. 86)

Im Hinblick auf die erste Möglichkeit hat der Kläger zu 1) sich bemüht, bei der Beklagten in Erfahrung zu bringen, wer die Key Custodians sind. Die Beklagte hat eine dahingehende Auskunftserteilung mit der Begründung abgelehnt, dass deren Identität aus Sicherheitsgründen nicht offengelegt werden könne und sie der Bekanntgabe ihrer Identität widersprochen hätten. Es handele sich jedenfalls um Mitglieder der Geschäftsführung der Beklagten. Über die IFG-Klage des Klägers hat das VG Berlin noch nicht entschieden.

Andererseits hat die Beklagte in dem Rechtsstreit – I AGH 6/18 – mit dem Schriftsatz vom 11.04.2019 die Anlage B4 vorgelegt und dazu ausgeführt, dass dies ein Katalog von Fragen und Antworten sei, den Atos im Auftrag der Beklagten im Januar 2018 erarbeitet habe. Auf S. 7 oben der Anlage B4 wurden als Key Custodians benannt Herr Thomas Fenske, Frau Frederike Lummel, Herr Christopher Brosch und Frau Julia von Seltmann. Von diesen Personen ist nur Frau Julia von Seltmann Geschäftsführerin bei der Beklagten. Wir überreichen hierzu in der Anlage den **Schriftsatz der Beklagten vom 12.06.2019** und **unseren Schriftsatz vom 18.06.2019** an das VG Berlin (VG 2 K 85/18).

/
/

Im Hinblick auf das zumindest etwas seltsame und widersprüchliche Verhalten der Beklagten hinsichtlich der Identität der Key Custodians kann nach Auffassung der Kläger bereits die erste von secunet aufgezeigte Möglichkeit eines Missbrauches nicht „sicher“ ausgeschlossen werden. Drei der von der Beklagten gegenüber dem Senat be-

nannten Key Custodians sind entgegen ihren Behauptungen gegenüber dem Kläger zu 1) nicht Mitglieder ihrer Geschäftsführung. Dies muss aber nicht einmal vertieft werden.

Secunet hat nämlich auch die Möglichkeit aufgezeigt, dass beim Betreiber des beA nach der Erzeugung der Schlüssel und vor der Übergabe an den Auftraggeber (die Beklagte) eine Kopie erstellt worden sein könnte. Wenn eine Kopie erzeugt worden sein könnte, könnte auch eine Vielzahl von Kopien erzeugt worden sein. Das Kopieren elektronischer Daten geht schnell und mit minimalem Aufwand. Der Kläger zu 1) hat versucht bei der Beklagten in Erfahrung zu bringen, welche konkreten Sicherheitsmaßnahmen von der Beklagten seinerzeit getroffen wurden, um dieses Risiko auszuschließen, und welche natürlichen Personen an der Erzeugung der Schlüssel und deren Transport zur Beklagten beteiligt waren. Auch dazu erteilt die Beklagte keine bzw. keine ausreichenden Auskünfte. Sie hat sich offenbar einfach darauf verlassen, dass Atos und die mehreren tausend Mitarbeiter von Atos schon alles richtig machen würden. Wie das secunet-Gutachten in aller Deutlichkeit zeigt, ist ein solches Vertrauen in Kompetenz und Zuverlässigkeit von Atos und der mehreren tausend Mitarbeiter von Atos aber nicht angebracht. Das secunet-Gutachten hat an vielen Stellen aufgezeigt, das Atos weder ausreichend kompetent noch ausreichend zuverlässig war. Solange die Beklagte nicht darlegt und gegebenenfalls bewiesen wird, dass und wie sie dieses Risiko seinerzeit ausgeschlossen hat, ist die Benutzung des beA bereits deshalb mit einem nicht hinnehmbaren und unkalkulierbaren Sicherheitsrisiko behaftet.

Ein weiteres Risiko, das von secunet nicht geprüft wurde, weil dies nicht Auftragsgegenstand war, ergibt sich aus der Wartung der HSM. Die Wartung geschieht in der Weise, dass ein neues HSM in das Computerzentrum gebracht wird. Dann werden von Mitarbeitern von Atos die Schlüssel aus dem alten HSM in das neue HSM überspielt. Anschließend löschen Mitarbeiter von Atos die Schlüssel in dem alten HSM, wird dieses ausgebaut und zu Atos verbracht und kann gewartet und dann anderweitig verwandt. Nominell sind zwar die Key Custodians verantwortlich. Die Key Custodians zeichnen aber lediglich später entsprechende Arbeitsprotokolle ab. Sie sind weder vor Ort anwesend noch prüfen Sie in irgendeiner Weise, ob die von den Mitarbeitern von Atos erstellten Arbeitsprotokolle inhaltlich richtig sind. Insbesondere gibt es keinerlei Prüfung, ob die Löschung der Daten in dem alten HSM wirklich durchgeführt wurde und wirklich erfolgreich war. Nach den Angaben der Beklagten hat es bisher bereits zumindest einen Austausch von HSMs gegeben, bei dem so verfahren wurde. Im Hinblick darauf, dass das secunet Gutachten deutlich zeigt, von welcher Qualität die Arbeit von Atos war, kann auch insoweit nicht unterstellt werden, das Atos schon alles richtig machen wird und in der Vergangenheit immer alles richtig gemacht hat. Es gibt zumindest ein HSM außerhalb der gesicherten Computerzentren und in der Verfügungsgewalt von Atos oder mittlerweile Dritten, auf dem sich alle Schlüssel befanden und bei dem die Beklagte nicht

geprüft und mithin auch nicht festgestellt hat, dass die Schlüssel auch wirklich gelöscht sind. Auch dies ist ein nicht hinnehmbares und unkalkulierbares Sicherheitsrisiko.

Ein weiteres Sicherheitsrisiko ergibt sich daraus, dass weder die Beklagte noch secunet jemals geprüft haben, ob die verwandte Hardware wirklich den Spezifikationen entspricht. Es wäre technisch nicht besonders schwierig, in einem HSM einen mikroskopisch kleinen Chip einzubauen, der bei jedem Umschlüsselungsvorgang Nachricht und Schlüssel kopiert und entweder nach außen überträgt oder speichert, um dann bei der nächsten Wartung ausgelesen zu werden. Die Beklagte hat sich auch insoweit einfach blind darauf verlassen, dass Atos schon alles richtig und korrekt machen wird. Das secunet-Gutachten zeigt aber auch hinsichtlich dieses Risikos, dass ein solches Vertrauen in Kompetenz und Zuverlässigkeit von Atos nicht angebracht ist.

Wir weisen vorsorglich darauf hin, dass sich an diesen Risiken auch nichts dadurch ändert, dass die Beklagte jetzt einen neuen Betreiber ausgewählt hat. Wenn die Schlüssel jemals in der Vergangenheit kompromittiert worden sein sollten, sind sie für immer kompromittiert.

Beglaubigte und einfache Abschrift anbei

Martin Heidemann, Rechtsanwalt