Verwaltungsgericht Cottbus
Vom-Stein-Straße 27
03050 Cottbus
Telefax: 0355 4991-6499
Doppelte Ausführung
AZ: VG 8 K 556/21

Von:
Marcel Langner
[redacted]

Sehr geehrte Vorsitzende Richterin [redacted] sehr geehrte Kammer,
mich erreichte noch eine weitere Stellungnahme der LDA, die Sie in Anlage 1 finden. Mir ist wichtig, dass Ihnen alle Fakten transparent bekannt sind. Ich möchte die folgenden zwei Punkte ergänzen.

1. Gefahr immer noch nicht erkennbar
Immer noch vermag die Argumentation der Hochschule bezüglich des Gefahrenpotenzials der Offenlegung gesperrter Ports die LDA nicht zu überzeugen. Trotzdem erscheint ihr die Begründung formal als Ablehnungsgrund ausreichend zu sein. Sie weißt darauf hin, dass es nicht ihre Aufgabe ist, die Stichhaltigkeit der Begründung zu prüfen.

2. BVerwG 7 C 20.15
Ich hatte es versäumt in meiner Klageschrift direkt auf dieses Urteil einzugehen. Indirekt gehe ich jedoch vielfach darauf ein und greife vor allem die fehlende Konkretisierung an.
Der mir zentral zu untersuchende Aspekt scheint sich in folgendem Zitat des Gerichtes zu finden, den die Hochschule in dieser Vollständigkeit nicht erwähnt:

*„Die Feststellung der konkreten Möglichkeit nachteiliger Auswirkungen setzt voraus, dass die informationspflichtige Stelle **Tatsachen darlegt, aus denen sich im jeweiligen Fall** eine Beeinträchtigung des Schutzgutes ergeben kann. Diese Einschätzung kann insbesondere bei Vorgängen, die eine typisierende Betrachtungsweise ermöglichen, auch auf allgemeinen Erfahrungswerten beruhen.“*
(***Hervorhebung*** von mir)

Der für mein Verfahren „jeweilige Fall“ ist die fehlende Kenntnis darüber, welche Ports/IP Protokolle gesperrt sind. Es geht nicht um einen Fall der Kryptographie und die Gefährdung dieses speziellen auf elliptischen Kurven beruhenden Verfahrens. Es geht auch nicht (ganz abstrakt) um das Konzept des Kerckhoff’schen Prinzips.
Nach erneutem Studium des Schriftverkehrs erscheint mir auch noch unklar, was genau die Hochschule zu schützen gedenkt, bzw. wofür konkret sie eine Gefahr sieht. In ihrem Schreiben vom 23.02.2021 spricht sie vom Fall des Abhandenkommens von Daten und in ihrem Widerspruchsbescheid vom 26.04.2021 ganz allgemein von IT Systemen, ohne diese genauer zu spezifizieren.

Ich möchte versuchen meinen Fall auf das Urteil des BVerwG zu übertragen. Das ist in dem Sinne nicht ganz vergleichbar, da bereits die Kommunikationsrichtung eine andere ist. Ich frage nach Informationen über eine Kommunikationsrichtung von innerhalb der Behörde nach außen, während das Urteil die Richtung von außen nach innen in den Fokus nimmt.
Für meinen Fall könnte man jedoch so argumentieren, dass sich innerhalb der Behörde eine böswillige Person befindet, die Zugriff auf das Kommunikationsnetz (ein Telefon) hat. Die Argumentation der Hochschule greift nun nur, sofern man auch davon ausgeht, dass diese irgendwie in den Besitz zu schützender Daten gelangt ist. Diese böswillige Person ist im Gebäude der Behörde „gefangen“ und kann ihren Datenbestand nur über die Telefone nach außerhalb übertragen. Man könnte auch annehmen, dass

sie einer Ausgangskontrolle entgehen möchte und daher die Daten beim Verlassen des Gebäudes nicht bei sich tragen möchte.

Option 1
Der Person ist nun bekannt, dass bestimmte Telefonnummern nicht angerufen werden können. Sie kennt diese gesperrten Nummern jedoch nicht. Bekannt ist ihr jedoch, dass alle Nummern, die auf eine 8 enden angerufen werden können. Die Person wählt nun eine ihr als nicht gesperrt bekannte Nummer und überträgt darüber ihren Datenbestand. Die Daten sind abgeflossen, obwohl die gesperrten Ports nicht bekannt waren.
Option 2
Eine alternative Erklärung wäre das Vorhandensein eines grünen und eines roten Telefons. Während das rote Telefon nur Nummern anrufen kann, die der böswilligen Person nicht bekannt sind, kann das grüne Telefon quasi jedes andere Telefon der Welt erreichen, sofern die Telefonnummer nicht mit einer 8 endet. Das muss auch so sein, da auch die normalen Behördenmitarbeiter für ihre Kommunikation das grüne Telefon zwingend benötigen (und jeder auf der Welt weiß, dass es solche grünen Telefone gibt) und die im normalen Geschäftsbetrieb verwendeten Nummern nie auf einer 8 enden.

Auch eine erhöhte Gefahr einer böswilligen Person aktiv zu werden erschließt sich mir nicht, sofern diese die gesperrten Nummern erfährt oder dass es ein rotes Telefon überhaupt gibt. Es ist ihr ja trotzdem immer noch bekannt, dass es nicht gesperrte Nummern bzw. das grüne Telefon gibt und wird selbstverständlich von Anfang an diese nutzen.

Die Telefonanlage selbst kann nun mit (zumindest einem Teil) der von der Hochschule genannten IT Systeme verglichen werden. Wieso die Telefonanlage durch den Datentransfer/Anruf selbst gefährdet war erschließt sich mir nicht. Noch weniger, wie das Wissen um die gesperrten Rufnummern eine zusätzliche Gefährdung auslösen sollen, da über diese ja sowieso nicht kommuniziert werden kann und auch nicht wird.
Das ein Schadprogramm, sofern es sich innerhalb eines Netzwerkes befindet durch Ausnutzung weiterer (ganz anderer) Probleme in diesem Netzwerk weiteren Schaden anrichten kann sei unbenommen. Das Schadprogramm kann ja aber nicht dadurch in das Netzwerk der Hochschule gelangt sein, weil es Kenntnis über die gesperrten Ports/IP Protokolle hatte, die es sowieso nicht zur Kommunikation hätte nutzen können (Kausalitätsbruch). Die nicht explizit geäußerte Annahme, es würde seine Anwesenheit dadurch verraten, dass es versucht auf den gesperrten Ports zu kommunizieren, zeugt von fehlendem Verständnis über die Funktionsweise heutiger Angriffsszenarien. Wie dargestellt verwendet ein solches Schadprogramm immer die (jedem) bekannten Ports und IP Protokolle (grünes Telefon), um in der Masse der Verbindungen nicht aufzufallen. Ein Schutzkonzept dass darauf beruht, ein Schadprogramm ließe sich so erkennen und rechtzeitig eindämmen, muss dringend hinterfragt werden. Ähnliche Ansichten vertrat die Hochschule jedoch auch gegenüber der BNetzA und ihren Störungen gegen jede anderen WLAN Signale auf ihrem Gelände. Die BNetzA teilte diese Ansichten nicht.

Bleibt man so abstrakt wie die Hochschule, kann man letztlich jegliche Information so auslegen, dass sie eine Gefahr darstellen kann. Jede Ankündigung einer Kooperation in den News der Hochschule kann einen Angreifer anlocken, jeder Fachvortrag eines Hochschulmitgliedes, jeder Zuschlag einer Förderung, jede Kenntnis über die Inhalte eines Studienganges… Alle diese Information lassen irgendwie eine Situation konstruieren, aus der sich Gefahr ableiten lässt.

[redacted] 20.05.2021
[redacted]

Anlage 1: Stellungnahme der LDA vom 19.05.2021

WWW.LDA.BRANDENBURG.DE

Landesbeauftragte
für Datenschutz
und Akteneinsicht

LDA Brandenburg · Stahnsdorfer Damm 77 · 14532 Kleinmachnow

Bereich Recht

Herrn
Marcel Langner

Nur per E-Mail: [redacted]

Datum: 19. Mai 2021
Bearbeite[redacted]
Telefon:
Telefax:
Zeichen:
(Zeichen bei Antwortschreiben bitte angeben)

Ihr Antrag auf Informationszugang bei der TH Wildau vom 30. August 2020
Unsere E-Mail vom 30. März 2021, fragdenstaat.de (#196330)

Sehr geehrter Herr Langner,

wie wir Ihnen in unserer Nachricht vom 30. März 2021 mitteilten, haben wir die Technische Hochschule Wildau um eine erneute Überprüfung der Gründe für die Ablehnung Ihres Antrags auf Informationszugang im Hinblick auf die Fragen 4 und 5 (gesperrte Ports und IP-Protokolle sowie Gründe für die Sperrung) sowie um eine Beratung im Hinblick auf die Verzeichnisse der Verarbeitungstätigkeiten gebeten.

Im Ergebnis übersandte uns die Hochschule eine Kopie des an Sie gerichteten Widerspruchsbescheids vom 26. April 2021. Sie stützt sich nunmehr auf den Ablehnungstatbestand des § 4 Absatz 1 Nummer 4 Akteneinsichts- und Informationszugangsgesetz (AIG – erhebliche Gefahr für die öffentliche Sicherheit) sowie auf die Rechtsprechung des Bundesverwaltungsgerichts zu einem entsprechenden Ausnahmegrund des Informationsfreiheitsgesetzes. Darin sah das Gericht bereits die Verweigerung der Herausgabe dienstlicher Telefonnummern der Bediensteten von Jobcentern als von der Ausnahme zum Schutz der öffentlichen Sicherheit umfasst an. Inhaltlich bezieht sich die Technische Hochschule auf Ausführungen des Bundesamtes für Sicherheit in der Informationstechnik, denen entnommen werden könne, dass die Gefährdung von IT-Systemen steigt, wenn Kenntnisse über die Konstruktion, den Aufbau oder die Architektur bekannt sind. Außerdem informierte die Hochschule Sie über drei Verzeichnisse der Verarbeitungstätigkeiten, die sie Ihnen als Anlage zu dem Widerspruchsbescheid übersandt habe.

Ihren Antrag auf Informationszugang zu den Verzeichnissen der Verarbeitungstätigkeiten sehen wir damit als erfüllt an. Auch wenn uns die Argumentation der Technischen Hochschule bezüglich des Gefahrenpotenzials einer Offenlegung der Informationen über die gesperrten Ports und IP-Protokolle nicht restlos überzeugt, sind wir doch der Auffassung, dass die im Vergleich zu früheren Versionen wesentlich substantiierteren Ausführungen dem Begründungserfordernis des § 6 Absatz 1 Satz 8 AIG genügen.

Eine weitere Überprüfung fachlicher Grundlagen auf dem Gebiet der IT-Sicherheit wäre aus unserer Sicht angesichts der angeführten, hochrichterlichen Rechtsprechung bzw. der in Bezug genommenen Aussagen des Bundesamtes für Sicherheit in der Informationstechnik jedoch nicht zielführend. Sie würde zudem die auf das Informationszugangsrecht beschränkten Kompetenzen der Landesbeauftragten überschreiten. Wir bitten Sie daher um Verständnis, dass wir von weiteren Vermittlungsbemühungen gegenüber der Technischen Hochschule Wildau absehen. Dessen ungeachtet hoffen wir, Ihnen mit unserer Tätigkeit in Bezug auf die übrigen Aspekte Ihres Informationszugangsbegehrens weitergeholfen zu haben.

Mit freundlichen Grüßen

[redacted]