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, sehr geehrte Kammer,
mich erreichte am 28.07.2021 Ihr Schreiben vom 21.07.2021 mit Bitte um Stellungnahme.
Ich verstehe das Schreiben der Hochschule vom 20.07.2021 so, dass es als vollständige Auskunftserteilung der noch fehlenden Fragen gedacht war.
Es tut mir sehr leid, aber das sehe ich nicht so.

1. Berechtigte Zweifel am Wahrheitsgehalt der bisherigen Antworten

Aus dem Schreiben der Hochschule geht nun erstmalig hervor, dass diese (mindestens) Einschränkungen des Internetzugriffes auf Basis von, wie sie sie nennt, Reputationsfiltern vornimmt. Sie beschreibt diese zunächst so, dass das Kriterium für diese Filter die IP Adresse des betroffenen Rechnersystems im Internet ist. Ist also eine IP Adresse auf der Liste, ist ein Zugriff auf dieses Rechnersystem nicht mehr möglich (Sperrliste). Diese Aussage widerspricht den bisherigen Angaben der Hochschule, wonach diese bis jetzt angab keine Filterung auf Basis von IP Adressen vorzunehmen. Es ist bereits die zweite nachgewiesene unwahre Auskunft (nach der Behauptung es gäbe kein Verfahrensverzeichnis) der Hochschule in diesem Verfahren. Nach Durchsicht der Begründung der Hochschule: „Neubewertung der Gefahrenlagen“, wurden die bisherigen Auskünfte also nicht dergestalt beantwortet, dass die Informationen nicht herausgegeben werden, sondern dem Petenten wird mitgeteilt, dass diese nicht vorliegen. Ich kann hier grobe Fahrlässigkeit einfach nicht mehr glauben. **Ich möchte daher (erneut) meine berechtigten Zweifel am Wahrheitsgehalt auch der bisher erteilten Antworten auf meine Fragen mitteilen und beantrage, dass die Hochschule sich mit allen bisherigen Fragen erneut auseinandersetzt.** Ich erachte es als einen Verstoß gegen die Wahrheitspflicht, wenn beauskunftet wird, die Unterlagen lägen nicht vor, obwohl diese jedoch vorliegen. Ich verweise bezüglich dieser erneuten (fachgerechten) Befassung auf meine Ausführungen in 2.
Das angeblich kein niedergeschriebener Prozess existieren soll, wie diese Listen ausgewählt werden, wer diese festlegt, oder das irgendwo steht, welche Listen welches Anbieters genutzt werden, oder die konkrete Liste selbst nicht vorliegen soll kann ausgeschlossen werden. Ja bereits auch dadurch, dass die Hochschule Auskunft erteilt (anstatt direkte Einsicht in die Originalakte oder Kopie). Diese Auskunft, kann sie ja nur aus einer Akte haben. Die Hochschule hat mehrfach auf ihre Zertifizierung verwiesen und diese als Grund genannt genau diese Informationen angeblich nicht herausgeben zu können. Es ist aber gerade Ziel eben dieser Zertifizierung die Prozesse zu beschreiben und dokumentiert den sich ändernden Rahmenbedingungen anzupassen. Dieser Prozess muss daher im Rahmen der Zertifizierung dokumentiert sein. Ebenso liegen die Quellen der Filterlisten sicherlich in irgendwelchen Dateien oder Konfigurationsoberflächen vor, welche auch dem AIG zugänglich sind. Der TÜV Süd könnte hier als neutraler Zeuge fungieren, da dieser die Zertifizierung durchgeführt hat. Und natürlich können die vor Ort Bearbeitenden und Mitarbeiter des Hochschulrechenzentrums als Zeugen, unter besonderem Hinweis auf Ihre Wahrheitspflicht, zur Aufklärung beitragen.

2. Zweifel an fachlicher Eignung der Bearbeitenden

Zum wiederholten Male werden fachlich bereits üblich verwendete Begriffe in einer Art in einen Zusammenhang gebracht, der bei mir mehr Fragen aufwirft, als das diese geklärt werden. Ich habe daher

in Anlage 1 die hier in Frage stehenden Begriffe erläutert und in den Kontext gerückt, um ein gemeinsames Verständnis in den hoffentlich folgenden Auskünften der Hochschule herzustellen. Ich gehe im Folgenden von den in Anlage 1 gemachten Definitionen aus, die Sie auch so (mehr oder weniger) in den etablierten Fachbüchern finden.
Die Hochschule führt an, IP Listen zu verwenden. Also Listen, in denen sich IP Adressen befinden. Dementsprechend kann sie nur gesamte Rechnersysteme sperren; mit allen darauf laufenden Diensten und allen darauf angebotenen Webseiten und Domains. Das Sperren von spezifischen Webseiten oder Diensten ist damit nicht möglich, obwohl die Hochschule ihren zweiten Teilsatz so ausgestaltet, als würden die Sperrungen nur bestimmte Webseiten oder Dienste betreffen. Eventuell meint sie damit auszudrücken, dass sie die Kollateralsperren in Kauf zu nehmen gedenkt.
Es steht in der Tat zu vermuten, dass die Bearbeitenden hier mehr Informationen preisgeben, als intendiert. Nämlich, dass eben nicht nur IP Filterlisten verwendet werden, sondern auch Filterungen auf Inhaltsebene (Protokollebene III), die eine Sperrung spezifischer Webseiten oder Dienste erlauben würden und rechtsstaatlich noch bedenklicher einzustufen wären. Wie mit den nun im Verfahren widerlegten Aussagen, es gäbe kein Verfahrensverzeichnis und es gäbe keine IP Sperren, steht also auch hier anzunehmen, dass doch weitere Filterungen stattfinden, die auch dokumentiert sind. Mindestens in Konfigurationsdateien, weil das ja eingestellt werden muss. Filterlisten, wie hier von mir im Einsatz vermutet, gibt es in der Tat auch und sind auch recht einfach technisch zu implementieren.
Die Hochschule bringt nun erstmalig, jedoch typisch für Ihre Kommunikation auch in anderen Anfragen, wieder ein neues Argument als Begründung für die Nutzung von IP Filterlisten (die es ja ursprünglich garnicht gab). Dieser Begründung zur Nutzung von IP Filterlisten zum Schutz gegen den Missbrauch des Netzwerkes der Hochschule als Bot Netzwerk kann ich nur insoweit zustimmen, als sich die in den IP Filterlisten befindlichen IP Adressen, auf die sogenannten Command&Control Server beziehen. Das sind die zentralen Steuersysteme (von denen es üblicherweise mehrere gibt), die ein Bot Netzwerk zu bestimmten Aktionen veranlassen. Diese IP Adressen von Command&Control Servern können jedoch erst in die Liste aufgenommen werden, wenn diese erkannt wurden. Dann ist es jedoch bereits zum Erkennen des Bot Netzwerkes gekommen, ein Angriff hat also bereits stattgefunden oder das Bot Netzwerk wurde anderweitig aufgedeckt. Der Fall, dass sich Schadsoftware im Netzwerk der Hochschule befindet, welche nicht erkannt wurde und die Command&Control Server jedoch bereits auf den Sperrlisten sind aber auch noch aktiv, sehe ich nicht als sehr wahrscheinlich an. Erkannte Command&Control Server werden relativ schnell abgeschaltet oder wie kürzlich geschehen und ein Novum, durch Behörden übernommen.
Sollten Sie, wertes Gericht, hier einen Vorschlag haben, wie sichergestellt werden kann, dass meine Anfragen auch fachgerecht beantwortet werden, bin ich für Vorschläge offen. Die Hochschule hat nachweislich Fachexpertise, warum diese nicht eingebunden zu werden scheint, ist mir schleierhaft. Solche Fachexpertise besitzt zum Beispiel der Fachbereichsrat INW.

3. Unvollständigkeit

Auch sonst fehlen noch weitergehende Informationen, deren Inhalt ich jedoch als von mir in meinen ursprünglichen Fragen als erfasst ansehe.
Welche konkreten IPs werden gesperrt und Warum? Genau diesen konkreten von mir gestellten Fragen, die ja am wichtigsten sind, weil sie den Kern der grundrechtlichen Einschränkungen betreffen, entzieht sich die Hochschule, obwohl die Logik klar gebietet, dass die Information vorliegen und auch Teil einer Akte im Sinne des AIG ist.
Aufgrund der Formulierungen (siehe 2.) der Hochschule ist stark zu vermuten, dass weitere Filter auf Inhaltsebene (Dienste, Protokolle II/III) existieren und natürlich auch dokumentiert (z.B. durch Konfigurationsdateien) sind. Wobei ich generell auf meine Ausführungen von 1. bezüglich meiner Zweifel am Wahrheitsgehalt der bisherigen Antworten verweise. Ich bin für Vorschläge des Gerichtes offen, wie diese Zweifel, die mir mehr als begründet erscheinen, ausgeräumt werden könnten.
Ebenso weiß ich aus meiner Zeit an der Hochschule, dass zu dieser Zeit weit mehr Ports gesperrt waren, als der eine, den die Hochschule bisher angegeben hat. Besonders in Umgebungen, die im Rahmen von Lehre eingesetzt wurden und durch den vor Ort zuständigen IT Dienstleister bereitgestellt wurden, waren eine erhebliche Anzahl von Protokollen und Ports nicht nutzbar. Gleiches gilt für das

Studierendenwohnheim, wo mir entsprechende Beschwerden von Studierenden bekannt geworden sind. Sofern meine eigene Aussage dazu nicht ausreicht, schlage ich vor, die vor Ort ansässigen Bereichsadministratoren als Zeugen zu vernehmen. Ebenso Lehrpersonal, dass von solchen Sperrungen betroffen war. Aufgrund des bisherigen Verhaltens der Hochschulleitung in solchen Verfahren unter Wahrung der Anonymität der Zeugen (Ich verweise auf mein Arbeitsgerichtsverfahren).
Die Hochschule gibt hier lediglich über TCP Port 23 und den Dienst Telnet Auskunft. Diese „Feigenblattauskunft“ stellt sich mir so dar, als dass jedem Fachkundigen klar ist, dass der Dienst Telnet seit über 10 Jahren nicht mehr als Standard auf Rechnersystemen zum Einsatz kommt. In der Bekanntgabe demnach also wenig substantiell ist. Die von der Hochschule beschriebene Begründung der Sperrung kann ich inhaltlich nachvollziehen, ist praktisch jedoch ohne jede Relevanz, weil Telnet im Internet nicht mehr eingesetzt wird. So ist auch bei keiner anderen Hochschule, die ich in Anlage 10 meiner Klageschrift aufführte, Telnet für in das Internet gerichtete Verbindungen gesperrt. Auch meine Ausführungen in 2. wären eine mögliche Erklärung für diese Aussage der Hochschule.
Aber auch sonst passt die Erklärung logisch nicht, wobei dies für das Auskunftsverfahren unerheblich ist, aber erneut das geringe Fachwissen der Bearbeitenden aufzeigt. Wenn eine unverschlüsselte Verbindung aus dem Netz der Hochschule nach außen geht, inwiefern ist dann das Netz der Hochschule stärker gefährdet, als bei einer verschlüsselten? Es gibt auch viele andere Dienste, die ihre Daten unverschlüsselt senden. Es gibt hier lediglich einen einziges Szenario, welches mir dafür einfällt, wo ich einer Gefahr zustimmen könnte. Nämlich wenn Administratoren der Hochschule sich selbst per Telnet auf einem entfernten Rechnersystem einloggen (wollen) und zum (unverschlüsselten) Zugriff auf dieses Rechnersystem die gleichen Passwörter verwenden, wie sie auch für die Infrastruktur der Hochschule verwendet werden. Bei einer unverschlüsselten Verbindung sind dann nämlich sowohl das Passwort, als auch die Aktionen auf dem entfernten Rechnersystem durch einen Angreifenden mitzulesen und auch veränderbar. Damit ist die Sperrung dann natürlich sinnvoll, um eigene (eigentlich geschulte) Administratoren mit Zugriff auf kritische Passwörter daran zu hindern nach außen gerichtete Telnetverbindungen zu Systemen zu öffnen, die die gleichen Passwörter besitzen, also von eben jenen Administratoren auch so installiert worden sind.
Und letztlich sperren auch andere Hochschule wesentlich mehr Ports, wobei diese von sich aus öffentlich Auskunft geben. Es ist daher bei dem bisher offenbarten Habitus der Hochschule auch schon allein deswegen folgerichtig anzunehmen, dass nicht nur ein einziger (praktisch irrelevanter) Port gesperrt sein soll.

Über eine Filterung, wie sie hier bisher zu Tage getreten ist, wird nicht an der Hochschule informiert. Erstmalig in diesem Verfahren wird darüber überhaupt öffentlich bekannt.

Ich möchte mich erneut für meine umfangreichen Ausführungen entschuldigen, hoffe jedoch meine Sicht der Dinge dargelegt zu haben und die technischen Sachverhalte auch ausreichend genug in einen Rechtskontext gesetzt zu haben. Ich habe auch versucht klarzumachen, dass ich bei der Hochschule erhebliche Defizite auf mehreren Ebenen bei der Bearbeitung meiner Anfrage sehe und dementsprechendes Misstrauen hege.

Anlage 1: Begriffsdefinition
Ich beschränke mich in der Folge auf IPv4 (das aktuell am häufigsten verwendete Übertragungsprotokoll im Internet). Ich lasse einige Dinge weg, die mir für diesen Fall keine Relevanz zu scheinen haben.

IP Adresse
Diese ist üblicherweise mit einem Rechnersystem verknüpft. Sie macht überhaupt erst die Kontaktaufnahme über ein Datennetz möglich und entspricht in etwa der Postleitzahl einer Stadt. IP Adressen werden in lesbarer Form so dargestellt: X.X.X.X, wobei jedes X eine Zahl von 0 bis 255 darstellt z.B. 193.58.39.129.

Protokoll I
Mithilfe einer IP Adresse lassen sich bereits Daten mit einem anderen Rechnersystem austauschen. Wie dieser Austausch genau von statten geht ist im (konsequenterweise gleichnamigen) IP Protokoll festgelegt, bei dem die IP Adresse Teil der Definition ist. Es stellt das erste in einer ganzen Reihe von folgenden Protokollen dar. Tatsächlich ist es garnicht das erste, ich lasse die weiteren Ebenen jedoch weg, da sie mir für den hier relevanten Rechtskontext unerheblich erscheinen. Neben dem IP Protokoll, gibt es noch weitere, auch wenn das IP Protokoll heute wohl am verbreitetsten ist.
Das IP Protokoll erlaubt nur wenig. Man kann Datenpakete verschicken und man kann welche empfangen. Ob diese Pakete dann angekommen sind oder nicht, oder ob diese Veränderungen erfahren haben, weil z.B. Leitungsstörungen vorlagen ist mit diesem Protokoll nicht ermittelbar. Ähnlich einer visuellen Verbindung mit Rauchzeichen. Ob die Gegenstelle meinen Rauch überhaupt sehen kann, ist mir nur mithilfe von IP nicht zu ermitteln. Es konzentriert sich auf die Vermittlung der Pakete zum richtigen Empfänger.
Sperrungen auf dieser Protokollebene nutzen die IP Adresse als Filterkriterium.

Port/Portnummer (hier synonym)
Innerhalb einer Stadt werden verschiedene Dienstleistungen angeboten (z.B. Supermarkt, Friseur…). Dies ist auch für ein Rechnersystem der Fall. Auf solchen wird nur selten ein einziger Dienst angeboten. Um nun auf einen der Dienste eines Rechnersystems zuzugreifen, muss eine Portnummer genutzt werden. Dieser Port ist Teil einer Protokolldefinition (siehe Protokoll II). Portnummern sind für häufige/standardisierte Dienste weltweit festgelegt. Dies wäre in etwa mit einem Stadtbezirk vergleichbar, der eben in jeder Stadt Friseurbezirk heißt. Will ich einen Friseur in Anspruch nehmen, muss ich eben in diesen Bezirk mit diesem Namen
Port und IP Adresse werden bei jeder Verbindung zwischen Rechnersystemen benötigt, um dem entfernten Rechnersystem mitteilen zu können, welchen Dienst man überhaupt in Anspruch nehmen möchte. Ports sind letztlich lediglich Zahlen, die von 0 bis 65535 reichen. Beispielhaft sei Port 80 genannt, der für den Dienst der Auslieferung unverschlüsselter Webseiten festgelegt ist.

Protokoll II
Der zuvor eingeführte Begriffes des Ports ist im IP Protokoll selbst unbekannt. Dieser Begriff ergibt sich erst durch auf das IP Protokoll aufbauende Protokolle. Vergleichbar einer russischen Matroschka. Die äußerste Matroschka ist das IP Protokoll und transportiert innere (Daten). Das empfangene Rechnersystem öffnet die äußere Matroschka und schaut sich die darin liegende an. Je nach z.B. Farbe der Matroschka kann das empfangene Rechnersystem dann entscheiden, wie es mit der Matroschka/Datenpaket umgeht.
Diese zweite Matroschka/Protokollebene (nach IP) definiert Protokolle mit Namen wie TCP und UDP (wobei diese Liste nicht abschließend ist). TCP und UDP führen u.A. den Begriff des Ports ein. Ebenso erlauben sie weitere „Features“. So erlaubt TCP, dass sich Empfänger und Sender sicher sein können, dass ihre Datenpakete auch empfangen worden sind. Auf mein Beispiel zuvor zurückkommend verwendet der Dienst zur Auslieferung von unverschlüsselter Webseiten den TCP Port 80, eines bestimmten per IP Adresse ansprechbaren Rechnersystems. Aufgrund der starken Nutzung von TCP findet man auch häufig die Begriffskombination TCP/IP.

Sperrungen auf dieser Protokollebene nutzen als Filterkriterium den Protokolltyp (TCP,UDP) und/oder die Portnummer.

Protokoll III/Dienst
Sofern ein Rechnersystem Daten z.B. per TCP auf Port 80 erhält, wird es diese einer auf dem Rechnersystem laufenden Software übergeben, die diese Daten dann weiterverarbeiten kann. Da für TCP Port 80 festgelegt wurde, dass hier unverschlüsselt Webseiten angefragt werden können, wird auf Rechnersystemen dann eine Software installiert sein, die diese Aufgabe übernimmt. Man nennt diese Software dann üblicherweise Webserver. Oft, sofern das Rechnersystem vorrangig diese Aufgabe übernimmt, wird damit auch das gesamte Rechnersystem gemeint. Ich möchte es jedoch in der Folge als die Software verstanden wissen.
Wird dieser Software nun das empfangene Datenpaket zugereicht, so schaut sich diese Software dieses an. Und wir erreichen die Protokollebene III. In diesem Datenpaket muss nämlich vermerkt sein, welche Webseite oder welches Bild oder welches Video denn der Anfragende empfangen möchte. Dieses Protokoll wird HTTP genannt. Es ist seit jeher Teil einer Webseitenadresse (Synonym URL) und veranlasst Ihren Browser dazu, eben jene TCP Port 80 Verbindung zu verwenden.
Sperrungen auf dieser Ebene nutzen als Filterkriterium eine ganz bestimmte Webseitenadresse oder ganze Bereiche von Webseitenadressen. Da zu erkennen ist, dass für eine solche Filterung recht viele Matroschkas geöffnet werden müssen, nennt man eine solche Filterung auch Deep Paket Inspection oder Application Level Filterung, weil recht tief in die Protokollebenen des gesamten Datenpaketes hineingeschaut wird. Tatsächlich ist dadurch genau ermittelbar welche Person, welche Webseite wann besucht und was diese dort abruft.

Webseite
Eine Webseite ist letztlich nur ein Dokument auf einem Rechnersystem, auf dem der Dienst Webserver angeboten wird. Ein solches Dokument verweist auf weitere und ein Browser sorgt nun dafür diese weiteren beim Webserver anzufragen und baut daraus eine graphische Darstellung mit Bildern, Tönen und Videos zusammen. Der Begriff Webseite wird häufig im Sprachgebrauch als die gesamte Präsenz (bzw. Domain) einer Organisation verwendet. Letztlich besteht diese jedoch aus vielen Einzeldokumenten.

Domains
Da wir Menschen uns kontextlose Zahlen (IP Adressen) schlecht merken können, wurde ein weiterer Dienst etabliert. Dieser hat die Aufgabe IP Adressen in Namen umzuwandeln und umgekehrt. Diese Umwandlung findet automatisch durch das genutzte Betriebssystem statt, immer dann, wenn wir Namen statt IP Adressen verwenden. Dabei werden spezielle Rechnersysteme befragt, die eine Liste zusammensuchen können, bzw. diese vorrätig haben, welche IP Adresse welchem Namen zugeordnet ist. Im Übrigen werden dafür sowohl TCP als auch UDP verwendet und üblicherweise Port 53. Über diese Verbindung wird das DNS Protokoll „gesprochen“. Dieses besteht unabhängig von den anderen Protokollen, da ein Rechnersystem für einen Verbindungsaufbau keinen Namen verwendet, sondern IP Adressen. Es findet also immer zuerst eine Umwandlung eines Namens in eine IP Adresse statt, bevor eine Verbindung zum Zielrechnersystem aufgebaut wird. Diese Namen werden auch Domains genannt.
Sperrungen auf dieser Ebene nutzen den Namen als Filterkriterium und sind üblicherweise im DNS Dienst (DNS Sperren) implementiert. Hier verhält es sich in Verbindung mit einem Webserver so, dass ein Rechnersystem nicht nur eine Webseite eines einzigen Kunden ausliefern kann, sondern dies für unterschiedliche Kunden tun kann. Die Unterscheidung ist dann natürlich vorrangig der Domainname. Auch dieser ist daher Teil des zuvor angesprochenen HTTP Protokolls. In der Folge ist es dann eben auch so, dass wenn Filter auf IP Basis eingesetzt werden, alle Domains, die von einem auf dieser Basis gesperrten Rechnersystem ausgeliefert werden könnten gesperrt sind (Problem Overblocking), weil eben auf Protokollebene I gesperrt wurde. Das ist in der Vergangenheit auch bereits vorgekommen.