Verwaltungsgericht Cottbus
Vom-Stein-Straße 27
03050 Cottbus
Telefax: 0355 4991-6499
Doppelte Ausführung

K L A G E

des Herrn Marcel Langner, [redacted]

- Kläger -

g e g e n

Technische Hochschule Wildau, Hochschulring 1, 15745 Wildau, vertreten durch den Präsidenten, ebd.,

- Beklagte -

wegen: Akteneinsicht AIG Brandenburg

Ich erhebe Klage und beantrage:
Auskunft/Teilauskunft in den bisher abgelehnten/unbeantworteten Fragestellungen entsprechend der Klageschrift zu erteilen.
Die Beklagte trägt die Kosten des Verfahrens und Widerspruchsverfahrens.

1. Sachverhalt

Ich betreibe private Forschungen darüber, inwiefern Hochschulen in Deutschland im Rahmen der Erbringung ihrer IT Dienstleistungen Einschränkungen der Forschungs-, Wissenschafts- und Lehrfreiheit durchführen.
Ein Teilaspekt solcher Einschränkungen ist das Sperren bestimmter Ports und Dienste zum Zugriff auf Ressourcen vom Hochschulnetzwerk aus in das Internet.
Ich war selbst Betroffener aktiver, administrativer, intransparenter und auch rechtswidriger Einschränkungen, die meine eigene Forschung und Lehre eingeschränkt haben und will aus dieser Erfahrung heraus die Lage in Deutschland zu diesem Thema erforschen. Ich vertrete mich in diesem Erstinstanzlichen Verfahren selbst. Mein „Rechtswissen“ ist angelesen, ich bitte Sie um Nachsicht und den umfangreichen Schriftverkehr und Schreibstil. Eventuell fehlende Schriftstücke liefere ich bei Bedarf nach, können jedoch auch hier öffentlich und ohne Login: https://fragdenstaat.de/a/196330 eingesehen werden.

2. Bisheriger Verfahrensverlauf

Ich stellte am 30.08.2020 Antrag auf Aktensicht nach dem AIG (Anlage 1). Ich erhielt daraufhin den Bescheid der Hochschule vom 16.09.2020, in dem (bis auf eine) sämtliche meine Fragen abgelehnt wurden (Anlage 2).
Daraufhin bat ich am 18.09.2020 die Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht in Brandenburg um Vermittlung. Daraufhin erreicht mich der Änderungsbescheid der Hochschule vom 22.12.2020 (vermutlich als Ergebnis der Vermittlung der LDA, Anlage 3). In diesem rückte die Hochschule von vielen Teilen ihrer bisherigen Einschätzung ab. Gegen die noch verbleibenden nicht erteilten Auskünfte legte ich erneut Widerspruch am 11.01.2021 ein (Anlage 4). Auf meine Erinnerung an die Beantwortung meines Widerspruchs am 18.02.2021, erhielt ich den Bescheid der Hochschule vom 23.02.2021, der sich bezüglich der Ablehnungsgründe, wie der vorherige (Änderungs-)Bescheid verhält (Anlage 5). Am 15.03.2021 bat ich die LDA um fachliche Sachstandmeldung. In rechtlicher Unklarheit über den Stand des Vorverfahrens, legte ich am 22.03.2021 (erneut) umfangreich Widerspruch ein mit der Bitte um rechtsmittelfähige Bescheidung (Anlage 6). Am

30.03.2021 erreichte mich die Sachstandmeldung der LDA (Anlage 8). Am 29.04.2021 erreichte mich der belastende Widerspruchsbescheid der Hochschule vom 26.04.2021 (Anlage 7).

2. Fachliche Einschätzung

Sie finden meine konkreten fachlichen Einwände bezüglich der Sicherheitsbedenken der Hochschule in meinen Widersprüchen Anlage 4 und Anlage 6. Diese werden meiner Lesart nach fachlich von der LDA gestützt (Anlage 8).

Ich bezeichne mich selbst als einen in der technischen Materie Sachkundigen, bin jedoch, wie jeder andere Mensch, nicht unfehlbar. Ich rate deshalb an, einen unabhängigen Sachverständigen hinzuzuziehen, sofern die bereits dargelegten Belege nicht ausreichend scheinen oder weitere Einordnung/Bestätigung benötigen. Zusätzlich bietet sich an die Konferenz der Informatikfachschaften (KIF) zu kontaktieren und um Stellungnahme zu bitten (siehe Anlage 11).

Weitere Gegenbelege

Ich möchte hier noch zusätzlich auf Anlage 9 und 10 verweisen.
Dort habe ich Screenshots von Informationen von Unternehmen hinterlegt, die auf dem vergleichbaren Gebiet ISO27001 zertifiziert sind und Portsperren entsprechend der EU Telecom Single Market (TSM) Verordnung (EU) 2015/2120 angeben und wie solche Angaben aussehen. Sie widerlegen die Sicherheitsbedenken der Hochschule und die Behauptung eines Normverstoßes.
Ebenso habe ich eine Linkliste von Hochschulen hinterlegt, die die von mir erfragten Informationen öffentlich jedem zur Verfügung stellen. Ich habe auch die Größe dieser Hochschulen durch die Anzahl der dort Studierenden vermerkt. Die Anzahl der Studierenden sehe ich als Indiz für die Vergleichbarkeit der IT Komplexität und Angriffsfläche an. Die Technische Hochschule Wildau hat derzeit ca. 3500 Studierende. Weit weniger als jede der aufgelisteten Hochschulen.

3. Speziell zum Widerspruchsbescheid (Anlage 7)

Ergänzend zu den in meinen Erwiderungen bereits getätigten Ausführungen möchte ich folgendes zum Widerspruchsbescheid (Anlage 7) der Hochschule erwidern.

„Zitat“ des BSI

Die Hochschule führt eine Aussage des BSI an, welche im Rahmen einer von mir gestellten IFG Anfrage erfolgte und zieht daraus verschiedene Schlussfolgerungen, die ich so in ihrer Verallgemeinerung nicht teile und auch das BSI meiner Lesart nach nicht auszusagen gedachte.
In ihrem Widerspruchsbescheid schreibt die Hochschule:
„Sie begehren die Kenntnisse über gesperrte Ports. Jede Netzwerkkarte verfügt über eine eindeutig zugeordnete MAC-Adresse. Jeder Netzwerkkarte wird eine IP Nummer zugeordnet und konfiguriert, welche über insgesamt 65.5S5 Ports verfügt. Über diese Ports wird der Zugriff auf entsprechende Dienste gewährleistet.
Das BSI führt dazu aus:...“
Die hier als folgend dargestellten Ausführungen des BSI beziehen sich ***nicht*** auf die zuvor gemachten Angaben der Hochschule. Die Aussageveränderung durch Entfernung des Kontextes wird dann jedoch durch die Hochschule fortgeführt und durch Entfernung von Textpassagen noch verstärkt, so dass die Aussagen des BSI der Hochschulargumentation zuträglich werden. So schreibt die Hochschule:
„Nach dieser etablierten und weltweit anerkannten Methodik trägt aber eine verringerte Kenntnis über den TOE grundsätzlich dazu bei, Angriffe schwieriger zu machen und das entsprechende Angriffspotential einzuschätzen.“
Das BSI führt jedoch aus:
„Nach dieser etablierten und weltweit anerkannten Methodik trägt aber eine verringerte Kenntnis über den TOE grundsätzlich dazu bei, Angriffe schwieriger zu machen und das entsprechende ***Produkt als widerstandsfähig gegen ein bestimmtes*** *Angriffspotential einzuschätzen.“*

Die von mir fett hervorgehobene Passage führt genau jene Einschränkung in dieser Aussage ein, die die Hochschule in sämtlichen ihrer Aussagen vermissen lässt, symptomatisch für ihre gesamte Argumentation ist und auch von der LDA bemängelt wird. Nämlich konkrete Belege für ihre Aussagen bei Annahme des von ihr beschriebenen Angriffsszenarios. Ich kann mir für diesen „Zitierfauxpas“ grobe Fahrlässigkeit nur noch sehr schwer vorstellen. Die Hochschule ist nicht auf meine Anfrage an das BSI wie in Anlage 6 dargestellt eingegangen. Das BSI bestätigt für den hier konkret strittigen Fall, dass es keinerlei Unterlagen dahingehend vorliegen hat, dass die fehlende Kenntnis gesperrter Ports einen Sicherheitsgewinn erzeugen würde.

Kenntnis über den Prüfgegenstand=sichereres Produkt

Das BSI (bzw. die Prüfkriterien der Common Criteria) wählen zur Einschätzung der Sicherheit eines Prüfgegenstandes (neben vielen anderen Punkten) zwischen den Fällen aus, dass Wissen über dessen internen Aufbau/Struktur vorhanden ist, oder eben nicht. Man geht bei der Einschätzung der Widerstandsfähigkeit (je nach Angriffsszenario und Prüfziel) vom „worst case“ aus. Wenn man also einen Prüfgegenstand für einen bestimmten Angriffsfall testen möchte, und dieser dagegen in besonderem Maße sicher sein soll, ist der „worst case“ regelmäßig jener, bei dem der interne Aufbau/Struktur ***bekannt*** ist. Ein Prüfgegenstand ist in der Folge davon also umso sicherer gegen den spezifischen Angriffsfall geschützt, je mehr über den Prüfgegenstand bekannt ist (und dieser trotzdem sicher seinen Dienst erfüllt). Sofern die Hochschule vorgibt besonders sicher sein zu wollen, ist die Kenntnis über den Prüfgegenstand (hier also gesperrte und auch nicht gesperrte Ports) bei einer Prüfung eines konkreten Angriffsszenarios regelmäßig zu bejahen. Im Umkehrschluss kann ich ich also schlussfolgern, dass die Hochschule Sicherheit nur herzustellen vermag, wenn die gesperrten Ports nicht bekannt sind. Dies widerspricht jedoch den Anforderungen des IT Grundschutzes und der ISO27001, in welchem die Geheimhaltung solcher Informationen nicht gefordert wird. Ich kann mir daher nur eine fachliche Fehleinschätzung vorstellen.

Von der Hochschule beschriebenes Angriffsszenario, konkret

Ich möchte das von der Hochschule beschriebene Szenario einmal **konkret**, soweit wie ich es verstanden habe, durchspielen.

Schutzgut:

Dazu führt die Hochschule aus, dass es ihr um den Schutz davor geht, dass (zu schützende) Daten aufgrund eines Angriffes gegen die Hochschule in das Internet übertragen werden können (Anlage 5).

Prüfgegenstand:

Einstellungen der Netzwerkkomponenten, Dienste und deren Aufbau und Architektur bezüglich der Blockade von nicht autorisiertem Datenverkehr mit dem Internet.

Angriffsszenario:

Dies kann ich nur versuchen zu konkretisieren, da die Hochschule hier größtenteils abstrakt bleibt. Die Hochschule geht nicht von einem unkoordinierten Angriff aus, sondern von einem speziell auf sie vorbereiteten Angriff. Also inklusive der Vorbereitung der Angreifenden mit den öffentlich einsehbaren Informationen (weshalb sie ja auch meine Fragen nicht beantworten möchte). Ebenso gehen ich in dem Szenario davon aus, dass die Daten auf irgendeine nicht bekannte Weise durch z.B. ein Schadprogramm innerhalb der Hochschule bereits erlangt wurden und nun nur noch in das Internet übertragen werden müssen.

Erfolgseinschätzung bei fehlender Kenntnis gesperrter Ports:

Das Schadprogramm muss nun lediglich ***einen*** aus den von der Hochschule bereits zitierten 65535 Ports auswählen, mit dem es in das Internet kommunizieren kann. Es kennt die gesperrten Ports nicht. Ich führte bereits in Anlage 4 aus, dass jedoch bereits funktionsfähige Ports bekannt sind. Würden diese (auch sonst allgemein) bekannten Ports (z.B. 80,443) gesperrt werden, wäre ein Abruf von Webseiten nicht

mehr möglich. Ein Schadprogramm wird sich also immer darauf verlassen können, dass die genannten Ports nutzbar sind. In der Folge dieser (notwendigerweise) bekannten Information können die Daten abfließen.

Sachfremde Argumente
Aber auch sonst sind die Aussagen des BSI im gesamten Kontext des Dokumentes wesentlich differenzierter und scheinen durch die Bearbeitenden fachlich nicht durchdrungen worden zu sein. So führt das BSI Beispiele für und gegen die Argumentation des Kerckhoff'schen Prinzips aus. Es lässt sich also keine allgemeingültige Regel ableiten, sondern es ist immer der Einzelfall zu berücksichtigen. Im Übrigen spricht meiner Lesart nach das BSI genau deshalb immer im Konjunktiv (kann). Genau so verstehe ich gerade keine hinreichend sichere prognostische Einschätzung und mit regelmäßiger Wahrscheinlichkeit auftretende Situation.
So führt die Hochschule als sachfremdes Argument noch ein vom BSI genanntes Angriffsszenario an, bei dem mithilfe von Quantencomputern eine Verschlüsselung einfacher aufzubrechen ist, wenn Parameter elliptischer Kurven bekannt sind. Was das damit zu tun hat, ob die Sicherheit eines Netzwerkes/von Daten gefährdet ist, sofern bekannt wird welche Ports gesperrt sind, erschließt sich mir nicht.

Verfahrensbeschreibungen
Die als Verfahrensbeschreibung betitelten Unterlagen entsprechen meiner Einschätzung (inhaltlich) grundsätzlich nicht den Anforderungen an ein solches Dokument. Die LDA wird hier sicherlich eine ähnliche Einschätzung haben, sofern ihr diese vorgelegt werden. Sie geben keinerlei Auskunft, die für mich oder Betroffene der verarbeiteten Daten oder für die LDA als Kontrollbehörde hilfreich wären.

4. Allgemeines über das Verfahren bisher

Missverständnis §4 Abs. 1 Nr. 4 vs. §4 Abs. 2 Nr. 4
Ich habe tatsächlich versehentlich §4 Abs. 1 Nr. 4 angenommen, als ich meine ersten Schreiben verfasste. Die Hochschule begründet aber bis zum Widerspruchsbescheid meiner Lesart nach eindeutig immer mit §4 Abs. 2 Nr. 4 und meint auch diesen, da sie sich immer wieder auf ihren ersten Bescheid bezieht, bei dem sie zusätzlich die textuelle Beschreibung von §4 Abs. 2 Nr. 4 hinzufügte. Erstmalig im Widerspruchsbescheid führt sie §4 Abs. 1 Nr. 4 an. Vermutlich weil die LDA in ihrer Sachstandmeldung (Anlage 8) auf diesen Umstand hingewiesen hat. Die Hochschule behauptet jedoch (den Tatsachen widersprechend) bereits in ihren vorherigen Bescheiden §4 Abs. 1 Nr. 4 gemeint zu haben.

Fehlende Korrekturprozesse der Hochschule
Wenn ich mir im Vergleich die Bescheide der Hochschule vom 16.09.2020 (Anlage 2) und 22.12.2020 (Anlage 5) anschaue, dann fällt mir in der Rückschau umso mehr auf, wie unverständlich mir die erste Ablehnung erscheint. Man hätte doch erkennen müssen, dass zumindest Punkt 6. und 8. und 9. nichts darstellen, was überhaupt mit dem Netzwerk der Hochschule zu tun hat.
Bereits zu diesem Zeitpunkt hätte der Hochschule klar sein müssen, dass ihre bisherige Art der Bearbeitung nicht sachgerecht ist und durch Hinzuziehung von Fachexpertise zu verändern gewesen wäre.

Übliches „Lebensrisiko"
Und letztlich bleibt nur zu wiederholen, dass die Hochschule nicht konkret dargelegt hat, dass mit hinreichender Wahrscheinlichkeit der von ihr abstrakt dargestellte konstruierte Fall eintritt, bzw. jemals eingetreten wäre. Sie verwendet in diesem Zusammenhang ja auch immer wieder nicht belegte quantifizierende Worte. Mir sind keine Informationen darüber bekannt, dass aufgrund fehlender Kenntnis gesperrter Ports konkrete auf eine Einrichtung speziell vorbereitete Angriffe nicht erfolgreich oder weniger erfolgreich waren. Es ist mir auch nicht offensichtlich, dass dies so wäre, wie ich bereits zuvor

darlegte. Und auch alle von mir genannten Quellen, die Portsperren offenlegen, haben hier offensichtlich eine andere fachliche Einschätzung. Inklusive des Gesetzgebers EU.

Falschaussage
Nachdem zuerst darauf hingewiesen wurde, es gäbe überhaupt kein Verzeichnis von Verarbeitungstätigkeiten, zeigen die mir übermittelten Verfahrensbeschreibungen in ihren Überschriften das Gegenteil. Ebenso lässt die gleichartige Formatierung darauf schließen, dass eine einheitliche Vorlage zu existieren scheint oder eine Software verwendet wird. Zu existieren scheinen die Verfahrensbeschreibungen bereits seit 08.04.2019. Sie führen im Übrigen auch jene Informationen auf, die ich im Rahmen meines eigenen Konkretisierungsversuches genannt habe. Warum die Hochschule auch mit diesen von mir gelieferten Informationen dann vorerst nicht in der Lage war diese Verfahrensbeschreibungen zu ermitteln, bleibt mir unklar.

Kompromisse
Auf meinen Kompromissvorschlag in interner Zusammenarbeit mit den Gremien eine Teilauskunft zu erwirken, ist die Hochschule nicht eingegangen.

5. Was fehlt noch
Zweifel am Wahrheitsgehalt der bereits erteilten Auskünfte
In der Rückschau kann ich nur ernsthaft daran zweifeln, dass meine Anfrage fach- und sachgerecht bearbeitet wurde. Ich gehe aktuell mindestens von grober Fahrlässigkeit aus.
Dementsprechend kann ich auch bei den bereits beantworteten Fragen nicht davon ausgehen, dass diese den Tatsachen entsprechend beantwortet wurden oder die Bearbeitenden die notwendige Fachkenntnis besaßen. Da die Hochschule angibt ISO27001 zertifiziert zu sein, muss ich vom Vorhandensein einer solchen Fachkenntnis jedoch ausgehen.
Ich möchte Sie daher bitten zu prüfen, ob Sie es angesichts dieser Lage für angemessen halten, dass sich die Hochschule erneut auch mit den bereits beantworteten Fragen beschäftigt. Es liegen meiner Ansicht nach genug Anhaltspunkte vor, um eine solche Anordnung vornehmen zu können.

Gesperrte Ports
Ich möchte auch weiterhin wissen, welche Ports in welchen Netzsegmenten der Hochschule gesperrt sind und welche Gründe dafür vorliegen.

Gesperrte Protokolle
Auch wenn ich auf die gesperrten Protokolle nicht explizit eingegangen bin, so verhält es sich hier, wie mit den Ports. Auch diese wurden mir bisher nicht genannt.

Prozessbeschreibung wer, wie Sperrungen vornimmt
Die mir nicht nachvollziehbare Behauptung der Hochschule, es gäbe eine solche Beschreibung nicht habe ich bereits in meinem Widerspruch (Anlage 6) dargelegt. Ich begehre die Information weiterhin. Sie geht jedoch in ihrem Widerspruchsbescheid darauf nicht ein.

6. Hinweise zu den Gesamt- und Einzelumständen
Die Hochschule hat auch in der Vergangenheit bereits erfahren, dass ihre eigene Einschätzung bezüglich Fragen der Sicherheit nicht mit denen anderer übereinstimmt. So hat sie auf ihrem Gelände jahrelang sämtliche andere WLAN Signale mithilfe von aktiven Störabstrahlungen zu unterbinden versucht, bis dies (trotz vorheriger interner Beschwerden) durch die Bundesnetzagentur untersagt werden musste. Hier auch vor dem Hintergrund der Behauptung, dies aus Sicherheitsgründen durchführen zu müssen und mit der Bitte um stillschweigende Duldung gegenüber der BNetzA (BNetzA AZ: Berl8 D001/00658/18).
An der Abschaffung dieser jahrelangen Störmaßnahmen war ich, als damals noch Angestellter der beklagten Hochschule, maßgeblich beteiligt. In die darauf folgenden arbeitsgerichtlichen Auseinandersetzungen gewähre ich Einsicht, sofern das Gericht es für notwendig erachtet [redacted]

[redacted] z.b. weil die beklagte Hochschule hier versucht Zusammenhänge herzustellen, die mir nachteilig sein sollen.

7. Formale Einschätzung

In ihrem Widerspruchsbescheid beschäftigt sich die Hochschule nicht substanziell mit den von mir dargelegten Aussagen meiner Widersprüche. Allein aus diesem Grund empfand ich die Klage jetzt auch als angemessen. Sie hat sich also fachlich nicht mit meinen Argumenten auseinandergesetzt und wiederholt lediglich bereits Gesagtes mit anderen Worten. Ebenso werden neue Ablehnungsgründe aufgeführt, ohne jedoch auf die vorherigen einzugehen. So bleibt mir unklar, ob diese weiterhin Bestand haben oder sich die Meinung der Hochschule (erneut) geändert hat. Bereits deswegen hat die Hochschule aus meiner Sicht die Kosten des nicht fachgerecht durchgeführten Widerspruchsverfahrens zu tragen.

Ich denke alle Fristen eingehalten zu haben und alles mir mögliche getan zu haben, um Kompromisse zu erarbeiten. Die Hochschule selbst hat mir keine alternativen Vorschläge unterbreitet. Auf meine konkreten Vorschläge von Teilauskünften ist sie nicht eingegangen. Ich gehe im Moment davon aus, dass auch den Mitgliedern der Hochschule jegliche Informationen darüber, welche Ports/Protokolle aus welchen Gründen gesperrt sind verweigert werden.

Ich sehe aus Abwägungsgründen für zukünftige Mitglieder dieser Hochschule (was mich einschließt) die Frage vor Beginn eines Studiums oder einer Arbeit, ob nicht auch ein erhebliches und vor allem überwiegendes öffentliches Interesse daran besteht, ermitteln zu können, welche Möglichkeiten der Forschung an einem Hochschulstandort eingeschränkt werden, warum und in welchem Maße. Für mich überwiegt dieses Interesse bei weitem das für mich sowieso nicht existente Sicherheitsinteresse der Hochschule.

8. Ergebnis

Die Klage erachte ich als zulässig und begründet und hoffe durch meine Ausführungen auch zur konkreten Streitwertberechnung beigetragen zu haben.

[redacted] 08.05.2021

[redacted]

Marcel Langner

Anlage 1: Antrag nach AIG vom 30.08.2020
An:
Technische Hochschule Wildau
Die Präsidentin
Hochschulring 1
15745 Wildau
Fax: 03375 500 324

Von:
Marcel Langner
[redacted]

Betreff: Verletzung der Netzneutralität an der TH Wildau, Einschränkung der Wissenschafts- und Lehrfreiheit, Overblocking
Datum 30.08.2020
Mein Zeichen: #196330
Via Fax und Email
2 Seiten

Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG), BbgUIG, VIG

Sehr geehrte Damen und Herren,

bitte senden Sie mir Folgendes zu:

1. Eine Liste der Domains, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

2. Eine Liste der IP Adressen, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

3. Eine Liste der Dienste (z.B. realisiert über Deep Paket Inspection), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

4. Eine Liste der Ports (TCP, UDP), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

5. Eine Liste der IP Protokolle (z.B. IPSEC), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

6. Die Anzahl der Forderungen/Abmahnungen, seit dem Jahr 2015 für jedes Jahr als Summe aufgelistet, von Rechteinhabern oder anderen gegen die Hochschule, die die Hochschule dazu veranlasst hat, bestimmte Netzsperren einzurichten und welche Netzsperren daraufhin eingerichtet wurden.

7. Die Prozessbeschreibung zum Einrichten, Prüfen und wieder Entfernen von Netzsperren jeglicher Art (z.B. Wer entscheidet, Wer verantwortet, Gremienbeteiligung).

8. Anweisungen/Dienstanweisungen/Ordnungen usw., die den Zugang zu bestimmten Seiten untersagen (z.B. Verbot des Besuches von Seiten mit bestimmten Inhalten).

9. Anzahl meldepflichtiger Datenschutzvorfälle, die im Zusammenhang mit den eingerichteten Netzsperren stehen.

10. Sämtliche Verfahrensverzeichnisse, es fallen ja zweifelsohne personenbezogene Daten an, die im Zusammenhang mit allen zuvor genannten Fragen stehen.

Dies ist ein Antrag nach dem Akteneinsichts- und Informationszugangsgesetz Brandenburg (AIG), dem Brandenburgischen Umweltinformationsgesetz (soweit Umweltinformationen betroffen sind) und dem Verbraucherinformationsgesetz (soweit Verbraucherinformationen betroffen sind).

Sollte dieser Antrag Ihres Erachtens gebührenpflichtig sein, bitte ich Sie, mir dies vorab mitzuteilen und dabei die Höhe der Kosten anzugeben. Meines Erachtens handelt es sich bei dieser Anfrage um einen einfachen Fall, der darum nach der Akteneinsichts- und Informationszugangsgebührenordnung (AIGGebO) kostenfrei zu beantworten ist.

Mit Verweis auf § 6 Abs. 1 AIG möchte ich Sie um eine unverzügliche Antwort bitten, spätestens aber innerhalb eines Monats.
Sollten Sie für diesen Antrag nicht zuständig sein, bitte ich Sie, ihn an die zuständige Behörde weiterzuleiten und mich darüber zu unterrichten. Ich widerspreche ausdrücklich der Weitergabe meiner Daten an sonstige Dritte.

Mit Verweis auf AIG §7 Abs. 3 möchte ich Sie hiermit um eine Antwort per E-Mail bitten. Ich möchte Sie um eine Empfangsbestätigung bitten und danke Ihnen für Ihre Mühe!

Mit freundlichen Grüßen

Marcel Langner

Anlage 2: Bescheid der Hochschule vom 16.09.2020

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

TH Wildau Hochschulring 1 15745 Wildau

Herrn
Marcel Langner
[redacted]

[redacted]
www.th-wildau.de

Wildau, 16. September 2020
Ihr Zeichen #196330 | *Unser Zeichen*

Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG), BbgUIG, VIG
Ihr Antrag vom 30. August 2020

Sehr geehrter Herr Langner,

Sie begehren mit Ihrem o.g. Schreiben Auskunft wie folgt:

1. Eine Liste der Domains, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

2. Eine Liste der IP Adressen, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

3. Eine Liste der Dienste (z.B. realisiert über Deep Paket Inspection), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

4. Eine Liste der Ports (TCP, UDP), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

5. Eine Liste der IP Protokolle (z.B. IPSEC), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

6. Die Anzahl der Forderungen/Abmahnungen, seit dem Jahr 2015 für jedes Jahr als Summe aufgelistet, von Rechteinhabern oder anderen gegen die Hochschule, die die Hochschule dazu veranlasst hat, bestimmte Netzsperren einzurichten und welche Netzsperren daraufhin eingerichtet wurden.

7. Die Prozessbeschreibung zum Einrichten, Prüfen und wieder Entfernen von Netzsperren jeglicher Art (z.B. Wer entscheidet, Wer verantwortet, Gremienbeteiligung).

8. Anweisungen/Dienstanweisungen/Ordnungen usw., die den Zugang zu bestimmten Seiten untersagen (z.B. Verbot des Besuches von Seiten mit bestimmten Inhalten).

9. Anzahl meldepflichtiger Datenschutzvorfälle, die im Zusammenhang mit den eingerichteten Netzsperren stehen.

10. Sämtliche Verfahrensverzeichnisse, es fallen ja zweifelsohne personenbezogene Daten an, die im Zusammenhang mit allen zuvor genannten Fragen stehen.

Gemäß § 4 Abs. 2 Nr. 4 AIG soll ein Antrag auf Akteneinsicht abgelehnt werden, wenn die ordnungsgemäße Erfüllung der Aufgaben der öffentlichen Stelle erheblich beeinträchtigt würde.

Die von Ihnen erbetenen Informationen werden - mit Ausnahme Nr. 7 - als relevant für die IT-Sicherheit eingestuft. Der öffentliche Zugang zu diesen Informationen ist zwingend zu vermeiden, um die IT-Sicherheitsinfrastruktur sowie die verarbeiteten Daten zu schützen.

Unzweifelhaft überwiegt hier auch das öffentliche Interesse, nämlich der Schutz verarbeiteter Daten sowie der Aufrechterhaltung der IT-Infrastruktur der TH Wildau gegenüber dem Interesse an der Einsichtnahme.

Zu 7.) Eine entsprechende Prozessbeschreibung liegt nicht vor.

[redacted]

Anlage 3: Änderungsbescheid der Hochschule vom 22.12.2020

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

TH Wildau Hochschulring 1 15745 Wildau
Herrn
Marcel Langner
[redacted]

[redacted]
www.th-wildau.de

Wildau, 22. Dezember 2020
Ihr Zeichen | *Unser Zeichen* #196330

Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG), BbgUIG, VIG
Antrag vom 30. August 2020, Unser Schreiben vom 16. September 2020

Sehr geehrter Herr Langner,

Bezug nehmend auf Ihren o.g. Antrag ändern wir unseren Bescheid vom 16. September 2020 wie folgt:

1. Eine Liste der Domains, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor.

2. Eine Liste der IP Adressen, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor.

3. Eine Liste der Dienste (z.B. realisiert über Deep Paket Inspection), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor.

4. Eine Liste der Ports (TCP, UDP), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Ihr Antrag wird gemäß § 4 Abs. 2 Nr. 4 AIG abgelehnt.

Die Technische Hochschule Wildau ist ISO 27001 zertifiziert. Diese Zertifizierung setzt eine genau definierte Dokumentenlenkung voraus, welche den Abfluss an Informationen steuert. Für das Informationssicherheitsmanagementsystem der TH Wildau (ISMS) gibt es daher genaue Festlegungen zur Dokumentenlenkung. Diese basieren auf der ISO 27001:2013, Abschnitt 7.5 Dokumentierte Informationen, insbesondere 7.5.3 Lenkung dokumentierter Informationen. Diese laut ISO 27001:2013 geforderte Festlegungen haben das Ziel, Informationen zu schützen, die für die Informationssicherheit gesonderte Priorität haben. Weiterhin ist in der Norm festgelegt Schutzklassen zu bilden, in die Informationen und die dazu beschriebenen Unterlagen eingeordnet werden.

Die in Punkt 4 und 5 angefragten Inhalte haben eine höhere Schutzklassifizierung und dürfen nicht zugänglich gemacht werden.
Technisch weiterführende Beschreibungen der angefragten Inhalte bergen die Gefahr, die Sicherheit der Infrastruktur und damit schützenswerten Informationen der TH Wildau zu gefährden und führen bei Weitergabe zu einem Normverstoß.

5. Eine Liste der IP Protokolle (z.B. IPSEC), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Ihr Antrag wird gemäß § 4 Abs. 2 Nr. 4 AIG abgelehnt. Begründung siehe 4.

6. Die Anzahl der Forderungen/Abmahnungen, seit dem Jahr 2015 für jedes Jahr als Summe aufgelistet, von Rechteinhabern oder anderen gegen die Hochschule, die die Hochschule dazu veranlasst hat, bestimmte Netzsperren einzurichten und welche Netzsperren daraufhin eingerichtet wurden.

Es liegen keine entsprechenden Fälle vor.

7. Die Prozessbeschreibung zum Einrichten, Prüfen und wieder Entfernen von Netzsperren jeglicher Art (z.B. Wer entscheidet, Wer verantwortet, Gremienbeteiligung).

Eine entsprechende Prozessbeschreibung liegt nicht vor.

8. Anweisungen/Dienstanweisungen/Ordnungen usw., die den Zugang zu bestimmten Seiten untersagen (z.B. Verbot des Besuches von Seiten mit bestimmten Inhalten).

Die Regelungen befinden sich in der Amtlichen Mitteilungen 06/2000. Die Satzung ist abrufbar unter: https://www.th-wildau.de/hochschule/zentrale-einrichtungen/hochschulrechenzentrum/satzungen-nutzungsordnungen/

9. Anzahl meldepflichtiger Datenschutzvorfälle, die im Zusammenhang mit den eingerichteten Netzsperren stehen.

Der Datenschutzbeauftragte der TH Wildau teilte mit, dass ihm keine entsprechenden Datenschutzvorfälle bekannt.

10. Sämtliche Verfahrensverzeichnisse, es fallen ja zweifelsohne personenbezogene Daten an, die im Zusammenhang mit allen zuvor genannten Fragen stehen.

Ihre Anforderung ist unkonkret gefasst. Des Weiteren teilen Sie mit, dass „zweifelsohne" personenbezogene Daten „anfallen". Die von Ihnen erbetenen Informationen sind hinreichend zu konkretisieren. Dabei ist auch die Aussage „es fallen ja zweifelsohne personenbezogene Daten an" in die Konkretisierung mit

einzubeziehen. Ich gehe davon aus, dass Sie für die Konkretisierung Ihrer Anfrage unsere Antworten zu den Fragen 1. bis 9. einbeziehen.

Gemäß § 6 Abs. 1 a.E. AIG weise ich Sie darauf hin, dass jede Person gemäß § 11 Abs. 2 Satz 1 AIG das Recht hat, die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht anzurufen.

Für Rückfragen stehen wir Ihnen selbstverständlich sehr gerne zur Verfügung.

Mit freundlichen Grüßen

[redacted]

Anlage 4: Widerspruch vom 11.01.2021 gegen Änderungsbescheid vom 22.12.2020

Präsidentin der Technischen Hochschule Wildau
Senat der Technischen Hochschule Wildau
z. Hd. U. Tippe
Hochschulring 1
15745 Wildau
Fax: 03375 500 324

Marcel Langner
[redacted]

Betreff: Verletzung der Netzneutralität an der TH Wildau, Einschränkung der Wissenschafts- und Lehrfreiheit, Overblocking
Datum 15.01.2021
Mein Zeichen: #196330
Via Fax und Email
3 Seiten

Sehr geehrte Damen und Herren,
ich wünsche uns allen ein gesundes und erfolgreiches gemeinsames 2021.
Es ist mir nicht entgangen, dass Sie in Ihrem letzten Schreiben erstmalig darauf hingewiesen haben, für Rückfragen selbstverständlich sehr gern zur Verfügung stehen. Ich wünsche mir, auch auf zukünftig gerichtete Anfragen, dass dieses Angebot auch durch entsprechenden Taten untermauert wird und wir nicht jedes einzelne Mal die LDA bemühen müssen, die auch nicht zu wenig Arbeit hat.

Inzwischen haben Sie mit Ihrem Schreiben auf einen Teil meiner Fragen zu meiner Zufriedenheit geantwortet. Strittig erscheint mir nun nur noch eine Auskunft darüber, welche konkreten Ports/Protokolle/Dienste gesperrt sind. Ebenso konnte ich lesen, dass Ihnen noch Informationen darüber fehlen, in welche konkreten Verfahrensverzeichnisse ich Einsicht wünsche.

Auskunft über konkrete gesperrte Ports/Protokolle/Dienste
Ich kann hier zwei Argumentationslinien erkennen. Zum einen die Einstufung von vorhandenen Dokumenten und zum anderen den Ablehnungsgrund nach § 4 Abs. 2 Nr. 4 AIG.

Einstufung der Dokumente
Letztlich sehe ich die Einstufung von Dokumenten als (mehr oder weniger) willkürlich an, sofern die Kriterien nicht offengelegt werden und nachprüfbar sind. Auch eine ISO27001 Zertifizierung nimmt nur stichprobenartige Prüfungen vor. Der TÜV schreibt dazu auf seiner Webseite: *„Das Prüfzeichen gilt nicht: für die Qualität der Produkte und Dienstleistungen sowie die Informationssicherheit an sich.“* und weiter: *„Das Prüfzeichen gilt: für die Befähigung einer Organisation, Informationen sicher zu handhaben.“*
Die Zertifizierung stellt lediglich sicher, dass der Zertifizierte einen entsprechenden Prozess vorhält, um Informationen sicher zu handhaben und auf entsprechende Veränderungen zu reagieren. Ob die konkret getroffenen Entscheidungen angemessen sind, wird gerade nicht zertifiziert. Dementsprechend ist auch die Herausgabe (nach sowieso höherrangigem Recht) eines auf selbst eingeschätzten Sachverhalten eingestuftes Dokument, kein Normverstoß. Die Einschätzung kann jederzeit ohne Verlust der Zertifizierung angepasst werden. Tatsächlich ist dafür sogar ein Prozess vorgesehen, der Teil der Zertifizierung ist.

Daraus folgend ist deshalb nur, weil ein Dokument z.B. als VS – nur für den Dienstgebrauch oder höher eingestuft ist (oder irgendeiner anderen Einstufungsrichtlinie z.B. ISO 27001), dies nicht gleichbedeutend damit, eine Anfrage abzulehnen oder eine Begründung dafür. In dem Sinne hat auch bereits das BVerwG 7 C 21.08 vom 29.10.2009 entschieden: *„Der Anspruch auf Zugang zu einer Information ist nicht allein deshalb nach § 3 Nr. 4 IFG ausgeschlossen, weil die Information formal als Verschlusssache eingestuft ist. Vielmehr kommt es darauf an, ob die materiellen Gründe für eine solche Einstufung vorliegen.“*
Hier zwar auf das IFG bezogen, das jedoch gleichlautend dem AIG ist und letztlich würde ja auch ein Rechtsverfahren dort landen. In diesem Sinne wird erst durch ein Gericht oder externe Sachverständige zu klären sein, ob diese materiellen Gründe hier vorliegen.

Ablehnungsgrund nach § 4 Abs. 2 Nr. 4 AIG
Somit ist einzig ein Ablehnungsgrund nach AIG rechtlich für mich (und sicherlich auch einem Gericht) relevant.
Nr. 4 enthält mehrere Aspekte der Ablehnung. Ich konnte nicht erkennen, auf welchen Sie sich hier berufen. Mir erscheint jedoch ausschließlich der Aspekt der Gefahrenabwehr relevant. Hier vor allem im Kontext der Aufrechterhaltung des ordnungsgemäßen Dienstbetriebes, was ich jedoch nur vermuten kann.
In der Interpretation der Ablehnung gehe ich davon aus, dass Sie der Auffassung sind, dass es bei Bekanntgabe der Informationen zu einer Beeinträchtigung von nicht näher genannten „Dingen“ kommen kann. Leider reicht mir das als Begründung nicht ganz aus. Weil auf einer solch unkonkreten Aussage quasi alles ablehnbar ist.
Mir sind keine Studien oder ähnliches bekannt, die nachweisen würden, dass es bei dem Wissen darum, welche Ports/Protokolle/Dienste in einem Netzwerk gesperrt sind, zu einer erhöhten oder erstmaligen Gefahr irgendeiner Art kommen kann. Dass die Sperrung bestimmter Ports/Protokolle/Dienste bestimmte Gefahren abmildern (aber nicht verhindern) kann, dem kann ich zustimmen. Das Wissen oder Nichtwissen um diese Sperrungen hat darauf jedoch keinen nachgewiesenen Einfluss.
Heutige (und auch bereits vergangene) Angriffsszenarien beschränken sich nicht auf bestimmte Ports/Protokolle/Dienste. Eine Sicherheitsstrategie die darauf setzt, die Kenntnis über die konkreten Sperrungen geheimzuhalten, und dadurch auf dessen Wirksamkeit vertraut, setzt meiner Einschätzung nach nicht den Stand der Technik nach DSGVO Art. 32 ein. Dieses Konzept der Security through Obscurity wird von einem Großteil der Sicherheitsexperten abgelehnt. So ist es auch nicht verwunderlich, dass viele Hochschule mit wesentlich größeren Netzwerken und damit auch wesentlich größerem Angriffsfeld, klar angeben, welche Ports/Protokolle/Dienste in ihren Netzen aus welchen Gründen gesperrt sind. Die Experten dieser Hochschulen scheinen also eine andere Sicherheitsauffassung zu vertreten.
Im übrigen sieht auch die Rechtsstelle des DFN in ihrem Rechtsbrief 10/2018 Sperrungen von Ports/Protokollen/Diensten sehr kritisch. Jede Sperre stellt dahingehend eine Einschränkung der Wissenschaftsfreiheit dar. Dementsprechend bedarf es auch einer entsprechend starken Begründung, sofern ein grundrechtlich geschütztes Gut eingeschränkt wird. Zu Ihrer Information möchte ich Ihnen die vielzitierte Entscheidung des VGH Mannheim zum Alkoholverbot in Teilen der Freiburger Innenstadt (Urteil vom 28.07.2009 – 1 S 2200/08) bezüglich dem Begriff der abstrakten Gefahr zur Kenntnis geben:

> *„[…] eine abstrakte Gefahr ist gegeben, wenn eine generell-abstrakte Betrachtung für bestimmte Arten von Verhaltensweisen oder Zuständen zu dem Ergebnis führt, dass mit hinreichender Wahrscheinlichkeit ein Schaden im Einzelfall einzutreten pflegt und daher Anlass besteht, diese Gefahr mit abstrakt generellen Mitteln, also einem Rechtssatz, zu bekämpfen. Auch die Feststellung einer abstrakten Gefahr verlangt mithin eine in tatsächlicher Hinsicht genügend abgesicherte Prognose: es müssen – bei abstrakt-genereller Betrachtung – hinreichende Anhaltspunkte vorhanden sein, die den Schluss auf den drohenden Eintritt von Schäden rechtfertigen. Der Schaden muss regelmäßig und typischerweise, wenn auch nicht ausnahmslos, zu erwarten sein.“*

Einer negativen Prognose (mögliche erstmalige oder erhöhte oder erfolgreichere Angriffe) mangelt es an hinreichenden Anhaltspunkten. Nur noch zusätzlich sehen es die vielen anderen Hochschulen offensichtlich anders.

Letztlich kann ich aber auch der Logik der Argumentation nicht folgen. Ist es in Ihrer Sichtweise nicht viel gefährlicher, wenn stattdessen bekannt wäre, was **nicht** gesperrt ist? Genau das ist ja aber bereits (mehr oder weniger) bekannt. So ist in den Eduroam Policies beschrieben, welche Ports/Protokolle/Dienste nicht gesperrt werden dürfen. Zumindest das hätten Sie doch als Teilauskunft „gefahrlos" beantworten können, dass Sie sich an diese Vorgaben auch halten. Ebenso bekannt ist, dass Ports 80 und 443 nicht generell gesperrt sind bzw. über einen Proxy erreichbar sind. Jeder vermeintliche Angreifer kann sich nun also darauf verlassen, diese Ports/Protokolle/Dienste für einen Angriff verwenden zu können. Seit Jahren! Welchen vermeintlichen Sicherheitsmehrwert hat dann die Geheimhaltung der gesperrten Ports/Protokolle/Dienste?

Eventuell lässt sich hier jedoch ein Kompromiss finden. Wie wäre denn eine Teilauskunftserteilung, indem nur für bestimmte Kategorien/Klassen von Netzen, die von einem größeren Personenkreis auch genutzt werden (z.B. Eudroam, Übungslabore, Wohnheim usw.) eine Liste bekannt wäre, auf was man sich dort als funktionierend bzw. gesperrt verlassen kann? Mich interessiert ja nicht wirklich jedes einzelne VLAN, welches es gibt. Spannend wären jene Netze, auf welche ich als Student üblicherweise auch angewiesen wäre. Eventuell kann diese Liste mit den Bedürfnissen der beiden Fachbereiche und der Studierendenvertretung erstellt und dann veröffentlicht werden. Ich wäre in diesem Sinne auch geduldig, sofern ich kontinuierlichen Fortschritt erkennen kann.

<u>Konkrete Benennung der Verfahrensverzeichnisse</u>
Sofern Sperren an Ihrer Hochschule vorliegen, wovon ich aufgrund Ihrer Antworten ausgehe, fallen im Rahmen dieser Sperrmaßnahmen mind. IP Adressen und MAC Adressen als personenbezogene Daten an. Diese werden in Ihren Systemen vermutlich gespeichert, zumindest jedoch ausgewertet oder auch von Intrusion Detection Systemen analysiert und je nach Software auch an Dienstleister (z.B. Cisco) weitergeleitet. Ebenso setzen Sie Proxyserver ein, auf denen diese Daten ebenso anfallen (z.B. als Logdateien).
Da mir eine Gesamtliste der Verfahren nicht bekannt ist, wüsste ich nicht, wie ich darauf noch konkreter antworten soll. Gern können Sie mir ein Inhaltsverzeichnis der Verfahren zukommen lassen, so dass ich aus diesen auswählen kann.
Ansonsten möchte ich mir weitere Unterstützung Ihrerseits entsprechend AIG § 6 (1) erbitten: *„Sofern dem Antragsteller Angaben zur hinreichenden Bestimmung seines Antrages fehlen, ist er von der öffentlichen Stelle zu beraten und zu unterstützen."*

Ich bedanke mich und möchte auf meine zuoberst genannte Faxnummer hinweisen. Eventuell reicht Ihnen diese, anstatt einen Postbrief zu versenden. Vielleicht lassen sich so ein paar kg CO2 und Kosten sparen. Alternativ sehr gern Ende-zu-Ende verschlüsselte Emails via PGP.

Mit freundlichen Grüßen
Marcel Langner

Anlage 5: Bescheid der Hochschule vom 23.02.2021

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

TH Wildau Hochschulring 1 15745 Wildau

Herrn
Marcel Langner
[redacted]

[redacted]
www.th-wildau.de

Wildau, 23. Februar 2021
Ihr Zeichen | Unser Zeichen #196330

Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG), BbgUIG, VIG
Antrag vom 30. August 2020, unsere Schreiben vom 16. September 2020 und vom 22. Dezember 2020
Ihr Schreiben vom 15. Januar 2021, eingegangen am 11. Januar 2021

Sehr geehrter Herr Langner,

ich nehme Bezug auf Ihr Schreiben vom 15. Januar 2021.
Ihrem Schreiben ist nicht zu entnehmen, auf welche Korrespondenz Sie sich beziehen. Lediglich das Kürzel #196330 gibt einen entsprechenden Anhaltspunkt.

Zu diesem Kürzel erhielten Sie mein Schreiben vom 22. Dezember 2020. Sowohl Ihr Antrag vom 30. August 2020 als auch mein Schreiben vom 22. Dezember 2020 enthielten durchnummerierte Fragen und entsprechende Antworten.

Eine solche Struktur liegt bei Ihrem Schreiben vom 15. Januar 2021 nicht vor. Nachfolgend erhalten Sie meine Antwort an Hand der anfänglich gewählten Strukturierung. Meine bisherigen Ausführungen werden dabei fortgeschrieben. Des Weiteren erlaube ich mir Ergänzungen zu den einzelnen Punkten, welche aus Ihren Ausführungen als erledigt anzusehen sind.

1. Eine Liste der Domains, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor (erledigt).

2. Eine Liste der IP Adressen, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor (erledigt).

3. Eine Liste der Dienste (z.B. realisiert über Deep Paket Inspection), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Es liegen keine entsprechenden Fälle vor (erledigt).

4. Eine Liste der Ports (TCP, UDP), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Ihr Antrag wird gemäß § 4 Abs. 2 Nr. 4 AIG abgelehnt.

Die Technische Hochschule Wildau ist ISO 27001 zertifiziert. Diese Zertifizierung setzt eine genau definierte Dokumentenlenkung voraus, welche den Abfluss an Informationen steuert. Für das Informationssicherheitsmanagementsystem der TH Wildau (ISMS) gibt es daher genaue Festlegungen zur Dokumentenlenkung. Diese basieren auf der ISO 27001:2013, Abschnitt 7.5 Dokumentierte Informationen, insbesondere 7.5.3 Lenkung dokumentierter Informationen. Diese laut ISO 27001:2013 geforderte Festlegungen haben das Ziel, Informationen zu schützen, die für die Informationssicherheit gesonderte Priorität haben. Weiterhin ist in der Norm festgelegt, Schutzklassen zu bilden, in die Informationen und die dazu beschriebenen Unterlagen eingeordnet werden.

Die in Punkt 4 und 5 angefragten Inhalte haben eine höhere Schutzklassifizierung und dürfen nicht zugänglich gemacht werden.

Technisch weiterführende Beschreibungen der angefragten Inhalte bergen die Gefahr, die Sicherheit der Infrastruktur und damit schützenswerten Informationen der TH Wildau zu gefährden und führen bei Weitergabe zu einem Normverstoß.

Wahrscheinlich sind Ihre Ausführungen in Ihrem Schreiben vom 15. Januar 2021, welches bereits am 11. Januar 2021 bei uns einging, zur Überschrift „Einstufung der Dokumente" diesem Ordnungspunkt 4. zuzuordnen.
Wie bereits in meinen Schreiben vom 22. Dezember 2020 dargestellt, haben die geforderte Festlegungen in der ISO 27001:2013 das Ziel, Informationen zu schützen, die für die Informationssicherheit gesonderte Priorität haben. Die von Ihnen begehrten Informationen unterliegen einer höheren Schutzklassifizierung und dürfen demnach nicht zugänglich gemacht werden. Nachvollziehbare Gründe, warum die TH Wildau davon abweichen soll, sind Ihren Ausführungen nicht zu entnehmen.

Ihr Auskunftsersuchen haben wir im Wege einer Gefahrenprognose geprüft und kommen zu folgendem Ergebnis:

Zum Schutz der IT Infrastruktur ist es notwendig, neben einer Anzahl von anderen Maßnahmen, Personen, welchen ein Angriff möglich ist oder einen solchen planen könnten, möglichst wenig Informationen über die verwendeten Produkte und deren Konfiguration zur Verfügung zu stellen.
Diese Informationen können Personen, welchen ein Angriff möglich ist oder einen solchen planen (unter bestimmten Umstände und nur teilweise), möglicherweise auch auf anderem Weg erlangen. Diese Informationen sind dann jedoch nicht gesichert und der Umfang wird in wesentlichen Bereichen verhindert.
Bei Fehlen der gesicherten Informationen ist der Aufwand, die Infrastruktur der TH Wildau zu kompromittieren, für Personen, welchen ein Angriff möglich ist oder einen solchen planen könnten, wesentlich größer.
Im Falle eines Angriffs auf die IT-Infrastruktur muss der Aufwand für die Personen, welchen ein Angriff möglich ist oder einen solchen planen könnten, möglichst hoch sein. Damit wird versucht sicherzustellen, dass die notwendige Zeit für die Identifikation der Quelle und für die Auswahl der optimalen Gegenmaßnahmen vorhanden ist. Bei Offenlegung der von Ihnen gewünschten Informationen verringert sich der Aufwand für Personen, welchen ein Angriff möglich ist oder einen solchen planen könnten. Im Falle eines Angriffs werden die Möglichkeiten der TH Wildau, diesen abzuwehren, erheblich eingeschränkt.

Bei einem erfolgreichen Kompromittieren der IT Infrastruktur der TH Wildau ist der Eintritt eines erheblichen Schadens sehr wahrscheinlich. Es besteht dann eine sehr hohe Gefahr, dass datenschutzrelevante Informationen oder auch Daten aus Forschung, Lehre, Studium, Transfer, Kooperationen und internationaler Zusammenarbeit abfließen, manipuliert oder sabotiert werden. Bei der Zurverfügungstellung der angefragten Informationen würde sich die Schadenseintrittswahrscheinlichkeit signifikant erhöhen. Sowohl die Gefahren für die IT-Infrastruktur, als auch die Abschätzung möglicher Schäden überwiegen deutlich Ihr Auskunftsinteresse, zumal Sie dieses nicht begründet haben.

Unsere Entscheidung, Ihren Antrag weiterhin gemäß § 4 Abs. 2 Nr. 4 AIG abzulehnen, erhalten wir aufrecht.

Sie führen an anderer Stelle aus, dass Ports 80 und 443 nicht gesperrt werden dürfen. Ich verweise hiermit auf § 6 Abs. 4 AIG, nach welchem ein Antrag abgelehnt werden kann, wenn der Antragsteller bereits über die begehrten Informationen verfügt oder sich diese in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann. Auf Grund Ihrer Ausführungen gehe ich davon aus, dass Sie in zumutbarer Weise allgemein zugängliche Quellen nutzen können.

5. Eine Liste der IP Protokolle (z.B. IPSEC), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

Ihr Antrag wird gemäß § 4 Abs. 2 Nr. 4 AIG abgelehnt. Begründung siehe 4.

Unsere Entscheidung, Ihren Antrag weiterhin gemäß § 4 Abs. 2 Nr. 4 AIG abzulehnen, erhalten wir aufrecht. Begründung siehe 4.

6. Die Anzahl der Forderungen/Abmahnungen, seit dem Jahr 2015 für jedes Jahr als Summe aufgelistet, von Rechteinhabern oder anderen gegen die Hochschule, die die Hochschule dazu veranlasst hat, bestimmte Netzsperren einzurichten und welche Netzsperren daraufhin eingerichtet wurden.

Es liegen keine entsprechenden Fälle vor (erledigt).

7. Die Prozessbeschreibung zum Einrichten, Prüfen und wieder Entfernen von Netzsperren jeglicher Art (z.B. Wer entscheidet, Wer verantwortet, Gremienbeteiligung).

Eine entsprechende Prozessbeschreibung liegt nicht vor. (erledigt)
8. Anweisungen/Dienstanweisungen/Ordnungen usw., die den Zugang zu bestimmten Seiten untersagen (z.B. Verbot des Besuches von Seiten mit bestimmten Inhalten).

Die Regelungen befinden sich in den Amtlichen Mitteilungen Nr. 06/2000. Die Satzung ist abrufbar unter: https://www.th-wildau.de/hochschule/zentrale-einrichtungen/hochschulrechenzentrum/satzungen-nutzungsordnungen/ (erledigt).

9. Anzahl meldepflichtiger Datenschutzvorfälle, die im Zusammenhang mit den eingerichteten Netzsperren stehen.

Der Datenschutzbeauftragte der TH Wildau teilte mit, dass ihm keine entsprechenden Datenschutzvorfälle bekannt sind (erledigt).

10. Sämtliche Verfahrensverzeichnisse, es fallen ja zweifelsohne personenbezogene Daten an, die im Zusammenhang mit allen zuvor genannten Fragen stehen.

Ihre Anforderung ist unkonkret gefasst. Des Weiteren teilen Sie mit, dass „zweifelsohne" personenbezogene Daten „anfallen". Die von Ihnen erbetenen Informationen sind hinreichend zu konkretisieren. Dabei ist auch die Aussage „es fallen ja zweifelsohne personenbezogene Daten an" in die Konkretisierung mit einzubeziehen. Ich gehe davon aus, dass Sie für die Konkretisierung Ihrer Anfrage unsere Antworten zu den Fragen 1. bis 9. einbeziehen.

In Ihrem Schreiben vom 15. Januar 2021 erbitten Sie die Übersendung eines Inhaltsverzeichnisses über die Verfahren der TH Wildau. Ein solches Inhaltsverzeichnis wird nicht geführt.

Gemäß § 6 Abs. 1 a.E. AIG weise ich Sie darauf hin, dass jede Person gemäß § 11 Abs. 2 Satz 1 AIG das Recht hat, die Landesbeauftragte für Datenschutz und das Recht auf Akteneinsicht anzurufen.

Mit freundlichen Grüßen

[redacted]

Anlage 6: Erneuter Widerspruch vom 22.03.2021, per Fax und Email

Sehr geehrte Damen und Herren,
ich möchte dieses Schreiben (und auch mein vorheriges) als Widerspruch verstanden wissen und Sie bitten diesen rechtsmittelfähig innerhalb der nächsten 4 Wochen zu bescheiden.

Ergänzend zu den in meinen Erwiderungen bereits getätigten Ausführungen möchte ich folgendes hinzufügen.

Sicherheitsfunktion
Unstrittig scheint mir, dass die Sperrung bestimmter Ports/IP Protokolle Angriffe abmildern kann. Strittig ist jedoch, ob die Kenntnis dieser Sperrungen einen Sicherheitsmehrwert erzeugt, wie Sie es darzustellen versuchen. Dabei verwenden Sie quantitative Beschreibungen wie „in wesentlichen Bereichen verhindert", „wesentlich größer", „erheblich eingeschränkt" usw., für die bereits aufgrund der abstrakten Angriffsbeschreibung keine Annahme bestehen kann. Einen Nachweis erbitte ich sofern aktenkundig.
Dass die Kenntnis, welche Ports/IP Protokolle gesperrt sind, eine Sicherheitsfunktion darstellen soll, wird auch noch durch weitere (als die in meinen Erwiderungen bereits genannten) Argumente widerlegt.

EU Verordnung
Laut EU Telecom Single Market (TSM) Verordnung (EU) 2015/2120, sind zumindest die öffentlichen Telekommunikationsanbieter verpflichtet entsprechende Portsperren auch anzugeben. Die Netzwerke solcher Anbieter unterscheiden sich strukturell nicht von denen einer Hochschule. Letztlich unterliegen sie auch den gleichen gesetzlichen Regelungen. Sie sind lediglich größer und bieten damit auch eine breitere Gefahrenfläche. Auch wenn Hochschulen dieser Verordnung nicht unterliegen, lässt sich doch daraus ableiten, dass die Kenntnis solcher Angaben die Sicherheit eines (viel größeren und komplexeren) Netzwerkes nicht in einem Maße beeinflusst, wie Sie es darzustellen versuchen. Unternehmen, die dieser EU Richtlinie unterliegen sind auf den mit Ihnen vergleichbaren Gebieten ISO27001 zertifiziert. Im übrigen sehe ich auch einen Normverstoß gegenüber jedweder selbst auferlegten Zertifizierung als nachrangig gegenüber höherrangigen Auskunftsansprüchen an (Normenhierarchie). Dass zertifizierte Unternehmen solche Informationen herausgeben (müssen), widerlegt jedoch Ihre Behauptung eines Normverstoßes.

Stellungnahme des Forums der Rechteinhaber zum Referentenentwurf für ein Drittes Gesetz zur Änderung des Telemediengesetzes (3. TMGÄndG) vom 23. Februar 2017
Dort nehmen die Rechteinhaber wie folgt zur technischen Wirksamkeit von Portsperren Stellung:
„Entgegen der Annahme des Entwurfs stellen Portsperren aufgrund der technologischen Entwicklung kein wirksames Mittel mehr dar, Rechtsverletzungen, die über Filesharing-Netzwerke begangen werden, zu verhindern. Bei den gegenwärtig üblicherweise verwendeten Filesharing-Programmen wird bei jedem Programmstart für die Kommunikation auf einen beliebigen Port zugegriffen. Die Vergabe des genutzten Ports erfolgt also rein zufällig. Eine wirksame Portsperre würde also bedeuten, dass der WLAN-Betreiber sämtliche möglichen Ports sperren müsste."

Den Rechteinhabern ist durchaus klar, wie wenig technisch wirksam Portsperren sind. Jeder heutzutage durchgeführte Angriff, der sich auf eine Kommunikation mit dem Internet verlässt, nutzt mehrere (beliebige) Ports, eine Reihe von IP Adressen und Domain Namen. Bevorzugt beginnen solche Programme mit jenen Ports, die üblicherweise bekannt nicht gesperrt sind/sein können (z.B. TCP/443 für https).

BSI Stellungnahme
Das BSI bestätigt mir im Rahmen einer IFG Anfrage (Geschäftszeichen: BL23-010 03 05/2021-013):
„Existieren bei Ihnen Unterlagen (z.B. Stellungnahmen oder Handreichungen), aus denen (vielleicht auch nur implizit) hervorgeht, ob es aus Sicht der Sicherheit von IT Systemen sinnvoll ist nicht bekannt zu geben, welche TCP/UDP Ports aus einem Netzwerk einer Hochschule (oder vergleichbar Behörde) von innen nach außen gerichtet zugreifbar sind? Ich möchte mind. gleichwertige Rechtsaspekte der Abwägung von Grundrechten hier nicht als Teil der Frage verstanden wissen. Falls ja, bitte ich um Übermittlung und

frage weiter: Existieren für diese Unterlagen Belege (z.B. Studien oder Statistiken), die nachweisen, dass genau die fehlende Kenntnis von geblockten Ports Angriffe verhindert hat? Gibt es eventuell Unterlagen, die das Gegenteil nahelegen?"

,dass es dazu keinerlei Dokumente vorliegen hat. Ich interpretiere daraus, dass auch das BSI dahingehend keinen Sicherheitsgewinn erkennen kann (und konnte), wenn Portsperren/Protokollsperren geheim gehalten werden, da diese ja sonst Teil irgendeiner Technischen Richtlinie wären.

Herausgabe doch mind. gleich gefährlicher Informationen

Aus fachlicher Sicht ist mir ebenso nicht nachvollziehbar, warum Sie eine Unterscheidung der „Gefährlichkeit" bezüglich Ports/IP Protokollen und IP Adressen/Domainnamen vornehmen. Während Sie Auskunft darüber geben, dass keine Häuser/Häusernamen (=IP Adressen/Domainnamen) sperren, sehen Sie es als Sicherheitsrisiko, wenn bekannt würde, welche Wohnungsnummern/Sprachen der Bewohner (Ports/IP Protokolle) in allen Häusern nicht zugreifbar sind.

Geheimnisbegriff

Die Sicherheit beruht Ihrer Argumentation folgend darauf, dass nicht bekannt wird, welche Ports/IP Protokolle gesperrt sind. Dieses „Geheimnis" lässt sich jedoch trivialst mithilfe von legalen Programmen legal ermitteln, sofern man sich innerhalb eines Hochschul(teil)netzwerkes befindet (auch durch Schadprogramme/Angreifer). Hier in dem man schlicht versucht sich mit einem bestimmten Port/IP Protokoll im Internet zu verbinden. Ein Geheimnis im Sinne des GeschGehG ist daher nicht erkennbar. Sie können daher auch keine Veröffentlichung dieser einfach zu ermittelnden Information verhindern, sofern z.B. eine Abschlussarbeit solche Sperren untersucht und die wissenschaftlich ermittelten Ergebnisse konkret öffentlich darlegt. Unter dieser Voraussetzung ist grundsätzlich Ihre fachliche Einschätzung zu hinterfragen, da Ihre Argumentation ja darauf beruht, das Geheimnis geheim halten zu können. Da dies nicht möglich ist, kann es auch ganz folgerichtig nicht die Basis eines Sicherheitskonzeptes nach Stand der Technik sein oder überhaupt eines Sicherheitskonzeptes.

Kausaler Zirkelschluss

Für das von Ihnen vorgebrachte abstrakte Angriffsbeispiel, welches in dieser Abstraktheit Universalgültigkeit für jede Ablehnung bilden kann, fehlt es an Belegen, die begründen könnten, das Intransparenz für diesen konkreten Fall einen substanziellen Sicherheitsgewinn darstellt. Ihrer Argumentation folgend ist es danach die beste Strategie keinerlei Informationen über den Aufbau von IT Systemen bekannt zu machen. Dies steht dem Ansatz, auch des BSI diametral entgegen, welches versucht Sicherheit dadurch zu erzeugen, dass es aufklärt, was sicher bedeutet und welche Konstruktionsprinzipien sich bewährt haben. In seinem jährlich aktualisierten IT Grundschutzkompendium (ca. 800 Seiten), werden Architektur und Einstellungen von sicheren IT Systemen detailliert für unterschiedliche Szenarien dargelegt.
Nicht inhaltlich eingegangen sind Sie auf mein Argument, dass sie selbst (und auch die Eduroam Policies) bereits nicht gesperrte Ports öffentlich bekannt geben, also genau für jenes abstrakte Szenario, welches Sie selbst als Ablehnungsbegründung darlegen, selbst eine ideale Vorlage für einen Angreifenden schaffen.

Fehlende Auskunft über vorhandene Informationen

Meine Frage bezüglich der Portsperren im Eduroam Teilnetzwerk blieben unbeantwortet. Die Policies dieses durch alle Hochschulen genutzten Zugriffs auf ein Hochschul-WLAN geben jedoch verpflichtend nicht zu sperrende Ports an. Auch auf meinen konkreten Hinweis darauf, haben Sie nicht beantwortet, ob die anderen Ports alle gesperrt sind, bzw. ob Sie die Policies auch umsetzen. Die Beantwortung ist deswegen relevant, weil es in der Vergangenheit bereits vorgekommen ist, dass Hochschulen sich nicht an diese Policies halten.

Unkonkrete Anfrage

Bezüglich des Verfahrensverzeichnis haben Sie mir keinerlei weitere Hilfe angeboten. Dies ist mir in mehrfacher Hinsicht nicht nachvollziehbar. Sie geben an ISO27001 zertifiziert zu sein und verweisen in

Ihren eigenen Antworten darauf, dass sie ein Dokumentenlenkungssystem besitzen. Inwiefern dann überhaupt kein Verzeichnis von relevanten Dokumenten existieren soll, aus denen zu schützende personenbezogene Daten hervorgehen, erschließt sich mir nicht.
Eine mögliche Erklärung wäre die nur diffuse Kenntnis dessen, was ein personenbezogenes Datum in diesem Kontext überhaupt ist. Ich hatte beispielhaft Daten genannt, um Sie zu unterstützen und selbst um Hilfe bei der Konkretisierung gebeten. Darauf sind Sie nicht eingegangen. Die konkreten Kategorien personenbezogener Daten können mir ja schon deshalb nicht bekannt sein, weil ich die konkrete technische Umsetzung eventueller Sperren nicht kenne.
Warum Sie kein Verzeichnis über ihre Verfahren/Verarbeitungen besitzen, welches jedoch nach DSGVO verpflichtend zu führen ist, ist mir schleierhaft.

Vorschläge dahingehend, wie die Informationen möglichst einfach zur Verfügung gestellt werden können oder welche anderen Teilauskünfte möglich wären (§25 VwVfG, AIG § 6 (1)) haben Sie nicht getätigt. Sie vertreten eine pauschale Ablehnung hinsichtlich der nicht erteilten Auskünfte bzw. behaupten meine Anfrage wäre Ihnen zu unkonkret.

Fehlauskunft, Fehlende Kontrollprozesse
Erst jetzt mit dem Verfassen dieses erweiterten Widerspruchs fällt mir auf, dass Sie mit höchster Wahrscheinlichkeit unvollständig geantwortet haben. Sie verneinen das Vorhandensein von Unterlagen darüber, wer wie Sperren einrichtet. Da diese im Rahmen eine ISO27001 Zertifizierung jedoch zu dokumentieren sind (ganz besonders doch wenn es sich, wie Sie behauptenm um eine Sicherheitssache handelt), ist auch zu dokumentieren, wer dort in welcher Rolle die Berechtigungen besitzt. Vermutlich meinten Sie auszusagen, was ich Ihnen glaube, dass außer einer Einzelperson niemand an Sperrentscheidungen beteiligt wird. Trotzdem würde ich diesen dokumentierten Prozess gern sehen bzw. wer dort berechtigt ist. Auch hier veröffentlichen andere Hochschulen, wie dieser Prozess bei ihnen abläuft.

Ich sehe auch aus Abwägungsgründen für zukünftige (und aktuelle) Mitglieder Ihrer Hochschule (was mich einschließt) die vor allem rechtliche Frage, ob nicht auch ein erhebliches und vor allem überwiegendes öffentliches Interesse daran besteht, ermitteln zu können, welche Möglichkeiten der Forschung an einem Hochschulstandort eingeschränkt werden, Warum und in welchem Maße. Für mich überwiegt dieses Interesse bei weitem das für mich sowieso nicht existente Sicherheitsinteresse.

Unter der Modellannahme, dass sich eine Gesamtinformation C (Sperrzustand aller Ports/IP Protokolle) aus den beiden disjunkten Mengen A (gesperrte Ports/IP Protokolle) und B (nicht gesperrte Ports/IP Protokolle) ergibt, ist grundsätzlich zu fragen, ob die Herausgabe von A nach Lesart des AIGs dann auch zu verweigern ist, sofern nur nach A gefragt wird, auch wenn sich daraus B herleiten lässt. Neben der Auslegung des AIGs stellt sich aber auch die Frage, inwiefern Teilmengen von A oder B herauszugeben sind, sofern man dem Argument folgt, es würde sich wirklich um eine Sicherheitsfrage handeln. Auch diese Abwägung erwarte ich von Ihnen. Bisher haben Sie eine pauschale Ablehnung vertreten.
Aber auch das vollständige Wissen um A (und damit auch B) kann jedoch dann ein dahingehend nicht unbedeutenden Grad an Unwissen auf anderen Ebenen aufweisen, da die eigentlich wirksamen und vorgeschriebenen Umsetzungen der Schutzmaßnahmen IDS und IPS unklar bleiben.

Mit freundlichen Grüßen

[redacted]

Anlage 7: Finaler Widerspruchsbescheid der Hochschule vom 26.04.2021 mir zur Kenntnis am 29.04.2021

Technische · Hochschule Wildau *Technical University of Applied Sciences*

WILDAU

TH Wildau Hochschulring 1 15745 Wildau

Herrn
Marcel Langner
[redacted]

[redacted]

www.th-wildau.de

Mit Postzustellungsurkunde

Wildau, 26. April 2021
Ihr Zeichen #196330 | *Unser Zeichen* #196330

Ihr Antrag nach dem Akteneinsichts- und Informationszugangsgesetz (AIG),
Ihr Antrag vom 30. August 2020, unsere Schreiben vom 16. September 2020 und 22. Dezember 2020
Ihr Schreiben vom 15 Januar 2021, eingegangen am 11. Januar 2021
Ihr Schreiben vom 18. Februar 2021
Unser Schreiben vom 23. Februar 2021
Ihr Schreiben vom 22. März 2021

Sehr geehrter Herr Langner,

auf Ihren Widerspruch vom 22. März 2021, eingegangen am 22.03.2021, ergeht folgender

Widerspruchsbescheid

1. Der Widerspruch wird in den Punkten 4. und 5. Ihrer Anfrage als unbegründet zurückgewiesen. Dem Widerspruch wird in Punkt 10. Ihrer Anfrage stattgegeben.

2. Die Kosten des Verfahrens sind vom Widerspruchsführer in Höhe von 90 v.H. zu tragen.

3. Verwaltungsgebühren werden in Höhe von 35,00 Euro erhoben.

Begründung:

I.

Mit Fax vom 30. August 2020 beantragten Sie Akteneinsicht wie folgt:

1. Eine Liste der Domains, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.
2. Eine Liste der IP Adressen, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

3. Eine Liste der Dienste (z.B. realisiert über Deep Paket Inspection), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

4. Eine Liste der Ports (TCP, UDP), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

5. Eine Liste der IP Protokolle (z.B. IPSEC), auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt ist und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.

6. Die Anzahl der Forderungen/Abmahnungen, seit dem Jahr 2015 für jedes Jahr als Summe aufgelistet, von Rechteinhabern oder anderen gegen die Hochschule, die die Hochschule dazu veranlasst hat, bestimmte Netzsperren einzurichten und welche Netzsperren daraufhin eingerichtet wurden.

7. Die Prozessbeschreibung zum Einrichten, Prüfen und wieder Entfernen von Netzsperren jeglicher Art (z.B. Wer entscheidet, Wer verantwortet, Gremienbeteiligung).

8. Anweisungen/Dienstanweisungen/Ordnungen usw., die den Zugang zu bestimmten Seiten untersagen (z.B. Verbot des Besuches von Seiten mit bestimmten Inhalten).

9. Anzahl meldepflichtiger Datenschutzvorfälle, die im Zusammenhang mit den eingerichteten Netzsperren stehen.

10. Sämtliche Verfahrensverzeichnisse, es fallen ja zweifelsohne personenbezogene Daten an, die im Zusammenhang mit allen zuvor genannten Fragen stehen.
Mit Schreiben der TH Wildau vom 22. Dezember 2020 wurde Ihnen mitgeteilt, dass zu den genannten Punkten 1., 2., 3., 6. und 9. keine entsprechenden Fälle vorliegen. Die unter 7. angefragte Prozessbeschreibung liegt ebenso nicht vor. Zu 9. angefragte Datenschutzfälle sind nicht bekannt.

Ihre Anfragen zu 4. und 5. wurden von der TH Wildau abgelehnt. Ihre Anfrage zu 10. war zu unkonkret gestellt und es wurde Ihnen die Möglichkeit einer weiteren Konkretisierung eingeräumt.

Mit Schreiben vom 15. Januar 2021, welches bereits am 11. Januar 2021 einging, wenden Sie sich gegen die Entscheidung der Ablehnung Ihrer Anfragen zu 4. und 5 des Schreibens vom 30. August 2020. Ein konkreter Bezug zu Ihren Anfragen erfolgt dabei nicht. Ihren Antrag zu 10. konkretisieren Sie dahingehend, dass Ihnen eine Gesamtliste der Verfahren nicht bekannt ist und Sie *„nicht wüssten, wie* [Sie] *darauf noch konkreter antworten sollen*".

Mit Schreiben vom 23. Februar 2021 lehnt die TH Wildau Ihre Begehren zu 4. und 5. ab. Begründet wird diese Ablehnung mit der Gefahr für die Sicherheit der Infrastruktur und der schützenswerten Informationen der TH Wildau sowie mit einem Normverstoß gegen die Zertifizierung des ISMS nach ISO 27001:2013.
Zu 10. wurde Ihnen mitgeteilt, dass ein entsprechendes Inhaltsverzeichnis über die Verfahren nicht geführt wird.

Gegen diesen Bescheid legten Sie per Fax vom 22. März 2021 Widerspruch ein.

Sie begründen Ihren Widerspruch damit, dass die Sperrung bestimmter Ports/IP Protokolle Angriffe abmildern kann, strittig jedoch ist, ob die Kenntnis dieser Sperrungen einen Sicherheitsmehrwert erzeugt.

Ihren Widerspruch zu 10. begründen Sie damit, dass die TH Wildau Ihnen keinerlei weitere Hilfe angeboten habe. Sie verweisen darauf, dass Ihnen die konkreten Kategorien personenbezogener Daten schon deshalb nicht bekannt sein können, weil Ihnen die konkrete technische Umsetzung eventueller Sperren nicht bekannt ist.

II.

1.
Der Widerspruch ist zulässig, aber unbegründet.

Sie begehren Akteneinsicht in die Liste der gesperrten Ports sowie der IP Protokolle, auf die der Zugriff aus den unterschiedlichen Netzwerken (eduroam, Studentenwohnheime, Produktivnetz...) der Hochschule in das Internet gesperrt sind und, sofern aktenkundig, der Grund jeder einzelnen Sperrung.
Gemäß § 2 Abs. 1 AIG besteht das Akteneinsichtsrecht auch gegenüber sonstigen Körperschaften.
Jedoch bestimmt § 4 Abs. 1 Nr. 4 AIG, dass der Antrag auf Akteneinsicht abzulehnen ist, wenn das Bekanntwerden des Akteninhaltes eine erhebliche Gefahr für die öffentliche Sicherheit verursachen könnte.
Der Begriff der öffentlichen Sicherheit ist wie im allgemeinen Gefahrenabwehrrecht zu verstehen. Zu ihren Schutzgütern gehören neben den Rechtsgütern des Einzelnen und der Unversehrtheit der Rechtsordnung auch die grundlegenden Einrichtungen und Veranstaltungen des Staates, mithin die Funktionsfähigkeit der staatlichen Einrichtungen. Die TH Wildau ist eine staatliche Einrichtung. Der Ausschlussgrund ist zu bejahen, wenn die Möglichkeit nachteiliger Auswirkungen auf das Schutzgut gegeben sei. Nachteilige Auswirkungen in diesem Sinne liegen vor, wenn aufgrund einer konkreten Tatsache beruhende prognostische Bewertungen mit hinreichender Wahrscheinlichkeit zu erwarten sei, dass das Bekanntwerden der Informationen das Schutzgut beeinträchtigt. Eine Prognose, dass die TH Wildau ihrer Funktion überhaupt nicht mehr gerecht werden könne, ist dabei nicht erforderlich. Der Ausschlussgrund greife bereits dann, wenn die organisatorischen Vorkehrungen

staatlicher Stellen zur effektiven Aufgabenerledigung gestört würden und die Arbeit der betroffenen Amtsträger beeinträchtigt oder erschwert werde.[1]
Das BverwG führt weiterhin dazu aus, dass eine Gefährdung vorliegt, wenn aufgrund einer an konkreten Tatsachen beruhenden prognostischen Bewertung mit hinreichender Wahrscheinlichkeit zu erwarten ist, dass das Bekanntwerden der Informationen das Schutzgut beeinträchtigt. Das Vorliegen des Ablehnungsgrundes hängt dabei nicht von der Person des Antragstellers ab; maßgeblich ist, ob das Bekanntwerden der Information objektiv geeignet ist, sich nachteilig auf das Schutzgut auszuwirken.[2]
In Anwendung dieses Maßstabs ist eine Gefährdung der öffentlichen Sicherheit nicht erst dann zu bejahen, wenn die informationspflichtige Stelle ihrer Funktion voraussichtlich überhaupt nicht mehr gerecht werden könnte, sondern schon dann, wenn die effektive Aufgabenerledigung gestört und die Arbeit der Bediensteten beeinträchtigt werden kann.[3]

Sie begehren die Kenntnisse über gesperrte Ports. Jede Netzwerkkarte verfügt über eine eindeutig zugeordnete MAC-Adresse. Jeder Netzwerkkarte wird eine IP-Nummer zugeordnet und konfiguriert, welche über insgesamt 65.535 Ports verfügt. Über diese Ports wird der Zugriff auf entsprechende Dienste gewährleistet.
Das BSI führt dazu aus: Als Teil der Betrachtungen fließt insbesondere im Rahmen der Schwachstellenanalyse der Aspekt „Wissen über den Prüfgegenstand (TOE)" in die Betrachtungen mit ein. Abhängig von der Art des Prüfgegenstandes und der von ihm zu erbringenden Sicherheitsleistungen spielt dieser Aspekt eine wesentliche Rolle in der Bewertung der Wirksamkeit der implementierten Schutzmechanismen des Produktes. Nach dieser etablierten und weltweit anerkannten Methodik trägt aber eine verringerte Kenntnis über den TOE grundsätzlich dazu bei, Angriffe schwieriger zu machen und das entsprechende Angriffspotential einzuschätzen. In diesem Sinne ist die Anwendung der Common Criteria selbst als Beleg dafür zu sehen, dass das Wissen über den Prüfgegenstand einen Einfluss darauf haben kann,

---

[1] BVerwG 7 C 20.15, 20. Oktober 2016, Rn. 2 zu OVG Münster 8 A 2429/14 vom 16. Juni 2015
[2] BVerwG 7 C 20.15, 20. Oktober 2016, Rn.18 m.w.N.
[3] BVerwG 7 C 20.15, 20. Oktober 2016, Rn.19

potentielle Schwachstellen leichter oder schwerer identifizieren und ausnutzen zu können.[4]
In Anlehnung an die o. g. Anfrage führt das BSI zur Nutzung von geheim zuhaltenden Parametern eines Kryptoalgorithmus aus: *„Für Kryptografie auf elliptischen Kurven bringt die Verwendung von geheim gehaltenen Kurvenparametern einen gewissen Schutz gegen Angriffe mit Quantencomputern."*[5]
Den Ausführungen des BSI kann entnommen werden, dass die Gefährdung von IT-Systemen steigt, wenn Kenntnisse über die Konstruktion, den Aufbau oder die Architektur bekannt sind.

Auf Grund dieser konkreten Einschätzung beruhenden prognostischen Bewertung ist mit hinreichender Wahrscheinlichkeit zu erwarten, dass das Bekanntwerden der Informationen das Schutzgut beeinträchtigt.

Gemäß § 4 Abs. 1 Nr. 4 AIG ist Ihr Antrag auf Akteneinsicht abzulehnen.

Der Ablehnungsbescheid vom 23. Februar 2021 ist daher zu den Punkten 4. und 5. Ihrer Anfrage vom 30. August 2020 rechtmäßig ergangen und verletzt Sie nicht in Ihren Rechten. Daher ist Ihr Widerspruch teilweise zurückzuweisen.

Zu 10. Ihrer Anfrage teile ich Ihnen mit, dass Verzeichnisse der Verarbeitungstätigkeiten mit folgenden Bezeichnungen vorliegen:

- Netzwerkzugang kabelgebunden
- Netzwerkzugang Studentenwohnheim
- WLAN

Diese übersende ich Ihnen in der Anlage.

[4] BSI, 22. März 2021 zu Anfrage Marcel Langner vom 27.02.2021

[5] BSI, 22. März 2021 zu Anfrage Marcel Langner vom 27.02.2021

2.

Die Kostenentscheidung beruht auf §§ 72, 73 Abs. 3 Satz 3 VwGO i. V. m. §§ 79, 80 Abs. 1 Satz 3 VwVfG i.V.m. §1 VwVfGBbg.

3.

Die Gebührenentscheidung erfolgt aus § 10 Abs. 1, 2 AIG i. V. m. § 1 Akteneinsichts- und Informationszugangsgebührenordnung (AIGGebO)* i. V. m. Tarifstelle 2.1 der Anlage zur AIGGebO. Danach werden für Amtshandlungen beim Vollzug des Akteneinsichts- und Informationszugangsgesetzes Gebühren erhoben. Die Gebühr für die Erteilung von Bescheiden über Widersprüche - wenn und soweit sie zurückgewiesen werden - beträgt mindestens 10 Euro und höchstens 50 Euro, Die festgesetzte Gebühr i. H. v. 35 Euro ist angemessen und berücksichtigt den mit der Amtshandlung verbundenen Aufwand.

Hinweis zur Zahlung:
Bitte überweisen Sie den Gesamtbetrag in Höhe von 35 Euro innerhalb von 14 Tagen ab Zustellung dieses Bescheides an:

Empfänger:	TH Wildau
BIC:	WELADED1PMB
IBAN:	DE74 1605 0000 3667 0209 79
Institut:	Mittelbrandenburgische Sparkasse (MBS)
Verwendungszweck:	#196330

Rechtsbehelfsbelehrung:

Gegen diesen Widerspruchsbescheid kann innerhalb eines Monats nach Bekanntgabe Klage bei dem Verwaltungsgericht Cottbus, Vom-Stein-Straße 27, 03050 Cottbus, erhoben werden.

Sollten Sie separat gegen die vorliegende Gebührenfestsetzung vorgehen wollen, können Sie innerhalb eines Monats nach Zustellung dieses Widerspruchsbescheides gegen die Gebührenfestsetzung unter Ziffer 3 Widerspruch erheben. Der Widerspruch ist bei der Technischen Hochschule Wildau, Hochschulring 1, 15745 Wildau einzulegen.

Mit freundlichen Grüßen

[redacted]

B. Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit

(Art. 30 Abs. 1 lit. b DS-GVO)

Aktualisiert: 08.04.2019

1. Bezeichnung der Verarbeitungstätigkeit

Studentenwohnheim

2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (falls zutreffend)

[redacted]

2.1 Bei gemeinsamer Verantwortlichkeit

3. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Kontrolle von Funktionalitäten, Fehleranalyse

4. Rechtsgrundlage für die Erhebung/Speicherung/Verarbeitung

Protokollierung zur Aufrechterhaltung des Hochschulbetriebes unter Berücksichtigung der Datenminimierung

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

5.1 Betroffene Personengruppen

Beschäftigte, Studierende

5.2 Kategorien personenbezogener Daten

Name, Vorname, Mac-Adresse, IP-Adresse

5.3 Datenschutz-Folgenabschätzung

nein – keine Kriterien der DSFA_Muss_Liste werden erfüllt

5.3. Quelle der Datenerhebung, wenn nicht bei den betroffenen Personen erhoben wird (Art. 14 Abs. 2 lit.f DS-GVO)

keine

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden
(Art. 30 Abs. 1 lit. d DS-GVO)

6.1. Kategorien von Empfänger innerhalb der verantwortlichen Stelle

intern (Zugriffsberechtigte)

6.2 Dienstleister, die Verarbeitung im Auftrag durchführen

entfällt

7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Übermittlung: Nein

7.1. Name des Drittlandes / der internationalen Organisation (DS-GVO)

8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

in Archivierungsordnung geregelt

9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

9.1 Art der eingesetzten DV-Anlagen und Software (optional)

9.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

über ISMS der TH Wildau geregelt

10. Optionale Angaben

11. Sonstiges / Referenzdokumente

Revisionen

Datum	Name	Änderungen

B. Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit

(Art. 30 Abs. 1 lit. b DS-GVO)

Aktualisiert: 08.04.2019

1. Bezeichnung der Verarbeitungstätigkeit

Netzwerkszugang kabelgebunden

2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (falls zutreffend)

Hochschulrechenzentrum

[redacted]

2.1 Bei gemeinsamer Verantwortlichkeit

3. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Kontrolle von Funktionalitäten, Fehleranalyse

4. Rechtsgrundlage für die Erhebung/Speicherung/Verarbeitung

Protokollierung zur Aufrechterhaltung des Hochschulbetriebes unter Berücksichtigung der Datenminimierung

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

5.1 Betroffene Personengruppen

Beschäftigte, Studierende

5.2 Kategorien personenbezogener Daten

Name, Vorname, Mac-Adresse, IP-Adresse, Betriebssystem, Clientinformationen

5.3 Datenschutz-Folgenabschätzung

nein – keine Kriterien der DSFA_Muss_Liste werden erfüllt

5.3. Quelle der Datenerhebung, wenn nicht bei den betroffenen Personen erhoben wird (Art. 14 Abs. 2 lit.f DS-GVO)

keine

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden
(Art. 30 Abs. 1 lit. d DS-GVO)

6.1. Kategorien von Empfänger innerhalb der verantwortlichen Stelle

intern (Zugriffsberechtigte)

6.2 Dienstleister, die Verarbeitung im Auftrag durchführen

7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Übermittlung: Nein

7.1. Name des Drittlandes / der internationalen Organisation (DS-GVO)

8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

in Archivierungsordnung geregelt

9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

9.1 Art der eingesetzten DV-Anlagen und Software (optional)

Server

9.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

über ISMS der TH Wildau geregelt

10. Optionale Angaben

11. Sonstiges / Referenzdokumente

Revisionen

Datum	Name	Änderungen

B. Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit

(Art. 30 Abs. 1 lit. b DS-GVO)

Aktualisiert: 08.04.2019

1. Bezeichnung der Verarbeitungstätigkeit

WLAN

2. Verantwortlicher Fachbereich/verantwortliche Führungskraft (falls zutreffend)

[redacted]

[redacted]

[redacted]

[redacted]

2.1 Bei gemeinsamer Verantwortlichkeit

3. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

Kontrolle von Funktionalitäten, Fehleranalyse

4. Rechtsgrundlage für die Erhebung/Speicherung/Verarbeitung

Protokollierung zur Aufrechterhaltung des Hochschulbetriebes unter Berücksichtigung der Datenminimierung

5. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DS-GVO)

5.1 Betroffene Personengruppen

Beschäftigte, Studierende

5.2 Kategorien personenbezogener Daten

Name, Vorname, Mac-Adresse, IP-Adresse, Betriebssystem, Clientinformationen

5.3 Datenschutz-Folgenabschätzung

nein – keine Kriterien der DSFA_Muss_Liste werden erfüllt

5.3. Quelle der Datenerhebung, wenn nicht bei den betroffenen Personen erhoben wird (Art. 14 Abs. 2 lit.f DS-GVO)

keine

6. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden
(Art. 30 Abs. 1 lit. d DS-GVO)

6.1. Kategorien von Empfänger innerhalb der verantwortlichen Stelle

intern (Zugriffsberechtigte)

6.2 Dienstleister, die Verarbeitung im Auftrag durchführen

7. Datenübermittlungen in Drittländer oder internationale Organisationen (Art. 30 Abs. 1 lit. e DS-GVO)

Übermittlung: Nein

7.1. Name des Drittlandes / der internationalen Organisation (DS-GVO)

8. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DS-GVO)

in Archivierungsordnung geregelt

9. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

9.1 Art der eingesetzten DV-Anlagen und Software (optional)

Server

9.2 Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen
(Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DS-GVO)

über ISMS der TH Wildau geregelt

10. Optionale Angaben

11. Sonstiges / Referenzdokumente

Revisionen

Datum	Name	Änderungen

Anlage 8: Sachstandmeldung der LDA vom 30.03.2021

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: 30. März 2021

[redacted]

Ihr Antrag auf Informationszugang bei der TH Wildau vom 30. August 2020
Unsere E-Mail vom 8. Oktober 2020, fragdenstaat.de (#196330)
Ihre E-Mails vom 27. Februar und 15. März 2021

Sehr geehrter Herr Langner,

vielen Dank für Ihre E-Mail vom 15. März 2021. Sie bemängelten, seit unserer E-Mail vom 8. Oktober 2020 noch keine Rückmeldung von uns erhalten zu haben und baten um eine Information über den Sachstand. Ihrer Bitte kommen wir gerne nach.

Nachdem wir Sie per E-Mail vom 8. Oktober 2020 über unser Herantreten an die Technische Hochschule Wildau informiert hatten, informierte uns diese über die beabsichtige Beantwortung Ihres Antrags. Mit Schreiben vom 8. Dezember 2020 gingen wir gegenüber der Hochschule auf einige informationszugangsrechtliche Gesichtspunkte ihrer Argumentation ein. Dies betraf insbesondere das Begründungserfordernis für die Geltendmachung von Sicherheitsgründen sowie den Umgang mit der Einsicht in Verfahrensverzeichnisse nach § 4 Abs. 3 Brandenburgisches Datenschutzgesetz. Die Angelegenheit war zudem Gegenstand einer telefonischen Erörterung am 22. Dezember 2020. Zu Beginn des neuen Jahres übersandte uns die Hochschule eine Kopie des daraufhin ergangenen Änderungsbescheids vom 22. Dezember 2020 sowie Ihres Schreibens vom 11./15. Januar 2021. Aus Letzterem ging hervor, dass Sie zunächst von dem Angebot der Hochschule, für Rückfragen zur Verfügung zu stehen, Gebrauch machen wollten. Vor diesem Hintergrund hatten wir uns entschieden, das Ergebnis Ihrer Bemühungen abzuwarten.

In der Zwischenzeit erhielten wir vonseiten der Technischen Hochschule Wildau eine Kopie ihres Schreibens vom 23. Februar 2021, mit der sie auf Ihr Schreiben vom 11./15. Januar 2021 einging. Am 27. Februar 2021 informierten Sie uns über diesen zwischenzeitlich angefallenen Schriftverkehr. Schließlich ergänzten Sie in Ihrer E-Mail vom 15. März 2021 an uns Ihre Argumentation und baten uns darum, auf den Änderungsbescheid der Hochschule vom 22. Dezember 2020 einzugehen. Die Inhalte der hier genannten Schriftwechsel sind Ihnen bekannt, sodass es sich erübrigt, sie im Rahmen der Sachverhaltsdarstellung aufzuführen.

Aus dem Schriftverkehr ergibt sich, dass die Hochschule die meisten Ihrer Fragen beantwortet hat. Strittig ist lediglich die Ablehnung der Beantwortung der Fragen 4 und 5 (gesperrte Ports und IP-Protokolle sowie Gründe für die Sperrung) sowie der Umgang mit der Einsicht in die Verfahrensverzeichnisse.

Zu den Fragen 4 und 5 wies die Technische Hochschule Wildau in ihrem Änderungsbescheid vom 22. Dezember 2020 auf die erfolgte Umsetzung eines Zertifizierungsstandards zur Informationssicherheit hin und erläuterte das Ziel dieser Maßnahme, nämlich die Erhöhung der Informationssicherheit. Zudem erwähnte sie, dass in der Norm festgelegt sei, Schutzklassen zu bilden. Die Offenlegung der beantragten Informationen berge „die Gefahr, die Sicherheit der Infrastruktur und damit schützenswerten Informationen der TH Wildau zu gefährden und [führe] bei Weitergabe zu einem Normverstoß". Die Hochschule bezog sich auf § 4 Absatz 2 Nummer 4 Akteneinsichts- und Informationszugangsgesetz (AIG). Im Hinblick auf die Verfahrensverzeichnisse bat die Hochschule Sie um eine Konkretisierung Ihres Anliegens.

Den Änderungsbescheid vom 22. Dezember 2020 bewerten wir wie folgt:

- Die Ablehnung eines Antrags bedarf nach § 6 Absatz 1 Satz 8 AIG einer Begründung. Diese muss sowohl für den Antragsteller als auch für die Kontrollbehörde nachvollziehbar sein. Aus unserer Sicht erschließt sich aus der Argumentation der Hochschule lediglich, dass sie der Auffassung ist, die Offenlegung der beantragten Informationen verstoße gegen das Akteneinsichts- und Informationszugangsgesetz, nicht jedoch, weshalb. Weder der Hinweis auf den Ablehnungsgrund des § 4 Absatz 2 Nummer 4 AIG noch die Ausführungen zur Zertifizierung enthalten nach unserem Verständnis eine solche Begründung.

- Ob die Hochschule sich ausschließlich auf den Ablehnungsgrund des § 4 Absatz 2 Nummer 4 AIG stützen wollte, vermögen wir von hier aus nicht einzuschätzen. Der inhaltliche Bezug der Ablehnung zu Fragen der Informationssicherheit dürfte dafür sprechen, dass § 4 Absatz 1 Nummer 4 AIG und damit der Ablehnungsgrund einer erheblichen Gefahr für die öffentliche Sicherheit zumindest auch betroffen ist. Auch die Kommunikation zwischen Ihnen und der Hochschule ist in dieser Hinsicht mehrdeutig. Soweit sich die Hochschule auf § 4 Absatz 2 Nummer 4 AIG stützt, muss sie eine Interessenabwägung vornehmen und dies im Bescheid darstellen. Auf § 6 Absatz 1 Satz 4 AIG ist in diesem Zusammenhang hinzuweisen.

- Soweit der Hinweis der Hochschule auf den Zertifizierungsstandard sowie auf die Einstufung von Informationen in Schutzklassen eine Ablehnung nach § 4 Absatz 3 AIG darstellen soll, würde sich auch hier die Frage nach der Begründung stellen. Ob ein bloßer Zertifizierungsstandard, bei dem in der Regel die Prozesse im Vordergrund stehen, als vorrangige Geheimhaltungspflicht zu werten wäre, bezweifeln wir zudem – allerdings unter dem Vorbehalt einer genaueren Prüfung. Selbst wenn es um eine herkömmliche Klassifizierung im Sinne der Verschlusssachenanweisung handelt, bedürfte es einer Erläuterung, weshalb die zum Zeitpunkt der Einstufung vorliegende Schutzbedarfs noch fortbesteht. Siehe hierzu Urteil des Bundesverwaltungsgerichts vom 29. Oktober 2009 (7 C 21.08).

- Zu Ihrer Information möchten wir Sie zudem auf das Urteil des Bundesverwaltungsgerichts vom 20. Oktober 2016 (7 C 20/15) aufmerksam machen, das sich unter anderem mit den Schutzgütern der öffentlichen Sicherheit sowie der ordnungsgemäßen

Aufgabenerfüllung befasst – wenngleich auf der Grundlage des Informationsfreiheitsgesetzes.

- Die Einsichtnahme in die Verzeichnisse der Verarbeitungstätigkeiten richtet sich ausschließlich nach § 4 Absatz 3 Brandenburgisches Datenschutzgesetz. Die konkreten Vorschriften des Akteneinsichts- und Informationszugangsgesetzes zur hinreichenden Bestimmung des Antrags durch den Antragsteller einerseits sowie zur Beratungs- und Unterstützungspflicht der Akten führenden Stelle andererseits gelten hier nicht. Die Bitte der Hochschule zur Konkretisierung Ihres Antrags im Hinblick auf die Verfahrensverzeichnisse halten wir vorliegend zwar für nachvollziehbar. Dennoch sollte unseres Erachtens auch im Rahmen einer datenschutzrechtlichen Bearbeitung des Antrags eine Beratung dahingehend stattfinden, dass die Hochschule Anhaltspunkte nennt, nach denen sich die erbetene Konkretisierung des Antrags ausrichten kann.

Mit Schreiben vom 23. Februar 2021 ging die Technische Hochschule Wildau auf Ihren per Schreiben vom 11./15. Januar 2021 geäußerten Wunsch einer Begründung recht ausführlich ein. Sie erläuterte – kurz zusammengefasst –, dass sich die für einen Angriff auf die IT-Infrastruktur der Hochschule erforderlichen Informationen zwar auch auf anderem Wege beschaffen ließen. Die Herausgabe der Informationen auf dem Wege der Akteneinsicht verringere jedoch den Aufwand für die angreifende Person und schränke folglich die (zeitlichen) Möglichkeiten der Hochschule ein, einen solchen Angriff abzuwehren. Außerdem beschrieb sie die Schäden, die bei einem erfolgreichen Kompromittieren der IT-Infrastruktur der Hochschule entstehen können. Obwohl die Hochschule selbst feststellte, dass Sie Ihr Auskunftsinteresse nicht begründet haben, sie es also nicht zu kennen scheint, hielt sie im Ergebnis fest, dass die beschriebenen Gefahren Ihr Auskunftsinteresse deutlich überwögen, und hielt die Ablehnung Ihres Antrags aufrecht. Zu den Verfahrensverzeichnissen teilte sie mit, dass es hierzu kein Inhaltsverzeichnis gebe.

Die aus dem Schreiben der Technischen Hochschule Wildau vom 23. Februar 2021 hervorgehende Begründung überzeugt uns nach wie vor nicht:

- Insbesondere vermögen wir mangels genauerer informationstechnischer Erläuterungen nicht nachzuvollziehen, weshalb es der Sicherheit der IT-Infrastruktur dienen soll, die Offenlegung der Sperrung von Ports bzw. IP-Protokollen zu verhindern. Auch nach Konsultation der fachlich zuständigen Organisationseinheit in unserem Hause sind wir der Auffassung, dass die erneute Darlegung durch die Hochschule keine ausreichende Begründung im Sinne des § 6 Absatz 1 Satz 8 AIG darstellt.

- Nach wie vor erschließt sich uns die alleinige Geltendmachung des § 4 Absatz 2 Nummer 4 AIG nicht, da schließlich der Aspekt der öffentlichen Sicherheit – und dazu kann unseres Erachtens auch die Integrität der IT-Infrastruktur einer Einrichtung zählen – in § 4 Absatz 1 Nummer 4 AIG geregelt wird. Darüber hinaus geht die Hochschule auf den von ihr geltend gemachten Schutzbedarf der ordnungsgemäßen Erfüllung ihrer Aufgaben nur insoweit ein, als sie pauschal den Schaden beschreibt, welcher ihr durch die Kompromittierung der IT-Infrastruktur entstehen könnte.

- Das aus unserer Sicht bestehende Erfordernis zur Beratung und Unterstützung bei der erbetenen Konkretisierung Ihres Antrags im Hinblick auf die Verzeichnisse der Verarbeitungstätigkeiten besteht auch dann, wenn es, wie von der Hochschule angegeben, keine Auflistung der vorhandenen Verzeichnisse gibt. Eine Konkretisierung und somit

die Inanspruchnahme des voraussetzungslosen und unentgeltlichen Rechts nach § 4 Absatz 3 Brandenburgisches Datenschutzgesetz ist nur durch die Zurverfügungstellung einer entsprechenden Übersicht möglich.

Mit Schreiben vom heutigen Tage haben wir die Technische Hochschule Wildau auf die oben stehenden Gesichtspunkte aufmerksam gemacht und eine erneute Überprüfung der Begründung bzw. eine Beratung im Hinblick auf die Verzeichnisse der Verarbeitungstätigkeiten gebeten. Wir bitten Sie um Verständnis, dass eine solche Beratung nur durch die Stelle erfolgen kann, die solche Verzeichnisse selbst führt. Insofern können wir Ihrer Bitte um Mithilfe bei der Konkretisierung Ihres Antrags nur mittelbar entsprechen.

Mit freundlichen Grüßen

Anlage 9: Angaben von Portsperren durch Telekommunikationsanbieter; hier Vodafone und Telekom

Vodafone:

Was sind Portsperren und wie wirken sie sich aus?

Um die Sicherheit und Integrität unseres Netzes sicherzustellen, dürfen wir Portsperren einrichten. Und zwar nach EU Telecom Single Market (TSM) Verordnung (EU) 2015/2120. Dadurch können einzelne Anwendungen oder Dienste beeinträchtigt sein, die über die gesperrten Ports laufen. Das heißt, Du kannst sie nicht oder nur eingeschränkt nutzen.

Aktuell haben wir diese Ports mit Erlaubnis der Bundesnetzagentur dauerhaft gesperrt:

Mobilfunk

- Port TCP/UDP 0
- Port TCP 445

Kabel

- TCP/UDP 135-139
- udp 67/DHCP
- udp 69/TFTP

DSL

- keine dauerhaften Sperren eingerichtet

Glasfaser

- keine dauerhaften Sperren eingerichtet

So wirken sich die Portsperren auf die Nutzung aus:

Wahl bitte aus

Port TCP/UDP 0	Ports TCP 445 und TCP/UDP 137-139	Port TCP/UDP 135	Port TCP/UDP 136

Port TCP/UDP 0

Wir sperren diesen Port zu Deiner Sicherheit, damit er aus dem Internet nicht zu erreichen ist. Das hat normalerweise keine Auswirkungen auf Deine

Telekom:

Anhang: Liste eingerichteter Portsperren

Um die Integrität und Sicherheit des Netzes, der über dieses Netz erbrachten Dienste und der Endgeräte der Endnutzer zu wahren, darf die Telekom nach Artikel 3 Abs.3 Unterabsatz 3 b) der EU- Verordnung 2015/2120, soweit und solange dies erforderlich ist, Verkehrsmanagementmaßnahmen, wie z.B. Portsperren einrichten. Dadurch können einzelne Anwendungen oder Dienste beeinträchtigt sein, die über die gesperrten Ports laufen. Das bedeutet, dass diese dann nicht oder nur eingeschränkt nutzbar sind.
Die Telekom sperrt aktuell folgende Ports (länger als einen Monat) zur Sicherheit des Kunden Richtung Internet:

1. Mobilfunk

67-68 (DHCP Bootstrap Protokoll)
Endgeräte nutzen über diese Ports LAN-Dienste, die lokal innerhalb des LAN bereitgestellt werden Diese Dienste können von den Endgeräten nicht über den mobilen Internetzugangsdienst genutzt werden (Internet ist kein LAN). Diese Ports werden aus Sicherheitsgründen geblockt, um Endgeräte vor möglichen Angriffen aus dem Internet zu schützen.

135-139 (Netbios)
Endgeräte nutzen über diese Ports LAN-Dienste, die lokal innerhalb des LAN bereitgestellt werden. Diese Dienste können von den Endgeräten nicht über den mobilen Internetzugangsdienst genutzt werden (Internet ist kein LAN). Diese Ports werden aus Sicherheitsgründen geblockt, um Endgeräte vor möglichen Angriffen aus dem Internet zu schützen. In der Vergangenheit haben Angreifer diese Ports auch zur Verbreitung von Würmern/Viren (z.B. WannaCry) genutzt.

445 (Microsoft SMB)
Endgeräte nutzen über diese Ports LAN-Dienste, die lokal innerhalb des LAN bereitgestellt werden Diese Dienste können von den Endgeräten nicht über den mobilen Internetzugangsdienst genutzt werden (Internet ist kein LAN). Diese Ports werden aus Sicherheitsgründen geblockt, um Endgeräte vor möglichen Angriffen aus dem Internet zu schützen. In der Vergangenheit haben Angreifer diese Ports auch zur Verbreitung von Würmern/Viren (z.B. WannaCry) genutzt.

2. Festnetz

Im Festnetz hat die Telekom derzeit keine dauerhaften Sperren eingerichtet.
Die Telekom behält sich eine Änderung der Portsperren vor, wenn und soweit dies zur Wahrung der Integrität und Sicherheit des Netzes, der über dieses Netz erbrachten Dienste und der Endgeräte der Endnutzer erforderlich ist. Die Telekom behält sich ebenso kurzfristige Sperrungen zur Erreichung der in Artikel 3 Abs.3 Unterabsatz 3 b) der EU- Verordnung 2015/2120 genannten Ziele vor.

Anlage 10: Linkliste von öffentlich einsehbaren Sperren deutscher Hochschulen nach kurzer Suche mit Google

Universität Tübingen (27205 Studierende)
https://uni-tuebingen.de/einrichtungen/zentrum-fuer-datenverarbeitung/dienstleistungen/sicherheit/sperrungen/

Universität Würzburg (27613 Studierende)
https://www.rz.uni-wuerzburg.de/dienste/it-sicherheit/firewall/

Leibniz Universität Hannover (29895 Studierende)
https://www.luis.uni-hannover.de/de/services/it-sicherheit/firewall/netzschutz/port-und-protokollsperren/

Leibniz Rechenzentrum (betreut 3 Hochschulen über 100.000 Studierende)
https://www.lrz.de/services/netz/einschraenkung/

HU Berlin (38062 Studierende)
https://www.cms.hu-berlin.de/de/dl/netze/firewall

TU Chemnitz (10449 Studierende)
https://www.tu-chemnitz.de/urz/security/net-security.html

Universität Ulm (10304 Studierende)
https://www.uni-ulm.de/einrichtungen/kiz/service-katalog/informationssicherheit/firewall-aussennetzanbindung/

TU Berlin (35050 Studierende)
https://www.campusmanagement.tu-berlin.de/menue/dienste/kommunikation_internet/ip_adressendns/anleitungen_und_informationen/#c13590

KIF430:Resolutionen/Netzneutralitaet

Resolution Netzneutralität [Bearbeiten]

Die 43,0. Konferenz der deutschsprachigen Informatikfachschaften begrüßt das weit verbreitete Angebot von eduroam an deutschsprachigen Hochschulen und hält die Qualitätssicherung des eduroam-Netzwerkes für die wissenschaftliche Arbeit für unerlässlich.

Folgende Punkte werden für besonders kritisch gehalten und daher explizit auf diese hingewiesen:

- Wir fordern die Einhaltung der eduroam Policy Service Definition, festgelegt von der GÉANT Association, in der Version 2.8 vom Juli 2012, da in der Vergangenheit von einigen Hochschulen einige Empfehlungen sowie Forderungen hierin nicht beachtet wurden.

  Herausheben wollen wir dabei:

  1. Die Einhaltung der in Abschnitt 6.3.3, Unterpunkt Network, aufgeführten Liste der unbedingt anzubietenden Ports. Leider wurden wir auf zahlreiche Verstöße gegen diesen Punkt aufmerksam gemacht. Wir unterstützen darüber hinaus die Empfehlung keine bzw. möglichst wenige Portrestriktionen vorzunehmen, sowie keine Anwendungs- und Abfangproxies zu verwenden.
  2. Die Einhaltung der in Abschnitt 6.3.2 festgelegten Unterstützung von anonymer Authentifizierung. Wir bitten diese Unterstützung auch in den entsprechenden Anleitungen zu dokumentieren.

- Falls Portrestriktionen unumgänglich sind, sollten diese öffentlich zugänglich dokumentiert und begründet werden, sowohl für ein- als auch für ausgehende Beschränkungen. Wir bitten die GÉANT Association dies in die eduroam Policy Service Definition als *MUST*-Anforderung aufzunehmen.
- Aufgrund der herausragenden Bedeutung des eduroam-Netzes für die wissenschaftliche Gemeinschaft fordern wir eine ausreichende Ausstattung mit personellen und finanziellen Mitteln zur Aufrechterhaltung, zur Verbesserung und zum Ausbau des Netzwerkes durch die betreibenden Hochschulen.

Wir bitten diese Hinweise analog für andere hochschulöffentliche Netze zu beherzigen.

Erläuterung [Bearbeiten]

Die Verbreitung von eduroam über mittlerweile fast alle deutschsprachigen Hochschulen ist eine hervorragende Entwicklung. Leider lässt die Umsetzung manchmal zu wünschen übrig und entspricht nicht den Vorgaben für das eduroam Netz. Diese Resolution soll Fachschaften dazu ermuntern, falls sie Probleme mit eduroam an ihrer Hochschule haben, diese Probleme mit Verweis auf die Vorgaben bei ihren Hochschulrechenzentren zu melden und falls sie nicht gelöst werden weiter zum DFN oder der GÉANT Association zu eskalieren.

Darüber hinaus enthält diese Resolution Verbesserungsvorschläge für die die eduroam-Vorgaben der GÉANT Association.

Im Konsens angenommen