Präsidentin der Technischen Hochschule Wildau
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 22.03.2021
Mein Zeichen: #196330
Via Fax und Email
4 Seiten

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]