



Außenstelle Berlin

Bundesnetzagentur • Seidelstraße 49 • 13405 Berlin



Ihr Zeichen, Ihre Nachricht vom
17.12.2019

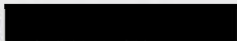

Mein Zeichen, meine Nachricht vom
Berl 8
Berl8-IFG-001-19

☎(030)
43741200
oder -0

Berlin
16.01.2020

Auskunft IFG

Sehr 

als Anlage erhalten Sie die von Ihnen beantragten Kopien der Korrespondenz mit 
 zum Thema Deauther. Es gab keine weiteren Kontakte mit
anderen Hochschulen zu diesem Thema.

Für diese Auskunft werden keine Gebühren erhoben.



Anlage:
Kopie aus Auftrag
D001/00658/18

[REDACTED]
Bundesnetzagentur
DLZ8

[REDACTED]
Seidelstraße 49

13405 Berlin

Unser Zeichen:

Ihr Zeichen:

Datum: 19.09.19

Umgang mit Rogue Access Points

Sehr [REDACTED]

vielen Dank für das sehr konstruktive Gespräch. Ich möchte an der Stelle Ihren Vorschlag aufgreifen und die aktuelle Situation an [REDACTED] beschreiben.

1. Gegebene Situation


Die Bundesnetzagentur ist eine oberste deutsche Regulierungsbehörde und besitzt die Aufgabe, die Aufrechterhaltung und die Förderung des Wettbewerbs in sogenannten „Netzmärkten“ zu sichern. Die BNetzA ist nach § 55 Telekommunikationsgesetz (TKG) befugt, die Nutzung für Frequenzen durch sogenannte Frequenzuteilungen zu regeln. Nach S. 2 der Vorschrift darf die BNetzA dabei auch Bedingungen für die Frequenznutzung erlassen. Mit ihrer Verfügung 151/2018 (*Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN („Wireless Access Systems including Wireless Local Area Networks“)*) hat die BNetzA u.a. festgeschrieben:

„Aussendungen, die absichtlich bestimmungsgemäße WAS/WLAN-Nutzungen stören oder verhindern, wie z.B. Aussendungen von Funksignalen und/oder Datenpaketen, die die Abmeldung oder Beeinflussung von WAS/WLAN-Verbindungen anderer Nutzer gegen deren Willen zum Ziel haben, sind nicht gestattet.“


Diese Bedingung für die Nutzung der Frequenzen stellt eine für den Adressaten rechtverbindliche Einschränkung der Erlaubnis dar.

Dieser Nutzungsbedingung der BNetzA stehen aber gleichzeitig Regelungen gegenüber, welche ebenfalls beim Betreiben einer WLAN Infrastruktur einer Organisation zu beachten sind. Hierzu gehört u.a. die Erstellung einer Nutzerordnung, für die das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem BSI-Grundschutzkatalog und die ISO 27 00x die wesentlichen Inhalte vorgeben. Zudem werden in diesen Richtlinien genaue Festlegungen formuliert, die die Regelungen der Zuständigkeiten für die Verwaltung und den Betrieb von Netzwerkkomponenten, im speziellen Fall von WLAN Access Points und dem WLAN Management, betreffen. Diese Anforderungen sind durch die Satzung [REDACTED] und die dazugehörigen Dokumente erfüllt, die Informationssicherheitsrisiken sind dadurch reduziert und [REDACTED] zertifiziert worden.

Gemäß der Satzung des [REDACTED] ist das Betreiben eines fremden Access Points (sogenannte Rogue Access Points) innerhalb der Infrastruktur [REDACTED] welcher nicht vom Hochschulrechenzentrum administriert wird, aus den folgenden Gründen ausgeschlossen:



In den genannten Richtlinien wird davon ausgegangen, dass ohne eine institutionelle Kontrolle des WLANs ein generelles Sicherheitsrisiko besteht. Es liegt in der Verantwortung des Betreibers, eine Risikoanalyse durchzuführen, um dieses Sicherheitsrisiko auf ein umsetzbares Minimum zu reduzieren. Eine Schwerpunktaufgabe eines Hochschulrechenzentrums besteht gerade darin, bei dem Betrieb der WLAN-Infrastruktur sowohl die Verfügbarkeit des Netzes als auch die Informationssicherheit zu gewährleisten.

Der von der BNetzA zur Verfügung gestellte Frequenzbereich wird durch insgesamt 850 Access Points  und die notwendige Verteilung zur Sicherstellung einer vollständigen Campusabdeckung ausgeschöpft. Jeder neu hinzukommende Rogue Access Point würde denselben Standard und somit den gleichen Frequenzbereich nutzen, was zu einer Frequenzüberlagerung und somit zwangsläufig zu Einschränkungen der Verfügbarkeit der zentralen Infrastruktur führen würde.

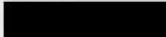
Hinsichtlich dieses Sicherheitsrisikos sei an dieser Stelle exemplarisch ein Beispiel genannt: Ein Rogue Access Point kann sich mit einer schon verwendeten SSID (Service Set Identifier -, Bezeichnung beinhaltet den Name von einzelnen WLAN-Netzwerken), wie z.B. „eduroam“ ausgeben. Ein Endgerät verbindet sich automatisch immer mit dem stärksten Signal und so möglicherweise mit dem fremden Access Point. Dies würde dazu führen, dass Nutzerinnen und Nutzer sich in Unkenntnis an einem fremden, einem Rogue Access Point anmelden und ihre Nutzerdaten unwissentlich an einen Dritten weiterleiten. Zudem öffnen diese Nutzer damit unbemerkt ein Tor, um datenschutzrelevante Informationen nach außen und damit für Dritten sichtbar zu machen. Auch ein Abfluss von Forschungsdaten ist über den Zugang durch unberechtigte Dritte möglich.

Um den Anforderungen an IT-Sicherheit und Datenschutz gerecht zu werden, ist die IT-Administration - in unserem Fall das HRZ - angehalten, Sicherheitsrisiken zu analysieren und negative Auswirkungen auf die Informationssicherheit und der damit verbundenen Verfügbarkeit der Infrastruktur zu verhindern. Hierzu sind nach BSI Grundschutzkatalog und der ISO 2700x bei einem controllerbasierten Netzwerk „*technisch Maßnahmen zu ergreifen*“, die durch das Netzwerkmanagementsystem (NMS) zur Verfügung gestellt werden.

An dieser Stelle wird bereits deutlich, dass wir es ganz offensichtlich mit so genannten „konfligierenden Vorgaben“ zu tun haben: Auf der einen Seite steht die BNetzA mit der Vorgabe, „bestimmungsgemäße WLAN Nutzungen nicht zu stören oder zu unterbinden“, auf der anderen Seite gibt es die DSGVO sowie IT-sicherheitsrelevante Aspekte für eine Organisation zu beachten.

Entscheidungen in einem solchen Spannungsfeld erfordern daher sorgfältige Prüfungen und Abwägungen.

2. Prüfung und Abwägung

 hat hinsichtlich dieser technisch und rechtlichen Frage den Kontakt zur BNetzA aufgenommen. Wir haben das Gespräch offensiv gesucht. Darüber haben wir Anfragen zu diesem Sachverhalt bei der Rechtsstelle des Vereines zur Förderung eines Deutschen Forschungsnetzes (DFN) sowie bei DFN CERT (Mit dem DFN-CERT bietet der DFN-Verein seinen Anwendern Hilfe bei der Reaktion auf Sicherheitsvorfälle sowie Unterstützung bei der Durchführung vorbeugender Sicherheitsmaßnahmen) gestellt.

Interessanterweise haben die Recherchen und Gespräche mit Fachleuten zwischenzeitlich ergeben, dass wir uns ganz offensichtlich in einem aus juristischer Sicht weitgehend unerschlossenen Terrain

befinden, zu dem es in Deutschland noch keine Rechtsprechungen und entsprechende Kommentarliteratur zu geben scheint. So bleibt offen, was die BNetzA meint, wenn sie von absichtlichen Störungen „bestimmungsgemäßer WAS/WLAN-Nutzungen“ spricht bzw. was unter „bestimmungsgemäßer Nutzung“ zu verstehen ist.

Fest steht aber, dass der Netzbetreiber ein legitimes Interesse daran hat, gegen Rogue Access Points vorzugehen, um die Sicherheit seines Netzes zu gewährleisten. Er ist nach § 109 TKG auch verpflichtet, die erforderlichen technischen Vorkehrungen und sonstigen Maßnahmen zum Schutz des Fernmeldegeheimnisses und der Verletzung des Schutzes personenbezogener Daten zu ergreifen, wobei der Stand der Technik zu berücksichtigen ist. Insbesondere müssen wir als Forschungseinrichtung, die darauf angewiesen ist, mit anderen Institutionen zu kooperieren, aber die Sicherheit unserer Infrastruktur gewährleisten, um unserem Forschungsauftrag gerecht zu werden.

Natürlich hat die BNetzA als eine oberste Bundesbehörde mit Satzungsautonomie eine ausgeprägte Wirkmächtigkeit, doch muss eine solche Verbotsverfügung, wie sie allgemein formuliert ist, mit der Zielsetzung eine sicherheitstechnisch umsetzbare Lösung zu finden hinterfragt werden. Dies insbesondere schon deswegen nicht, weil es nicht nur um die Rechte und/oder den Schutz einzelner Personen, sondern um den Schutz der gesamten Organisation der Hochschule geht.

3. Gründe für das derzeitige Vorgehensweise

Aufgrund der sich ständig ändernden Anforderungen in Studium, Lehre und Forschung ergibt sich die Notwendigkeit, diese aufzunehmen und mit der bereitgestellten IT-Infrastruktur bestmöglich zu erfüllen. Dabei wurde und wird unsere IT-Infrastruktur nachweislich kontinuierlich angepasst, z.B. in Form von Integration von WLAN Infrastrukturen einzelner Labore in die gesamte IT-Infrastruktur unserer Hochschule. Die dabei entwickelten und bereitgestellten Lösungen sind im Regelfall Einzelfalllösungen. Jedes Problem wird mit der Nutzerin bzw. dem Nutzer besprochen, mit dem Ziel, gemeinsam ein Konzept für die Integration ins Netzwerk zu entwickeln. Somit stehen in diesem Fall der Nutzerin bzw. dem Nutzer für Sonderkomponenten am Ende stets Lösungen zur Verfügung. Insgesamt stellt das HRZ hochschulweit für Zwecke dieser Art aktuell zehn zusätzliche SSID's zur Verfügung, in denen über 390 Geräte mit besonderem Konfigurationsanforderungen in die WLAN Infrastruktur [REDACTED] integriert worden sind, wie z.B. ssid's [REDACTED] u.a.m..

Das heißt, dass auch unter Berücksichtigung aller relevanten Anforderungen an Datenschutz und Datensicherheit die Integration von WLAN Komponenten in das [REDACTED] nicht nur bereits möglich ist, sondern auch aktiv vom HRZ unterstützt wird.

Leider stehen Betreibern von komplexen WLAN Infrastrukturen nur wenige technische Möglichkeiten zur Verfügung, den Datenschutz und die Verfügbarkeit sicherzustellen. Diese zur Verfügung stehenden Mittel werden aktuell ausgeschöpft. Dabei geht es nicht um das pauschale Stören. Es wurden die Schwellwerte so hoch gewählt, dass die Störung von Rogue AP's erst dann erfolgt, wenn eine sichtbare Beeinträchtigung der Infrastruktur zu verzeichnen ist. Dies zeigen auch die zwei erfolglosen Versuche des Messwagens der BNetzA, die betreiberseitigen Störungen nachzuweisen. Es soll an dieser Stelle nochmals explizit darauf hingewiesen sein, dass das Ziel diese einzige und zur Verfügung stehende technische Lösung zu nutzen darin besteht, Nutzerdaten und die Verfügbarkeit in einem Forschungsnetzwerk zu sichern. Die Störungen nicht [REDACTED] eigener WLAN Sender erfolgt ausschließlich innerhalb der [REDACTED]. Die Wohnheime und angrenzende Installationen sind davon nicht betroffen. Ein Nachfragen bei den Betreibern angrenzenden Installationen ergab keinerlei Einschränkungen durch [REDACTED].

4. Resultierende Schlussfolgerungen

Die aufgeworfene Fragestellung ist für uns von zentraler Bedeutung, denn ein „Freigeben“ unseres Netzes insofern als jede und jeder spontan und ohne Abstimmung ein eigenes Netzwerk einrichten kann, konterkariert alles, was in den letzten Jahren an Maßnahmen in den Bereichen IT-Sicherheit und Datenschutz an [REDACTED] verlangt und aufgebaut worden ist. Die Konsequenzen wären sehr weitreichend und würden nicht nur dazu führen, dass bewährte Partnerschaften insbesondere in Forschung und Transfer aufgrund der von uns nicht mehr zu gewährleistenden IT Sicherheit und der eingegangenen Geheimhaltungsvereinbarungen in Gefahr geraten. Allein bei Verletzungen gegen die unter Art. 83 Abs. 5 DSGVO aufgelisteten besonders gravierenden Verstöße beträgt der Bußgeldrahmen bis zu 20 Millionen Euro. Weiterhin ist [REDACTED] Hochschule in Deutschland nach dem Standard [REDACTED] zertifiziert. Die grundlegende Basis einer erfolgreichen Zertifizierung ist hierbei u.a. ein Nachweis über ein gesichertes Netzwerk, mit speziellen Augenwerk auf die WLAN Installation und die dafür getroffenen TOM's. Eine Abschaltung der einzigen zur Verfügung stehenden TOM kann ggf. dazu führen, die Sicherheitszertifizierung zu verlieren. Diese ist aber für [REDACTED] sehr wichtig, da Forschungs- und Kooperationspartner für eine Zusammenarbeit einen IT Sicherheitsnachweis zunehmend voraussetzen.

Die [REDACTED] kann seit Jahren auf eine zuverlässige und stabile sowie sichere IT Infrastruktur zurückgreifen, die in der bundesdeutschen Hochschullandschaft beispielhaft ist. Wir bitten Sie zu prüfen, welche Wege ggf. beschritten werden können, die berechtigten Forderungen der BNetzA umzusetzen aber in einem geschlossenen Forschungsnetzwerk die gegebenen Anforderungen trotzdem zu erfüllen. Uns ist bewusst, dass diese Anfrage aktuell eine Sonderlösung Ihrerseits voraussetzt, doch sind wir davon überzeugt, dass dieser Widerspruch zwischen einerseits den umzusetzen Sicherheitsanforderungen nach BSI und ISO und den Aufgaben der BNetzA die Frequenzbereiche zu sichern, eine zunehmende Brisanz bekommen wird. Die [REDACTED] ist da sicher aktuell eine der ersten Forschungseinrichtungen, doch die notwendigen Zertifizierungen anderer Forschungseinrichtungen mit geschlossene WLAN Campusnetzen werden zunehmend mit gleiche Fragestellungen konfrontieren werden.

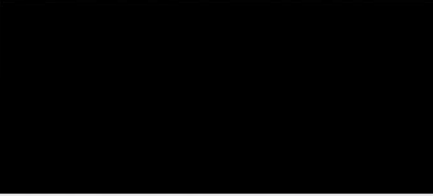
Sehen Sie eine Möglichkeit über beispielsweise einer stillschweigenden Duldung oder anderer Ihnen zur Verfügung stehenden Mittel die [REDACTED] bei der Lösung der o.g. Fragestellung zu unterstützen? Wir bitten Sie freundlichst um Unterstützung zur Lösung dieses Problems. Gerne möchten wir mit Ihnen ins Gespräch kommen, um eine tragbare Lösung für beide Seiten zu finden.

[REDACTED]
Mit freundlichen Grüßen
[REDACTED]



Außenstelle Berlin

Bundesnetzagentur • DLZ8 • Seidelstraße 49 • 13405 Berlin



Ihr Zeichen, Ihre Nachricht vom

Mein Zeichen, meine Nachricht vom
Berl8
D001/00658/18

☎ 030)
43741200
oder -12 10

Berlin
15.10.2019

Umgang mit Rogue Access Points

Sehr 

Ihre Anfrage bezüglich der Duldung von Deauthentifizierung vom 19.09.2019 habe ich mit unseren zuständigen Juristen diskutiert.

Laut Ihrem Schreiben soll der Wirkungsbereich des Störmechanismus auf den Campus der Hochschule begrenzt sein. Die rechtliche Bewertung von Deauthern unterscheidet sich allerdings nicht danach, ob diese innerhalb oder außerhalb von Grundstücken eingesetzt werden. Auch, wenn ein Störsender innerhalb eines privaten Grundstücks oder Gebäudes eingesetzt wird, gelten die Regelungen des Telekommunikationsgesetzes uneingeschränkt. Diese sehen vor, dass Frequenzen effizient und störungsfrei sowie mit anderen Frequenznutzungen verträglich genutzt werden (vgl. etwa § 2 Abs. 2 Nr. 7, § 52 Abs. 1, § 55 Abs. 5 Satz 1 Nr. 4 TKG).

Angesichts dieser eindeutigen Gesetzeslage vermögen auch datenschutzrechtliche Erwägungen auf Ihrer Seite keine andere rechtliche Beurteilung zu rechtfertigen. Die Gewährleistung eines stabilen und sicheren WLAN-Netzwerks fällt in den originären Aufgabenbereich der Hochschule. Das von Ihnen angeführte Spannungsverhältnis zwischen Datenschutz und störungsfreier Frequenznutzung kann auch durch hochschulinterne Maßnahmen gelöst werden. Dass unbefugte Dritte Zugriff auf hochschulinterne Daten erhalten, kann etwa durch eine sichere Verschlüsselung des hochschuleigenen WLANs sichergestellt werden. Auch bleibt es der Hochschule unbenommen, ihre Nutzer auf privatrechtlichem Weg, etwa mit einer Hausordnung oder entsprechend gestalteten Arbeitsverträgen dazu zu verpflichten, keine eigenen WLAN-Sender neben dem hochschuleigenen Netzwerk zu nutzen oder sensible Forschungsinformationen nicht über das allgemein zugeteilte und somit öffentlich zugängliche WLAN zu verschicken. Hierdurch würde sowohl das Problem des Datenschutzes als auch der Stabilität des WLAN-Netzes adressiert. Durch die genannten Maßnahmen wäre es Ihnen somit möglich, die gesetzlichen und untergesetzlichen Anforderungen des Datenschutzes (insbes. § 109 TKG, BSI-Grundschutzkatalog) zu wahren.

Die Deauthentifizierung fremder WLANs mittels sog. Deauther und Wireless Protection Policies verstößt auch bei Berücksichtigung von Aspekten des Datenschutzes und der Datensicherheit gegen den Grundsatz einer effizienten und störungsfreien Frequenznutzung sowie gegen die WLAN-Allgemeinzuteilungen und ist daher unzulässig. Sie kann deshalb nicht geduldet werden.

Ich möchte Sie darauf hinweisen, dass der Verstoß gegen eine Allgemeinzuteilung nach § 149 Abs. 1 Nr. 10 TKG als Ordnungswidrigkeit geahndet werden kann.

Mit freundlichen Grüßen
Im Auftrag

