

Transkript Podcastfolge: Die Strafbarkeit des digitalen Hausfriedensbruchs

Ein Beitrag von Johanna Voget, Klaus Palenberg und Nicolas John, 6. Juli 2022

Beschreibung:

Kriminalität macht bekanntermaßen auch vor dem Internet keinen Halt. Schon jetzt sind Hasskommentare und Drohungen in sozialen Netzwerken allgegenwärtig. Doch nicht nur Taten gegen die persönliche Ehre nehmen im digitalen Raum weiter zu, sondern auch Angriffe gegen Unternehmen und Einrichtungen werden immer häufiger wahrgenommen. So sind DDoS-Angriffe oder Verschlüsselungstrojaner auch für IT-Laien keine völlig unbekanntenen Begriffe mehr. Aufgrund dieser Entwicklungen legte der Bundesrat nach hessischer Initiative dem Bundestag einen Gesetzesentwurf zur Strafbarkeit des „Digitalen Hausfriedensbruchs“ vor. Die Wissenschaftlichen MitarbeiterInnen Nicolas John und Johanna Schaller diskutieren in dieser Folge von Weggeforscht nicht nur die Hintergründe und den Inhalt des Gesetzesentwurfs, sondern geben einen kleinen Überblick über die vielseitige Kritik an dem Gesetzesvorschlag.

Vertiefend erscheint zu dieser Thematik im August ein Beitrag im DFN-Infobrief Recht, welcher [hier](#) abrufbar sein wird.

Transkript

00:00:06 Palenberg

Weggeforscht: Der Podcast der Forschungsstelle Recht im DFN.

00:00:14 John

Herzlich Willkommen zu einer neuen Folge unseres Podcasts. Mein Name ist Nicolas John und ich sitze hier heute mit meiner Kollegin Johanna Schaller. Ja, eigentlich sollten heute hier unsere Kollegen Owen und Klaus zu hören sein, leider fallen sie jetzt wegen Krankheit aus, aber wir dachten uns, wir springen einfach spontan ein, was aber nicht heißt, dass das Thema heute weniger spannend ist.

Es geht heute um einen vom Bundesrat vorgelegten Gesetzesentwurf zum digitalen Hausfriedensbruch. Zu dieser Thematik wird dann auch im August einen Infobrief Beitrag erscheinen, den wir dann später verlinken werden. Aber zuerst: was gibt es Neues?

00:00:47 Voget

Fluggastdaten: der Europäische Gerichtshof hat der Datenspeicherung bei Flügen durch eine Entscheidung enge Grenzen gesetzt. Zwar wurde die Speicherung von Fluggastdaten nicht grundsätzlich gestoppt, jedoch wurde sie in einigen Punkten erheblich eingegrenzt. Daten von Flügen innerhalb Europas, dürfen nach dieser Entscheidung nicht mehr anlasslos, sondern nur noch im Fall einer konkreten terroristischen Bedrohung ausgewertet werden. Außerdem dürfen die Daten nur noch 6 Monate anstatt von 5 Jahren gespeichert werden. Nur wenn sich innerhalb dieser 6 Monate einen Zusammenhang zu einer gefährlichen Straftat ergibt, ist eine längere Speicherung zulässig. Ganz verboten wurde die Speicherung der Daten von Bus- und Bahnreisenden.

Und noch eine weitere Entscheidung: höhere Geldbußen für SUV Fahrer:innen. Das Amtsgericht Frankfurt am Main hat entschieden, dass SUV Fahrer:innen ein höheres Bußgeld zahlen müssen als

andere Verkehrsteilnehmende. Als Grund führt das Gericht an, dass die Bauweise eines SUVs das Verletzungsrisiko für andere Verkehrsteilnehmende deutlich erhöhe, weil hierdurch die Gefährdung bei einem Rotlichtverstoß höher sei als normalerweise, sei eben auch eine höhere Geldbuße gerechtfertigt. Das Urteil ist aber noch nicht rechtskräftig. Das heißt die Parteien können noch Rechtsmittel dagegen einlegen.

00:01:58 John

Nun zu unserem Hauptthema.

Kriminalität, wissen wir alle, macht bekanntermaßen keinen Halt auch vor dem Internet. Hasskommentare, Drohungen, all das gehört leider zu unserem Alltag in der digitalen Welt.

Doch nicht nur Straftaten gegen die sogenannte persönliche Ehre häufen sich im Internet, sondern auch koordinierte Angriffe gegen Einrichtungen nehmen stetig zu, bekommen wir regelmäßig in der Zeitungen mit, aber während die Delikte gegen die persönliche Ehre bereits unter existierende Straftatbestände unseres deutschen Strafgesetzbuchs fallen, ist das bei digitalen Handlungen gegen Einrichtungen teilweise vielleicht ein bisschen anders. Der Bundesrat zumindest sieht hier Handlungsbedarf und hat deshalb auf hessische Initiative dem Bundestag nun einen Gesetzentwurf zur Strafbarkeit des sogenannten digitalen Hausfriedensbruchs vorgelegt.

00:02:42 Voget

Ja, hallo und herzlich willkommen auch meinerseits das klingt alles schon mal sehr spannend. Was hat es denn mit dem Entwurf genau auf sich?

00:02:49 John

Ja, im Zentrum dieses Vorschlags stehen vor allem digitale Angriffe also sowas wie die DDos Angriffe oder Angriffe mit Trojanern.

00:02:57 Voget

Okay, jetzt wissen Sie ja nicht alle unsere Zuhörenden und ich ebenso was das genau für Angriffe sind? Wie funktionieren die denn?

00:03:04 John

Ja, das ist verständlich, auch ich habe mich da erstmal im Vorfeld dazu einlesen müssen. DDos-Angriffe sind vereinfacht gesagt Angriffe, die das Ziel haben, ein zum Beispiel im Web Space einen Server, eine Website lahmzulegen und damit das die angreifenden auch umsetzen können, nutzen sie dafür teilweise hunderttausende verschiedene Computer, die zeitgleich auf dieses Internetangebot zugreifen. Und durch dieses sogenannte Bot Netz und diese Größe schaffen das die Server nicht mehr aktiv zu bleiben, und brechen sozusagen zusammen und die Erreichbarkeit des Dienstes ist dann in diesem Fall dann nicht mehr gegeben.

00:03:38 Voget

Okay, klingt kompliziert? Und was ist mit Trojanern?

00:03:42 John

Ja, Trojaner haben wir jetzt in letzter Zeit leider auch schon öfter in der Presse lesen müssen, dass diese Angriffe immer mehr und mehr zunehmen. Meistens läuft es so, dass die Angreifenden eine harmlos und sehr echt aussehende Email an Mitarbeitende in einem in einer Behörde oder einem Unternehmen oder auch in den Hochschulen versenden und innerhalb dieser Email ist dann ein Link oder eine Software zum Download angeboten. Und wenn diese Software dann runtergeladen ist und installiert wird, dann geht eigentlich der Angriff an sich erst so richtig los, weil diese Software fängt zum Beispiel an bei Verschlüsselungstrojanern alle Daten einfach, die es greifen kann, zu verschlüsseln und teilweise installiert sich diese Software automatisch auf weiteren PCs. Das Problem an diesen ganzen verschlüsselten Daten ist dann eben, dass niemand mehr auf diese Daten zugreifen kann, wenn er nicht den entsprechenden Schlüssel hierfür hat und das bedeutet, dass die Hochschulen oder auch Behörden, die angegriffen worden sind, keinerlei Daten mehr verwenden können und damit praktisch handlungsunfähig sind, weil ohne die Daten die Arbeit natürlich digital nicht mehr gemacht werden kann, und da setzen die Angreifenden dann da drauf, dass dann eine entsprechende Lösegeldforderung erfüllt wird.

00:04:48 Voget

Okay. Lösegeldforderung das klingt ja fast nach Entführung und all diese Handlungen sind bis jetzt in Deutschland nicht strafbar?

00:04:55 John

Ja, so pauschal lässt sich das leider gar nicht beantworten. Wir haben natürlich in Deutschland diverse Tatbestände, die im digitalen Raum schon da zuschlagen, zum Beispiel eben die Paragraphen 202a, 303a und 303b des Strafgesetzbuches zum Beispiel 202a stellt das Ausspähen von Daten unter Strafe. Wenn sich also jemand unbefugt Zugang zu Daten verschafft, die nicht für ihn bestimmt sind oder wenn er sich unberechtigten Zugang zu besonders gesicherten Daten verschafft, dann ist diese Handlung eben strafbar und auch die anderen Paragraphen haben entsprechende Tatbestände. Letztendlich ist aber immer eine Auslegungssache, wie es leider im Juristischen ja der Fall ist und ob die jetzt darunter fallen oder nicht, das ist eben die Frage.

00:05:38 Voget

Ok, also es existieren bereits umfassende Regelungen im Strafrecht, die auch kontrollierte Angriffe aus dem Netz unter Strafe stellen. Welche Handlungen sind denn dann bislang nicht von den bestehenden Normen umfasst, also inwiefern besteht dann überhaupt noch Regelungsbedarf?

00:05:52 John

Ja, genau. Der Bundesrat vertritt hier die Position, dass zum Beispiel bei eben mit 202a wie eben gesagt, die Daten nur dann geschützt sind, wenn bei dem unberechtigten Zugriff eine besondere Zugangssicherung überwunden wird. Und wenn jetzt der Täter oder die Täterin zum Beispiel schon alle Passwörter kennt, weil sie über die Schulter zum Beispiel geschaut haben, dann fällt das eben nicht mehr unter diesen Tatbestand und auch bei den anderen Tatbeständen eben 303 a oder 303b StGB sieht hier der Bundesrat entsprechende ja Strafbarkeitslücken, also kurzum er möchte mit der Einführung dieses neuen Tatbestandes, was er vorgelegt hat, diesen Strafbarkeitslücken entgegenwirken.

00:06:29 Voget

Das macht natürlich Sinn. Und wie genau soll der digitale Hausfriedensbruch dann die angenommenen Strafbarkeitslücken schließen und wie soll die Verfolgbarkeit von Computerstraftaten verbessert werden?

00:06:39 John

Der Bundesrat hat jetzt in seinem Vorschlag einfach einen neuen Paragraphen vorgeschlagen den sogenannten 203e, nun, wir haben noch mehr Buchstaben, das ist schön, aber was bringt das jetzt? Inhaltlich soll diese neue Regelung die unbefugte Benutzung informationstechnischer Systeme unter Strafe stellen. Das heißt also jetzt ein bisschen einfacher gesprochen: dieser Tatbestand soll einfach digitale Angriffe jeglicher Art umfassen, insbesondere eben auch die Benutzung fremder Computer, eben wenn man einen Angriff durchführt, weil, was wichtig ist zu wissen, diese großen bot-Netze von diesen hunderttausenden Computern, das sind meistens nicht die Rechner der Angreifenden selbst sondern die bedienen, sich wieder fremder Rechner und damit auch eigentlich nicht berechtigter Weise natürlich. Keiner möchte, dass sein Rechner für einen Angriff verwendet wird und genau darauf zielt dieser Tatbestand eben ab, dass das auch sicher unter Strafe steht nach Ansicht des Bundesrates. Und wenn es dann zu einem Angriff kommt, muss dieser Angriff nicht mal erfolgreich sein, um den Tatbestand zu erfüllen, sprich es muss nur eine Handlung vorgenommen werden. Das ist besonders weil normalerweise gibt es, also es gibt sehr viele Tatbestände im Strafgesetzbuch, die eben eine Erfolg verlangen. Hier reicht allein schon die Handlung aus, allerdings muss diese Handlungen dafür geeignet sein, berechnete Interessen eines anderen zu beeinträchtigen. Wenn das dann eben erfüllt sein sollte, sieht hier der Tatbestand recht empfindliche Strafen vor. Höchststrafen sind tatsächlich bis zu 10 Jahre, wenn kritische Infrastrukturen wie Energie, Versorger oder sowas angegriffen werden.

00:08:07 Voget

Okay? Der Bundesrat sieht also erhebliche Lücken in der Strafbarkeit. Sehen das denn jetzt andere, zum Beispiel die Bundesregierungen oder Stimmen in der Literatur auch so und wird das Strafrecht bald um den Tatbestand eines digitalen Hausfriedensbruchs erweitert?

00:08:21 John

Ja, momentan kann man kann man genau das eigentlich nicht sagen. Es mehren sich mehr und mehr Stimmen, die das diesen Vorschlag ganz klar kritisieren. Die Meinungen hierzu sind vielfältig. Die Gründe eben reichend von es gibt diese Regelungslücke eigentlich gar nicht, es hat keine Praxisrelevanz, der vorgeschlagene Tatbestand, sei viel zu weit gefasst oder auch in der Begründung des Bundesrates beziehen sie sich zum Beispiel auf eine bestimmte Rechtsprechung des Bundesverfassungsgerichts hier, diese Rechtsprechung sei einfach auch falsch interpretiert worden. Und diese Kritiken stehen momentan doch mehrheitlich im Raum.

00:08:57 Voget

Okay ja, auch nochmal für mich zum Festhalten. Es werden also grundsätzlich schon nahezu alle Cyberangriffe ob mittels eines Bot Netzes oder eines Verschlüsselungstrojaners von den existierenden Regelungen des Strafrechts erfasst?

00:09:09 John

Ja, zumindest die Kritiker:innen des Entwurfs sind sich da einig, dass die angebliche Regelungslücke in diesem Ausmaß, wie es der Bundesrat darstellt, gar nicht existiert. Denn zum Beispiel das

Programmieren einer Schadsoftware, welche die Errichtung eines bot-Netztes eben zum Beispiel ermöglichen kann, fällt nach der Meinung der Kritiker innen schon unter 202c StGB, dem Vorbereiten des Ausspähen und Abfangen von Daten. Oder auch der Aufbau eines bot Netztes fällt nach deren Meinung unter den Tatbestand des 202a StGB, eben dem Ausspähen von Daten, also die Kritiker:innen sind sich da ziemlich einig, dass diese große Regelungslücke, wie es der Bundesrat darstellt, gar nicht existiert.

00:09:48 Voget

Okay, aber wie ich das jetzt verstanden habe, ist das auch gar nicht nur der einzige Kritikpunkt. Was wird denn alles noch gegen den Entwurf des Bundesrats vorgebracht?

00:09:54 John

Ja, ich habe es gerade eben ja schon mal so kurz angeteasert. Es gibt auch die Meinung, dass der Tatbestand einfach viel zu weit gefasst ist. Tatsächlich ist es so, dass man momentan fast nur so interpretieren kann, dass auch Alltagsverhalten plötzlich kriminalisiert wird. Durch diesen 203e StGB, also zum Beispiel jetzt ganz praktisch, wenn man ein Smartphone anschaltet, das nicht nur durch ein Passwort gesichert ist, aber das halt nicht berechtigterweise anschaltet, dann wäre so eine Handlung plötzlich strafbar oder wenn man sich in ein ungesichertes WLAN einwählt, obwohl man das nicht darf und sie nicht um Erlaubnis gefragt hat. Das werden plötzlich Alltags Handlungen, die unter Strafe stehen würden.

00:10:30 Voget

Okay, und es war ja auch noch Ziel des Gesetzentwurfs ist, dass die Verfolgbarkeit von Straftaten erleichtert werden soll. Gibt es denn hierzu auch Stimmen oder Kritik?

00:10:40 John

Ja. Der Bundesrat stellt sich das eben genauso vor dadurch, dass nur die Handlung ausreichen soll für die Strafbarkeit wäre die Beweisführung vor Gericht am Ende etwas vereinfacht. Tatsächlich sagen aber die Kritiker:innen naja, es passiert alles im Geheimen, man kriegt das ja noch nicht mal mit, wenn ein bot-Netz überhaupt errichtet wird, also sprich die Verfolgung wird nicht vereinfacht durch diesen Tatbestand, sondern die, die Fakten sind einfach so, dass das gar nicht bemerkt wird.

00:11:04 Voget

Gut. Der vom Bundesrat vorgelegte Entwurf wird also durch die Bundesregierung und juristische Literatur fast ausschließlich kritisiert aber wie geht es dann jetzt weiter?

00:11:14 John

Ja, wie es nun konkret mit dem Entwurf des Bundesrates weitergeht, ist erstmal offen. Die Entscheidung über eine Annahme dieses Gesetzesentwurfs obliegt dem Bundestag, logischerweise. Was hier an dieser Stelle jetzt aber nochmal anzumerken ist, ist, dass das nicht der erste Vorstoß des Bundesrates in dieser Art ist. Sowohl 2016 als auch 2018 hatte der Bundesrat genau diesen gleichen Paragraphen im selben Wortlaut auch dem Bundestag schon mal vorgelegt. Das Problem war nur damals, dass die Legislaturperiode endete und am Ende hat man das ganze Verfahren nicht mehr weiterverfolgt und für erledigt erklärt. Ob der Bundestag dann diesmal einen eventuell anderslautenden Beschluss fassen wird, scheint aber eben aufgrund dieser ähnlichen Verhältnisse, die schon 2016 und 18 der Fall waren, unwahrscheinlich, aber es bleibt erstmal abzuwarten.

00:11:59 Voget

Ok, danke dir Nicolas für diese ausführlichen Erläuterungen.

00:12:02 John

Ja, an an dieser Stelle möchte ich auch noch mal ganz kurz auf den kommenden Infobrief Beitrag im August hinweisen. Aufgrund des kurzfristigen Einsprungs komplett erst nach der Folge raus, aber wir werden hier natürlich verlinken, sobald er veröffentlicht ist.

00:12:12 Voget

Da haben wir heute auf jeden Fall wieder einiges weggeforscht und wir bedanken uns auch bei Ihnen und Euch allen fürs Zuhören und freuen uns schon auf das nächste Mal.

00:12:21 John

Ja, auch vielen Dank dir, liebe Johanna auf Wiedersehen. Tschüss.