Portscans im Lichte des Rechts: eine straf- und zivilrechtliche Analyse

Ferdinand Grieger

Eingegangen: 27. Juli 2021 / Angenommen: 16. August 2021 / Online publiziert: 4. Oktober 2021
© Der/die Autor(en) 2021

Zusammenfassung Die Prüfung von IT-Sicherheitsstrukturen mithilfe von Portscans wurde im Rahmen des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (nachfolgend auch „IT-SiG 2.0“ genannt) kontrovers diskutiert. Das Bundesamt für Sicherheit in der Informationstechnik (nachfolgend „BSI“ genannt) ist nach Umsetzung des IT-SiG 2.0 zur Vornahme von Portscans zur Prüfung der IT-Sicherheitsstruktur bestimmter Unternehmen berechtigt. Angesichts des dem IT-SiG 2.0 vorgelagerten Gesetzgebungsverfahrens haben sich die Schwächen bei der rechtlichen Einschätzung von Portscans unter dem StGB und dem Deliktsrecht offenbart. Mit unterschiedlichen oder gänzlich ohne Begründungen wurden Portscans durch verschiedene Interessenverbände als Computerstraftat oder deliktsrechtlich relevant eingestuft, während andere diese minimal-invasive Maßnahme zur Sicherstellung der IT-Sicherheit von Unternehmen uneingeschränkt willkommen heißen haben. Die vorgenannte Diskrepanz in der rechtlichen Beurteilung von Portscans ist auch in der juristischen Literatur und Praxis wiederzufinden. Der Beitrag versucht diese Unsicherheiten aufzugreifen und Klarheit in den Fragen der rechtlichen Bewertung von Portscans unter dem StGB und dem Deliktsrecht zu schaffen. Richtungsweisende Rechtsprechung hierzu existiert bislang nicht. Angesichts der steigenden Bedeutung der IT-Sicherheit für alle Marktteilnehmer unterschiedlichster Art und Größe ist die Frage nach der rechtskonformen Einsatzmöglichkeit dieses Sicherheitstools auch abseits vertraglicher Beziehungen von elementarer Bedeutung. Die besonderen Anforderungen für Portscans staatlicher Stellen bleiben bei der hiesigen Analyse außen vor.

Ferdinand Grieger (✉)

Chief Legal Officer, Deutsche Gesellschaft für Cybersicherheit, Zürich/Berlin, DGC Switzerland AG,
Beethovenstrasse 7, 8002 Zürich, Schweiz
E-Mail: ferdinand.grieger@dgc.org

Schlüsselwörter Computerstrafrecht · IT-Sicherheit · IT-SiG 2.0 · Deliktsrecht · Mitverschulden

Port scans in the light of the law: a criminal and civil law analysis

Summary The testing of IT security structures with the help of portscans was controversially discussed in the context of the German Second Act to Increase the Security of Information Technology Systems (hereinafter also referred to as “IT-SiG 2.0”). Following implementation of the IT-SiG 2.0, the Bundesamt für Sicherheit in der Informationstechnik (hereinafter also referred to as “BSI”) is authorized to perform port scans to examine the IT security structure of certain companies. In light of the legislative process leading up to IT-SiG 2.0, weaknesses in the legal assessment of portscans under the German penal code and tort law have become apparent. With varying or no justification at all, portscans have been classified by various interest groups as a computer crime or relevant under tort law, while others have unreservedly welcomed this minimally invasive measure for ensuring corporate IT security. The aforementioned discrepancy in the legal assessment of portscans can also be found in legal literature and practice. This article attempts to address these uncertainties and provide clarity on the legal assessment of port scans under the German Penal Code (StGB) and tort law. To date, there is no case law that points the way forward. In view of the increasing importance of IT security for all market participants of different types and sizes, the question of the legally compliant use of this security tool is of fundamental importance, even outside of contractual relationships. The special requirements for port scans of governmental agencies are left out of the analysis here.

Keywords Computer criminal law · IT security · IT SiG2.0 · Law of torts · Contributory negligence

1 Einleitung

Die Umsetzung des IT-SiG 2.0¹ ermöglicht es dem Bundesamt für Sicherheit in der Informationstechnik (nachfolgend „BSI“ genannt) unter bestimmten Voraussetzungen, zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken, Portscans bei Einrichtungen des Bundes, KRITIS-Unternehmen, Anbietern digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse durchzuführen, § 7b Abs. 1 S. 1 BSIG². Diese Ermächtigungsgrundlage soll es dem BSI ermöglichen, nach Sicherheitslücken zu suchen und die Betroffenen zu informieren, damit diese sie schließen. Zweifelsohne sind die Ergebnisse solcher Portscans für die Arbeit des BSI und die Cybersicherheit der durch den Portscan geprüften Systeminhaber

¹ Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, Bundesgesetzblatt Jahrgang 2021, Teil I NR. 25, S. 1122, 17. Mai 2021.

² Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), Bundesgesetzblatt Jahrgang 2009 Teil I Nr. 54, 19. August 2009.

ber von großer Bedeutung. Offene Ports sind ein potenzielles Einfallstor für Hacker. Diese können nahezu jede Art von Datenpaket zur Schädigung oder Übernahme von Systemen durch den Port senden. Die oben genannten Unternehmen, deren reibungsloser Betrieb von gesamtgesellschaftlicher Bedeutung ist, könnten hierdurch Ausfälle erleiden.

Automatisierte Portscans sind ein wichtiges Tool zur Entdeckung von kritischen Schwachstellen in IT-Systemen. Dennoch waren Portscans schon im Gesetzgebungsverfahren auf dem Weg zum IT-SiG 2.0 keinesfalls unumstritten. Von einem Teil der zur Stellungnahme zum Gesetzesentwurf aufgeforderten Verbände wurde die vorgenannte Ermächtigung des BSI ausdrücklich begrüßt,³ während sie von anderen Verbänden kritisch beurteilt und im Ergebnis abgelehnt⁴ wurde. Das Gesetzgebungsverfahren hat außerdem gezeigt, dass Portscans rechtlich sehr unterschiedlich eingeschätzt werden. Während diese von einem Großteil der Praxis und einem Teil der Interessenverbände als wirksames, rechtlich unbedenkliches Mittel zur Erkennung von Schwachstellen bezeichnet werden, halten andere Meinungen Portscans für einen unzumutbaren Eingriff in die Sphäre der Gescannten oder sogar für strafrechtlich⁵ relevant.⁶ Diese Unsicherheit der rechtlichen Bewertung von Portscans ist im Hinblick auf deren Bedeutung für die Cybersicherheitsstrategien vieler Marktteilnehmer mehr als misslich. Portscans gehören (oder sollten es zumindest) zum festen Bestandteil der Cybersicherheitsstrategie jedes Unternehmens, welches sich ernsthaft mit Cybersicherheit beschäftigt. Auch die Arbeit von auf Cybersicherheit spezialisierten Unternehmen, welche auf Portscans zurückgreifen, ist von dieser wahrgenommenen Unsicherheit geprägt. Vor allem abseits vertraglicher Beziehungen ist der Einsatz von Portscans äußerst umstritten.

Dieser Beitrag untersucht die Funktionsweise eines Portscans (hierzu sogleich unter 2.) im Lichte der im deutschen Strafgesetzbuch enthaltenen „Computerstraftaten“ (hierzu sogleich unter 3.) und des Zivilrechts (hierzu sogleich unter 4.). Die strafrechtliche Beurteilung beschränkt sich dabei ausschließlich auf Sachverhalte, die eine Überprüfung einer strafbaren Beihilfe nicht zulassen.

Sofern eine Beauftragung des Scannenden mit einer IT-Sicherheitsanalyse vorliegt, ergeben sich die wesentlichen Pflichten des Auftragnehmers im Verhältnis zum gescannten Auftraggeber aus dem zwischen ihnen begründeten Schuldverhältnis. Die hier dargestellte Analyse bezieht sich daher ausschließlich auf das Deliktsrecht.⁷ Dabei soll die Frage beantwortet werden, ob Portscans von auf Cybersicherheit spezialisierten Unternehmen ähnlich wie vom BSI auch ohne vertragliche Beziehung

³ Stellungnahme des BDEW zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 10; Stellungnahme der DENIC zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 2; Stellungnahme der AG KRITIS zum Gesetzesentwurf zum IT-SiG 2.0 vom 3. Dezember 2020, S. 9.

⁴ Stellungnahme des Bitkom zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 10. Stellungnahme des BvD zum Gesetzesentwurf zum IT-SiG 2.0 vom 8. Dezember 2020, S. 7.

⁵ Eine (höchst)richterliche Entscheidung hierzu liegt derzeit noch nicht vor, vgl. Böken in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 15, Rdn. 72.

⁶ So bspw. die Vertretung des Verbands der Internetwirtschaft e. V., vgl. Stellungnahme des eco zum Gesetzesentwurf zum IT-SiG 2.0 vom 9. Dezember 2020, S. 4.

⁷ Aus Vereinfachungsgründen wird dem Scannenden der Fremdgeschäftsführungswille hier pauschal abgesprochen.

zu den Inhabern der gescannten Systeme konform mit der deutschen Rechtsordnung eingesetzt werden können. Die hiesigen Betrachtungen sind dabei auf Portscanner mit der unter der Ziffer 2 dargestellten Funktionsweise beschränkt.

2 Funktionsweise eines Portscans und Abgrenzung zu (D)DoS-Attacken

2.1 Funktionsweise

Um Portscans sinnvoll einer rechtlichen Analyse unterziehen zu können, ist es zwingend notwendig, zuvor die Funktionsweise eines Portscanners verbindlich festzulegen. Mit dem Internet verbundene Computersysteme haben zum Internet hin mehrere Ein- und Ausgänge (Ports).⁸ Ein System kann bis zu 65.535 Ports haben. Hinter jedem Port kann sich eine Applikation verbergen.⁹ Beim Portscanning werden diese Ports von außen „abgetastet“. Durch das Aussenden von Anfragen (sogenannten Requests) in Form kleiner Datenpakete¹⁰ kann der Portscanner anhand des Antwortverhaltens¹¹ des gescannten Systems herausfinden, ob der angefragte Port offen ist und welche Netzwerkdienste auf den jeweiligen Ports laufen.¹² Besteht bei einer mit einem Port verknüpften Applikation eine Sicherheitslücke,¹³ wird die Kommunikation zwischen Absender und Empfänger der Requests fehlerhaft.

Solche Sicherheitslücken im Bereich der Portkommunikation treten sehr häufig auf. Diese werden üblicherweise im Internet veröffentlicht, um jedem Systembetreiber die Möglichkeit zu bieten, sein System auf Lücken zu testen und diese zu schließen. Weder das Portscanning noch die Art und Häufigkeit der gefundenen Sicherheitslücken sind dabei heimlich. Der Portscanner selbst steht ebenso wie die hierdurch in Erfahrung gebrachten Erkenntnisse jedermann zur Verfügung. Schließlich handelt es sich bei der Portkommunikation um eine vom System selbst vorhergesehene Kommunikation nach außen mit jedem Anfragenden.¹⁴ Ein Eingriff in die Systeme findet zu keinem Zeitpunkt statt.

Üblicherweise ist einem Portscanner auch ein Schwachstellenscanner nachgeschaltet. Dieser nimmt auf den gefundenen offenen Ports portspezifische Analysen vor und protokolliert die hieraus entstehenden Ergebnisse. Diese werden üblicherweise nicht dazu genutzt, in die zuvor gescannten Systeme einzudringen oder Daten zu verändern.

⁸ Rinker, MMR 2002, 664.

⁹ Bspw. Port 80 als Standard für einen Webserver.

¹⁰ Böken in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 15, Rdn. 72.

¹¹ Man kann insoweit auch vom „Abklingeln“ von Ports sprechen; vgl. Stellungnahme der DENIC zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 2.

¹² Rinker, MMR 2002, 664.

¹³ Fehlt bspw. bei einem Remote-Shell-Dienst das Passwort, können sich Hacker ohne Beschränkung bei diesem System anmelden.

¹⁴ Man kann insoweit auch von einer Art Grundrauschen im Internet sprechen, vgl. Stellungnahme der DENIC zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 2.

2.2 Abgrenzung zu DoS- und DDoS-Attacken

In der Praxis und in Teilen der juristischen Fachliteratur werden Portscans immer wieder fälschlich als Denial-of-Service(DoS)- oder Distributed-Denial-of-Service(DDoS)-Angriffe bewertet. Auch im Gesetzgebungsverfahren zum IT-SiG 2.0 gab es Hinweise darauf, dass Portscans innerhalb der dort gehörten Interessenverbände zum Teil als Angriff gewertet werden.¹⁵ Ohne Zweifel sind die vorgenannten Angriffe, sofern sie denn vorliegen, auf kriminelle Intentionen zurückzuführen. Keinesfalls kann mit einem DoS- oder einem DDoS-Angriff das Ziel eines redlich agierenden Unternehmens oder im Falle des BSI einer staatlichen Einrichtung nach mehr Cybersicherheit erreicht oder unterstützt werden. Erfolgreiche (D)DoS-Angriffe können je nach dem zugrunde liegenden Sachverhalt die Tatbestände der §§ 303a, 303b StGB¹⁶ erfüllen. Hinzu kommen möglicherweise lauterkeitsrechtliche Implikationen.¹⁷ Jedoch weicht die Vorgehensweise bei diesen Angriffen von der oben beschriebenen Funktionsweise eines Portscans erheblich ab.

Bei einem DoS-Angriff besteht das Ziel in der Überlastung des Zielrechners. Durch massenhafte und gleichzeitige Zugriffe in Form von Requests soll ein Server außerstande gesetzt werden, diese Anfragen zu bedienen.¹⁸ Das Zielsystem wird dabei mit hoher Geschwindigkeit und einer großen Zahl von Requests adressiert. Dies wird so lange durchgeführt, bis die beabsichtigte Systemüberlastung eingetreten ist. Bei DDoS-Attacken wird mithilfe einer großen Anzahl von angreifenden Rechnern ein koordinierter Angriff auf ein Zielsystem gefahren, um dessen Überlastung hervorzurufen. Der Angreifer übernimmt im Vorfeld oft unbemerkt eine Vielzahl von Einzelrechnern¹⁹ und verwandelt sie in ein Netz („Botnetz“) sogenannter Zombierechner.²⁰ Auf ein Triggersignal löst der Angreifer eine Vielzahl von Requests der zuvor gekaperten Rechner des Botnetzes aus und überlastet so das Zielsystem. Die Zombierechner wissen oft nichts von ihrer Funktion als Werkzeug. Die Vielzahl der Systeme aus dem Botnetz macht es für das Opfer nahezu unmöglich, den Ursprung der Attacke parallel zur Bekämpfung ihrer Auswirkung zu lokalisieren.

Die Funktionsweise des Portscanners ist mit der Blaupause solcher Angriffe in mehrerlei Hinsicht nicht vergleichbar. Angreifer hinterlassen entweder keine, gezielt wenige fremde oder unzählige Hinweise, welche die Ermittlung des für einen Angriff Verantwortlichen erschweren. Bei einem einfachen Portscan wird üblicherweise auf Heimlichkeiten und Spurenverwischen verzichtet. Zum Teil wird im User-Agent-String sogar ausdrücklich auf den Scanner hingewiesen. Durch einfache Recherchen kann dann Kontakt zum Betreiber des Scanners aufgenommen werden.

¹⁵ Stellungnahme des BvD zum Gesetzesentwurf zum IT-SiG 2.0 vom 8. Dezember 2020, S. 7.

¹⁶ Ggf. in Verbindung mit § 202c StGB.

¹⁷ Bspw. nach §§ 4 Nr. 4, 4a oder 7 Abs. 1 UWG.

¹⁸ Ernst, NJW 2003, 3235.

¹⁹ Universitäten sind wegen des geringen Sicherheitsniveaus und der hohen Zahl von Rechnern hierbei ein beliebtes Ziel.

²⁰ Sohr/Kemmerich in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 2, Rdn. 183.

Dieser Umstand wäre bei einer inkriminierten Herangehensweise wie bei (D)DoS-Angriffen nicht im Sinne des Täters.

(D)DoS-Angriffe zeichnen sich weiterhin durch eine sehr hohe Zahl von Anfragen binnen einer sehr kurzen Zeit aus. Je nach Größe des aufgebauten Botnetzes können so zig Millionen, hunderte Millionen oder gar Milliarden Anfragen in sehr kurzer Zeit an die Opfersysteme ausgesendet werden. Da ein Portscanner aber nicht den Absturz eines Systems anstrebt, werden durch ihn (bzw. durch einen evtl. dahinter geschalteten Schwachstellenscanner) in der Regel zwischen einer und einer Million Anfragen gestellt.²¹ Während ein Portscanner mit wenigen IP-Adressen auf das zu scannende System zugeht, verwenden Angreifer so viele IP-Adressen wie möglich, um das Ziel des Systemkollapses zu erreichen.

3 Strafrechtliche Analyse

3.1 § 202a StGB Ausspähen von Daten

Nach § 202a Abs. 1 StGB macht sich strafbar, wer sich oder einem Dritten Zugang zu Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Das geschützte Rechtsgut ist hierbei die Verfügungsbe-fugnis über Daten. Daten im Sinne dieser Vorschrift können nur solche sein, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden, § 202a Abs. 2 StGB. Der Täter muss sich den Zugang zu solchen Daten, die nicht für ihn bestimmt sind, unter Überwindung einer Zugangs-sicherung verschaffen. Diese Vorschrift wird allgemein auch als „elektronischer Hausfriedensbruch“ bezeichnet.²² Ähnlich wie das Spiegelbild dieses Tatbestandes aus der analogen Welt in § 123 Abs. 2 StGB setzt die Verfolgung eines solchen elektronischen Hausfriedensbruchs gem. § 205 Abs. 1 S. 2 StGB einen Strafantrag voraus, sofern die zuständige Strafverfolgungsbehörde nicht wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält. Der Versuch ist hingegen nicht strafbar.

Ein Portscan greift nicht das durch § 202a Abs. 1 StGB geschützte Rechts-gut an. Bereits das Vorliegen des Tatbestandsmerkmals „Daten“ im Sinne des § 202a Abs. 2 StGB ist bei den durch einen Portscan erlangten Informationen problematisch. Das Antwortverhalten des gescannten Systems unter den Datenbegriff des § 202a Abs. 2 StGB zu subsumieren, ist zumindest nicht ohne die Inkaufnahme einer validen juristischen Gegenargumentation möglich. Folgt man dem sehr weiten Datenbegriff einiger Vertreter und subsumiert hierunter auch Informationen ohne direkten Verarbeitungszweck, könnte hierunter auch die Information über (offene) Ports fallen.²³

²¹ Beim Schwachstellenscanner ist dies von der Zahl der Unterseiten abhängig.

²² Ernst, NJW 2003, 3236.

²³ Insoweit wäre eine Diskussion zu Informationen, die über sogenannte Standardports (häufig Portnum-mern 0 bis 1023) gewonnen werden, im Lichte dieses weiten Datenbegriffs von großem Interesse.

Unabhängig vom Vorliegen von Daten im Sinne des § 202a Abs. 2 StGB überwindet ein Portscan jedoch zu keiner Zeit eine Zugangssicherung, die Daten vor unbefugter Kenntnisnahme besonders schützt. In der Praxis hat sich insbesondere durch die Analogie zum Hausfriedensbruch das Fehlbewusstsein etabliert, dass die Prüfung von Systemen nach offenen Ports (analog dem Rütteln an Haustüren und Fenstern) bereits eine strafbewehrte und dem Verschaffen des Zugangs notwendigerweise vorgeschaltete Tathandlung sei. An dieser Stelle zeigt sich einmal mehr das Dilemma der Betrachtung digitaler/elektronischer Sachverhalte aus dem Blickwinkel der auf den Schutz analoger Rechtsgüter ausgerichteten Rechtsvorschriften. Auch dass der Gesetzgeber zur Art der Zugangssicherung keine weiteren Angaben gemacht und bei der Auslegung dieses Begriffs auf die Regelungen zu § 202 StGB (Verletzung des Briefgeheimnisses) und § 243 StGB (Besonders schwerer Fall des Diebstahls) verwiesen hat,²⁴ zeigt die Schwierigkeiten bei der Definition der Zugangssicherungen deutlich auf. Da die vorgenannten Regelungen lediglich körperliche Gegenstände schützen und Daten in unkörperlicher Form vorliegen, kann bei der Auslegung des Tatbestandsmerkmals „Zugangssicherung“ auf diese Regelungen nicht abschließend Bezug genommen werden.²⁵ Auch in der Praxis wird häufig erfolglos versucht, die vorgenannte Problematik mit altbekannten Sachverhalten aus der analogen Welt zu vergleichen und darüber zu lösen.

Vom Zugangssicherungsbegriff des § 202a Abs. 1 StGB sind nach herrschender Meinung physische Maßnahmen, biometrische Verfahren und Softwaresicherungen (bspw. VPN-Datenleitungen oder Firewalls) erfasst.²⁶ Firewalls sind im hiesigen Kontext die am häufigsten genannte Zugangssicherung, die nach Ansicht vieler²⁷ durch einen Portscan überwunden werden soll. Ein Portscan versucht jedoch nicht, eine Firewall zu überwinden. Eine Firewall verhindert, sofern sie korrekt konfiguriert ist, Antworten des Systems auf Anfragen nach offenen Ports. Erhält der Portscanner durch die Firewall bedingt keine Antwort von einem potenziell offenen Port, respektiert er diesen Umstand und protokolliert hierzu einen geschlossenen Port. Mithin verwirklicht der Einsatz eines Portscans nicht den Straftatbestand des § 202a StGB.

3.2 § 202b StGB Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, macht sich des Abfangens von Daten im Sinne des § 202b StGB strafbar. Die Vorschrift soll alle Fälle erfassen, in denen ein Täter mithilfe technischer Mittel die Herrschaft über für ihn nicht bestimmte Daten erlangt. Hiervon erfasst sind alle Fälle des Mithörens von Telefongesprächen oder des Mitlesens von E-Mails.²⁸ Da

²⁴ BT-Drs. 10/5058, 29.

²⁵ Graf in MüKo-StGB, 4. Aufl. 2020, § 202a, Rdn. 40.

²⁶ Graf in MüKo-StGB, 4. Aufl. 2020, § 202a, Rdn. 41 ff.

²⁷ Eisele in Schönke/Schröder, StGB, 30. Aufl. 2019, § 202a StGB, Rdn. 14; Graf in MüKo-StGB, 4. Aufl. 2021, § 202a, Rdn. 52.

²⁸ Weidemann in BeckOK StGB, v. Heintschel-Heinegg, 49. Edition, Stand: 01.02.2021, § 202b, Rdn. 9.

der Portscan nicht für die Tatbestandsvarianten des § 202b StGB konzipiert ist, kommt eine Strafbarkeit hiernach nicht in Betracht.

3.3 § 202c StGB Vorbereiten des Abfangens oder Ausspähens von Daten („Hackerparagraf“)

Große Diskussionen erzeugt regelmäßig die Frage, ob Portscans bzw. die hierfür konzipierten Computerprogramme ein Vorbereiten des Abfangens und Ausspähens von Daten darstellen. Nach § 202c Abs. 1 StGB, welcher im Volksmund auch fälschlicherweise als „Hackerparagraf“ bezeichnet wird, macht sich strafbar, wer das Ausspähen oder Abfangen von Daten vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer der vorgenannten Straftaten ist, herstellt, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Durch entsprechende Verweise in § 303a Abs. 3 und § 303b Abs. 5 StGB gilt § 202c StGB ferner entsprechend für die Vorbereitung von Straftaten der Datenveränderung und der Computersabotage. Der Tatbestand des § 202c StGB betrifft vor allem die Fälle, in denen Cybersicherheitsunternehmen oder Entwickler einen Portscanner entwickeln, selbst betreiben und/oder deren Verwendung einem Dritten (unentgeltlich) bspw. zu Marketingzwecken anbieten. Die Einführung des § 202c StGB hat sowohl bei Programmentwicklern und -anbietern als auch bei Rechtsanwendern für erhebliche Verunsicherung gesorgt.²⁹ Die neue Regelung führte dazu, dass dem Wortlaut nach bereits das Herstellen, Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonstiges Zugänglichmachen von Hackertools, welche auch der Detektion von Sicherheitsrisiken zu deren Beseitigung dienen können, strafrechtliche Relevanz entfalten können. Schon im Gesetzgebungsprozess gab es Diskussionen darüber, dass diese Vorschrift dem Wortlaut nach deutlich über das angestrebte Ziel hinausgehen würde, für die Begehung von Straftaten nach §§ 202a, 202b StGB konzipierte Programme unter Strafe zu stellen.

In der Gesetzesbegründung wurde klargestellt, dass die strafrechtliche Pönalisierung der Verbreitung von Hackertools dann eintreten soll, wenn das betreffende Computerprogramm in erster Linie entwickelt worden ist, um bestimmte Computerstraftaten zu begehen.³⁰ Hiervon werden insbesondere solche Tools erfasst, die bereits nach der Art und Weise ihres Aufbaus darauf angelegt sind, illegalen Zwecken zu dienen, und aus dem Internet weitgehend anonym geladen werden können.³¹ Hiernach kam es auf die objektivierte Zweckrichtung des jeweiligen Tools an. Die Befürchtungen, dass auch der gutwillige Umgang mit Software, welche der Sicherheitsüberprüfung dienen kann, von § 202c StGB erfasst sein könnte, sah der Gesetzgeber als unbegründet an.³² Dies sah der Gesetzgeber durch die beiden Einschränkungen auf Tatbestandsebene, dass (i) ein Computerprogramm entwickelt wird, dessen Zweck die Begehung von Straftaten ist, und (ii) die Tathandlung – das Herstellen,

²⁹ Böken in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 15, Rdn. 67.

³⁰ BT Drucks. 16/3656, S. 11, 12.

³¹ BT Drucks. 16/3656, S. 12.

³² BT Drucks. 16/3656, S. 18.

Verschaffen, Verkaufen, Überlassen, Verbreiten oder sonstige Zugänglichmachen – zur Vorbereitung einer Computerstraftat erfolgen muss, hinreichend verdeutlicht.³³

Der Gesetzgeber stellte außerdem klar, dass durch die objektive Beschränkung auf Computerprogramme, deren Zweck die Begehung einer Computerstraftat ist, bereits auf Tatbestandsebene sichergestellt sei, dass keine Computerprogramme erfasst werden, die beispielsweise der Überprüfung der Sicherheit oder Forschung in diesem Bereich dienen. Bei Programmen, deren funktionaler Zweck nicht eindeutig inkriminiert ist und die erst durch ihre Anwendung zu einem Tatwerkzeug werden können (z. B. bei Sicherheitsüberprüfungen oder im Forschungsbereich, sog. Dual-Use-Tools), sei § 202c StGB nicht anwendbar. Die bloße Eignung von Software zur Begehung von Computerstraftaten reicht hiernach nicht aus. Des Weiteren muss durch die Tathandlung die Vorbereitung einer Computerstraftat beabsichtigt werden. Sofern ein Computerprogramm zur Sicherheitsüberprüfung, zur Entwicklung von Sicherheitssoftware oder Ausbildungszwecken in der IT-Sicherheitsbranche hergestellt, erworben oder einem anderen überlassen wurde, ist dies gerade nicht der Fall.

Endgültige Klarheit und Sicherheit für Entwickler und Anbieter von sogenannten Dual-Use-Tools aus der IT-Sicherheitsbranche wie beispielsweise einem Portscanner brachte das Ergebnis dreier Verfassungsbeschwerden³⁴ aus dem Jahr 2007.³⁵ In seinem auf die Beschwerden ergangenen Beschluss stellte das Bundesverfassungsgericht fest, dass bei der Anwendung des § 202c StGB die Absichten des Programmentwicklers maßgeblich sind und zusätzlich eine äußere Manifestation dieser Absichten erforderlich ist.³⁶ Nach dieser Klarstellung ist vor allem bei Dual-Use-Tools wie einem Portscanner ein restriktiver, zweistufiger Ansatz zu verfolgen. Über die Eignung eines Programms zur Straftatbegehung hinaus muss zudem noch die Absicht bei der Entwicklung des Programms hinzutreten, dieses zu kriminellen Zwecken zu verwenden, und diese muss sich nach außen erkennbar im Programm manifestieren.³⁷

Auch nach systematischer Auslegung ist § 202c StGB nicht auf Dual-Use-Tools und damit auf Portscanner anwendbar. Das StGB verweist an anderen Stellen ausdrücklich auf die Eignung konkreter Gegenstände für die Verwirklichung bestimmter Straftatbestände, bspw. in § 149 StGB (Vorbereitung der Fälschung von Geld und Wertzeichen) und § 275 StGB (Vorbereitung der Fälschung von amtlichen Ausweisen). Beide vorgenannten Straftatbestände sind so auszulegen, dass die darin genannten Fälschungsmittel nur zur Fälschung tauglich sein dürfen. Schon deshalb sollen solche Gegenstände ausscheiden, die auch anderen Zwecken dienlich sein können (bspw. leistungsstarke Farbkopierer im Hinblick auf die Möglichkeit

³³ BT Drucks. 16/3656, S. 18.

³⁴ Geklagt hatten ein Geschäftsführer einer auf Cybersicherheit spezialisierten GmbH, ein Hochschullehrer aus dem Bereich Fachinformatik und Medien und ein Softwareentwickler.

³⁵ Zwar wurden die Verfassungsbeschwerden mangels unmittelbarer Betroffenheit der Beschwerdeführer von der angegriffenen Norm nicht zur Entscheidung angenommen, jedoch machte das Bundesverfassungsgericht die hier dargestellten relevanten Ausführungen.

³⁶ Bundesverfassungsgericht, Beschluss vom 28. Mai 2009, Az.: 2 BVR 2233/07.

³⁷ Brodowski in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 13, Rdn. 42.

zur Geldfälschung nach § 149 StGB). Das Bundesverfassungsgericht führte außerdem die Entstehungsgeschichte des § 202c StGB an und begründete auch hiermit, dass lediglich auch zur Begehung von Straftaten geeignete Programme nicht von § 202c StGB erfasst seien.³⁸

Die vom Bundesverfassungsgericht geforderte Manifestation der Absichten des Entwicklers kann durch die Gestaltung des Programms oder die Bewerbung und den Vertrieb desselben geschehen. Sofern das Programm direkt für die Verwirklichung einer Tatbestandsvariante aus § 202a StGB oder § 202b StGB geschrieben wurde und lediglich heimlich und auf illegalen Kanälen vertrieben wird, kann hieraus auf eine entsprechende Absicht des Entwicklers zurückgeschlossen werden. Im Umkehrschluss ist eine redliche Absicht des Entwicklers zu vermuten, sofern keine der Tatbestandsvarianten aus §§ 202a, 202b StGB durch die Anwendung des Programms direkt erfüllt würden und das Programm auch auf legalen Vertriebskanälen beworben wird. Da dies bei Portscannern, welche durch Cybersicherheitsunternehmen angeboten werden, regelmäßig der Fall ist, kann diesen auch kein inkriminierter Zweck im Sinne des vorgenannten innewohnen. Folglich liegt im Betreiben von Portscans auch keine unter § 202c StGB subsumierbare Tathandlung.

3.4 § 303a StGB Datenveränderung

§ 303a Abs. 1 StGB pönalisiert das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten.³⁹ Anders als bei § 202a StGB müssen die Daten hier nicht speziell gegen unberechtigten Zugriff gesichert sein. Dieser Straftatbestand schützt das Interesse an der ungestörten und jederzeit möglichen Nutzung der in gespeicherten Daten enthaltenen Informationen.⁴⁰ Die zeitweilige⁴¹ Entziehung von Daten ist nach § 303a StGB ebenso strafbar wie Sachverhalte, in denen für den Berechtigten bestimmte Daten gar nicht erst in seinen Zugriffsbereich gelangen können.⁴² Soweit Daten jedoch dem Zugriff Dritter entzogen werden, spielt § 303a StGB hierbei keine Rolle. Sollte bspw. eine Internetseite wie ein Onlineshop für Kunden eines Anbieters nicht verfügbar sein, liegt hierin mangels tauglicher Rechtsgutträgerschaft der Kunden keine Tatbestandsverwirklichung nach § 303a Abs. 1 StGB vor, da der Betreiber der Website noch auf die darin enthaltenen Daten zugreifen kann. Da ein Portscan Daten nicht unterdrückt, löscht, unbrauchbar macht oder verändert, wird dadurch auch keine Strafbarkeit nach § 303a Abs. 1 StGB begründet. Demnach scheidet eine mögliche Strafbarkeit gemäß § 303a Abs. 1 StGB beim Portscan aus.

³⁸ Das Bundesverfassungsgericht führte aus, dass eine solche Auslegung dem Wortlaut der Norm und dem Willen des Gesetzgebers widersprechen und damit gleichzeitig einen Verstoß gegen das Bestimmtheitsgebot gem. Art. 103 Abs. 2 GG darstellen würde.

³⁹ Der Datenbegriff ist an denjenigen des § 202a StGB angelehnt.

⁴⁰ Wieck-Noodt in MüKo-StGB, 3. Aufl. 2019, § 303a, Rdn. 2.

⁴¹ Eine geringe Zeitspanne von einigen Minuten ist hierbei jedoch unerheblich, vgl. Wieck-Noodt in MüKo-StGB, 3. Aufl. 2019, § 303a, Rdn. 13; das Oberlandesgericht Frankfurt hat auch einen Zeitraum von zwei Stunden noch nicht als ausreichend für eine Strafbarkeit nach § 303a StGB erachtet, Oberlandesgericht Frankfurt, Beschluss vom 22. Mai 2006, Az.: 1 Ss 319/05.

⁴² Bspw. bei Blockierung des Empfängerbriefkastens durch Versenden von „Junk-Mails“.

3.5 § 303b StGB Computersabotage

Den Straftatbestand der Computersabotage erfüllt, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, erheblich stört. Der Tatbestand des § 303b Abs. 1 StGB kennt drei Alternativen. Die erste Alternative knüpft an eine Vortat im Sinne des § 303a Abs. 1 StGB an. Da eine solche beim Portscanning nicht vorliegt,⁴³ scheidet diese Variante an der Stelle bei der strafrechtlichen Analyse von Portscans aus. Auch § 303b Abs. 1 Nr. 3 StGB kommt beim Portscanning nicht in Betracht, da die Datenverarbeitungsanlage oder ein Datenträger des Gescannten nicht zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird.⁴⁴ Die Tathandlungen *Zerstören* und *Beschädigen* sind mit denen des § 303 StGB identisch und bei einem Portscan somit nicht einschlägig. Auch die Tatbestandsalternativen *Beseitigen* und *Verändern* erfordern eine direkte, physische Einwirkung auf die Datenverarbeitungsanlage. Da dies bei einem Portscan nicht möglich ist, scheiden auch diese Tatbestandsalternativen hier aus. Das Unbrauchbarmachen einer Datenverarbeitungsanlage liegt vor, sofern diese in ihrer Gebrauchsfähigkeit so stark beeinträchtigt wird, dass sie nicht mehr ordnungsgemäß verwendet werden kann. Es ist umstritten, ob es zur Erfüllung dieser Tatbestandsvariante einer Substanzeinwirkung auf die Datenverarbeitungsanlage durch den Täter bedarf oder ob bereits ein Einwirken auf Datenübertragungsleitungen oder das Stromnetz ausreicht.⁴⁵ Dies kann hier dahinstehen, da durch den Portscan in jedem Fall kein physisches Einwirken stattfindet.

Die einzig hier in Betracht kommende Sabotagehandlung läge im Eingeben⁴⁶ oder in der Übermittlung von Daten⁴⁷ in der Absicht, einem anderen einen Nachteil zuzufügen,⁴⁸ § 303b Abs. 1 Nr. 2 StGB. Hier muss zunächst zwischen den Tatbestandsvarianten des Eingebens und Übermittels unterschieden werden. Die Tathandlung des Eingebens von Daten im Sinne von § 303b Abs. 1 Nr. 2 Alt. 1 StGB erfasst nur Vorgänge, bei denen einem Rechner von außen Daten von einem externen Datenträger manuell zugeführt werden (bspw. durch einen USB-Port oder eine Tastatur).⁴⁹ Da beim Portscanning diese Art der Eingabe von Daten nicht erfolgt, ist § 303b Abs. 1 Nr. 2 Alt. 1 StGB bereits tatbestandlich nicht anwendbar.

⁴³ Vgl. 3.4.

⁴⁴ Bei der Auslegung dieser Tatbestandsmerkmale wird auf die Regelungen der §§ 316b, 303 und 109e StGB zurückgegriffen (vgl. Hecker in Schönke/Schröder 30. Aufl. 2019, § 303b, Rdn. 8).

⁴⁵ Pro Wieck-Noodt in MüKO-StGB, 3. Aufl. 2019, § 303b, Rdn. 16, contra: Hecker in Schönke/Schröder 30. Aufl. 2019, § 303b, Rdn. 8, der auf die Ausführungen zu § 316 b StGB verweist, vgl. Stoll in BeckOK StGB, v Heintschel-Heinegg, 50. Edition, Stand: 01.05.2021, § 316b, Rdn. 10.

⁴⁶ Diese an sich neutralen Handlungen durch das Hinzutreten besonderer Umstände zur Straftat zu machen, war weder von der Cybercrime Convention noch vom Rahmenbeschluss des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme gedeckt (vgl. BT Drucks. 16/5449, S. 5).

⁴⁷ Im Sinne des § 202a Abs. 2 StGB.

⁴⁸ Im Hinblick auf Nachteilszufügungsabsicht wird auf die Auslegung des § 274 Abs. 1 Nr. 1 StGB zurückgegriffen.

⁴⁹ Hecker in Schönke/Schröder StGB, 30. Aufl. 2019, § 303b, Rdn. 7.

Die Übermittlung von Daten im Sinne des § 303b Abs. 1 Nr. 2 Alt. 2 StGB kann hingegen auch vom eigenen Rechner eines Täters über einen Fernmeldeweg⁵⁰ erfolgen. Die Verwirklichung des Straftatbestands aus § 303b Abs. 1 Nr. 2 Alt. 2 StGB findet in der Praxis überwiegend durch komplexe Attacken gegen Computersysteme bspw. durch Computerviren, digitale trojanische Pferde, logische Bomben, Würmer oder auch (D)DoS-Attacken statt.⁵¹ Diese Vorgehensweisen zeigen deutlich, welches Verhalten § 303b Abs. 1 Nr. 2 Alt. 2 StGB unter Strafe stellen möchte. Es ließe sich hier diskutieren, ob die Funktionsweise eines Portscanners mit der Datenübermittlung, welche § 303b Abs. 1 Nr. 2 Alt. 2 StGB pönalisiert, vergleichbar ist. Während § 303b Abs. 1 Nr. 2 Alt. 2 StGB von schädlichen Daten ausgeht, die an das Opfersystem übermittelt werden, sind die Requests eines Portscans jedoch keinesfalls schädlich, sondern absolut „üblich“. Die Anfrage nach offenen Ports enthält schließlich weder Viren, trojanische Pferde noch Computerwürmer. Eine durch den Portscan gegebenenfalls verursachte Verlangsamung der Datenverarbeitungssysteme stellt keine Störung im Sinne des § 303b Abs. 1 StGB dar. Eine Störung der Datenverarbeitungsanlage käme jedoch in Fällen in Betracht, in denen die Häufigkeit und Frequenz der Requests eine einem (D)Dos-Angriff ähnliche Erscheinung annehmen und zu (vorübergehenden) Ausfällen oder Fehl- bzw. Nichtfunktionen der Datenverarbeitungsanlage führt. Letztlich kann dahinstehen, ob bereits das Tatbestandsmerkmal der fehlenden Datenübermittlung eine Strafbarkeit eines Portscanners entfallen lässt. Spätestens beim Tatbestandsmerkmal der Nachteilzufügungsabsicht kommt die Subsumtion der Funktionsweise des Portscanners zu dem Ergebnis, dass kein strafbares Verhalten nach § 303b Abs. 1 Nr. 2 StGB vorliegt.

4 Zivilrechtliche Analyse

4.1 § 823 Abs. 1 BGB

Wer vorsätzlich oder fahrlässig ein in § 823 Abs. 1 BGB genanntes Rechtsgut eines anderen widerrechtlich verletzt, ist diesem zum Schadenersatz verpflichtet. Portscans werden in der Praxis mit unterschiedlichen Argumenten unter deliktsrechtliche Ansprüche aus dem BGB und üblicherweise unter die Tatbestandsvariante des Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb⁵² subsumiert. Dabei begehren Gescannte Unterlassung⁵³ und/oder Schadenersatz⁵⁴ vom Scannenden. Die hierfür notwendigen Tatbestandsmerkmale werden dabei oft ohne tiefergehende Auseinandersetzung⁵⁵ damit als gegeben angesehen.

⁵⁰ Wie bspw. W-LAN.

⁵¹ Wieck-Noodt in MüKO-StGB, 3. Aufl. 2019, § 303b, Rdn. 3.

⁵² Als „sonstiges Recht“ im Sinne des § 823 Abs. 1 BGB.

⁵³ §§ 823 Abs. 1 BGB i. V.m. § 1004 Abs. 1 S. 2 BGB (analog).

⁵⁴ §§ 823 Abs. 1 BGB i. V.m. §§ 249 ff. BGB.

⁵⁵ Man könnte hier auch vom Bauchgefühl des Anspruchstellers sprechen, welcher naturgemäß immer im eigenen Sinne argumentieren wird.

Für eine Rechtsgutsverletzung im Sinne des § 823 Abs. 1 BGB bedarf es eines unmittelbaren, betriebsbezogenen Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb des Anspruchstellers durch den Anspruchsgegner. Zur Erfüllung der vorgenannten Voraussetzungen müsste sich der durch den Anspruchsteller gerügte Eingriff in seiner Stoßrichtung gegen den betrieblichen Organismus oder die unternehmerische Entscheidungsfreiheit des Anspruchstellers richten und dabei eine Schadensgefahr begründen, die über eine bloße Belästigung hinausgeht⁵⁶ und geeignet ist, den Betrieb des Anspruchstellers in empfindlicher Weise zu beeinträchtigen.⁵⁷ Auch die Willensrichtung des Anspruchsgegners kann beim Merkmal des Eingriffs in den eingerichteten und ausgeübten Gewerbebetrieb und bei der Betriebsbezogenheit eines Eingriffs konstituierend wirken.⁵⁸

4.1.1 Eingriff

Ein Portscan erfüllt nicht die vorgenannten Voraussetzungen eines unmittelbaren betriebsbezogenen Eingriffs. Er ist in seiner Stoßrichtung nicht darauf ausgerichtet, den betrieblichen Organismus oder die unternehmerische Entscheidungsfreiheit des Gescannten empfindlich zu stören. Man kann sogar noch weitergehen und dem Portscan die generelle Eignung hierzu absprechen. Sofern man bei einem Portscan von einer Stoßrichtung überhaupt reden kann, richtet sich dieser keinesfalls gegen den betrieblichen Organismus oder die unternehmerische Entscheidungsfreiheit des Gescannten. Vergleicht man die höchststrichterlich entschiedenen Fälle, in denen ein Eingriff in den Gewerbebetrieb bejaht wurde, wird sehr schnell deutlich, dass diese in ihrer Intensität und konkreten Erscheinungsform weit von den Umständen eines Portscans entfernt liegen.⁵⁹ Der Portscan ist in seiner Funktionsweise nicht darauf ausgerichtet, betriebliche Abläufe zu stören oder die Entscheidungsfreiheit des Unternehmens gegen dessen Willen zu manipulieren. Trotzdem wird in der Praxis versucht, einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb mit unterschiedlichsten Ansätzen zu konstruieren.

Mit Rechtsfragen zu Portscans häufig befassten Juristen begegnet oftmals das Argument, der Portscan führe beim Gescannten zu einer erhöhten Prozessorleistung und hierin läge bereits ein betriebsbezogener Eingriff im Sinne des § 823 Abs. 1 BGB begründet. Wie beschrieben liegt ein Eingriff jedoch nur dann vor, wenn die Grundlagen des Betriebs bedroht werden oder der Funktionszusammenhang der Betriebsmittel auf längere Zeit aufgehoben und in der Folge die Tätigkeit des Betriebs als solche infrage gestellt ist.⁶⁰ Eine Belästigung⁶¹ oder sozialübliche Behinderung ge-

⁵⁶ Förster in BeckOK BGB, Hau/Poseck, 58. Edition, Stand: 01.05.2021, § 823, Rdn. 184, 185.

⁵⁷ Wagner in MüKo-BGB, 8. Aufl. 2020, § 823, Rdn. 369.

⁵⁸ Wagner in MüKo-BGB, 8. Aufl. 2020, § 823, Rdn. 369.

⁵⁹ Die einzige Ausnahme hiervon ist die Rechtsprechung des Bundesgerichtshofs zum ungefragten Versand von Werbe-E-Mails, vgl. Bundesgerichtshof, Urteil vom 14. März 2017, Az.: VI ZR 721/15; Beschluss vom 20. Mai 2009, Az.: I ZR 218/07.

⁶⁰ Förster in BeckOK BGB, Hau/Poseck, 58. Edition, Stand: 01.05.2021, § 823, Rdn. 184.

⁶¹ Sofern man bei einem Portscan, der zum Grundrauschen des Internets gehört, von Belästigungen reden kann.

nügt hingegen nicht.⁶² Sofern nur eine erhöhte Prozessorleistung behauptet wird, ist dies noch nicht ausreichend für einen betriebsbezogenen Eingriff. Insbesondere die Tatsache, dass die in Deutschland für den Betrieb und die Verwaltung aller Top-Level-Domains verantwortliche Institution, die DENIC eG, Portscans als – gelegentlich lästiges – Grundrauschen des Internets⁶³ bezeichnet, lässt auf einen mittlerweile allzu gewöhnlichen Vorgang schließen, der zwar lästig sein kann, jedoch keinen Eingriff im Sinne des Deliktsrechts darstellt.

Vor diesem Hintergrund stellt sich auch die Frage des sozialadäquaten Verhaltens des Scannenden. Hier treffen mehrere Komponenten aufeinander, die einen Portscan als sozialadäquat und vielleicht sogar rechtlich geboten erscheinen lassen. Die Zahlen von Cyberangriffen steigen stetig und rasant. Die Haftung der Unternehmen und ihrer Führungsorgane steigt ebenso schnell an. Diese Tendenzen sind unverkennbar.⁶⁴ Angesichts immer stärker vernetzter IT-Strukturen und eines stark ansteigenden Datenaustausches kann es heutzutage als fahrlässig bezeichnet werden, wenn Unternehmen im Hinblick auf (zukünftige) Kunden, Geschäftspartner oder Lieferanten nicht auch minimal-invasivste Maßnahmen wie einen Portscan durchführen würden, um vor Aufnahme der Geschäftsbeziehungen auch deren Cybersicherheitslevel zumindest in dem Umfang, wie es ein Portscan tut, zu prüfen. Schließlich wird auch Kunden oder Geschäftspartnern der Zugriff auf die eigene IT in gewissem Ausmaß erlaubt.⁶⁵ Ein Portscan ist daher unter bestimmten Gesichtspunkten nicht nur kein Eingriff und sozialadäquat, sondern sogar (sozial) notwendig. Hiernach wäre der Eingriff durch einen Portscan zwingend zu verneinen.

In der Praxis ebenso häufig vorkommende Argumente zur Begründung eines Eingriffs wie beispielsweise ein Integritätsinteresse der Gescannten oder die ohne Grundlage und über Gebühr in Anspruch genommene Aufmerksamkeit eines Systemverantwortlichen vermögen keinen Eingriff im Sinne des § 823 Abs. 1 BGB darzustellen. Als argumentative Grundlage wird dabei das Urteil des Bundesverfassungsgerichts vom 27. Februar 2008⁶⁶ bemüht. Der Gegenstand des dortigen Verfahrens waren zwei Verfassungsbeschwerden gegen das nordrhein-westfälische Verfassungsschutzgesetz (nachfolgend „VSG“ genannt). Die mit der Verfassungsbeschwerde angegriffenen Vorschriften regelten die Ermächtigung der Verfassungsschutzbehörden zur heimlichen Beobachtung des Internets⁶⁷ und zum heimlichen Zugriff auf informationstechnische Systeme.⁶⁸ Unter der heimlichen Beobachtung im Sinne des § 5 Abs. 2 Nr. 11 Alt. 1 VSG a.F. waren Maßnahmen zu verstehen, mithilfe derer die Verfassungsschutzbehörde Inhalte von Internetkommunikation zur Kenntnis nehmen konnte. Beim heimlichen Zugriff sollten durch die Behörden Sicherheitslücken des Zielsystems zu dessen Infiltration ausgenutzt werden oder die

⁶² Wagner in MüKo-BGB, 8. Aufl. 2020, § 823, Rdn. 369.

⁶³ Stellungnahme der DENIC zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 2.

⁶⁴ Grieger, WM 2021, 8 ff.; ders., Der Aufsichtsrat, 06/2021, 85 ff.

⁶⁵ Heckmann, MMR 2006, 283.

⁶⁶ Az.: 1 BvR 370/07; 1 BvR 595/07.

⁶⁷ § 5 Abs. 2 Nr. 11 Alt. 1 VSG NRW a.F.

⁶⁸ § 5 Abs. 2 Nr. 11 Alt. 2 VSG NRW a.F.

Installation von Spähprogrammen erfolgen, um in der Folge ggf. sogar das Zielsystem fernsteuern zu können.⁶⁹

Abseits der Tatsache, dass es sich bei dem dortigen Rechtsstreit um eine öffentlich-rechtliche Streitigkeit verfassungsrechtlicher Art handelte, können auch die dortigen Feststellungen zum Eingriff in Grundrechte nicht auf diejenigen im Sinne des § 823 Abs. 1 BGB übertragen werden.⁷⁰ Die im vorgenannten Urteil des Bundesverfassungsgerichts gerügten Eingriffsvarianten sind nicht ansatzweise mit der Funktionsweise eines Portscans vergleichbar. Weder findet eine Beobachtung von Internetkommunikation statt noch verschafft sich der Scannende Zugriff auf fremde (Ziel-)Systeme. Die durch den Portscan erlangten Erkenntnisse betreffen lediglich die Erreichbarkeit eines Systems, das der Gescannte seinerseits öffentlich abrufbar gemacht hat. Ein irgendwie gearteter Zugriff auf Daten, deren öffentliche Preisgabe der Gescannte nicht wünscht, findet gerade nicht statt. Insoweit handelt es sich schon nicht um einen Eingriff/Zugriff auf (System-)Bestandteile, die dem grundrechtlich verbürgten Schutz informationstechnischer Systeme unterfallen. Eine auf dem vorgenannten Urteil basierende Begründung eines Eingriffs in ein Integritätsinteresse des Gescannten bei einem Portscan ist daher nicht nachvollziehbar.⁷¹

Mitunter behaupten Anspruchsteller, die Informationen über offene Ports oder Applikationen, die hierauf laufen, seien als Geschäftsgeheimnis unter einen besonderen Schutz gestellt. Die Erlangung von Informationen über offene Ports tangiere daher den Kern des gescannten Unternehmens und stelle somit einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb dar. Zieht man die Definition eines Geschäftsgeheimnisses aus dem Geschäftsgeheimnisgesetz (nachfolgend „GeschGehG“ genannt)⁷² heran, wird schnell die Abwegigkeit dieser Argumentation deutlich. Gemäß § 2 Nr. 1 GeschGehG ist ein Geschäftsgeheimnis eine Information, die (i.) weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich und daher von wirtschaftlichem Wert ist, die (ii.) Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und bei der (iii.) ein berechtigtes Interesse an der Geheimhaltung besteht. Die Informationen über erreichbare Ports und Applikationen, die ggf. auf den offenen Port laufen, können auch bei extensivster Auslegung nicht unter die vorgenannte Definition eines Geschäftsgeheimnisses subsumiert werden. Weder sind sie allgemein unbekannt noch Gegenstand von Geheimhaltungsmaßnahmen. Ein Interesse an der Geheimhaltung der Erreichbarkeit bestimmter Systeme besteht schon aufgrund der Tatsache, dass diese durch den Gescannten betrieben werden, nicht. Vereinfacht gesagt stehen

⁶⁹ Bundesverfassungsgericht, Urteil vom 27. Februar 2008, Az.: 1 BvR 370/07; 1 BvR 595/07, Rdn. 4, 5.

⁷⁰ Die Begründetheit der Verfassungsbeschwerden der dortigen Beschwerdeführer ergab sich zudem u.a. aus einem Verstoß der streitgegenständlichen Normen gegen das Bestimmtheitsverbot aus Art. 80 Abs. 1 S. 2 GG und das Verhältnismäßigkeitsprinzip.

⁷¹ Das relevante „IT-Grundrecht“ schützt darüber hinaus nur vor dem heimlichen Zugriff auf solche Daten, die der Grundrechtsträger in informationstechnische Systeme einbringt, nicht jedoch Daten des informationstechnischen Systems selbst.

⁷² Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (BGBl. I S. 466).

die vorgenannten Informationen jedem zur Verfügung, der dort nachschaut. Folglich kann durch einen Portscan auch nicht auf Geschäftsgeheimnisse zugegriffen und damit in den Gewerbebetrieb des Gescannten eingegriffen werden.

4.1.2 Rechtswidrigkeit

Sofern man in einem Portscan dennoch einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb sieht, müsste dessen Rechtswidrigkeit im Rahmen einer Interessenabwägung positiv festgestellt werden. Beim Eingriff in den Gewerbebetrieb wird die Rechtswidrigkeit nicht bereits durch die Erfüllung des Tatbestandes indiziert.⁷³ Der Schutzbereich des § 823 Abs. 1 BGB für den eingerichteten und ausgeübten Gewerbebetrieb ist vielmehr nur dann eröffnet, wenn ein Eingriff, sofern dieser vorliegt, den Spielregeln einer freiheitlich-demokratischen Marktgesellschaft widerspricht.⁷⁴ Anders ausgedrückt begründet ein Verhalten dann keinen Eingriff, wenn es als „subjektiv redlich“ einzustufen ist.⁷⁵ In diesem Fall hat folglich ein Gescannter zu beweisen, dass das von ihm als rechtswidriger Eingriff gerügte Verhalten seines Anspruchsgegners gegen die Gebote der gesellschaftlichen Rücksichtnahme verstößt. Ein rechtswidriger Eingriff liegt nur dann vor, wenn das Interesse des vom Eingriff Betroffenen die schutzwürdigen Belange der anderen Seite überwiegt.⁷⁶

Einem gängigen, wichtigen und nicht invasiven Cybersecuritytool wie einem Portscanner den rechtmäßigen Gebrauch wegen eines Verstoßes gegen Gebote der gesellschaftlichen Rücksichtnahme abzusprechen, wird der konkreten Bedrohungslage aller Unternehmen unabhängig von Größe, Branche und Standort nicht gerecht. Cybersecurity stellt für Unternehmen im Hinblick auf Compliance-Richtlinien und die Anforderungen an den Datenschutz eine große Herausforderung und mitunter auch eine bußgeldbewehrte rechtliche Verpflichtung dar.⁷⁷ Sofern Unternehmen keine hinreichenden Cybersecuritymaßnahmen vorhalten, begeben sie sich in die Gefahr, durch Angriffe wettbewerbsunfähig zu werden. Im Zuge der Abwägung ist es daher widersinnig, einem Unternehmen aufzutragen, bei sich für Cybersicherheit zu sorgen, und es gleichzeitig, sofern es dies dann mithilfe eines nichtinvasiven und gängigen Cybersicherheitswerkzeugs tut, eines Eingriffs in die betriebliche Sphäre eines anderen Unternehmens zu bezichtigen. Es kann daher nicht subjektiv unredlich sein, ein nicht verbotenes Tool in einer nicht strafrechtlich relevanten Art und Weise (durch Dritte) einzusetzen, um eigene rechtliche Verpflichtungen zu erfüllen. Ähnlich wie Klimaschutz und Globalisierung keine örtlich zu lösenden Herausforderungen darstellen, kann auch Cybersicherheit schließlich nicht nur bis zu den Grenzen der eigenen Unternehmensstruktur gedacht werden und macht den Scan anderer Unternehmen zwingend notwendig. Ein Portscan kann als ein wichtiger Indikator für Cybersicherheit dienen. Angesichts dieser Sachlage ist es nicht darstellbar,

⁷³ Förster in BeckOK BGB, Hau/Poseck, 58. Edition, Stand: 01.05.2021, § 823, Rdn. 188.

⁷⁴ Wagner in MüKo-BGB, 8. Aufl. 2020, § 823, Rdn. 371.

⁷⁵ Förster in Beck-OK-BGB, Hau/Poseck, 56. Edition, Stand: 01.11.2020, § 823, Rdn. 189.

⁷⁶ Bundesgerichtshof, Urteil vom 15. Januar 2019, Az.: VI ZR 506/17.

⁷⁷ Art. 32 DS-GVO.

einen Portscanner wegen eines Verstoßes gegen die Gebote der gesellschaftlichen Rücksichtnahme als subjektiv unredlich einzustufen. Der Scan ist nicht invasiv und erzeugt lediglich Ergebnisse in Form von Antworten, die die von Gescannten vorgehaltenen IT-Infrastrukturen ohnehin abgeben. Auch unter diesem Gesichtspunkt ist der Schutzbereich des § 823 Abs. 1 BGB durch den Portscan nicht tangiert.

4.1.3 Mitverschulden

Sofern es durch einen Portscan – bei hier hilfsweise unterstelltem Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb – zu einem Schaden kommt, sind die Verschuldensbeiträge für diesen Schaden im Lichte des § 254 BGB zu analysieren. Trifft den Geschädigten ein Verschulden bei der Entstehung des Schadens, verschiebt sich nach einer Abwägung der Verursachungs- und Verschuldensbeiträge des Schädigers und des Geschädigten gem. § 254 BGB die Schadensquote. Dabei kann es dazu kommen, dass der schadensbegründende Beitrag des Schädigers vollständig hinter demjenigen des Geschädigten zurücktritt. Ausgangspunkt eines Mitverschuldens ist die Außerachtlassung der eigenen Interessen des Geschädigten. Das Verschulden des Geschädigten kann in einem Tun⁷⁸ oder dem pflichtwidrigen Unterlassen⁷⁹ begründet sein.

Für ein solches Mitverschulden gibt es in der Praxis viele Anhaltspunkte, bei denen ein Mitverschulden des Gescannten zumindest diskutabel ist. Hierzu gehören die fehlenden Installationen eines Informationssicherheitsmanagementsystems oder das Unterlassen simpelster IT-Sicherheitsmaßnahmen.⁸⁰ Für die Annahme eines Mitverschuldens spricht dabei schon der hohe Stellenwert von Cybersicherheit für das Funktionieren eines Gewerbebetriebs. Auch der Umstand, dass Cybersicherheit ähnlich wie Datenschutz und Compliance als Teil eines Pflichtenkanons in jedem umsichtig agierenden Unternehmen angekommen ist, lässt die Nichtbeachtung gewisser Grundsätze zur Cybersicherheit ein Mitverschulden als naheliegend erscheinen. Cybersicherheit ist schließlich eine gewichtige Anforderung an ein geordnetes, die (Rechts-)Güter des Einzelnen und der Allgemeinheit schonendes Zusammenleben.⁸¹

Sofern ein Gescannter ein System betreibt, welches durch veraltete Komponenten oder Fehlkonfigurationen nicht in der Lage ist, mit dem sich stetig anpassenden Stand der Technik auf dem Gebiet der Internetkommunikation mitzuhalten und es hierdurch zu einem Schaden kommen sollte, kann hierin ein Mitverschulden des Gescannten begründet sein. Eine richtungsweisende Entscheidung für das Mitverschulden eines Geschädigten aufgrund der Unterhaltung einer IT-Sicherheit unter einem dem Stand der Technik entsprechenden Standard fällt das Oberlandesgericht

⁷⁸ § 254 Abs. 1 S. 1 BGB.

⁷⁹ § 254 Abs. 2 S. 1 BGB.

⁸⁰ Das BSIG definiert IT-Sicherheit als Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen; § 2 Abs. 2 BSIG.

⁸¹ Heckmann, MMR 2006, 280.

Hamm bereits im Jahr 2003.⁸² Der dortige Kläger hatte nach den Feststellungen des Gerichts nicht für eine zuverlässige Sicherheitsroutine gesorgt. Diese sei aber gerade im gewerblichen Anwenderbereich selbstverständlich. Im dortigen Urteil hatte das Gericht den schadensverursachenden Beitrag des Geschädigten mit deutlichen Worten⁸³ beurteilt und im Ergebnis einen Mitverschuldensbeitrag angenommen, welcher den Beitrag des Schädigers vollumfänglich überwog.

Ein gutes Beispiel für ein mögliches Mitverschulden des Gescannten ist auch das Außerachtlassen der im BSI-Grundschrift dargestellten Maßstäbe. Der BSI-Grundschrift zeigt Empfehlungen und Best Practices für Informationssicherheit in Organisationen vor.⁸⁴ Soll beispielsweise eine neue Software oder Softwarekomponente getestet werden, und wird diese nicht von der gleichzeitig betriebenen Produktivumgebung getrennt⁸⁵ und entstehen hieraus Schäden beim Gescannten, ist ein Mitverschulden hier naheliegend. Der BSI-Grundschrift ist ein bis in das Jahr 1994 Jahre zurückreichender und immer wieder aktualisierter Mindeststandard. Unternehmen wird hier deutlich aufgezeigt, wie sie sich vor typischen Gefahren für ihre IT-Sicherheit schützen können. Der Grundschrift ist seit Langem als Messlatte der Informationssicherheit⁸⁶ anerkannt und zeigt seinen Anwendern den Stand der Technik⁸⁷ im Hinblick auf Cybersicherheit. Zwar ist es nicht jedem Unternehmen aufgetragen, diesen Maßstab umzusetzen,⁸⁸ jedoch spricht das absolute Außerachtlassen der dortigen Standards für ein Mitverschulden des Gescannten bei einem eingetretenen Schaden. Sofern nicht einmal die Basis⁸⁹- und Standardanforderungen⁹⁰ des Grundschriftes umgesetzt sind, kann dies ein Indiz für ein Mitverschulden darstellen.

Mangelnde IT-Sicherheit wird auch unter anderen Gesichtspunkten von der Allgemeinheit bzw. dem Rechtsverkehr gerügt. So kann beispielsweise eine mangelnde oder fehlende IT-Sicherheit zu einem Wegfall des Versicherungsschutzes führen. Die Begründung ist simpel und nachvollziehbar: Der Versicherer geht bei fehlenden oder mangelhaften Maßnahmen zur Sicherung der eigenen IT-Struktur von einem Mitverschulden des Versicherungsnehmers bei der Entstehung eines Schadens aus. Auch in anderen Gebieten machen Rechtssubjekte Cybersicherheit zur unverrück-

⁸² Oberlandesgericht Hamm, Urteil vom 1. Dezember 2003 – 13 U 133/03.

⁸³ Grob fahrlässig (blauäugig).

⁸⁴ Djeffal, MMR 2019, 290.

⁸⁵ Wie vom BSI Grundschriftkompendium vorgeschlagen, vgl. BSI-Grundschriftkompendium, Stand Februar 2021, S. 220.

⁸⁶ Ekrot/Fischer/Müller in Kipker, Cybersecurity, 1. Aufl. 2020, Kap. 3, Rdn. 33.

⁸⁷ Eine Definition zu diesem unbestimmten Rechtsbegriff findet sich lediglich in § 3 Abs. 6 BImSchG und § 3 Nr. 11 WHG als Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebswesen, welche zur Erreichung eines allgemeinen Schutzniveaus geeignet sind; der konkrete Stand der Technik in Sachen Informationssicherheit ist im jeweils aktuellen BSI-Grundschrift dargestellt.

⁸⁸ Andererseits kann das Außerachtlassen solcher Standards haftungsbegründend sein, vgl. Grieger, WM 2021, 8 ff.

⁸⁹ Dies sind absolut notwendige Anforderungen, bei deren Erfüllung mit geringem Aufwand ein hoher Nutzen für die IT-Sicherheit erzielt werden kann.

⁹⁰ Werden Basis- und Standardanforderungen erfüllt, entspricht dies dem Stand der Technik im Sinne des BSI-Grundschriftes.

baren Grundlage von Rechtsbeziehungen. So fordern öffentliche Auftraggeber zu Recht bei Ausschreibungen einen Nachweis ausreichender Maßnahmen zur Sicherung der IT-Strukturen des Ausschreibungsteilnehmers. In jedem Unternehmen stellt das Unterlassen hinreichend qualifizierter Cybersicherheitsmaßnahmen eine Pflichtverletzung der dafür verantwortlichen Leitungsorgane dar, welche unabhängig von oft nicht einbringbaren Schadenersatzansprüchen gegen einen Schädiger durch die Gesellschaft gegenüber dem pflichtwidrig handelnden Leitungsorgan im Wege eines Schadenersatzanspruchs verfolgt wird.

Im Zuge immer stärker vernetzter Systeme und angesichts stetig weiter steigender Zahlen von Cyberangriffen sollte es heutzutage üblich sein, dass ein verantwortungsbewusst denkendes Unternehmen⁹¹ nicht nur die eigene Cybersicherheit, sondern auch diejenige seiner Geschäftspartner, Zulieferer, Lieferanten etc. im Blick behält. Portscans und weitere Cybersicherheitsmaßnahmen, die mittlerweile zu standardmäßig verwendeten Instrumenten bei der Prüfung von Cybersicherheit gehören,⁹² können heutzutage als Grundrauschen im Internet und in der vernetzten Unternehmenswelt bezeichnet werden. Die Vorbereitung für erhöhten Traffic infolge solcher Scans und Tests sollte daher bei jedem Unternehmen ebenso standardmäßig sein. Daher ist es nicht angemessen, Unternehmen, die grundlegende Sicherheitsmaßnahmen außer Acht lassen, haftungsrechtlich zu privilegieren, und jene, die der aktuellen Bedrohungslage Rechnung tragen und damit einen essenziellen Beitrag zur Festigung und zum Schutz des Wirtschaftsstandorts Deutschland leisten, zu inkriminieren.⁹³ Bislang besteht abseits der allgemeinen Haftungstatbestände für die Unternehmensführungen⁹⁴ keine allgemeine Verpflichtung zur Ergreifung von IT-Sicherheitsmaßnahmen.⁹⁵ Soweit es (noch) keine einheitlichen Verhaltenskodizes zur Gefahrenabwehr gibt,⁹⁶ ist es das falsche Signal, das Missachten aller Sicherheitsmaßnahmen und grundlegender Gefahrenabwehrmaßnahmen haftungsrechtlich zu privilegieren, zumal das Außerachtlassen von Verkehrssicherungspflichten, das Schaffen einer überflüssigen Gefahrenlage, Sorgfaltsverletzungen und die Nichtüberwachung von Gefahrenquellen als ein Mitverschulden begründend anerkannt werden.

4.2 §§ 823 Abs. 2 S. 1 BGB i. V. m. einem Schutzgesetz, § 826 BGB

Da der Portscan nicht gegen ein Schutzgesetz im Sinne des § 823 Abs. 2 S. 1 BGB⁹⁷ verstößt, kann ein Anspruch des Gescannten nicht auf diese Grundlage gestützt werden. Da die hier dargestellte Funktionsweise des Portscanners nicht geeignet ist, in einer gegen die guten Sitten verstoßenden Weise einem anderen vorsätzlich

⁹¹ Und vor allem deren Geschäftsführer, vgl. § 93 Abs. 1 S. 1 AktG; § 43 Abs. 2 GmbHG.

⁹² Bspw. externe Schwachstellenscanner.

⁹³ Djeffal, MMR 2019, 284.

⁹⁴ §§ 93 AktG, 43 Abs. 2 GmbHG.

⁹⁵ Bräutigam/Klindt, NJW 2015, 1141.

⁹⁶ Oder geben kann.

⁹⁷ Als Schutzgesetze im Sinne des § 823 Abs. 2 BGB gelten bspw. der AEUV, die DS-GVO, das AktG, das ArbNErfG, das BGB, das StGB, das BetrVG, das BDSG, das BImSchG etc.

Schaden zuzufügen, scheidet auch ein Anspruch des Geschädigten nach § 826 BGB aus.

5 Fazit

Portscans sind ein wichtiges Tool zur Prüfung von IT-Strukturen nach offenen Ports. Sie sind heutzutage Teil des im Internet üblichen Grundrauschens.⁹⁸ Der Einsatz von Portscans kann einen wichtigen Indikator für die eigene IT-Sicherheit und diejenige von potenziellen Geschäftspartnern, Kunden und allen anderen Adressaten eigener Daten liefern. Das Inkriminieren von Portscans nach dem Strafgesetzbuch durch Teile der Literatur und der juristischen Praxis ist nach einer Analyse der Funktionsweise eines Portscans vor dem Hintergrund der relevanten Computerstraftaten nicht vertretbar. Auch im Hinblick auf eine deliktsrechtliche Analyse sind Portscans unbedenklich. Sie stellen keinen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb dar. Weder ist die Schwelle zum Eingriffsbegriff des § 823 Abs. 1 BGB bei einem Portscan überschritten noch kann die Rechtswidrigkeit bei ihm positiv festgestellt werden. Sofern man von einem Eingriff ausgehen mag und ein kompensationsfähiger Schaden besteht, ist das Mitverschulden des Geschädigten bei der Schadensquote zu berücksichtigen. Für ein solches Mitverschulden gibt es zahlreiche, in der Praxis häufig vorkommende Anhaltspunkte. Angesichts der Bedeutung der IT-Sicherheit nicht nur für den Geschädigten, sondern für alle Marktteilnehmer kann es im Sinne des § 254 BGB nicht folgenlos bleiben, wenn ein Geschädigter selbst ein Mindestmaß an Eigensicherungsmaßnahmen unterlässt. Ein hierzu richtungsweisendes Urteil kann in dieser Frage Klarheit schaffen und ist angesichts der dargestellten Sachlage wohl nur noch eine Zeitfrage.

Open Access Dieser Artikel wird unter der Creative Commons Namensnennung 4.0 International Lizenz veröffentlicht, welche die Nutzung, Vervielfältigung, Bearbeitung, Verbreitung und Wiedergabe in jeglichem Medium und Format erlaubt, sofern Sie den/die ursprünglichen Autor(en) und die Quelle ordnungsgemäß nennen, einen Link zur Creative Commons Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden.

Die in diesem Artikel enthaltenen Bilder und sonstiges Drittmaterial unterliegen ebenfalls der genannten Creative Commons Lizenz, sofern sich aus der Abbildungslegende nichts anderes ergibt. Sofern das betreffende Material nicht unter der genannten Creative Commons Lizenz steht und die betreffende Handlung nicht nach gesetzlichen Vorschriften erlaubt ist, ist für die oben aufgeführten Weiterverwendungen des Materials die Einwilligung des jeweiligen Rechteinhabers einzuholen.

Weitere Details zur Lizenz entnehmen Sie bitte der Lizenzinformation auf <http://creativecommons.org/licenses/by/4.0/deed.de>.

⁹⁸ Stellungnahme der DENIC zum Gesetzesentwurf zum IT-SiG 2.0 vom 10. Dezember 2020, S. 2.