Universität Hannover
Ergänzungsstudiengang Rechtsinformatik

Abschlussarbeit
zur Erlangung des Grades LL.M. (Master of Laws)

Die Strafbarkeit des Hacking und der elektronische Hausfriedensbruch

vorgelegt von:

Michael Lörke
Aachener Str. 10
40223 Düsseldorf

Betreuer der Arbeit:
Prof. Dr. Zielinski

Abgabe: 2. Januar 2004

Gliederung:

Literaturverzeichnis:

Achenbach, Hans	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, in: Neue Juristische Wochenschrift (NJW) 1986, Seiten: 1835ff. Zitiert: Achenbach, NJW 1986, 1835.
Arzt, Gunther/Weber, Ulrich	Strafrecht, Besonderer Teil: Lehrbuch, Bielefeld, 2000. Zitiert: Arzt/Weber, Strafrecht BT.
Binder, Jörg	Strafbarkeit intelligenten Ausspähens von programmrelevanten DV-Informationen, Dissertation, Trier, 1994. Zitiert: Binder, Strafbarkeit des Ausspähens von DV-Informationen.
Bühler, Christoph	Ein Versuch Computerkriminellen das Handwerk zu legen: Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, in: Monatsschrift für deutsches Recht (MDR) 1987, Seiten: 448ff. Zitiert: Binder, MDR 1987, 448.
Caelli, William Longley, Dennis Shain, Michael	Information Security Handbook, London, 1994.
Dannecker, Gerhard	Neuere Entwicklungen im Bereich der Computerkriminalität: Aktuelle Erscheinungsformen und Anforderungen an eine effektive Bekämpfung, in: Betriebs-Berater, Zeitschrift für Recht und Wirtschaft (BB), 1996, Seiten: 1285ff. Zitiert: Dennecker, BB, 1996, 1285.
Ernst, Stefan	Wireless LAN und das Strafrecht – Zur Strafbarkeit des „Abhörens“ ungesicherter Kommunikation, in: Computer und Recht (CR) 2003, Seiten, 898ff. Zitiert: Ernst, CR 2003, 898.
Frommel, Monika	Das Zweite Gesetz zur Bekämpfnug der Wirtschaftskriminalität, in: Juristische Schulung (JuS) 1987, Seiten: 667ff. Zitiert: Frommel, JuS 1987, 667.
Gerhards, Thomas	Computerkriminalität und Sachbeschädigung, Dissertation, Mannheim, 1993.

Goldmann, Günter Stenger, Hans-Jürgen	Unbefugtes Eindringen in Computersysteme, Eine Betrachtung aus polizeilicher Sicht, in: Computer und Recht (CR) 1989, Seiten: 543ff. Zitiert: Goldmann/Stenger, CR 1989, 543.
Granderath, Peter	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität, in: Der Betrieb (DB) 1986, Beilage 18, Seiten: 1ff. Zitiert: Granderath, DB, 1986, Beil.18, 1.
Gravenreuth, Frhr. von	Computerviren, Hacker, Datenspione, Crasher und Cracker, in: Neue Zeitschrift für Strafrecht (NStZ) 1989, Seiten: 201ff. Zitiert: Gravenreuth, NStZ 1989, 201.
Guder, Wolfgang	Computersabotage (§ 303b StGB) – technische Lebenswirklichkeit und ihre juristische Würdigung, Dissertation, Osnabrück, 2000. Zitiert: Guder, Computersabotage.
Haft, Fritjof	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), in: Neue Zeitschrift für Strafrecht (NStZ), 1987, Seiten:6ff. Zitiert: Haft, NStZ 1987, 6.
Haß, Gerhard	Der strafrechtliche Schutz von Computerprogrammen, in: Lehmann, Michael, Rechtsschutz und Verwertung von Computerprogrammen, Köln, 1988, Seiten: 299ff. Zitiert: Haß, Strafr. Schutz v. Computerprogr.
Hauptmann, Helge	Zur Strafbarkeit des sog. Computerhackens – Die Problematik des Tatbestandsmerkmals „Verschaffen“ in § 202a StGB, in: JurPC 1989, Seiten: 215ff. Zitiert: Hauptmann, JurPC 1989.
Hilgendorf, Eric	Grundfälle zum Computerstrafrecht, in: Juristische Schulung (JuS) 1996, Seiten: 509-512 und 702-706, 1997, Seiten: 323-331. Zitiert: Hilgendorf, JuS 1996, Seite.
Hoeren, Thomas Sieber, Ulrich	Handbuch Multimediarecht – Rechtsfragen des elektronischen Geschäftsverkehrs, München, Stand: 2003. Zitiert: Bearb., in: Handbuch Multimediarecht.

Lackner, Karl Kühl, Kristian	Strafgesetzbuch mit Erläuterungen, 23. Auflage, München, 1999. Zitiert: Bearbeiter, in: Lackner/Kühl.
Langenscheidt Wörterbuch	Teil 1, Englisch-Deutsch, Bearbeiter: Willmann, Helmut, Berlin, 1990. Zitiert: Langenscheidt Wörterbuch, Seite.
Leicht, Armin	Computerspionage – Die „besondere Sicherung gegen unberechtigten Zugang“ (§202a StGB), in: Informatik und Recht (iur), 1987, Seiten 45ff. Zitiert: Leicht, iur 1987, 45.
Leipziger Kommentar	Kommentar zum Strafgesetzbuch, Band V, 10.Auflage, München, 1986. Zitiert: Bearbeiter, in: LK.
Lenckner, Theodor Winkelbauer, Wolfgang	Computerkriminalität – Möglichkeiten und Grenzen des 2. WiKG, in Computer und Recht (CR), 1986, Seiten: 483ff. Zitiert: Lenckner/Winkelbauer, CR 1986,483.
Möhrenschlager, Manfred	Das Zweite Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG), in: Zeitschrift für Wirtschaft, Steuer, Strafrecht (wistra), 1986, Seiten 123ff. Zitiert: Möhrenschlager, wistra 1986, 123.
Möhrenschläger, Manfred	Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, in: Zeitschrift für Wirtschaft, Steuer, Strafrecht (wistra), 1991, 321ff. Zitiert: Möhrenschlager, wistra 1991, 321.
Mühle, Kerstin	Hacker und Computer-Viren im Internet – eine strafrechtliche Beurteilung, Dissertation, Passau, 1998. Zitiert: Mühle, Hacker und Computerviren.
Nolden, Mathias Franke, Thomas	Das Internet Buch, Düsseldorf, 1996
Nomos-Kommentar zum Strafgesetzbuch	Gesamtredaktion: Neumann, Ulfrid / Puppe, Ingeborg / Schild, Wolfgang, 1.Auflage, Baden-Baden, Stand: 2003. Zitiert: Bearbeiter, in: NK.

Rinker, Mike	Strafbarkeit und Strafverfolgung von „IP - Spoofing“ und „Portscanning“, in: Zeitschrift für Informations- Telekommunikations- und Medienrecht (MMR), 2002, Seiten 663ff. Zitiert: Rinker, MMR 2002, 663.
Rogge, Marco / Ruef, Marc Velten, Uwe / Gieseke, Wolfram	Hacking intern - Angriffe, Strategien, Abwehr, 1.Auflage, Düsseldorf, 2003. Zitiert: Rogge, Hacking intern.
Rubin, Aviel D.	Hackerabwehr und Datensicherheit – Angriff, Diagnose, Abwehr, München, 2002. Zitiert: Rubin, Hackerabwehr und Datensicherheit.
Schmitz, Roland	Ausspähen von Daten, § 202a StGB, in: Juristische Arbeitsblätter (JA), 1995, Seiten: 478ff. Zitiert: Schmitz, JA 1995,478.
Schönke, Adolf Schröder, Horst	Strafgesetzbuch – Kommentar, 26. Auflage, München, 2001. Zitiert: Bearbeiter, in: S/S.
Schrutzki, Reinhard	Die Hackerethik, in: Das Chaos-Computer-Buch – Hacking made in Germany, Herausgeber: Chaos Computer Club (Wieckmann, Jürgen), Reinbek, 1989. Zitiert: Schrutzki, Die Hackerethik.
Schulze-Heiming, Ingeborg	Der strafrechtliche Schutz der Computerdaten gegen die Angriffsformen der Spionage, Sabotage und des Zeitdiebstahls, Dissertation, Münster, 1994. Zitiert: Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten.
Sondermann, Markus	Die neuen Straftatbestände der Datenveränderung § 303a StGB und § 303b StGB, Dissertation, Münster, 1989.
Systematischer-Kommentar zum Strafgesetzbuch	Herausgeber: Rudolphi, Hans-Joachim; Horn, Eckhard; Samson, Erich Band II, Stand: April 2000, Neuwied, 2000. Zitiert: Bearbeiter, in: SK.

Tiedemann, Klaus	Die Bekämpfung der Wirtschaftskriminalität durch den Gesetzgeber – Ein Überblick aus Anlaß des Inkrafttretens des 2. WiKG am 1.8.1986, in: Juristen Zeitung (JZ), 1986, Seiten: 865ff. Zitiert: Tiedemann, JZ 1986, 865.
Tröndle, Herbert Fischer, Thomas	Strafgesetzbuch – Kommentar, 50.Auflage, München, 2001. Zitiert: T/F
Volesky, Karl-Heinz Scholten, Hansjörg	Computersabotage - Sabotageprogramme - Computerviren, in: Informatik und Recht (iur) 1987, Seiten: 280ff.. Zitiert: Volesky/Scholten, iur 1987, 280.
Welp, Jürgen	Datenveränderung (§303a), in: Informatik und Recht (iur), Teil 1, in: iur 1988, Seiten 443ff. Teil 2, in: iur 1989, Seiten 434ff. Zitiert: Welp, iur 1988.
Wessels, Johannes Beulke, Werner	Strafrecht Allgemeiner Teil: Die Straftat und ihr Aufbau, 33. Auflage, Heidelberg, 2003. Zitiert: Wessels, AT.
Winkelbauer, Wolfgang	Computerkriminalität und Strafrecht, in: Computer und Recht (CR), 1985, Seiten: 40-44. Zitiert: Winkelbauer, CR 1985.
Zielinski, Diethart	Der strafrechtliche Schutz von Software, in: Kilian, Wolfgang/Gorny, Peter, Schutz von Computersoftware, technische und rechtliche Aspekte, Darmstadt, 1987, Seiten: 115-123. Zitiert: Zielinski, Strafrechtlicher Schutz von Software.

A. EINFÜHRUNG

Das Internet hat die Welt der Telekommunikation revolutioniert. Durch die weltweite Vernetzung von Computeranlagen können Menschen überall auf der Erde mit anderen Personen in Kontakt treten. Neue Technologien und Anwendungen ermöglichen es, dass die Nutzer des Internets in sekundenschnelle ihre Daten an einen beliebigen Ort versenden können oder Informationen von dort abrufen. Für viele Bereiche unseres gesellschaftlichen Lebens ist dieser globale Datenaustausch nicht mehr wegzudenken. Doch der technische Fortschritt in der Informationstechnologie steht nicht nur für eine Vielzahl neuer Chancen. Er eröffnet auch Möglichkeiten zu neuen Missbräuchen und traditionellen Missbrauchstechniken neue Dimensionen. Dies gilt vor allem dann, wenn die modernen Techniken zur Begehung von Straftaten eingesetzt werden. Im Mittelpunkt dieser Arbeit steht die Bedrohung von Datenangeboten durch Angriffe über das Internet, insbesondere durch so genanntes Hacking.

I. Begriffsbestimmung

Mangels einer einheitlichen Definition kann der Begriff des „Hacking“ unterschiedlich verstanden werden. Das deutsche Strafrecht kennt den Begriff des Hackers nicht. Aus der Übersetzung des englischen Wortes ergibt sich der Begriff „zerhacken, herumhacken auf.“[1] Hacking könnte somit als Ausdruck für das energische Herumhämmern auf einer Computertastatur verstanden werden.

Die meisten Menschen sehen in einem Hacker jedoch wesentlich mehr. Allgemein stellt man sich unter ihm einen versierten, aber böswilligen Computerexperten vor, der sich unberechtigt Zugang zu fremden Systemen verschafft, um dort Informationen auszuspionieren oder Daten mutwillig zu zerstören.[2]

---

[1] Langenscheidt Wörterbuch, S.272.

[2] Vgl. Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi-fuer-buerger.de/12/12030105.htm; Symantec Security Response, http://www.symantec.com/region/de/avcenter/hacker.html.

In der Hackerszene selbst wird diese Definition abgelehnt. Nach dem Selbstverständnis eines Hackers zeichnet er sich durch seinen „virtuosen Umgang mit programmierbaren Systemen aus und durch seine Neugier, wie man die beste Leistung aus solchen Systemen herausholen kann.[3] Hacker sehen sich selbst somit nicht als „Cybervandalisten".[4] Vielmehr behaupten sie, gewisse ethische Grundprinzipien anzuerkennen. Ob diese Grundsätze der landläufigen Meinung von Ethik entsprechen, sei dahingestellt. Nicht zu bestreiten ist aber, dass sich ein Teil der Hacker an einen strengen Ehrenkodex hält. Danach ist es unzulässig, seine Kenntnisse und Fähigkeiten dazu zu benutzen, anderen zu schaden oder um sich selbst zu bereichern.[5] Diese aus den sechziger Jahren stammende „Hackerethik" besagt auch, dass der Zugriff zu Computersystemen - und „allen anderen Dingen, die Auskunft darüber geben, wie die Welt funktioniert" - für jeden uneingeschränkt möglich sein soll.[6] Nach Ansicht der Hacker obliegt jedem die Pflicht, seine Erfahrungen und Kenntnisse weiterzugeben.

Die von einer weiblichen Hackerin gegründete Organisation „antichildporn.org"[7] beweist, dass diese Kenntnisse gesellschaftlich auch durchaus sinnvoll zum Einsatz gebracht werden können. „Antichildporn.org" entwickelt ein Tool, mit dem kinderpornographische Inhalte im Internet aufgespürt und den Ermittlungsbehörden gemeldet werden können.

Dass außergewöhnliche Programmierfähigkeiten jedoch auch zu bösartigen und zerstörerischen Zwecken eingesetzt werden, ist in der Gegenwart kein Ausnahmefall mehr. Die globale Vernetzung ermöglicht es Computerexperten von nahezu überall auf der Welt, Daten auf entfernten, fremden Systemen auszukundschaften, sie zu manipulieren, unzugänglich zu machen oder gar zu vernichten.

---

[3] jargon file v.4.4.7 (Online-Wörterbuch der Hackersprache), http://www.hack.gr/jargon/html/lexicon.html.

[4] Cybervandalisten werden auch Cracker genannt; siehe jargon file v.4.4.7 (Online-Wörterbuch der Hackersprache), http://www.hack.gr/jargon/html/lexicon.html.

[5] Schrutzki, Die Hackerethik, S.168ff.; NJW-Hackerreport 1/96, S.62

[6] vgl. „Hacker ethics" des Chaos Computer Clubs, unter: http://www.ccc.de/hackerethics.

[7] http://www.antichildporn.org.

Angesichts der breiten Palette im Internet frei verfügbarer Hacking-Programme ist es für einige Angriffsvarianten nicht einmal mehr erforderlich, außergewöhnliche Programmierkenntnisse zu besitzen. Die verschiedenen Angriffe werden in entsprechenden Foren Schritt für Schritt erklärt, leicht handhabbare, elektronische Werkzeuge helfen bei der Durchführung. Das Hacking ist somit längst keine Tätigkeit mehr, die ausschließlich Spezialisten vorbehalten ist. Auch weniger versierte Anwender können mit einigen einfachen Schritten fremden Systemen erheblichen Schaden zufügen.

II. Problemstellung

Wie bedeutend die Gefahr durch Angriffe über das Internet ist, lässt sich nur erahnen. Über das volle Ausmaß der Computerkriminalität liegen nur wenige verlässliche Statistiken vor. Einer amerikanischen Studie zufolge wurden allein im letzten Jahr rund 2500 neue Methoden beobachtet, wie Hacker in fremde Computersysteme eindringen.[8] Die Anzahl der Angriffe stieg im Vergleich zum Vorjahr um 19 Prozent. Die Zahl der aufgedeckten und gemeldeten Fälle entspricht jedoch nicht im Entferntesten der tatsächlichen Zahl der Angriffe. Viele Unternehmen verschweigen Angriffe auf ihre Computersysteme aus Angst vor einer Rufschädigung.

Schätzungen zufolge haben im Jahr 2001 die Attacken auf und über das Internet allein in Deutschland Schäden in Höhe von rund zehn Milliarden Euro verursacht.[9] Die Verbreitung von Viren stellt zweifellos eine der häufigsten Gefahren dar. Nicht ganz so häufig, aber besonders folgenschwer sind gezielte Angriffe auf vertrauliche Daten, zu denen sich Hacker unerlaubt Zugang verschaffen.

Von zunehmender Bedeutung sind auch die so genannten Distributed Denial of Service Angriffe, die zum Ziel haben, bestimmte Datenangebote im Internet durch die Überflutung mit sinnlosen

---

[8] Untersuchung des Computer Security Institutes San Francisco in Zusammenarbeit mit dem amerikanischen FBI, vgl. http://www.gocsi.com/press/20020407.jhtml?requestid=654359 und http://www.zdnet.de/news/software/0,39023144,2121489,00.htm.

[9] Schätzung der Unternehmensberatung Mummert & Partner, unter: http://www.ftd.de/tm/hs/1277807.html.

Anfragen zu blockieren. Allein im letzten Jahr ist die Zahl solcher Attacken um 250 Prozent gestiegen.[10]
Trotz der wachsenden Bedrohung durch die beschriebenen Angriffsformen und den beträchtlichen Schaden, den sie verursachen, wächst das Sicherheitsbewusstsein der Betroffenen nur langsam. Umso mehr stellt sich die Frage nach dem strafrechtlichen Schutz vor solchen Attacken.

Während der Gesetzgeber in den unterschiedlichsten Bereichen durch zahlreiche Gesetzesänderungen auf den Fortschritt in der Informationstechnologie reagiert hat, blieben strafrechtliche Neuregelungen für den hier zu behandelnden Bereich die Ausnahme. Die geltenden Bestimmungen existieren unverändert seit den achtziger Jahren. Durch das 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) von 1986 wurden als Reaktion auf die ersten bekannt gewordenen Fälle der Computerspionage, -manipulation und -sabotage die Tatbestände des § 202a StGB (Ausspähen von Daten), § 303a StGB (Datenveränderung) und § 303b StGB (Computersabotage) neu in den Katalog des Strafgesetzbuches aufgenommen.
Obwohl es sich damit um vergleichbar junge Tatbestände handelt, stammen die Regelungen aus einer Zeit, in der das Internet als Massenmedium noch nicht existierte. Damals waren Angriffe auf Daten ein Spezialproblem, das das Sicherheitsgefühl der Öffentlichkeit kaum berührte. Der eigene PC zuhause oder am Arbeitsplatz war eine Seltenheit, die heute verwendeten Angriffsmethoden der Hacker waren noch unbekannt. Die geltenden Strafrechtsnormen stammen folglich aus einer Zeit, in der die von Hackern ausgehende Gefahr eine völlig andere war.

Diese Arbeit wird untersuchen, ob die damals in Kraft getretenen Vorschriften dennoch den Anforderungen der Gegenwart gerecht

[10] vgl. Studie „2003 Computer Crime and Security Survey“ des Computer Security Institutes (CSI), San Francisco in Zusammenarbeit mit dem amerikanischen FBI, http://www.gocsi.com/press/20030528.jhtml.

werden und aus strafrechtlicher Sicht einen ausreichenden Schutz vor den heute gängigen Angriffsformen auf Datenangebote im Internet gewährleisten.[11]

III. Aufbau der Arbeit

Die Arbeit unterteilt sich in vier Abschnitte. In dem sich an diese Einleitung anschließenden ersten Teil (B) wird das Hacking in der Form des Eindringens in fremde Computersysteme behandelt. Der strafrechtlichen Begutachtung ist ein kurzer Überblick über die Entwicklung des Hackings, sowie eine Einführung in die technischen Grundlagen und die Arbeitsweise von Hackern vorangestellt. Nach der strafrechtlichen Beurteilung dieser Angriffe, bildet die Behandlung einiger Sonderfälle den Abschluss dieses Kapitels. Unter einem eigenen Gliederungspunkt (C) wird die Verwendung Trojanischer Pferde als ein Spezialproblem behandelt. Die so genannten Denial of Service Angriffe, die eine gänzlich andere Zielrichtung haben als herkömmliche Hackerangriffe werden unter D. besprochen. Auch hier werden vor der strafrechtlichen Analyse die wesentlichen Grundlagen für diese Art von Angriffen beschrieben.
Der letzte Abschnitt (E) wird die Ergebnisse der Arbeit schließlich zusammenfassen unter Berücksichtigungen aktueller Vorhaben auf internationaler Ebene einen Ausblick auf zu erwartende Änderungen des Rechts geben.

[11] Um den Tatbeständen ausreichend Raum für Erörterungen zukommen zu lassen, beschränkt sich die Prüfung der Strafbarkeit auf die durch das 2. WiKG eingeführten Tatbestände. Andere strafrechtliche Vorschriften, wie § 17 UWG, §106 UrhG oder §§ 43,44 BDSG bleiben daher außer Betracht.

B. HACKING

I. Grundlagen

1) Die Geschichte des Hacking

a) Die Phone-Hacker der sechziger und siebziger Jahre

Die Ursprünge des Hackings gehen zurück auf die sechziger und siebziger Jahre. Ein simples Ereignis legte damals den Grundstein für die Entwicklung einer ganzen Subkultur. Der unter dem Namen „Captain Crunch“ bekannt gewordene Amerikaner John Draper entdeckte per Zufall, dass die einer Cornflakes-Packung beigelegte Pfeife sich zur Erzeugung bestimmter Tonsequenzen eignete, mittels derer ganze Telefonvermittlungsanlagen unter Kontrolle gebracht werden konnten.[12] Eine kleine Gruppe von Technikwütigen begann in der Folge damit, die so entdeckten Schwachstellen der Telefonsysteme zu ihren Gunsten auszunutzen. Durch den Bau von elektronischen Schaltungen gelang es, die Gebührenerfassung der US-amerikanischen Telefonnetzwerke auszutricksen. Unter Einsatz einer so genannten „Blackbox“ konnten durch das Vortäuschen eines Freizeichens kostenlose Gespräche geführt werden.

b) Die ersten Hacker der achtziger Jahre

Mit der langsam einsetzenden Verbreitung von Personal Computern Ende der siebziger Jahre bildete sich die erste Computer-Hacker-Generation. Da die Vernetzung von Computersystemen in dieser Zeit noch wenig fortgeschritten war, konzentrierte sich die Computerkriminalität vor allem auf den internen Missbrauch von Firmencomputern. Meist waren es die eigenen Mitarbeiter, die sich Zugang zu den firmeneigenen Rechnern verschafften, beispielsweise um eine Gehaltsabrechnung zu manipulieren. Mitte der achtziger Jahre häuften sich auch Einbrüche von außerhalb, in der Regel begangen von Einzeltätern. Die zunehmende Bedeutung von Computern in der Gesellschaft führte zu der Gründung von Hacker-Vereinigungen.

[12] Rogge, Hacking intern, S.26.

1984 entstand mit dem Hamburger Chaos Computer Club (CCC)[13] die bis heute bedeutendste Organisation für Hacker in Deutschland.

c) Hacker im Zeitalter des Internets

Die starke Ausbreitung von Computern im privaten Umfeld und die Kommerzialisierung des Internets haben in den neunziger Jahren dazu geführt, dass Hacking nicht mehr nur eine Eigenart unter hoch spezialisierten Computerfreaks war. Der Umgang mit Techniken, Protokollen und Standards wurde von Seiten der Softwareindustrie durch die Einführung benutzerfreundlicher Anwendungen erheblich vereinfacht. Dies eröffnete auch weniger versierten Anwendern die Möglichkeit, neue Technologien für kriminelle Machenschaften zu missbrauchen. Während sich die alte Hackerszene noch an eine Vielzahl ungeschriebener Gesetze für den sinnvollen Umgang mit den modernen Technologien einsetzte[14], sind heute für die Masse der Anwender solche Moralprinzipien kein Maßstab mehr. Die zahlreichen nicht-professionellen Anwender verkennen häufig die Gefahren, die sie durch ihre Attacken auf fremde Systeme verursachen. Ungeachtet der möglichen Folgen werden nur halbwegs bekannte Aktionen durchgeführt, bei denen nicht selten allein die Ungeschicktheit des Anwenders erheblichen Schaden anrichten kann.[15]

Im Zeitalter des Internets sind die konstruktiven Attacken der klassischen Hacker eine Seltenheit. Sabotageangriffe wie die durch Denial of Service Attacken sind hingegen an der Tagesordnung und können beinahe von jedem normalem Anwender eingeleitet werden.

2) Motivation eines Hackers

Mit der zunehmenden Zahl der Angriffe über das Internet haben sich auch die Motive für das Hacking verändert.

---

[13] Die Webseite des Chaos Computer Clubs ist abrufbar unter: http://www.ccc.de.
[14] zur „Hackerethik“ siehe oben: S.2.
[15] Granderath, DB 1986, Beil.18, S.2, Hier wird beschrieben, wie die New Yorker Cornell-Universität einen Teil ihrer Datenverarbeitungsanlage abschalten musste. Grund waren Schäden, die amerikanische und deutsche Hacker aus Unkenntnis, also ohne Schädigungsvorsatz angerichtet hatten.

Ursprünglich war es vor allem die Faszination an der Technik, die Hacker bei ihrem Tun antrieb. Der „klassische“ Hacker ist ein Computerspezialist mit ausgeprägtem Sicherheitsbewusstsein. Es ist sein Hobby, die Zugangssperren fremder Systeme zu überwinden. Nicht selten macht er die Betroffenen auf die von ihm entdeckten Sicherheitslücken aufmerksam. In der Regel begnügt er sich allein mit dem Erfolgserlebnis, in ein fremdes Rechnersystem eingedrungen zu sein. Qualität und Inhalt der Daten, zu denen er Zugang erlangt hat, interessieren ihn nicht. Er hält sich an die Hackerethik und lässt fremde Daten unbeschädigt.

Vor etwa 20 Jahren war neben dieser Begeisterung für die Technik noch ein anderer wichtiger Umstand Hauptmotivationsgrund für das Hacking. Damals waren vor allem intelligente Jugendliche, die sich selbst keine rechenstarken Geräte leisten konnten, daran interessiert, die Kapazitäten von Großrechenanlagen anzuzapfen.[16] Durch die massiven Preissenkungen im Hardwarebereich hat dieses Phänomen jedoch weitestgehend an Bedeutung verloren. Leistungsstarke Computer sind mittlerweile für jedermann erschwinglich, weshalb man auf fremde Rechenkapazitäten längst nicht mehr angewiesen ist.

Von Anfang an gab es auch immer einige Hacker, die ihre Fähigkeiten bewusst missbräuchlich eingesetzt haben und anderen dadurch teils erheblichen Schaden zufügten. Ein solcher, kriminell motivierter Hacker dringt gezielt in bestimmte Systeme ein, um wertvolle Informationen auszuspionieren oder zu manipulieren. Häufig stehen finanzielle Interessen hinter derartigen Angriffen, zum Beispiel wenn ein Mitarbeiter die Gehaltsliste zu seinen Gunsten manipuliert. Aber auch Frustration kann Antrieb für die Attacken eines Hackers sein, wenn beispielsweise ein entlassener Mitarbeiter vor seinem Weggang Hintertüren im Firmennetzwerk einrichtet oder durch Denial of Service Angriffe den Server seines ehemaligen Arbeitgebers lahm legt.

[16] Rogge, Hacking intern, S.22.

Technisch weniger bewanderte Anwender bewegt vor allem die Neugierde zur Ausführung eines Angriffs. Dieser wird dann oft laienhaft ausgeführt, kann aber trotzdem großen Schaden anrichten. Motiviert sind solche Angriffe häufig von dem Wunsch, dem Opfer dessen Beherrschung und die eigene Überlegenheit vorzuspiegeln.

3) Spektakuläre Fälle

Für die besonders Aufsehen erregenden Angriffe sind in der Regel die technisch sehr versierten Hacker verantwortlich. Ihre Angriffe verdeutlichen auch, welche einschneidenden und weit reichenden Konsequenzen das Hacking haben kann.

Durch den so genannten „NASA-Hack“ gelang es einer Gruppe deutscher Hacker im Frühjahr 1987 in das SPANNET[17] der US-Weltraumbehörde NASA einzudringen.[18] Durch einen Fehler des Betriebssystems konnten sie auf eine Datei zugreifen, in der die Kennwörter der 4000 berechtigten Benutzer hinterlegt waren. Diese waren jedoch verschlüsselt, weshalb sich die Hacker eines Trojanischen Pferdes[19] bedienten, das sie auf dem angegriffenen System installierten. Dieses Programm, das für den Benutzer unsichtbar im Hintergrund abläuft, war in diesem Fall so programmiert, dass das System auf die Eingabe von Kennwörtern durch sich anmeldende Benutzer überwacht wurde. Die so gewonnenen Informationen übermittelte das Programm anschließend an die Hacker, die mit Hilfe der Passwörter nach und nach ihre Benutzerrechte in dem 1600 Großrechner umfassenden System ausbauen konnten. Die Daten auf den 135 Einzelrechnern, zu denen sie sich letztlich Zugang verschafften, ließen sie jedoch unberührt. Wie sich später herausstellte, ging es ihnen nur um das Auskundschaften von Sicherheitslücken.

Einen anderen Plan verfolgten ebenfalls deutsche Hacker, die sich Ende der achtziger Jahre zusammenschlossen, um gemeinsam

---

[17] Space Physics Analysis Network.
[18] Frankfurter Allgemeine Zeitung vom 16.09.1987, S.17.
[19] Auf die Trojanischen Pferde wird in Teil C dieser Arbeit gesondert eingegangen. Informationen zu „Trojanern“ finden sich auch unter: http://www.anti-trojan.net/de/info.aspx.

Informationen zu erhacken, die später an sowjetische Geheimagenten verkauft werden sollten. Bei diesem auch politisch sehr brisanten, als „KGB-Hack“ bekannt gewordenen Angriff erlangten die jungen Hacker nicht nur die streng geheimen Quelltexte der damals gängigen Betriebssysteme UNIX und VMS, sondern sie gelangten auch an wertvolle militärische Daten über Radaranlagen, Nuklearwaffen und das amerikanische Programm zur Weltraumverteidigung SDI.[20] Erst nach etwa einem Jahr fielen die Eindringlinge auf. Eine Fangschaltung führte zu einem der Hacker nach Hannover. In dem sich anschließenden Strafprozess vor dem Oberlandesgericht Celle waren Staatsanwaltschaft und Gericht mit den technisch anspruchsvollen Rahmenbedingungen der Taten überfordert.[21] Kennzeichnend dafür war, dass der Straftatbestand des Ausspähens von Daten, obwohl er zu diesem Zeitpunkt bereits seit vier Jahren in Kraft war, von der Staatsanwaltschaft unberücksichtigt blieb. Sie stützte die Anklage auf den Vorwurf der Spionage.

Auch in jüngerer Vergangenheit machen Hacker immer wieder durch spektakuläre Attacken auf sich aufmerksam. 1998 gelang einem Hacker der Einbruch in das Rechenzentrum des Pentagon, wo er über mehrere Tage unerkannt Zugriff auf die Systeme hatte.[22]

Selbst der marktführende Softwarehersteller Microsoft ist vor den Angriffen durch Hacker nicht sicher. Im November 2000 mussten die Verantwortlichen der kalifornischen Firma eingestehen, dass aufgrund einer Sicherheitslücke ein Hacker sich erfolgreich Zugang zu wichtigen Servern des Unternehmens verschaffen konnte.[23]

4) Anatomie einer Attacke – die Arbeitsweise der Hacker

Mangelndes technisches Verständnis kann im Bereich des Hacking dazu führen, dass Sachverhalte juristisch falsch oder ungenau bewertet werden. Für eine verlässliche rechtliche Beurteilung sind

[20] SDI = „Strategic Defense Initiative“.
[21] Vgl. „Der Spiegel“ Heft 5/1990, S.181ff.
[22] Rogge, Hacking intern, S.1.
[23] Heise-Newsticker, Meldung vom 29.10.2000, abrufbar unter: http://www.heise.de/newsticker/data/jk-29.10.00-001/default.shtml.

daher technische Kenntnisse erforderlich. Einige Grundlagen für dieses Hintergrundwissen liefert dieser Abschnitt.

Angriffe durch Hacker unterscheiden sich oft erheblich im Hinblick auf ihre Art, Intensität und Durchschlagskraft. Trotzdem ähnelt sich eine Vielzahl der Attacken bei genauerem Hinsehen. Der „klassische“ Angriff durch Hacker läuft zumeist nach einem einheitlichen Grundschema ab.

a) Aufspüren und Auskundschaften eines Systems und seiner Sicherheitslücken

Üblicherweise beginnt jeder Angriff mit dem Auskundschaften des Zielsystems. Grundvoraussetzung für die Durchführung eines Angriffs sind die Kenntnis von Rechnernamen und das Vorhandensein von Informationen über die Netzwerkstruktur. Der Angreifer sammelt also möglichst viele Informationen zur Zielumgebung. Diese Spurensuche bezeichnet man auch als „Footprinting“.[24] Typische Informationen, nach denen der Hacker in diesem Stadium Ausschau hält, sind die Namen von Personen und Organisationen, die mit der Zielumgebung in Verbindung gebracht werden. Auch Telefonnummern können wertvolle organisatorische Informationen über das Zielsystem liefern. Häufig helfen bei der Suche nach entsprechenden Angaben bereits die herkömmlichen Suchmaschinen wie „Google“ oder „Fireball“. Nicht selten bieten die betroffenen Unternehmen sogar auf ihren eigenen Internetseiten technische und konzeptionelle Informationen zu ihren Systemen an.
Ist dies nicht der Fall, helfen dem Angreifer diverse im Internet verfügbare Dienste. Mit Hilfe einer so genannten „Whois“-Abfrage können von einem entsprechenden Server Informationen zu Adressbucheinträgen und Domainnamen ausgelesen werden. Mittels eines Netzwerkscans kann sich der Angreifer über die Erreichbarkeit fremder Systeme informieren.

[24] Rogge, Hacking intern, S.511.

Durch das Herstellen eines ersten direkten Kontakts wird der Status des Zielsystems ausfindig gemacht.

Ein als „Portscanning“ bezeichnetes Verfahren dient dazu, konkrete Angriffspunkte für die bevorstehende Attacke herauszufinden. Die von jedem an das Internet angeschlossenen Computer benutzten Ports dienen als Ein- und Ausgänge für die Verbindungen mit dem Netz.[25] Die einzelnen Ports werden für bestimmte Dienste genutzt, beispielsweise für das Senden und Empfangen von Emails[26] oder die Verbindung mit dem World Wide Web (WWW)[27]. Gelegentliche haben die angebotenen Dienste Schwachstellen, die von Angreifern ausgenutzt werden können.[28]

Mit den gesammelten Informationen kann der Angreifer seine Attacke gezielt vorbereiten.

b) Das Eindringen in fremde Systeme

In seltenen Fällen kann es einem Angreifer gelingen, Schlupflöcher zu finden, über die er, ohne eine besondere Zugangssperre überwinden zu müssen, in ein fremdes System eindringen kann. In der Regel wird er jedoch für den Zugang einen Benutzernamen und ein geheimes Kennwort (Passwort) eingeben müssen.

aa) Die Passwortsperre

Während sich Benutzernamen häufig nach einem bestimmten Schema richten und deshalb oft leicht erraten werden können, sind Passwörter geheim. Trotzdem bieten sich für das Herausfinden der Kennwörter zahlreiche Möglichkeiten.

Oft hilft schon das Ausprobieren nahe liegender Codewörter. Sofern seitens des Unternehmens bestimmte Richtlinien für die Wahl der

---

[25] In der Regel werden 16-Bit-Portnummern verwendet, mit der Folge, dass für eine Verbindung 65.535 Ports zur Verfügung stehen. Die wichtigsten Dienste werden allerdings nur auf den Ports im Nummernbereich 1 bis 1.023, den so genannten well-known Ports, angeboten.

[26] Der Emailverkehr erfolgt über die Dienste smtp (Simple Mail Transfer Protocol) auf Port 25 und für den Empfang mittels des Post Office Protocol in der Version 3 (pop3) auf Port 110.

[27] Der dazugehörige Dienst ist das „Hyper Text Transfer Protocol“ (http) auf Port 80.

[28] Rinker, MMR 2002, 663 (664f.).

Kennwörter fehlen, neigen viele Mitarbeiter dazu, sehr leichte und deshalb unsichere Passwörter auszusuchen. Die Eingabe der Namen von Familienmitgliedern oder Haustieren führt ebenso wie das Geburtsdatum des Benutzers oder einer ihm nahe stehenden Person häufig zum Ziel.

Oft werden Passwörter auch mehrfach verwendet. Gelangt der Angreifer an solche Kennwörter, die Benutzer für andere Systeme gebrauchen, wird er daher auch diese ausprobieren.

Doch selbst wenn weniger nahe liegende Kennwörter verwendet werden, gibt es Möglichkeiten diese herauszufinden. Hierbei sind spezielle Programme behilflich, die anhand einer großen Datenbank in kurzer Zeit eine Vielzahl von Wörtern ausprobieren. In diesem auch „Dictionary-Attacke“ genannten Verfahren werden die aus einem vorliegenden Wörterbuch stammenden Begriffe mit dem verschlüsselten Originalkennwort verglichen.[29] Selbst ein älterer Computer[30] schafft es, mit dieser Methode 500.000 Wörter pro Sekunde zu testen. „Hybrid-Dictionary-Attacken“ und „Brute-Force-Angriffe“ erweitern dieses Verfahren sogar noch, indem nicht nur Buchstabenketten getestet werden, sondern auch Zahlen und Sonderzeichen einbezogen werden. 30 Millionen noch so sinnlose Kennwörter können in der Minute geprüft werden. Somit ist es regelmäßig nur eine Frage der Zeit, bis sich ein Hacker Zugang zu einem fremden System verschaffen kann.

Sicheren Schutz vor Kennwortattacken gibt es lediglich, wenn ein System nur eine begrenzte Anzahl von Versuchen zulässt. Viele neuere Systeme sperren ein Benutzerkonto sobald ein Kennwort zum dritten Mal falsch eingegeben wurde.

In diesem Fall wird ein Hacker auf andere Weise versuchen, an das benötigte Kennwort zu gelangen. Eine verblüffend einfache, aber oft erfolgreiche Methode ist ein in der Hackerszene als „Social Engineering“ bezeichnetes Vorgehen. Hierbei tritt der Angreifer mit dem Inhaber eines geheimen Kennwortes persönlich in Kontakt. Er

---

[29] Rogge, Hacking Intern, S. 661.

[30] Das Beispiel bezieht sich auf einen nach heutigem Stand leistungsschwachen Rechner mit Pentium II-Prozessor und einer Taktfrequenz von 350 MHz.

gibt sich beispielsweise bei einem Anruf im Büro als Systemadministrator aus und verlangt die Herausgabe des Passwortes, weil es angeblich für Wartungsarbeiten oder zur Beseitigung eines Systemfehlers gebraucht werde. Erstaunlich viele gutgläubige Benutzer fallen auf diesen einfachen Trick herein.
Mit dem so erlangten Kennwort hat der Hacker ungehinderten Zugang zu dem fremden System.

bb) Zugriff auf Daten

Nach dem Eindringen in die Zielumgebung hat der Angreifer abhängig von „seinen" Benutzerrechten Zugriff auf eine bestimmte Menge von Informationen. Über das Herausfinden von Sicherheitslücken können diese Rechte ausgeweitet werden, um so letztlich Zugang zu allen auf dem System vorhandenen Daten zu erlangen. Beliebig viele Daten können dann vom Angreifer gestohlen oder manipuliert werden.
Damit das Eindringen des Hackers möglichst lange unentdeckt bleibt, ist der Angreifer in der Regel bemüht, die von ihm hinterlassenen Spuren zu verwischen. Außerdem richtet er sich Hintertüren ein, über die er später wieder unerkannt das System betreten und verlassen kann. Schließlich kann ein Hacker versuchen, andere Hosts zu finden, die der von ihm angegriffenen Maschine trauen, um seinen Angriff auch auf diese Systeme auszudehnen.

c) Schutzmaßnahmen

Bei einer geschickten Durchführung des Angriffs kann es lange dauern, bis das Eindringen in das System von den Administratoren erkannt wird. Aufwendige und teure „Intrusion Detection Systeme"[31] unterstützen die Suche nach Angreifern. Jedoch bieten auch sie keinen umfassenden Schutz vor Hacker-Angriffen.
Um das Eindringen von Angreifern zu erschweren, ist es unbedingt erforderlich, das interne Netzwerk einer wirkungsvollen Sicherheits-

[31] „Einbruchs-Erkennungs-Systeme", vgl. hierzu, Caelli, Information Security Handbook, S.525.

politik zu unterstellen. Diese sollte zum Beispiel Richtlinien für den Umgang mit Kennwörtern haben und allen Benutzern vorschreiben, ein langes und ungewöhnliches Kennwort zu benutzen.

Außerdem kann das Netzwerk nach außen hin durch „Firewalls“[32] geschützt werden. Solche „Brandschutzmauern“ befinden sich an den Schnittstellen zwischen einem geschlossenen Netzwerk und dem Internet. Die Firewall filtert an dieser Stelle alle eingehenden und ausgehenden Datenströme. Dabei werden alle Aktionen, die nicht ausdrücklich erlaubt sind, blockiert. Die Konfiguration einer solchen Schutzvorrichtung ist jedoch äußerst aufwendig und kompliziert. Um einen wirkungsvollen Schutz vor Angreifern zu erreichen, sind umfangreiche Fachkenntnisse erforderlich, die der private Anwender am Heim-PC in der Regel nicht besitzt.

[32] Nolden/Franke, Das Internetbuch, S.601.

II. Strafbarkeit des Hacking

Das deutsche Strafrecht kennt keine allgemeine Vorschrift gegen das unerlaubte Eindringen in ein Datenverarbeitungssystem. Zwar gab es Bestrebungen, bereits den unbefugten Zugang zu fremden Daten unter Strafe zustellen. Der Gesetzgeber sah diese Regelung jedoch als eine zu weitgehende Vorverlagerung der Strafbarkeit an.[33] Dennoch wurden durch das 2. WiKG Tatbestände in das StGB eingefügt, die wenigstens teilweise die Sanktionierung der Aktivitäten von Hackern ermöglichen.[34]

1) Das Ausspähen von Daten nach § 202a StGB

Im 15. Abschnitt des Besonderen Teils zur „Verletzung des persönlichen Lebens- und Geheimbereichs“ wurde durch die Einführung des § 202a das „Ausspähen von Daten“ unter Strafe gestellt.

a) Der objektive Tatbestand

Nach § 202a Abs. 1 StGB handelt tatbestandsmäßig, wer nicht für ihn bestimmte und gegen unberechtigten Zugang besonders gesicherte, nicht unmittelbar wahrnehmbare Daten sich oder einem anderen unbefugt verschafft.

aa) Der Datenbegriff

Was in diesem Zusammenhang unter dem Begriff „Daten“ zu verstehen ist, konkretisiert die Legaldefinition des § 202a Abs. 2 StGB. Danach sind taugliches Tatobjekt nur solche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

---

[33] BT-Drs. 10/5058, S.29.
[34] Möhrenschlager, wistra 1991, 321 (326f.).

(1) Technische Anforderungen

Die Daten müssen der sinnlichen Wahrnehmung entzogen sein,[35] das heißt ihr Bedeutungsgehalt wird erst nach einer technischen Umformung für den Betrachter erkennbar.[36] Hinsichtlich solcher Daten, die Hacker auf angegriffenen Computern vorfinden, ist diese Voraussetzung stets erfüllt. Die Daten auf Computern sind für den menschlichen Betrachter erst dann lesbar, wenn sie mittels eines entsprechenden Programms oder Betriebssystems verarbeitet und sichtbar gemacht wurden.

Geschützt sind diese Daten, wenn sie auf einem bestimmten System zur weiteren Verwendung erfasst, also gespeichert sind[37] oder aber, wenn sie sich in einem Übermittlungsstadium befinden. Die Übermittlung bezeichnet jede Weiterleitung der Daten, insbesondere im Online-Verkehr oder über interne Netzwerke.[38] Angriffe, die sich auf das „Anzapfen“ von Datenübertragungsleitungen beziehen, werden daher vom Schutzbereich ebenfalls umfasst.[39]

Ein Sonderfall betrifft solche Daten, die sich im Arbeitsspeicher eines Computers befinden, aber noch nicht auf der Festplatte oder einem anderen Datenträger abgespeichert sind. Im Arbeitsspeicher eines Computers werden Daten der jeweiligen Sitzung vorübergehend automatisch abgelegt. Spätestens beim Abschalten des Computers werden diese Daten jedoch wieder gelöscht. Vom Datenbegriff des §202a Abs. 2 StGB könnten solche, nur vorübergehend gespeicherte Daten ausgeklammert sein. Dies wäre jedenfalls dann der Fall, wenn unter der Speicherung von Daten nur der explizite Speicherungsvorgang verstanden werden soll, durch den die Daten dauerhaft auf einem Datenträger fixiert werden.[40]

Für die Erforderlichkeit einer dauerhaften Speicherung könnte der Wortlaut der Definition sprechen, wonach gespeicherte und übermittelte Daten gleichrangig behandelt werden. Genau wie alle über-

---

[35] Jähnke, in: LK, § 202a, Rn.4.
[36] Tröndle/Fischer, § 202a, Rn.2.
[37] Zum Begriff der „Speicherung“ vgl. auch § 3 Abs. 5, Nr. 1 BDSG.
[38] Welp, iur 1988, 445.
[39] BT-Drs. 10/5058, S.28; Kühl, in: Lackner/Kühl, § 202a, Rn.2.
[40] Mühle, Hacker und Computer-Viren, S. 63.

mittelten Daten müssten daher auch die übrigen Daten dauerhaft gespeichert sein, um in den Schutzbereich der Vorschrift zu fallen.
Es ist jedoch nicht einzusehen, warum zwischen solchen Daten, die sich im Verarbeitungsprozess befinden und denjenigen, die dauerhaft gespeichert werden, unterschieden werden muss. Gerade bei besonders sensiblen Daten wie einem Passwort wird aus Sicherheitsgründen oft bewusst vermieden, sie auf einem dauerhaften Datenträger abzulegen. Sie werden häufig ausschließlich im Arbeitsspeicher des Systems zwischengespeichert. Gerade diese Daten gegen ein Ausspähen schutzlos zu lassen, ist mit dem Sinn und Zweck der Vorschrift nicht vereinbar.[41]

Der Datenbegriff des § 202a Abs. 2 StGB ist somit weit auszulegen. Gemessen an den oben beschriebenen, gängigen Angriffsformen, treffen Hacker bei einem Eindringen in fremde Systeme üblicherweise auf solche Daten, die die genannten technischen Voraussetzungen erfüllen.

(2) Inhalt der Daten

Die rein technisch formulierte Definition des § 202a Abs. 2 StGB enthält jedoch keine Angaben in Bezug auf die Qualität der Daten.
Teilweise wird vertreten, dass nur solche Daten durch die Vorschrift geschützt werden, die einen wirtschaftlichen Wert besitzen.[42] Nach dieser Auffassung ist das durch § 202a StGB geschützte Rechtsgut das Vermögen. Dagegen sprechen jedoch mehrere Argumente.
Zum einen gibt der Wortlaut der Vorschrift eine Begrenzung auf Daten mit wirtschaftlichem Wert nicht her. Außerdem widerspricht die systematische Einordnung der Norm einer Begrenzung des Schutzbereiches auf vermögenswerte Rechtsgüter.[43] Im 15. Abschnitt des Besonderen Teils wird die Verletzung des persönlichen Lebens- und Geheimbereichs sanktioniert. Es geht folglich um den Schutz der Vertraulichkeit von Informationen. Diese Vertraulichkeit ist auch

[41] Mühle, Hacker und Computer-Viren, S.63.
[42] Haft, NStZ 1987, 6 (9).
[43] Frommel, JuS 1987, 668; Haß, Strafrechtlicher Schutz von Computerprogrammen, Rn.20.

schützenswert, wenn die Daten wirtschaftlich wertlos sind, beispielsweise wenn es sich um die Email-Korrespondenz zwischen Privatleuten handelt. Eine Begrenzung des Datenbegriffes würde dazu führen, dass bestimmte Handlungen, die in der Offline-Welt strafbar sind - beispielsweise die Verletzung des Briefgeheimnisses nach § 202 StGB - in der Online-Umgebung trotz ihres gleichartigen Charakters straffrei wären. Das Schließen solcher, durch die Fortentwicklung der Technik entstandenen Strafbarkeitslücken war jedoch gerade Sinn und Zweck der Einführung des § 202a StGB.[44]
Nach überwiegender Auffassung reicht der Schutz daher über das wirtschaftliche Interesse des Verfügungsberechtigten hinaus.[45] Zugrunde gelegt wird ein „weiter Datenbegriff", nach dem alle in Daten, Dateien oder Datenbanksystemen verkörperten Informationen vor unbefugtem Zutritt geschützt sein sollen.[46] Geschütztes Rechtsgut ist folglich das formelle Geheimhaltungsinteresse des Dateninhabers.[47] Dabei bedeutet „formal", dass es sich beim Tatobjekt der von § 202a StGB geschützten Daten - ebenso wie bei der Verletzung des Briefgeheimnisses in § 202 - nicht um geheime Daten handeln muss.[48] Die Qualität der Daten spielt folglich keine Rolle.[49]

bb) Die fehlende Empfangsberechtigung des Täters

Nach § 202a Abs. 1 StGB dürfen die vom Täter erlangten Daten „nicht für ihn bestimmt" sein. Eine Empfangsberechtigung fehlt dem Täter, wenn ihm die Daten nach dem Willen des Berechtigten im Zeitpunkt der Tathandlung nicht zur Verfügung stehen sollen.[50]
Ist der Berechtigte mit einem Zugriff auf die Daten jedoch allgemein oder im Einzelfall einverstanden, schließt dies die Tatbestandsverwirklichung aus.[51] Betriebsinterne, die zur Benutzung, Verarbeitung und Verwaltung von Datenbeständen ihres Arbeitgebers

---

[44] Haft, NStZ 1987, 6.
[45] Tröndle/Fischer, § 202a, Rn.2; Hilgendorf, JuS 1996, 509 (511).
[46] Lenckner, in: S/S, § 202a, Rn.3.
[47] Tröndle/Fischer, § 202a, Rn.2; Hilgendorf, JuS 1996, 509 (511).
[48] Sieber, in: Hoeren/Sieber, Handbuch Multimediarecht, Teil 19, R.418.
[49] So auch Granderath, DB 1986, Beil.18, 1f.; Arzt/Weber, BT 4, Rn.91.
[50] Kühl, in: Lackner/Kühl, § 202a, Rn.3;
[51] BT-Drs. 10/5058, S.29.

grundsätzlich berechtigt sind, verwirklichen selbst bei einer vertragswidrigen Nutzung nicht den Tatbestand des § 202a Abs.1 StGB. Speichert ein Angestellter beispielsweise Unternehmensdaten für eigene Zwecke, verhält er sich lediglich ungetreu.[52] Er dringt jedoch nicht in einen von § 202a geschützten fremden Herrschaftsbereich ein.[53]

Teilweise wird vertreten, dass eine Empfangsberechtigung für die Daten fehlt, wenn sich ein Mitarbeiter außerhalb seiner Dienstzeit und ohne betriebliche Veranlassung in das System seines Arbeitgebers „einhackt".[54] Angesichts des Zwecks von § 202a StGB, die Vertraulichkeit der Daten zu schützen, vermag diese Unterscheidung nicht zu überzeugen. Erfasst werden soll von der Vorschrift nicht der „Insider", sondern der in ein fremdes System Eindringende.[55] Solange grundsätzlich ein Zugang zu den Daten gewährt wird, ist eine Zweckbindung der Zugangserlaubnis für die strafrechtliche Beurteilung unbeachtlich.

Greift ein Hacker auf fremde Datenangebote zu, sind diese regelmäßig nicht für ihn bestimmt. Dies gilt auch dann, wenn die Daten sich auf den Täter selbst beziehen.[56] Allein dadurch werden die Daten noch nicht zu seinen eigenen Daten. Vielmehr kann gerade ein besonderes Interesse an dem Schutz vor einem Zugriff durch die betreffende Person bestehen, zum Beispiel bei einem Abruf von Daten aus der Datenbank des Bundeskriminalamtes.[57]

Die Bestimmung der Daten für den Täter fehlt auch dann, wenn sich das Datenangebot nicht an einen klar abgegrenzten Empfängerkreis richtet sondern grundsätzlich dem allgemeinen Publikum zugänglich ist, der Zugang selbst aber beispielsweise von einer Registrierung oder der Zahlung einer Gebühr abhängig ist.[58] Wenn der Täter zum

---

[52] Jähnke, in: LK, § 202a, Rn.9.
[53] Lenckner/Winkelbauer CR 1986, 483 (486).
[54] Jähnke, in: LK, § 202a, Rn.10.
[55] Lenckner, in: S/S, § 202a, Rn.6; T/F, § 202a, Rn.7; Mühle, Hacker und Computerviren, S.64.
[56] Möhrenschlager, wistra 1986, 128 (140).
[57] Mühle, Hacker und Computerviren, S.64; Granderath, DB 1986, Beil. 18, 2.
[58] BT-Drs. 10/5058, S.29; Jänke, in: LK, § 202a, Rn.9.

Tatzeitpunkt selbst keinen Anschluss zu der Datenbank besitzt, handelt er tatbestandsmäßig.

cc) Besondere Zugriffssicherung

Ein strafbares Ausspähen von Daten kann nur stattfinden, wenn die Daten „gegen unberechtigten Zugang besonders gesichert sind." Ohne das Vorhandensein einer solchen Zugriffssicherung sind die auf dem fremden Computer gespeicherten Daten für jedermann frei abrufbar. In diesem Fall kann und braucht das System nicht „gehackt" werden. Durch §202a StGB wird folglich nur der Dateninhaber geschützt, der nicht völlig „sorglos" mit seinen Daten umgeht.[59] Durch die Einrichtung einer besonderen Zugriffssicherung muss er sein Interesse an der Geheimhaltung der Daten dokumentieren.[60] Erst wenn ein Angreifer diese Schranke missachtet und überwindet beginnt kriminelles Unrecht.[61]

(1) Art und Umfang der Zugangssicherung

Fraglich ist, ob eine Zugangssperre gewissen Mindestanforderungen genügen muss. § 202a StGB enthält hierfür keine Maßstäbe. In den Gesetzesmaterialien verweist der Gesetzgeber jedoch auf die für § 243 Abs. 1 Nr. 2 StGB entwickelten Kriterien.[62] Danach muss die Schutzvorrichtung objektiv dazu geeignet und subjektiv dazu bestimmt sein, den ungehinderten Zugriff auf eine Sache auszuschließen, um eine drohende Wegnahme zu verhindern oder wenigstens zu erschweren.[63]

Übertragen auf § 202a Abs.1 StGB bedeutet dies, dass auch hier die Zugangssicherung sowohl nach ihrer Beschaffenheit als auch nach ihrem Zweck dem ungehinderten Zugriff auf die geschützten Daten als ein tatsächliches Hindernis im Weg stehen muss.[64]

Die Möglichkeiten Daten zu schützen unterscheiden sich je nachdem, ob es sich um den Schutz gespeicherter Daten oder um

[59] T/F, § 202a, Rn.7a.
[60] Möhrenschlager, wistra 1986, 126 (140); Tiedemann, JZ 1986, 865 (870f.).
[61] Jähnke, in: LK, § 202a, Rn.14.
[62] BT-Drs. 10/5058, S.29.
[63] Lackner, in: Lackner/Kühl, § 243, Rn.16; BGH, NJW 1974, 567.
[64] Schmitz, JA 1995, 478 (482).

Daten im Übermittlungsstadium handelt. Folglich ist auch hinsichtlich der Art und des Umfangs der jeweiligen Schutzvorrichtungen zu differenzieren.

(a) Bei gespeicherten Daten

Die auf einem System gespeicherten Daten können durch mehrere Maßnahmen gegen einen unberechtigten Zugriff geschützt werden.

(aa) Physische Hindernisse

Als Zugangssperre im Sinne des § 202a StGB kann bereits eine entsprechende räumliche Aufteilung ausreichen, zum Beispiel wenn jene Räume, in denen sich relevante Datenträger befinden, abgeschlossen werden.[65] Ebenso können Sperrvorrichtungen an der Hardware selbst ein hinreichendes mechanisches Hindernis darstellen.[66] Erforderlich ist jedoch immer, dass die Schutzmaßnahme gerade den Zugang zu den Daten verhindern soll und nicht vorrangig anderen Zwecken, wie beispielsweise der Diebstahlsicherung oder dem Brandschutz, dient.[67]

Eine auf betriebsorganisatorischer Ebene bekannte Datensicherungsmaßnahme ist ein so genannter „closed shop“.[68] Er bezeichnet einen räumlich abgegrenzten Bereich, zu dem nur eine bestimmte Zahl von Nutzern ein ausdrückliches Zugangsrecht hat. Die rein organisatorische Trennung oder das Aussprechen von Zugangsverboten sind als Zugangssperren jedoch noch nicht ausreichend. Menschliches Versagen wird gerade als die Schwachstelle angesehen, der das Erfordernis der Zugangssicherung gilt.[69] Erforderlich sind daher weitere Kontrollmechanismen. Bei den „closed shops“ wird der Zutritt durch die Verwendung von Ausweisen, Magnetkarten, Passwörtern oder neuerdings durch den Einsatz biometrischer Erkennungsverfahren kontrolliert.[70] Personen,

---

[65] Jähnke, in: LK, § 202a, Rn.16.
[66] Kühl, in: Lackner/Kühl, § 202a, Rn.4; Jähnke, in: LK § 202a, Rn.16.
[67] Schmitz, JA 1995, 478 (482); Hilgendorf, JuS 1996, 702 (702).
[68] Leicht, iur 1987, 45 (48); Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.52.
[69] Jähnke, in LK, § 202a, Rn.14.
[70] Lenckner, in: S/S, § 202a, Rn.8.

für die die Daten nicht bestimmt sind, werden so vom Zugang ausgeschlossen.

Die genannten physischen Schutzmaßnahmen können zwar eine besondere Zugangssicherung darstellen, einem Hacker werden diese Sicherungen aber nur selten im Weg stehen. Bei den klassischen Hackerangriffen verschafft sich der Angreifer keinen körperlichen Zugriff auf die Datenverarbeitungsanlagen. Seine Angriffe werden online über ein Netzwerk, insbesondere über das Internet durchgeführt.

(bb) Softwaresicherungen

Gegen diese Art von Angriffen bieten zumeist nur durch Software gestützte Sicherungsmaßnahmen adäquaten Schutz.

Zunehmend kommen hierfür die schon beschriebenen Firewalls zum Einsatz.[71] Sie kontrollieren fortlaufend den ein- und ausgehenden Datenverkehr auf einem einzelnen Computer oder in einem lokalen Netzwerk. Durch diese Kontrolle wird das Computersystem vor dem Eindringen Unbefugter geschützt. Das Sicherheitsniveau kann je nach Konfiguration der Firewall stark variieren. Regelmäßig erschwert eine Firewall aber zumindest den Zugang zu einem System und ist daher als besondere Zugangssicherung anzusehen.

Zusammenfassend lässt sich feststellen, dass an die Sicherheit der Zugangssperre keine besonderen Anforderungen zu stellen sind. Erforderlich ist lediglich, dass die Zugangssperre für jeden Angreifer ein objektives Hindernis darstellt.[72] Nicht ausreichend ist daher, dass nur ein Laie mangels bestimmter Kenntnisse nicht in das System eindringen kann, für den geschulten Anwender der Zutritt aber kein Problem ist.[73] So genügt es zum Beispiel nicht, wenn für den Zugang gewisse Befehle in einer Programmiersprache eingegeben werden müssen. Für den Laien, der diese Befehle nicht kennt, mag dies zwar eine wirksame Zugangssicherung sein, für den versierten Anwender stellt eine solche Maßnahme jedoch überhaupt kein Hindernis dar.

---

[71] siehe hierzu oben: S.15.
[72] Jähnke, in: LK, § 202a, Rn.15; Leicht, iur 1987, 45 (47).
[73] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.53.

Bei der Sicherung kommt es darauf an, dass die Vorrichtung jeden Täter zu einer Zugangsart zwingt, die der Verfügungsberechtigte erkennbar verhindern wollte.[74]

(cc) Die Passwortsperre

Die bekannteste und gebräuchlichste Art der Zugangssicherung ist die Verwendung von Passwörtern. Sie erlauben es, sich anmeldende Benutzer auf ihre Zugangsberechtigung zu überprüfen und Nicht-berechtigte auszuschließen.

Umstritten ist, ob an die Sicherheit von Passwörtern gewisse Mindestanforderungen zu stellen sind. Oft sind Passwörter leicht zu erraten, so dass ein Angreifer schon nach wenigen Versuchen Zugang zu einem System erhält und das Eindringen somit kaum Schwierigkeiten bereitet.[75] Teilweise wird daher argumentiert, dass eine besondere Zugriffssicherung erst dann gegeben ist, wenn durch die Komplexität der verwendeten Passwörter ein bestimmter Sicherungsgrad gewährleistet ist.[76]

Begründet wird dies damit, dass nur eine sichere Zugangssperre ein beachtliches Hindernis für Hacker darstellen kann. Durch die Überwindung dieses Hindernisses bringt der Angreifer seine kriminelle Energie zum Ausdruck, die er aufwenden muss, um in das fremde System einzudringen. Solche Vorrichtungen, die problemlos durchbrochen werden können und die bereits jeder interessierte Laie überwinden kann, sind nach dieser Ansicht keine hinreichende Sicherungsmaßnahme.[77]

Die Differenzierung zwischen leicht und schwer überwindbaren Zugangssperren führt jedoch zu einem kaum lösbaren Abgrenzungs-problem. Da grundsätzlich jede Passwortsperre mit dem ent-sprechenden Zeitaufwand geknackt werden kann, lassen sich für eine Grenzziehung zwischen sicheren und unsicheren Kennwörtern kaum sinnvolle Kriterien entwickeln.[78]

---

[74] T/F, § 202a, Rn.7a.
[75] siehe oben: S.13.
[76] Gravenreuth, NStZ 1989, 201 (202).
[77] Diese Auffassung vertritt Jähnke, in: LK, § 202a, Rn.5.
[78] Mühle, Hacker und Computerviren, S.68.

Gleiches gilt für andere technische Schutzvorrichtungen. Die von einem Laienanwender schlecht konfigurierte Firewall bietet keinen wirksamen Schutz vor Angreifern. Wird sie indes von einem Fachmann eingerichtet, kann ein Eindringen in das System fast unmöglich sein.

Legt man den Sicherheitsgrad einer Zugangssperre als Maßstab zugrunde, würde dies außerdem gerade jene benachteiligen, die auf den rechtlichen Schutz besonders angewiesen sind, weil sie sich mangels technischer Kenntnisse selbst nicht ausreichend schützen können. Von einem einfachen Anwender kann eine ausgereifte Sicherung nicht verlangt werden.[79] Folglich kann es auch nicht darauf ankommen, welchen Schutz eine Sperrvorrichtung tatsächlich bietet. Entscheidend ist, dass der Anwender durch die Zugangssperre sein Geheimhaltungsinteresse an den Daten dokumentiert.[80] Es genügt deshalb, dass irgendwie wirksame Vorkehrungen speziell zu dem Zweck getroffen sind, den Zugang Unbefugter zu verhindern oder zu erschweren.[81] Bereits diese Zweckbestimmung führt dazu, dass der Angreifer Kenntnis von dem Geheimhaltungsinteresse des Verfügungsberechtigten erhält. Versucht er dennoch in das System einzudringen, missachtet er dieses Geheimhaltungsinteresse und manifestiert durch die Überwindung des Hindernisses seine strafwürdige kriminelle Energie.[82] Welcher Aufwand für das Eindringen in das System erforderlich ist, spielt für die Verwirklichung des Tatbestandes keine Rolle.

Als besondere Zugangssicherung für gespeicherte Daten ist somit jedes faktische Hindernis, also auch ein einfaches Passwort ausreichend. An die Sicherheit der Zugangssperre sind keine erhöhten Anforderungen zu stellen.

---

[79] Hilgendorf, JuS 1996, 702.
[80] BT-Drs. 1058, S.29; Kühl, in: Lackner/Kühl, § 202a, Rn4; T/F, § 202a, Rn.7a; Lenckner, in: S/S, § 202a, Rn.7; Jähnke, in: LK, § 202a, Rn.5.
[81] Kühl, in: Lackner/Kühl, § 202a, Rn.4; Schmitz, JA 1995, 478 (482).
[82] Leicht, iur 1987, 45.

(dd) Das Passwort als geschütztes Datum

Hinsichtlich der Passwortsperren stellt sich ein weiteres Problem. Zwar werden die auf einem System gespeicherten Daten durch das Passwort gegen einen unberechtigten Zugriff besonders gesichert, die Passwörter selbst sind jedoch nicht mehr durch eine weitere Vorrichtung geschützt. Es ist daher fraglich, ob der Schutzbereich des § 202a StGB auch die besondere Sicherung selbst umfasst.

Das Passwort ist „Datum“ im Sinne des § 202a Abs. 2 StGB und naturgemäß für Außenstehende nicht bestimmt.[83] Um von einem Passwort Kenntnis zu erlangen, muss jedoch in der Regel keine besondere Zugangssicherung überwunden werden, denn das Passwort selbst ist diese Sicherung. Greift ein Hacker ein passwortgeschütztes System an, erfolgt dies normalerweise durch Ausprobieren einer Vielzahl möglicher Kennwörter.[84] Von dem richtigen Passwort erlangt der Angreifer Kenntnis, wenn das System die korrekte Eingabe bestätigt. Der Angreifer hat also schon vor dem Überwinden der Zugangssperre das richtige Kennwort eingegeben. Die Zugangssperre enthüllt durch die Bestätigung zwar das Passwort, dennoch ist das Kennwort selbst durch die Zugangssperre nicht geschützt.

Geschützt werden die Kennwörter lediglich durch ihre Geheimhaltung.[85] Teilweise wird vertreten, dass die Geheimhaltung, der ein Passwort üblicherweise unterliegt, bereits als eine Sicherung im Sinne des § 202a Abs. 1 StGB betrachtet werden kann.[86] Begründet wird dies damit, dass die Geheimhaltung - ebenso wie eine softwaretechnische Sicherung - ein wirksames Mittel gegen einen unberechtigten Zugang darstellt. Anders als ein Verbot habe die Geheimhaltung durchaus objektive Wirkung.[87] Diese Ansicht berücksichtigt jedoch nicht, dass es gerade das Geheimhaltungsinteresse an den Daten ist, das durch die Sicherung geschützt

[83] Hilgendorf, JuS 1997, 323 (324).
[84] Zu den hierbei verwendeten Methoden siehe oben: S.13.
[85] Dies gilt für einen Großteil der Kennwörter. Es ist aber auch möglich, Kennwörter durch Verschlüsselungen zu schützen.
[86] Hilgendorf, JuS 1997, 323 (324).
[87] Hilgendorf, JuS 1997, 323 (324).

werden soll.[88] Folglich kann die Geheimhaltung nicht selbst Sicherung sein, sondern umgekehrt ist die Sicherung dazu bestimmt, das Geheimhaltungsinteresse gegenüber dem Täter zu dokumentieren.

Anders zu beurteilen ist der Fall, wenn die Eingabe des Passwortes unter weitere Bedingungen gestellt ist. Um das Ausprobieren aller in Frage kommenden Passwörter zu verhindern, werden mittlerweile häufig die Zahl der Versuche oder die zulässige Zeit für die Eingabe des richtigen Kennwortes begrenzt. In diesem Fall ist der Angreifer darauf angewiesen, diese Begrenzung zu überwinden.[89] Hacker bedienen sich dafür so genannter Trojanischer Pferde, die Passwörter auf fremden Systemen auskundschaften und an den Angreifer übermitteln. Diese Form des Hacking betrifft jedoch einen Sonderfall, der unter einem eigenen Prüfungspunkt zu behandeln sein wird.[90]

An dieser Stelle bleibt vorerst festzustellen, dass Passwörter selbst nicht durch eine besondere Zugangssicherung geschützt sind und daher vom Schutzbereich des § 202a Abs. 1 StGB nicht umfasst werden.

(b) Bei übermittelten Daten

Bei der Übermittlung elektronischer Informationen bewegen sich die Daten außerhalb des Einflussbereichs des Verfügungsberechtigten. Werden Daten über das Internet übertragen, durchqueren sie den Herrschaftsbereich vieler anderer Nutzer, die potentiell dazu in der Lage sind, die Daten auszulesen. Je nach Ziel der Übertragungsleitung werden die Daten auf einer bestimmten Zahl fremder Systeme zwischengespeichert. Welche Systeme dies sein werden, ist im Vorfeld nicht oder nur sehr begrenzt prognostizierbar. In der Vielzahl der möglichen Übertragungswege liegt gerade eine Stärke des Internets, das durch seine dezentrale Struktur weniger störungs-

[88] Möhrenschlager, wistra 1986, 126 (140); Tiedemann, JZ 1986, 865 (870f.).
[89] vgl. Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.48.
[90] siehe unter C., S.54.

anfällig ist. Eine sichere Übertragung wird jedoch erschwert. Das einzige wirksame Verfahren zum Schutz von Daten während der Übermittlungsphase im Internet ist die Verschlüsselung.[91] Durch sie werden die Daten in ein unlesbares Format umgewandelt und können nur von demjenigen entziffert werden, der den passenden Schlüssel zur Dechiffrierung besitzt. Möglichen Angreifern auf Datenangebote wird dadurch die Kenntnisnahme des Inhalts der Informationen verwehrt. Allerdings wird nicht der Zugriff auf die Daten verhindert. Nach dem Wortlaut des § 202a StGB soll sich die Sicherung aber gerade gegen den Zugang und nicht gegen die Kenntnisnahme richten. Unter diesem Gesichtspunkt müssten Verschlüsselungsverfahren als besondere Zugangssicherung ausscheiden.

Zu berücksichtigen ist aber, dass die Kryptographie die einzige Möglichkeit ist, Daten während ihrer Übertragung zu schützen. Würde man sie als rechtlich unzureichend ablehnen, wäre die Regelung des § 202a StGB in Bezug auf die übermittelten Daten überflüssig.[92] Da der Schutzbereich nach dem Gesetzeswortlaut aber übermittelte Daten umfassen soll, muss nach dem Sinn und Zweck der Vorschrift die Verschlüsselung als besondere Zugangssicherung anerkannt werden.[93] Der Wortlaut lässt eine Anerkennung von Verschlüsselungsverfahren als Zugangssperren auch zu.[94] Denn durch die Verschlüsselung wird der Zugang zu den Originaldaten verhindert. Die Verschlüsselung wird daher auch als eine „den einzelnen Daten anhaftende Zugangssicherung“ angesehen.[95] Als einziges wirksames Mittel zum Schutz der Daten während ihrer Übertragung muss die Verschlüsselung jedenfalls als Zugangssicherung im Sinne des § 202a Abs.1 StGB gelten.

---

[91] Leicht, iur 1987, 45 (51).
[92] Mühle, Hacker und Computerviren, S.70.
[93] Lenckner, in: S/S, § 202a, Rn.8; Ernst, CR 2003, 898 (899).
[94] Jähnke, in; LK, § 202a, Rn16; Lenckner, in: S/S, § 202a, Rn.8.
[95] Lenckner, in: S/S, § 202a, Rn.8.

(c) Sonderfall: „Portscanning“

Die Prüfung der „besonderen Zugriffssicherung“ kann in einem weiteren Fall zu Problemen führen. Ein typischer Vorgang beim Hacking ist das so genannte „Portscanning“.[96] Hierbei untersucht der Angreifer ein fremdes System, indem er die Ports des Zielrechners abtastet. Ports sind die für eine Kommunikation mit anderen Geräten erforderlichen Ein- und Ausgänge eines Computers, über die das System Daten sendet und empfängt. Jeder mit dem Internet verbundene Computer besitzt eine Vielzahl solcher Ports. Die einzelnen Ports werden jeweils für bestimmte Netzwerkdienste benutzt.[97] Einige dieser Dienste haben Schwachstellen und können von einem Hacker für einen Angriff genutzt werden. Die Untersuchung der Ports durch einen Scanvorgang ist für Angreifer daher besonders interessant und häufig der erste Schritt bei der Durchführung eines Angriffs.

Die Besonderheit des Portscannings besteht darin, dass der Täter Daten über das System auskundschaftet, ohne aber in das System einzudringen. Die Informationen über die Ports, die sich der Hacker ansieht, befinden sich außerhalb und der Zugriff ist nicht durch eine besondere Sicherung gehindert. Die Einrichtung einer speziellen Schutzvorrichtung ist an dieser Stelle technisch auch gar nicht möglich. Als Maßnahme gegen Portscans kommt allenfalls eine Überwachung der Anlage und eine Protokollierung der empfangenen Anfragen in Betracht.[98]

Fraglich ist, ob dies schon ausreicht, um die Informationen über Ports in den Schutzbereich des § 202a StGB einzubeziehen. Möglicherweise sind die Daten bereits aus der „Natur der Sache“ geschützt, indem sie nicht ohne erheblichen Aufwand eingesehen werden können und es einer erhöhten kriminellen Energie bedarf, um das Sicherheitssystem in dieser Weise auszuspionieren.[99]

Richtigerweise kann es aber nicht darauf ankommen, ob Daten auch ohne eine besondere Sicherung schwer erreichbar sind. Denn wie

---

[96] siehe oben: S.12.
[97] siehe oben: Fußnoten 25-27.
[98] Rinker, MMR 2002, 663 (665).
[99] Rinker, MMR 2002, 663 (665).

bereits dargestellt wurde, ist Aufgabe der Zugangssperre nicht nur der objektive Schutz vor einem unberechtigten Zugang, sondern gleichzeitig eine Symbolwirkung, die dem Eindringling die Grenze zum geheimen Bereich des Verfügungsberechtigten aufzeigt.[100] Auch wenn der Angreifer in der Regel davon ausgehen wird, dass sein Zugriff auf die Port-Daten gegen den Willen des Berechtigten erfolgt, bedarf es dennoch einer speziellen Zugangssicherung, die dieses Interesse dokumentiert.

Das Protokollieren möglicher Zugriffe stellt keine Sicherung in diesem Sinne dar, sondern dient lediglich der Erkennung von Angriffen und der Beweissicherung.[101] Mangels einer besonderen Zugriffssicherung ist das „Portscanning“ somit kein tatbestandsmäßiges Verhalten im Sinne des § 202a Abs. 1 StGB.

(2) Fazit

Gegen unberechtigten Zugang besonders gesichert sind Daten, wenn Sicherungsvorkehrungen speziell zu dem Zweck getroffen worden sind, den Zugang Unbefugter zu verhindern oder zu erschweren. Hierfür kommen sowohl physische als auch softwaretechnische Sperren in Frage. Voraussetzung ist aber immer, dass sie gerade dem Schutz der Daten dienen. Der Schutz überwiegend anderer Rechtsgüter ist nicht ausreichend. Die Sicherungsmaßnahme muss wirksam, jedoch nicht absolut sein. Entscheidend kommt es darauf an, dass der Dateninhaber durch die Einrichtung der Sperre sein Geheimhaltungsinteresse an den Daten dokumentiert. Bei übermittelten Daten ist bereits die Verschlüsselung der Daten als Zugangssperre anzusehen. Zwar verhindert sie nicht den Zugriff auf die Daten, sie ist aber das einzige Mittel, um die Kenntnisnahme des Inhalts der Daten wirksam zu verhindern. Da Daten im Übermittlungsstadium vom Schutzbereich der Norm umfasst sein sollen, kann die einzig wirksame Schutzvorrichtung nicht als rechtlich unzureichend abgelehnt werden.

---

[100] siehe oben: S.25.
[101] T/F, § 202a, Rn.7a.

dd) Der Begriff des „Verschaffens“

Die Tathandlung des § 202a Abs. 1 StGB besteht darin, dass der Täter die gegen unberechtigten Zugang geschützten Daten „sich oder einem anderen verschafft“.

Gemessen an dem natürlichen und juristischen Sprachgebrauch[102] kann ein „Sich-Verschaffen“ als das Herstellen einer eigenen Herrschaft des Täters über die Daten verstanden werden.[103] Verschafft der Täter die Daten „einem anderen“, so bewirkt er die Herrschaft eines Dritten über die Daten. Letztlich kommt es entscheidend darauf an, dass eine fremde Datenherrschaft begründet wird, der Datenberechtigte also nicht mehr ausschließlich darüber bestimmen kann, was mit seinen Daten geschieht.[104]

Die Erlangung der Herrschaft über die Daten kann auf unterschiedliche Weise erfolgen. In Anlehnung an § 96 StGB, wo es um das „Sich-Verschaffen“ eines Staatsgeheimnisses geht, ist zu differenzieren: Liegt das Geheimnis in verkörperter Form vor, so muss der Täter es in Gewahrsam bringen, ansonsten reicht die sichere Kenntnis aus.[105] Übertragen auf § 202a bedeutet das: Erlangt der Täter also ein mit Daten versehenes körperliches Substrat, hat er sich die Daten „verschafft“.[106] Dies ist etwa dann der Fall, wenn sich der Täter Daten auf einen eigenen Datenträger überspielt, einen fremden Datenträger wegnimmt oder die angezeigten Daten ausdruckt oder aufschreibt. In diesem Fall ist es unerheblich, ob der Täter auch gleichzeitig Kenntnis vom Inhalt der Daten erlangt.[107]

Auf eine Kenntnisnahme kommt es aber an, wenn die Daten nicht materialisiert in den Herrschaftsbereich des Täters gelangen, ihm also nicht in der Form eines körperlichen Substrats zur Verfügung stehen.[108] Ein Verschaffen liegt dann nur vor, wenn der Täter von

---

[102] Grammatikalische Auslegungsmethode, vgl. Wessels, AT Rn.57.
[103] Jähnke, in: LK, § 202a, Rn.6.
[104] Kühl, in: Lackner/Kühl, § 202a, Rn.5.
[105] T/F, § 96, Rn.2; Hilgendorf, JuS 1996, 702 (704).
[106] Jähnke, in LK, § 202a, Rn.6.
[107] Sieber, in: Hoeren/Sieber, Handbuch Multimediarecht, Teil 19, Rn.421.
[108] Lenckner, in: S/S, § 202a, Rn. 10; Kühl, in: Lackner/Kühl, § 202a, Rn.5; T/F, § 202a, Rn.9.

den Daten auch Kenntnis genommen hat. Sind die Daten aufgrund einer Verschlüsselung für den Täter nicht lesbar und fehlt dem Täter auch der passende Schlüssel zur Dechiffrierung, so scheidet eine Kenntnisnahme aus.[109] Der Täter muss zumindest die Möglichkeit der Kenntnisnahme haben. Ein Verschaffen liegt daher selbst dann nicht vor, wenn der Täter zwar im Besitz eines Datenträgers ist, die darauf enthaltenen Daten aber wegen einer Chiffrierung nicht lesen kann.[110]

Die Auslegung der Tathandlung nach ihrem Wortlaut und ihrem Bedeutungszusammenhang führt im Ergebnis dazu, dass beinahe jede Aneignung von elektronischen Daten, die gegen unberechtigten Zugang besonders gesichert sind, ein „Verschaffen“ darstellt und deshalb strafbar ist.[111]

(1) Der Wille des Gesetzgebers

Dieses Resultat widerspricht der Intention des Gesetzgebers. Wie sich aus der Begründung des 2. WiKG ergibt, sollte der Versuch des Ausspähens von Daten und auch das Hacking als „bloßes Eindringen in ein Computersystem“ straflos bleiben.[112] Ursprünglich sah der Entwurf des Gesetzes sogar gar keinen Tatbestand für das Ausspähen von Daten vor.[113] Erst durch das Drängen einiger Experten,[114] die mit dem technischen Fortschritt auch eine wachsende Bedrohung für elektronische Datenbestände erwarteten, wurde § 202a StGB vom Rechtsausschuss des Deutschen Bundestages eingefügt.[115]

---

[109] Lenckner/Winkelbauer, CR 1986, 483 (488); T/F, § 202a, Rn9;
[110] T/F, § 202a, Rn.9; Jähnke, in: LK, § 202a, Rn.6.
[111] Zielinski, Strafrechtlicher Schutz von Software, S.120.
[112] BT-Drs. 10/5058, S.28; Hilgendorf, JuS 1996, 702 (704); Achenbach, NJW 1986, 1835 (1837).
[113] Haft, NStZ, 1987, 6.
[114] In einer öffentlichen Anhörung des Rechtsausschusses des Bundestages am 6. Juni 1984 forderten insbesondere der Computerrechtsexperte Sieber und der Vertreter der Nixdorf Computer AG Oertel einen strafrechtlichen Schutz vor dem unbefugten Zugriff auf fremde Datenbanken und Rechnersysteme (vgl. Sten. Protokoll Nr.26, S.177; Mühle, Hacker und Computerviren, S.57)
[115] Tiedemann, JZ 1986, 865 (870).

Der Gesetzgeber befürchtete jedoch eine Überkriminalisierung.[116] Zum Zeitpunkt der Entstehung des Gesetzes Anfang der achtziger Jahre war das Hacking eine Randerscheinung, die das Sicherheitsgefühl der Bevölkerung kaum beeinträchtigte. Die wenigen Fälle, in denen sich Hacker Zugang zu fremden Systemen verschafften, waren nicht geprägt von kriminellen Machenschaften. Durch ihre Angriffe wollten die Eindringlinge meist nur die Systemsicherheit prüfen und auf eventuelle Mängel aufmerksam machen. Der Gesetzgeber wollte nicht solche Verhaltensweisen unter Strafe stellen, die durch das Aufzeigen von Sicherheitsproblemen sogar zum technischen Fortschritt beitragen können.[117]

Strafrechtlich relevant sollten nur diejenigen Angriffe sein, bei denen die Eindringlinge kriminelle Zwecke verfolgten. Nach der vom Gesetzgeber vorgenommenen Abgrenzung sei dies immer dann der Fall, wenn der Angreifer „sich nicht mit dem unbefugten Zugang begnügt, sondern darüber hinaus Daten abruft."[118] Für einen Hacker, der sich nur für die Technik und Sicherheit des angegriffenen Systems interessiert, sei der Abruf von Daten anders als für einen Datenspion uninteressant. Vielmehr wird er, ohne auf die im fremden System gespeicherten Daten zuzugreifen, das System unmittelbar nach einem erfolgreichen Eindringen wieder verlassen.

Die sich aus der Entstehungsgeschichte ergebende Abgrenzung bereitet praktisch jedoch große Schwierigkeiten. Technisch ist die vom Gesetzgeber getroffene Unterscheidung zwischen dem „Eindringen" in ein System und dem „Abruf von Daten" nicht durchzuhalten.[119] Schon mit dem Eindringen ruft der Hacker zwangsläufig Daten des angegriffenen Computers auf seinen Bildschirm.[120] Anders kann er nicht kontrollieren, ob sein Eindringen in das fremde System gelungen ist.[121] Folglich kann sich ein Hacker auch nicht - wie es der Gesetzgeber angenommen hat - darauf beschränken, in ein System nur einzudringen. Das Hacking besteht

---

[116] BT-Drs. 10/5058, S.28.
[117] Mühle, Hacker und Computerviren, S.75.
[118] BT-Drs. 10/5058, S.29.
[119] Hauptmann, JurPC 1989, 215.
[120] Lenckner/Winkelbauer, CR 1986, 483 (488).
[121] Hauptmann, JurPC 1989, 215 (215).

immer aus beidem: dem Eindringen in ein System und dem Abrufen von Daten.

(2) Teleologische Reduktion

Will man entsprechend dem Willen des Gesetzgebers das bloße Eindringen in ein Computersystem straflos lassen, so ist dies nur durch eine teleologische Reduktion, also die Einschränkung des Tatbestandes nach dem Sinn und Zweck der Vorschrift, möglich.[122] Für die Durchführung dieser Begrenzung werden unterschiedliche Kriterien vorgeschlagen.

(a) Zugriff auf Systemdaten

Eine Möglichkeit besteht in der Abgrenzung danach, ob der Hacker lediglich auf Systemdaten zugreift oder ob er die auf dem System gespeicherten Daten ausliest.[123] Als straflos wird dabei das Betrachten von Daten angesehen, soweit sie mit dem Zugriff auf das System verbunden sind. Diese Systemdaten sollen vom Schutzbereich der Vorschrift nicht umfasst sein. Erst der Zugriff auf Daten, die auf dem System gespeichert sind, begründet nach dieser Ansicht eine Strafbarkeit.

Angesichts der Intention des Gesetzgebers, das Eindringen in ein fremdes Computersystem allein noch nicht unter Strafe zu stellen, erscheint diese Unterscheidung sinnvoll. Problematisch ist aber, dass eine klare Abgrenzung zwischen Systemdaten und anderen Daten schwer durchzuführen ist. Auch die Systemdaten sind wie alle anderen Daten auf dem fremden Computer gespeichert.[124] Aus technischer Sicht besteht daher kaum ein Unterschied.

Selbst wenn man die Unterscheidung so versteht, dass Systemdaten solche sind, die für das Funktionieren des Systems verantwortlich sind und nur die vom Benutzer erstellten Daten in den Schutzbereich fallen, ist die Abgrenzung nicht überzeugend. Ein Hacker bliebe nämlich auch dann straflos, wenn er nach dem Eindringen weitere

---

[122] Lenckner, in: S/S, § 202a, Rn.10; Mühle, Hacker und Computerviren, S.76.
[123] T/F, § 202a, Rn.9.
[124] Hilgendorf, JuS 1986, 702 (704).

Systemdaten suchen würde, beispielsweise um den Aufbau des Systems oder eine Netzwerkstruktur zu erkunden. In diesem Fall würde der Angreifer gerade nicht nach dem erfolgreichen Eindringen aufgeben, sondern tiefer in das System eindringen.

(b) Abspeichern

Nach anderer Ansicht ist darauf abzustellen, ob der Täter Daten des fremden Systems dauerhaft abspeichert.[125] Durch diesen zusätzlichen Akt bringt der Täter zum Ausdruck, dass er sich nicht mit dem bloßen Eindringen zufrieden gibt, sondern es ihm gerade auf den Zugriff auf bestimmte Daten ankommt. Würde der Hacker die gefundenen Daten nicht nutzen wollen, wäre es für ihn auch sinnlos, durch deren Aufbewahrung Speicherplatz zu belegen.[126] Erst durch das Abspeichern soll auch das Verfügungsrecht am Datenbestand verletzt werden. Die vorausgehende bloße Gefährdung des Integritätsinteresses an den Daten ist nach dieser Ansicht deshalb noch nicht strafwürdig.[127]

Richtig ist an dem Kriterium des Abspeicherns, dass es ein zuverlässiger Hinweis auf das Interesse des Täters an fremden Datenbeständen ist. Neben dem Abspeichern sind jedoch zahlreiche weitere Möglichkeiten denkbar, wie sich der Täter fremde Daten zueigen machen kann. Das Verfügungsrecht am Datenbestand kann unter Umständen auch durch das Ansehen der Daten auf dem Bildschirm verletzt sein, wenn die Daten unmittelbar für kriminelle Zwecke verwertet werden.[128] Ebenso kann der Täter sich Notizen anfertigen oder die Datenbestände ausdrucken.[129] Die vorgeschlagene Unterscheidung lässt folglich eine Vielzahl von Fällen unberücksichtigt, die in gleicher Weise geeignet sind, die Datenherrschaft des Berechtigten zu beeinträchtigen. Der Vorgang des Abspeicherns ist daher als Abgrenzungskriterium ungeeignet.

---

[125] so Hauptmann, JurPC 1989, 215 (217).
[126] Hauptmann, JurPC 1989, 215 (218).
[127] Frommel, JuS 1987, 667 (668).
[128] Zielinski, Strafrechtlicher Schutz von Software, S.120.
[129] Jähnke, in: LK, § 202a, Rn.6.

(c) Reproduzierbarkeit

Überzeugender ist ein Ansatz, der es für die Abgrenzung darauf ankommen lässt, ob dem Täter die Daten reproduzierbar zur Verfügung stehen.[130] Abhängig von Inhalt und Umfang der Daten kann es hierfür erforderlich sein, die Daten auf einem Datenträger abzuspeichern. Große Datenmengen, die lediglich auf dem Bildschirm angezeigt werden oder nur im Arbeitsspeicher abgelegt sind, können ohne eine dauerhafte Speicherung nicht reproduziert werden. Nach Abschalten des Gerätes stehen diese Daten dem Angreifer nicht mehr zur Verfügung. Bei kleineren Datenmengen kann es allerdings ausreichen, dass der Täter sich die in den Daten enthaltenen Informationen aufschreibt oder in sein Gedächtnis einprägt.[131] Entscheidend ist, dass der Eindringling dazu imstande ist, den wesentlichen Informationsgehalt der Daten später wiederzugeben.

Das alleinige Abstellen auf die Reproduzierbarkeit hätte streng genommen jedoch zur Konsequenz, dass die sofortige Verwertung der Daten straflos bliebe. Berücksichtigt man diese Besonderheit, so ist die Abgrenzung erst dann lückenlos, wenn neben der Reproduzierbarkeit auch die sofortige Verwertung der Daten zu einem tatbestandsmäßigen Verhalten führt.

Die teleologische Reduktion der Tathandlung nach § 202a Abs. 1 StGB kann daher folgendermaßen lauten: Ein „Verschaffen“ liegt immer dann vor, wenn der Täter die Daten entweder unmittelbar nutzt oder sie (beispielsweise durch ihre dauerhafte Speicherung) reproduzierbar zur Verfügung hat.[132]

(3) Kritische Würdigung

Durch die sehr restriktive Auslegung des Tatbestandes wird dem ursprünglichen Willen des Gesetzgebers Rechnung getragen. Es stellt sich aber die Frage, ob eine solch zurückhaltende Interpretation

[130] Hilgendorf, JuS 1996, 702 (705).
[131] Hilgendorf, JuS 1996, 702 (705).
[132] Vgl. Zielinski, Strafrechtlicher Schutz von Software, S.120.

auch knapp zwanzig Jahre nach der Einführung des Gesetzes noch zeitgemäß ist.

Zweifel ergeben sich aus mehreren Gründen. Zum einen hat sich seit dem Inkrafttreten des 2. WiKG die Computerlandschaft grundlegend verändert. Als der Gesetzgeber die neuen Straftatbestände formulierte, waren die Rahmenbedingungen mit den äußeren Umständen heute nicht vergleichbar. Nur wenige Bürger hatten Zugang zu einem Computer. Das Internet war noch weit davon entfernt, ein Massenmedium zu werden und das „Hacking“ war eine Randerscheinung, für die sich nur wenige Experten interessierten.[133]

In der Zwischenzeit aber sind Computer und das Internet in alle Bereiche des Lebens vorgedrungen und beherrschen unseren Alltag. Die Gesellschaft ist zu einem großen Teil vom Funktionieren ihrer Datenverarbeitungsanlagen abhängig. Ein Ausfall von Datenverarbeitungsanlagen kann in Extremsituationen lebensbedrohlich sein, von wirtschaftlichen Folgen ganz abgesehen. Folglich hat auch die Sensibilität für Angriffe auf Computersysteme stark zugenommen.[134]

Gleichzeitig werden Angriffe auf fremde Datenangebote immer häufiger.[135] Speziell das Hacking ist nicht mehr nur ein Zeitvertreib, der wenige „Computerfreaks“ beschäftigt. Einfache Angriffe auf fremde Systeme sind mittels der entsprechenden Software heute für jeden interessierten Anwender möglich.[136] Dementsprechend haben sich auch die Motive für das Hacking verändert. Das Hackerbild, das der Gesetzgeber bei der Regelung des § 202a StGB noch vor Augen hatte, ist mittlerweile die Ausnahme. Ein typischer Hackerangriff ist heute nicht mehr nach dem Überwinden der Zugangssperre beendet. Vielmehr wird der Eindringling das System nach weiteren Sicherheitslücken auskundschaften, Hintertüren einrichten, über die er später in das System zurückkehren kann und schließlich andere

---

[133] siehe oben: S.4.

[134] Man denke hier auch an die Angst vor terroristischen Angriffen auf Rechnersysteme, welche als eine potentielle Gefahr für eine ganze Volkswirtschaft gesehen werden.

[135] siehe oben: S.3.

[136] siehe oben: S.3.

Maschinen suchen, die dem System vertrauen, um seinen Angriff auf diese Geräte auszuweiten.

Ob dies nur aus technischer Neugierde geschieht oder ob der Angreifer auf dem fremden System gezielt nach Daten sucht, wird von Fall zu Fall unterschiedlich sein. Die Annahme aber, dass der rein technisch interessierte Angreifer nach Überwinden der Zugangssperre seinen Angriff sofort abbricht, ist keinesfalls mehr die Regel.[137]

Zugegebenermaßen ist das allein noch kein Argument für einen strengeren Maßstab bei der Auslegung der Tathandlung nach § 202a Abs.1 StGB. Denn das hier als typischer Hackerangriff skizzierte Verhalten ist auch nach der restriktiven Auslegung des Tatbestandes strafbar. Straflos soll nach dem Willen des Gesetzgebers nur das bloße Eindringen in einen Computer sein.[138]

Bereits dieses Eindringen kann jedoch ausreichen, um einen erheblichen Schaden zu verursachen. Typisch für das Internet ist, dass die Benutzer nicht persönlich miteinander in Kontakt treten. Die Sicherheit und Zuverlässigkeit der Systeme ist daher von besonderer Bedeutung. Gerade kommerzielle Anbieter sind darauf angewiesen, dass Kunden in die Sicherheit der Systeme vertrauen. Dringt ein Hacker in ein fremdes System ein, so ist genau dieses Vertrauen zerstört und kaum jemand wird noch bereit sein, seine Kreditkarteninformationen an den entsprechenden Server zu übermitteln. In den meisten Fällen gilt das selbst dann, wenn der Systembetreiber versichert, die Sicherheitslücke behoben zu haben.

Nun kann argumentiert werden, dass für Schwachstellen allein die Systembetreiber verantwortlich sind, der Staat aber nicht für die technische Sicherheit sorgen kann. Rechtlicher Schutz müsse erst dort beginnen, wo Schwachstellen so ausgenutzt werden, dass es zu der Verletzung von Rechtsgütern kommt.[139] Tatsache ist aber, dass auch das am besten geschützte System vor dem Eindringen

---

[137] Auf diese Annahme baut aber die juristische Argumentation in der Literatur auf; vgl.: Winkelbauer, CR 1985, 40 (44); Goldmann/Stenger, KR 1989, 464 (468); von Gravenreuth, NStZ 1989, 201; Möhrenschlager, wistra 1991, 236.

[138] BT-Drs. 10/5058, S.28.

[139] so Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.44.

Fremder nicht absolut sicher ist. Erfolgreiche Angriffe auf die Server von Microsoft oder der NASA beweisen das.[140] Daher kann auch schwer begründet werden, warum der Schutz solcher Systeme allein den Betreibern überlassen werden soll. Einen Diebstahl nicht zu bestrafen, weil die gestohlene Sache schlecht gesichert war, wäre ebenso absurd.

Hinzukommt, dass das bloße Eindringen in ein System schon erhebliche Schäden verursachen kann. Neben dem schon genannten immateriellen Schaden durch einen möglichen Vertrauensverlust drohen auch unmittelbare wirtschaftliche Schäden. Der Systembetreiber wird gezwungen, aufwendige und kostspielige Maßnahmen zu ergreifen, um die Sicherheit wiederherzustellen und Kundenvertrauen zurück zu gewinnen. Außerdem ist der zusätzliche Untersuchungsaufwand für jeden Einzelfall zu berücksichtigen, da stets ermittelt werden muss, ob das Eindringen erfolgreich war und welche Daten abgerufen wurden.[141]

Allein das Gefahrenpotential, das ein Eindringen in fremde Systeme in sich birgt, ist schon Grund genug, den unerlaubten Zugriff auf fremde Rechenanlagen von Beginn an zu verbieten.

Dies sieht man auch in anderen Ländern so. Ein Blick auf das englische Recht zeigt, dass dort schon das „Knacken der Tür“ als eine Art elektronischer Hausfriedensbruch bestraft wird.[142]

Der Vergleich mit dem Hausfriedensbruch wird auch hierzulande häufig herangezogen.[143] Das „Knacken“ des Systems wird dabei mit dem Öffnen einer Tür durch die Verwendung eines Dietrichs verglichen.[144] Der so geöffnete Raum wird jedoch weder betreten noch angesehen. Vielmehr wird die Tür unmittelbar nach ihrem Öffnen wieder zugezogen. Hierin könne kein Hausfriedensbruch gesehen werden, so die Argumentation. Denn der Täter sei nicht körperlich in den Raum eingedrungen. Die gleiche Situation sei auch beim

---

[140] vgl. Heise-Newsticker, Meldung v. 29.10.2000, unter: http://www.heise.de/newsticker/data/jk-29.10.00-001/.

[141] so auch die Argumentation der Law Commission in Groß-Britannien, siehe: Volesky, CR 1991, 553 (555).

[142] vgl. Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.43.

[143] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.43.

[144] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.43.

Hacking vorzufinden, wo der Hacker sich mit dem „Knacken der Tür“ zufrieden gibt und sich nicht nach weiteren Daten umsieht.[145]

Wie wenig überzeugend dieser Vergleich ist, zeigt ein einfaches anderes Beispiel. Danach kann das bloße Eindringen in ein Computersystem ebenso gut mit dem (körperlichen) Eindringen in ein Aktenzimmer verglichen werden. Der Täter öffnet aber nicht den Aktenschrank, um sich die darin enthaltenen Akten anzusehen. Vielmehr interessieren ihn nur die Sicherheitsvorrichtungen an der Tür und dem Schrank. Zweifellos erfüllt dieses Verhalten den Tatbestand eines Hausfriedensbruchs und müsste bestraft werden. Übertragen auf das Hacking ist unbestreitbar, dass der Täter in das System eingedrungen ist. Dies ist ja auch gerade sein Ziel. Er macht eben nicht vor der Tür Halt, wie es im ersten Beispiel angenommen wird. Dies ist allenfalls bei dem so genannten „Portscanning“[146] der Fall, wo der Angreifer die „Türen“ eines Systems von außen auf deren Sicherheit untersucht. Bildlich gesprochen rüttelt er nur an der Tür, um deren Stabilität zu testen.

Doch selbst wenn man das Ausgangsbeispiel bevorzugt, in dem der Täter bereits vor der Tür Halt macht, würde dies im Umkehrschluss bedeuten, dass ein Täter, der alle Haustüren öffnet, sei es nur aus Zeitvertreib oder um den Bewohnern die Einbruchsmöglichkeiten zu verdeutlichen, straflos bleiben soll.[147] Verständlicherweise würde die Mehrheit der Bevölkerung in diesem Fall strafrechtliche Konsequenzen fordern. Der Täter ist in eine Sphäre eingedrungen, die ihn nichts angeht. Das gilt auch, wenn er die Tür nach dem Öffnen gleich wieder zuzieht. Denn unabhängig davon, ist das Haus unsicher geworden und das Vertrauen der Bewohner in die Sicherheit zerstört.[148]

Für das Hacking mag dieses Urteil zum Zeitpunkt des Inkrafttretens des 2. WiKG noch anders ausgefallen sein. In den achtziger Jahren war das Bedürfnis nach zuverlässigen und sicheren Computersystemen für den Normalbürger noch kein Thema. In der Gegenwart

---

[145] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.43.
[146] siehe hierzu ausführlich oben: S.29.
[147] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S. 82.
[148] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S. 82.

ist aber die Sicherheit von Computern für die meisten Lebensbereiche elementar. Dieser Wandel hat zu einer völlig neuen Bedeutung des Schutzes von Computern geführt.

Zweck der Gesetzesauslegung ist es auch, auf solche Veränderungen zu reagieren und gegebenenfalls die Gesetze im Rahmen des Wortlautes an die veränderten Bedürfnisse und Anschauungen der Gegenwart anzupassen.[149] Der Tatbestand des §202a Abs.1 StGB lässt eine Strafbarkeit des bloßen Eindringens in fremde Computer ohne weiteres zu, da bereits diese Handlung unvermeidlich mit dem Abrufen von Daten („verschaffen“) verbunden ist.[150] Eine Strafbarkeit, die dort beginnt, wo ein Hacker unberechtigt in ein fremdes, geschütztes System eindringt, würde zudem eine klare Grenze zwischen strafbarem und straflosem Verhalten ziehen. Die restriktive Auslegung des Tatmerkmals „verschaffen“ hat diesbezüglich zu einer großen Grauzone geführt. Die von der Wissenschaft entwickelten Kriterien unterscheiden sich teilweise erheblich und lassen allesamt Lücken offen.

Eine Strafbarkeit des Eindringens in fremde Computer hätte ferner erhebliche Beweiserleichterungen zur Folge. Während die Feststellung eines Einbruchs in ein System oft keinen größeren Aufwand erfordert, kann die Untersuchung, ob der Eindringling in dem betroffenen System Daten angesehen oder kopiert hat, zu beträchtlichen Schwierigkeiten führen. Selbst wenn das Abrufen weiterer Daten nachgewiesen werden kann, hat der Täter die Möglichkeit, sich auf ein unvorsätzliches Verhalten zu berufen. Dies zu widerlegen dürfte ebenfalls in vielen Fällen schwierig sein.

Es sprechen also auch einige Argumente gegen die restriktive Auslegung des Tatbestandes. Aus strafrechtspolitischer Sicht ist allenfalls noch zu berücksichtigen, dass Aufgabe des Strafrechts nur die Sanktionierung besonders schwerwiegender Regelverstöße ist. Nicht alles was rechtswidrig ist, soll auch bestraft werden, sondern

[149] Wessels, Strafrecht AT, Rn.56.
[150] siehe oben: S.33.

nur solche Verhaltensweisen, die die grundlegenden Spielregeln des gesellschaftlichen Zusammenlebens in Frage stellen.[151]

Hinsichtlich des Hackings ist hierbei zu beachten, dass im Einzelfall stark unterschiedliche Interessen an einem Strafrechtsschutz bestehen können. Die Rechtsgüter einer Privatperson werden durch das bloße Eindringen eines Hackers noch nicht zwangsläufig verletzt. Als strafwürdiges Unrecht wird hier wohl erst der Abruf der persönlichen Daten empfunden. Insoweit bietet das Strafrecht ausreichenden Schutz. Anders liegt der Fall, wenn ein Hacker in ein Unternehmensnetzwerk eindringt oder sich beispielsweise Zugang zu der Datenverarbeitungsanlage eines Kraftwerkbetreibers oder den Computern der Flugsicherung verschafft.

Zumindest in letzterem Fall werden die Betroffenen eine Strafbarkeit für das bloße Eindringen verlangen.

(4) Fazit

Das Hacking in der Form des Eindringens in ein fremdes Computersystem wird in der Gesellschaft nicht mehr als ein Bagatelldelikt angesehen. Bereits das Eindringen in das System stellt in vielen Fällen eine abstrakte Gefahr für wichtige Rechtsgüter dar.[152] Ungeachtet der hier geäußerten Bedenken geht die überwiegende Meinung jedoch davon aus, dass das Hacking als bloßes Eindringen in einen Computer nicht strafbar sein soll. Die Tathandlung des „Verschaffens“ der Daten wird daher restriktiv ausgelegt. Für die Abgrenzung zwischen strafbarem und straflosem Verhalten gibt es unterschiedliche Lösungsvorschläge. Vorzugswürdig ist eine Auffassung, die für ein tatbestandsmäßiges „Verschaffen“ fordert, dass der Täter die Daten entweder reproduzieren kann oder sie unmittelbar nutzt.

[151] Zielinski, Strafrechtlicher Schutz von Software, S.115.
[152] so auch Schulze-Heiming, Strafrechtl. Schutz der Computerdaten, S. 82f.

b) Subjektiver Tatbestand

Für den subjektiven Tatbestand genügt bedingter Vorsatz.[153] Der Täter muss insbesondere nicht die Absicht haben, die Daten später verwerten zu wollen.[154] Es genügt, wenn er im Sinne der Bedeutungskenntnis weiß, dass es sich um Daten im Sinne des § 202a Abs. 2 StGB handelt, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind.[155] Nimmt der Täter irrtümlich an, dass die Daten für ihn bestimmt sind, so liegt ein vorsatzausschließender Tatbestandsirrtum vor.[156] Meint der Täter hingegen nur, dass er befugt sei, sich die Daten zu verschaffen, beispielsweise weil sie sich auf ihn beziehen, so handelt es sich gemäß §17 StGB um einen Verbotsirrtum.[157]

c) Rechtswidrigkeit

Als Rechtfertigungsgrund kommen bei § 202a StGB vor allem die Einwilligung des über die Daten Verfügungsberechtigten oder eine gesetzliche Erlaubnis (z.B. §94 StPO) in Betracht.[158] Das Merkmal „unbefugt“ im Wortlaut des §202a Abs.1 StGB ist als allgemeines Deliktsmerkmal der Rechtswidrigkeit anzusehen, weshalb der Tatbestand selbst dann erfüllt ist, wenn der Täter eine Befugnis hat, sich die Daten zu verschaffen.[159] Bei einer nachträglichen Zustimmung entfällt jedoch die Rechtswidrigkeit. Bringt der Verfügungs--berechtigte seine Einwilligung vor der Tathandlung zum Ausdruck, so kann bereits ein tatbestandsmäßiges Verhalten ausscheiden, wenn die Daten dadurch für den Täter bestimmt sind.[160] Rechtfertigend ist die Einwilligung nur, wenn der Erklärende auch verfügungsberechtigt ist. Dass er von den Daten lediglich betroffen ist, reicht hierfür nicht

[153] Lenckner, in: S/S, § 202a, Rn.12; T/F, § 202a, Rn.10; Lackner, in: Lackner/Kühl, § 202a, Rn.6.
[154] Granderath, DB 1986, Beil. 18, S.2.
[155] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S. 84.
[156] T/F, § 202a, Rn.10.
[157] Lenckner, in: S/S, § 202a, Rn.12.
[158] Lackner, in Lackner/Kühl, § 202a, Rn.7.
[159] Mühle, Hacker und Computer-Viren, S.79; Lenckner, in: S/S, § 202a, Rn.11.
[160] Hilgendorf, JuS 1996, 702 (705).

aus. Auch der Auskunftsanspruch nach § 19 BDSG verschafft dem Betroffenen insoweit keine Verfügungsbefugnis.[161]

d) Kein Versuch

Eine Versuchsstrafbarkeit sieht § 202a StGB nicht vor.

e) Absolutes Antragsdelikt

Gemäß § 205 Abs. 1 StGB wird das Ausspähen von Daten nur auf Antrag verfolgt. Das Antragserfordernis ist vom Gesetzgeber bewusst als Filter zur Vermeidung unnötiger Strafverfahren eingefügt worden.[162] Gerade in den Fällen, in denen Hacker ohne böswillige Absicht nur Sicherheitslücken aufdecken und diese dem Systembetreiber mitteilen, soll es vom Betroffenen abhängen, ob er das Verhalten des Eindringlings bestraft wissen will oder nicht. Konsequenz dieser Regelung kann jedoch auch sein, dass viele schwerwiegende Fälle nicht verfolgt werden, da Systembetreiber aus Angst vor einem Vertrauensverlust Einbrüche in ihre Rechenanlagen nicht bekannt machen wollen.

2) Die Datenveränderung nach § 303a Abs.1 StGB

Durch § 303a Abs.1 StGB wird das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit seiner Daten geschützt.[163] Dringt ein Hacker in ein fremdes System ein und ruft dort Daten ab, kann es zu einer Beeinträchtigung der Verwendbarkeit dieser Daten kommen.

a) Objektiver Tatbestand

Tatgegenstand sind Daten im Sinne des § 202a Abs. 2 StGB. Insoweit kann auf die Ausführungen oben verwiesen werden.[164] Die Daten, die ein Hacker auf einem angegriffenen System vorfindet,

---

[161] Hilgendorf, JuS 1996, 702 (705).
[162] BT-Drs. 10/5058; S.29.
[163] Kühl, in: Lackner/Kühl, § 303a, Rn.1; Stree, in: S/S, § 303a, Rn.1; Möhrenschlager, wistra 1986, 128 (141).
[164] siehe oben: S.16.

sind wie festgestellt Daten in diesem Sinne. Die Tathandlung besteht in dem Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern der Daten durch den Täter.

aa) Das Löschen der Daten

Gelöscht werden Daten, wenn sie vollständig und unwiederbringlich unkenntlich gemacht werden.[165] Hinsichtlich der Unwiederbringlichkeit der Daten ist zu unterscheiden: Gibt ein Hacker lediglich einen Löschbefehl ein, so wird normalerweise nur die ID (Identify Directory) der entsprechenden Datei gelöscht, was dazu führt, dass die Datei nicht mehr im Inhaltsverzeichnis des lokalen Speichers zu finden ist.[166] In diesem Fall spricht man von einem logischen Löschen der Daten. Physisch sind die Daten aber noch auf dem System vorhanden und können mit Hilfe geeigneter Werkzeuge rekonstruiert werden.[167] Endgültig verloren ist eine Datei erst, wenn sie auch physisch gelöscht ist, also der von ihr belegte Speicherplatz durch neue Daten überschrieben wurde.

Somit kann man davon ausgehen, dass bis zu diesem Zeitpunkt die Eingabe des bloßen Löschbefehls noch kein „Löschen“ im Sinne des § 303a Abs.1 StGB darstellt. Es ist allerdings fraglich, ob eine so strenge Unterscheidung überhaupt erforderlich ist. Durch die Nennung mehrerer Tathandlungsvarianten hat der Gesetzgeber ein Ineinandergreifen der Handlungsmodalitäten beabsichtigt, um einen möglichst umfassenden und lückenlosen Schutz vor Beeinträchtigungen der Daten zu gewährleisten.[168] Insofern ist es nicht einmal zwingend, dass die aufgezählten Tathandlungen eigenständige Bedeutung haben, sondern vielmehr jede vergleichbare Beeinträchtigung tatbestandsmäßig sein soll. Folgt man jedoch der strengen Unterscheidung der einzelnen Tathandlungsvarianten, wäre das Entfernen der Daten aus dem Inhaltsverzeichnis unter

---

[165] BT-Drs. 10/5058, S.34.
[166] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S. 173.
[167] v.Gravenreuth, NStZ 1989, 201 (206).
[168] Stree, in: S/S, § 303a, Rn.1; Gerhards, Computerkriminalität und Sachbeschädigung, S.66.

Umständen kein „Löschen“. In Betracht käme dann aber zumindest ein „Unterdrücken“ der Daten.[169]

bb) Das Unterdrücken der Daten

Das Unterdrücken von Daten bedeutet, dass dem Verfügungsberechtigten der Zugriff auf die Daten entzogen wird und die Daten dadurch nicht mehr von ihm genutzt werden können.[170] Fraglich ist dabei, ob der Entzug auf Dauer angelegt sein muss oder ob auch eine vorübergehende Beeinträchtigung für die Tatbestandsverwirklichung ausreicht. Praktisch relevant wird diese Frage bei der Beurteilung der Strafbarkeit eines Hackers, der durch seinen Aufenthalt in einem fremden System den Zugriff auf die dort gespeicherten Daten für andere Benutzer blockiert.[171] Je nach der Beschaffenheit eines Systems kann dies möglich sein, wenn ein gleichzeitiger Zugriff von mehreren Nutzern auf die Daten ausgeschlossenen ist. Die Benutzung einer Datenleitung durch einen Hacker kann somit zu einer vorübergehenden Unterdrückung von Daten führen.

Der zeitweilige Entzug der Verwendbarkeit von Daten kann als unzureichend angesehen werden, wenn man der Meinung ist, dass dies dem vom Gesetz nicht erfassten Fall der Gebrauchsanmaßung entspräche. Dagegen spricht aber, dass auch vorübergehende Beeinträchtigungen der Verwendbarkeit des Datenbestandes zu erheblichen Schäden führen können,[172] beispielsweise wenn Daten zu einem bestimmten Zeitpunkt benötigt werden aber nicht verfügbar sind. Gerade vor solchen Schäden soll § 303a Abs.1 StGB schützen.[173] Tatbestandsmäßig muss daher auch die zeitweilige Unterdrückung von Daten sein.

---

[169] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S. 175.
[170] Kühl, in: Lackner/Kühl, § 303a, Rn.3.
[171] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.58.
[172] Haß, in: Lehmann, Strafrechtlicher Schutz von Computerprogrammen, S. 299 (328); Samson, in: SK, § 303a, Rn.20.
[173] Kühl, in: Lackner/Kühl, § 303a, Rn.1; T/F, § 303a, Rn.2.

cc) Das Unbrauchbarmachen und Verändern von Daten

Ein Unbrauchbarmachen von Daten liegt vor, wenn die Daten in ihrer Gebrauchsfähigkeit so beeinträchtigt werden, dass sie ihren Zweck nicht mehr erfüllen können.[174] Dies wäre beispielsweise der Fall, wenn der Täter Daten nur teilweise löscht oder sie inhaltlich umgestaltet, dies aber bereits dazu führt, dass die Daten für ihren vorgesehenen Zweck nicht mehr zu gebrauchen sind.[175]

Zum Verändern der Daten gehört jede Form der inhaltlichen Umgestaltung.[176] Nicht erforderlich ist, dass die Daten auch in ihrer Gebrauchstauglichkeit beeinträchtigt werden.[177] Erfasst wird also der Fall, indem die Daten technisch einwandfrei zur Verfügung stehen, der Informationsgehalt aber durch einen Dritten verändert wurde.

Zusammenfassend bleibt festzustellen, dass die Angriffsformen des Hacking durchaus dazu geeignet sind, den Tatbestand des § 303a Abs.1 StGB zu verwirklichen. Zwar ist die Datenveränderung keine typische Folge des Eindringens in ein Computersystem, es ist jedoch auch nicht ungewöhnlich, dass durch einen Hacker der Datenbestand des betroffenen Systems beeinträchtigt wird. Vorstellbar ist zum einen, dass ein Hacker bewusst Daten manipuliert, beispielsweise um an ein Passwort zu gelangen oder um eine Passwortsperre zu umgehen.[178] Denkbar ist aber auch, dass mangelhafter Sachverstand des Eindringlings oder fehlende Aufmerksamkeit zu Veränderungen an den Daten führt, ohne dass der Angreifer dies beabsichtigt oder bemerkt.[179]

b) Subjektiver Tatbestand

Ist dem Angreifer die Beeinträchtigung der Daten nicht bewusst, so ergeben sich Probleme hinsichtlich des Vorsatzes. Bei Tatbegehung muss der Täter die Möglichkeit der Datenveränderung reflektiert

---

[174] BT-Drs. 10/5058, S.35; Hilgendorf, JuS 1997, 323 (325).
[175] Stree, in: S/S, § 303a, Rn.4.
[176] Kühl, in:Lackner/Kühl, § 303a, Rn.3.
[177] T/F, § 303a, Rn.8.
[178] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.57.
[179] Granderath, DB 1986, Beil. 18, 1 (2).

haben, andernfalls kommt nur ein insoweit strafloses fahrlässiges Verhalten in Betracht. Für eine Strafbarkeit ist mindestens bedingter Vorsatz erforderlich.[180] Dieser liegt unzweifelhaft vor, wenn der Angreifer bewusst Daten verändert. Bei einer nicht beabsichtigten Beeinträchtigung der Daten muss der Täter es ernstlich für möglich halten und sich damit abfinden, dass sein Verhalten zur Verwirklichung des gesetzlichen Tatbestandes führt.[181] In vielen Fällen wird es dem Täter aber gerade darauf ankommen, keine Daten zu verändern, um so wenige Spuren wie möglich zu hinterlassen. Weil er möchte, dass sein Eindringen unentdeckt bleibt, will er eine Beeinträchtigung der Daten vermeiden.[182] Letztlich kommt es hierbei auf die Beurteilung des Einzelfalles an. Gerade der Nachweis eines bedingten Vorsatzes wird jedoch häufig zu Problemen führen.

c) Kritische Würdigung

Betrachtet man dieses Ergebnis im Zusammenhang mit den Strafbarkeitsvoraussetzungen des § 202a Abs.1 StGB, so muss man feststellen, dass es zu empfindlichen Strafbarkeitslücken kommen kann. Ein einfaches Beispiel verdeutlicht dies.

Dringt ein Hacker lediglich in ein fremdes System ein, ohne sich dort weiter umzuschauen, so soll er durch die teleologische Reduktion des Tatbestandes nach herrschender Meinung nicht gemäß § 202a Abs.1 StGB strafbar sein.[183] Trotzdem kann er bereits durch das Eindringen selbst, wenn auch ungewollt, erheblichen Schaden an den auf dem System gespeicherten Daten anrichten.[184] Doch auch wenn das für die Schädigung unter Umständen ursächliche Eindringen in das System noch willentlich erfolgte, kann es - wie dargestellt - am Vorsatz hinsichtlich der Datenveränderung fehlen.

---

[180] Kühl, in: Lackner/Kühl, § 303a, Rn.5; T/F, § 303a, Rn.10.
[181] Wessels/Beulke, AT, Rn.216.
[182] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.58.
[183] vgl. oben:
[184] Granderath, DB 1986, Beil.18, 2: exemplarisch ist hierfür wiederum das oben genannte Beispiel, in dem die New Yorker Cornell-Universität einen Teil ihrer Datenverarbeitungsanlagen endgültig abschalten musste, weil amerikanische und deutsche Hacker, die in die Großrechenanlagen eingedrungen waren, aus Unkenntnis (also ohne Schädigungsvorsatz) erhebliche Schäden angerichtet hatten.

Der Täter bleibt also in diesem Fall straflos. Ein solches Ergebnis dürfte mit dem Rechtsempfinden der meisten Menschen im Widerspruch stehen.

d) Versuchsstrafbarkeit und Antragsdelikt

Der Versuch des § 303a Abs.1 StGB ist strafbar. Gemäß § 303c StGB wird die Tat ohne ein bestehendes öffentliches Interesse nur auf Antrag verfolgt.

3) Die Computersabotage nach § 303b StGB

§ 303b Abs.1 StGB stellt die Computersabotage unter Strafe. Tatbestandsmäßig handelt, „wer eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er eine Tat nach § 303a Abs. 1 begeht oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert."

Geschützt wird durch diese Vorschrift nicht wie in § 303a StGB die Unversehrtheit der Daten selbst, sondern vielmehr das Interesse von Wirtschaft und Verwaltung am ungehinderten Umgang mit den Daten.[185] Zu der Einführung des Tatbestandes durch das 2.WiKG sah sich der Gesetzgeber veranlasst, weil Wirtschaft und Verwaltung in zunehmender Weise auf das störungsfreie Funktionieren von Datenverarbeitungsanlagen angewiesen waren und weil Fehlfunktionen zu hohen Schäden bis hin zum wirtschaftlichen Ruin der Betroffenen führen konnten.[186]

a) Bedeutung für das Hacking

Es gibt unterschiedliche Formen des Hacking, die geeignet sind, den Tatbestand der Computersabotage zu erfüllen. An dieser Stelle sollen zunächst nur diejenigen Fälle behandelt werden, in denen sich der Hacker Zugang zu einem fremden System, beispielsweise einem

[185] Möhrenschlager, wistra 1986, 123 (142); BT-Drs. 10/5058, S.35.
[186] BT-Drs. 10/5058, S.35.

Unternehmensnetzwerk, verschafft und durch die Störung von Systemabläufen eine Beeinträchtigung der Datenverarbeitung verursacht. Zwar ist das Eindringen in das System keine zwingende Voraussetzung für das Stören der Datenverarbeitung und es gibt eine Reihe von Angriffsszenarien, die auch von außen erhebliche Funktionsstörungen bewirken können. Auf diese Formen des „Crashing“[187] soll jedoch erst später eingegangen werden.[188]
Gemeinsam ist allen Angriffsformen über ein Netzwerk[189], dass sie nur zur Verwirklichung der ersten Tathandlungsvariante (Nr.1) des §303b Abs.1 StGB führen können. Will der Täter von einem entfernten System aus die Funktionsfähigkeit einer Datenverarbeitung beeinträchtigen, so ist dies nur durch Einwirkungshandlungen auf der Softwareebene möglich, also zum Beispiel durch die Vornahme störungsrelevanter Manipulationen an den auf dem betroffenen System gespeicherten Daten. Die hardwareschützende Vorschrift des § 303b Abs.1 Nr.2 StGB erfordert ein unmittelbares Einwirken auf die Systemkomponenten, das einem Angreifer über den Online-Weg freilich nicht möglich ist.[190] Für einen Hacker stellt die Computersabotage daher stets eine Qualifikation zu der als Grunddelikt verwirklichten Datenveränderung gemäß § 303a Abs.1 StGB dar.[191]

b) Tatobjekt

Schutzgegenstand des § 303b Abs.1 StGB ist die Datenverarbeitung. Das Gesetz enthält keine Definition des Begriffes. Einigkeit besteht aber darüber, dass der Begriff entsprechend der Auffassung des Gesetzgebers weit auszulegen ist.[192]

---

[187] Der Ausdruck „Crasher“ bezeichnet im allgemeinen kriminelle Computerfreaks, die es gerade darauf absehen, fremde Daten und Programme zu zerstören, bzw. Systeme zum Absturz zu bringen. vgl. NJW-Hackerreport, NJW-CoR 1996, 62.
[188] siehe unten: Kapitel D.: Denial-of-Service-Attacken.
[189] und damit auch über das Internet
[190] vgl. Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.62.
[191] § 303b Abs.1 Nr.2 kann hingegen als Qualifikationstatbestand der Sachbeschädigung (§ 303 StGB) gesehen werden; vgl. T/F, § 303b, Rn.6; Möhrenschlager, wistra 1986, 123 (142); anders: Stree, in: S/S, § 303b, Rn.12.
[192] T/F, § 303b, Rn.3; Möhrenschlager, wistra 1984, 123 (142); Lenckner/Winkelbauer, CR 1986, 824 (830); Bühler, MDR 1987, 448 (456).

Nähert man sich dem Begriff aus Sicht der Informationstechnik, so kann darunter das Erfassen, Übermitteln, Ordnen und Umformen von Daten zur Gewinnung von Informationen mit Hilfe von automatisierten Datenverarbeitungsanlagen verstanden werden.[193]

Einschränkungen ergeben sich jedoch in zweierlei Hinsicht. Zum einen wird nur die Datenverarbeitung von fremden Betrieben,[194] fremden Unternehmen[195] oder Behörden[196] geschützt. „Fremd" sind die genannten Einrichtungen, wenn sie bei rechtlich-wirtschaftlicher Betrachtung nicht ausschließlich dem Tätervermögen zuzuordnen sind.[197] Bei einem Hackerangriff wird diese Voraussetzung regelmäßig erfüllt sein.

Zum anderen wird der Tatbestand dadurch eingeschränkt, dass die Datenverarbeitung für die betroffene Einrichtung von wesentlicher Bedeutung sein muss. Dabei kommt es nicht darauf an, welchem konkreten Zweck die Datenverarbeitung im einzelnen dient.[198] Entscheidend ist vielmehr, ob die Funktionsfähigkeit des Betriebes, des Unternehmens oder der Behörde aufgrund der tatsächlichen Arbeitsweise und Organisation von dem einwandfreien Funktionieren der Datenverarbeitung abhängt.[199] Hierbei ist stets auf den Einzelfall abzustellen. Es ist jedoch anzunehmen, dass durch den stark angestiegenen Einsatz von Informationstechnologien in Wirtschaft und Verwaltung eine Funktionsstörung der Datenverarbeitung in den meisten Fällen schon deshalb von wesentlicher Bedeutung ist, weil

---

[193] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S.197.

[194] Die Begriffe „Betrieb" und „Unternehmen" sind weit auszulegen. Als Betrieb anzusehen ist „jede nicht nur vorübergehende, organisatorisch zusammengefasste Einheit von Personen und Sachmitteln unter einheitlicher Leitung zu dem Zweck, bestimmte Leistungen zu erbringen oder zur Verfügung zu stellen." Ihre Rechtsform ist ebenso unerheblich wie die Art der Betriebstätigkeit und der von ihnen erbrachten Leistungen. Vgl. Gerhards, Computerkriminalität und Sachbeschädigung, S.84; Granderath, DB 1986, Beil. 18, 1 (3).

[195] Die Begriffe „Betrieb" und „Unternehmen" überschneiden sich und haben nach allgemeiner Auffassung keine eigenständige Bedeutung.

[196] Der Behördenbegriff ist in § 1 Abs.4 VwVfG legaldefiniert.

[197] vgl. Stree, in: S/S, § 303b, Rn.6.

[198] Stree, in: S/S, § 303b, Rn7.

[199] Lackner, in: Lackner/Kühl, § 303b, Rn.2; Frommel, JuS 1987 667 (668); Lenckner/Winkelbauer, CR 1986, 824 (830); die Grundsätze des § 305 a Abs.1 Nr.1 StGB anwendend: Haß, Strafrechtlicher Schutz von Computerprogrammen, Rn.57.

sie zu einem erheblichen Mehraufwand an Arbeit, Geld und Zeit führen kann.[200]

c) Tathandlung

Tathandlung ist das Stören einer Datenverarbeitung. Eine Datenverarbeitung ist gestört, wenn der reibungslose Ablauf der Verarbeitungsprozesse nicht unerheblich beeinträchtigt wird.[201] Die Angriffsformen des Hacking sind durchaus geeignet, diesen Taterfolg herbeizuführen. Dringt ein Hacker in ein fremdes System ein und nimmt dort Veränderungen am Datenbestand vor, ist eine Beeinträchtigung der Datenverarbeitung bis hin zu deren Erliegen vorstellbar. In diesem Fall müssen häufig Reparaturmaßnahmen oder ein Systemneustart durchgeführt werden. Während dieser Zeit steht den Benutzern die Datenverarbeitung nicht zur Verfügung.[202]
Fraglich ist, ob eine Störung der Datenverarbeitung im Sinne des §303b Abs.1 StGB auch dann vorliegt, wenn ihre Funktionsfähigkeit vorerst nur gefährdet ist, beispielsweise indem durch den Hacker ein schädigendes Programm auf dem System installiert wurde, dessen beeinträchtigende Wirkung aber noch nicht eingetreten ist.[203] Zu denken ist hier vor allem an die Installation von Virenprogrammen und so genannten logischen Bomben. Eine logische Bombe ist ein Programm, das seine spezifizierte Funktion so lange korrekt ausführt, bis durch das Erfüllen einer vorgegebenen Bedingung (zum Beispiel dem Ablauf einer Frist) ein vom Programmierer gewolltes Fehlverhalten (meist eine Schadensfunktion) ausgelöst wird.[204] Trotz der verzögerten Wirkung solcher Programme könnte bereits deren Installation auf einem fremden System eine Störung der Datenverarbeitung darstellen. Denn durch den Einbau des Programms sind bereits alle erforderlichen Maßnahmen für die

---

[200] Dies wird bereits als ausreichend angesehen, vgl. Lenckner/Winkelbauer, CR 1986, 824 (830).
[201] BT-Drs. 10/5058, S. 36; T/F, § 303b, Rn5; Volesky/Scholten, iur 1987, 280 (284).
[202] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.60.
[203] so Hoyer, in SK, § 303b, Rn.10.
[204] jargon file v.4.4.7 (Online-Wörterbuch der Hackersprache), http://www.catb.org/~esr/jargon.html/L/logic-bomb.html.

Bewirkung des Schadens getroffen worden und die Verzögerung der Schädigung dient unter Umständen nur der Verdeckung des Eingriffs oder der Verschleierung seiner Herkunft.

Der Wortlaut des § 303b Abs.1 StGB spricht aber gegen eine Ausdehnung des Tatbestandes auf solche noch bevorstehenden Störungsereignisse.[205] Solange die schädigende Wirkung noch nicht eingetreten ist, funktioniert die Datenverarbeitung einwandfrei, gestört ist allenfalls die Datenverarbeitungsanlage. Erst wenn sich die durch die Installation eines Programms geschaffene konkrete Gefahr auch tatsächlich realisiert, kommt es zu einer Störung der Datenverarbeitung. Bis zu diesem Zeitpunkt ist die Beeinträchtigung des Systems nicht vom Tatbestand des § 303b Abs.1 StGB erfasst.

d) Subjektiver Tatbestand

Für den subjektiven Tatbestand genügt bedingter Vorsatz.[206] Dieser muss sich auf den Grundtatbestand (§ 303a Abs.1) und die Qualifikation (§ 303b Abs.1 Nr.1) beziehen. Der Täter muss zumindest billigend in Kauf nehmen, dass er durch eine mögliche Datenveränderung Datenverarbeitungsabläufe stört. Ferner muss er sich bewusst sein, dass es sich um eine für den Betrieb, das Unternehmen oder die Behörde wesentliche Datenverarbeitung handelt. Hierfür genügt es, dass er die tatsächlichen Umstände kennt, aus denen sich die Wesentlichkeit ergibt.[207] Vorsätzlich muss der Täter schließlich auch hinsichtlich der Kausalität zwischen Störungshandlung und Störung der Datenverarbeitung handeln.[208]

e) Versuchsstrafbarkeit und Antragsdelikt

Nach § 303b Abs.2 StGB ist auch die versuchte Computersabotage strafbar. Gemäß § 303c StGB wird die Tat ohne ein bestehendes öffentliches Interesse ebenfalls nur auf Antrag verfolgt.

---

[205] T/F, § 303b, Rn.5.
[206] Kühl, in: Lackner/Kühl, § 303b, Rn.7.
[207] Sondermann, Die neuen Straftatbestände der Datenveränderung, S.125.
[208] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S.223.

C. TROJANISCHE PFERDE

Ein Sonderfall des Hacking, der hier besondere Berücksichtigung finden soll, betrifft die Verwendung von so genannten Trojanischen Pferden.

I. Begriff und Funktionsweise

Der aus der griechischen Mythologie stammende Begriff beschrieb ursprünglich ein gewaltiges hölzernes Pferd, das die Griechen ihren Feinden als vermeintliches Geschenk übergaben. Tatsächlich hatte das Pferd die Funktion, die in ihm versteckten Soldaten in die Stadt Troja einzuschleusen, um so die Stadt zu zerstören.

In der Informationstechnik wird der Begriff heute für Programme verwendet, die neben einer scheinbar nützlichen auch nicht dokumentierte, schädliche Funktionen enthalten und diese unabhängig vom Computeranwender und ohne dessen Wissen ausführen.[209] Hauptsächlich werden Trojanische Pferde zum Auskundschaften von Zugangskennungen und Passwörtern eingesetzt.

Anders als Computerviren können sich Trojanische Pferde nicht selbständig verbreiten. Oft sind sie einem anderen Programm unsichtbar angehängt und werden aktiviert, sobald der Nutzer dieses Programm auf seinem System einrichtet. Unter Umständen kann ein Hacker ein Trojanisches Pferd auch direkt auf einem fremden System platzieren. Häufig haben Computersysteme oder Netzwerke neben einem geschützten auch einen öffentlichen Bereich, der für jedermann zugänglich ist. In diesem Bereich ist ein Datenaustausch mit dem System ohne eine besondere Zugangsberechtigung möglich.[210] An dieser Stelle kann der Hacker deshalb sein Programm in die Rechenanlage einschleusen.

Die so in das System gelangten Trojanischen Pferde richten zunächst keinen Schaden an. Sie beeinträchtigen nicht die Daten,

---

[209] Bundesamt für Sicherheit in der Informationstechnik (BSI) – Kurzinformationen zu aktuellen Themen der IT-Sicherheit, Trojanische Pferde – Definition und Wirkungsweise, S.1; abrufbar unter: http://www.bsi-fuer-buerger.de/down/trojaner.pdf.

[210] Hauptmann, JurPC 1989, 215 (216).

indem sie sie verändern oder zerstören. Ein Trojanisches Pferd überwacht das befallene System auf die Eingabe vertraulicher Informationen durch die Nutzer. In ihrer einfachsten Form suchen Trojanische Pferde nur nach Nutzungsdaten, überwachen das System also auf die Eingabe von Anmeldenamen und Passwörtern. Es gibt aber auch komplexere Tools, die nach weiteren Informationen suchen und beispielsweise relevante Daten für das Online-Banking auskundschaften.[211]

Die so gewonnen Informationen werden durch das Trojanische Pferd gespeichert und können bei Bedarf an den Angreifer übermittelt und von ihm ausgelesen werden. Hat ein Hacker sich auf diesem Weg Kenntnis von den Zugangsdaten verschafft, kann er sich wie ein legaler Benutzer in das geschlossene System einloggen. Immer häufiger ist dies der einzige Weg, sich zu einem fremden System Zugang zu verschaffen. Herkömmliche Methoden wie das Ausprobieren zahlreicher Passwörter sind oft nicht mehr Erfolg versprechend, da durch Sicherheitsvorkehrungen auf den entsprechenden Anlagen die Zeit für die Eingabe des richtigen Passwortes oder die Zahl der möglichen Versuche beschränkt sind. Um in ein fremdes System eindringen zu können, sind Hacker daher zunehmend auf den Einsatz Trojanischer Pferde angewiesen.

II. Strafbarkeit der Verwendung Trojanischer Pferde

1) Das Ausspähen von Daten nach § 202a StGB

Der Straftatbestand des § 202a Abs.1 StGB wurde oben bereits behandelt.[212] Als es dort beim Ausspähen von Daten um die Suche nach fremden Passwörtern ging, wurde eine Strafbarkeit abgelehnt, wenn die Passwörter selbst nicht durch eine besondere Zugangssicherung gegen unberechtigten Zugriff geschützt sind.[213] Dies war immer dann der Fall, wenn ein Angreifer die Möglichkeit hatte, durch Ausprobieren einer Vielzahl möglicher Kennwörter zur richtigen Lösung zu gelangen. Hatte der Angreifer das korrekte Kennwort

[211] Bundesamt für Sicherheit in der Informationstechnik (BSI), aaO., S.2.
[212] siehe oben: S.16.
[213] siehe oben: S.26.

erraten, so besaß er schon in einer logischen Sekunde vor dem Überwinden der Zugangssperre Kenntnis von dem Datum, das somit selbst nicht durch die Zugangssperre gesichert sein konnte.

a) Tatobjekt: Passwort als geschütztes Datum

Der Fall ist jedoch anders zu beurteilen, wenn wie hier die Passwörter selbst durch Zeitbegrenzungen oder eine Beschränkung der Eingabeversuche geschützt sind. Dann nämlich hat ein Angreifer nicht die Möglichkeit, alle in Frage kommenden Kennwörter auszuprobieren. Er ist darauf angewiesen, eine Schutzvorkehrung zu überwinden und bedient sich deshalb eines Trojanischen Pferdes. Strafbar kann der Einsatz Trojanischer Pferde aber nur sein, wenn die Schutzvorrichtungen aus rechtlicher Sicht eine besondere Zugangssicherung im Sinne des § 202a Abs.1 StGB darstellen. Gegen unberechtigten Zugang besonders gesichert sind Daten, wenn Vorkehrungen getroffen wurden, die objektiv geeignet und subjektiv dazu bestimmt sind, den Zugriff zu den Daten auszuschließen oder zumindest erheblich zu erschweren.[214]
Die Einführung von Zeitsperren und Versuchsbeschränkungen machen es nahezu unmöglich, Passwörter durch Ausprobieren zu erraten. Genau dies ist auch der Zweck der Vorkehrungen. Sie sind daher objektiv geeignet und subjektiv dazu bestimmt, den Zugang zu den Kennwörtern zu verhindern.[215] Passwörter, die auf diese Art geschützt sind, stellen somit Daten dar, die im Sinne des § 202a Abs.1 StGB gegen unberechtigten Zugang besonders gesichert sind. Auch ein Passwort kann daher taugliches Tatobjekt sein.

b) Tathandlung: Installieren des Trojanischen Pferdes

Fraglich ist aber, durch welche konkrete Handlung der Tatbestand des Ausspähens von Daten erfüllt wird. Ansatzpunkt könnte zum einen das Installieren des Trojanischen Pferdes auf dem fremden System sein. Ein strafbares Ausspähen könnte aber auch erst zu

[214] Lenckner, in: S/S, § 202a, Rn.7.
[215] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.80.

dem Zeitpunkt angenommen werden, in dem der Angreifer die von seinem Programm gesammelten Informationen abruft.

Wird ein Trojanisches Pferd auf einem System installiert, so geschieht dies regelmäßig an einer Stelle, die für den Datenaustausch mit jedermann offen ist.[216] Die Daten, von denen der Angreifer während der Installation Kenntnis nimmt, sind folglich solche, die nicht durch eine besondere Sicherung gegen einen unberechtigten Zugriff geschützt sind.

Durch die Installation des Trojanischen Pferdes will der Angreifer an die Zugangsberechtigungen gelangen, die es ihm ermöglichen, in den geschützten und damit auch von § 202a Abs.1 StGB erfassten Bereich einzudringen.[217] Wäre der Täter schon bei der Installation in einem solchen geschützten Bereich, bräuchte er das Trojanische Pferd nicht mehr, denn die Zugangssicherung wäre bereits überwunden. Der Hacker dringt also vorerst nicht in die gegen unberechtigten Zugang gesicherten Bereiche ein. Zugang zu diesen Bereichen verschafft sich allenfalls das Trojanische Pferd, das der Angreifer auf dem System hinterlassen hat. Von den dadurch erlangten Informationen nimmt der Angreifer aber nicht unmittelbar Kenntnis. Diese erhält der Täter erst, wenn er die von dem Trojanischen Pferd gesammelten Informationen abruft. Ein Ausspähen von Daten durch den Angreifer kann daher auch erst angenommen werden, wenn der Angreifer selbst die Daten liest oder diese durch die Übermittlung von dem Trojanischen Pferd in seinen Herrschaftsbereich gelangen. Der Tatbestand des Ausspähens von Daten wird also nicht schon durch die Installation des Trojanischen Pferdes erfüllt, sondern erst durch das Abrufen der Daten durch den Angreifer verwirklicht.

c) Subjektiver Tatbestand

Für den subjektiven Tatbestand genügt bedingter Vorsatz. Regelmäßig wird der Täter aber in Kenntnis seiner fehlenden

---

[216] Hauptmann, JurPC 1989, 215 (216).
[217] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.79.

Berechtigung sogar beabsichtigen, die Sicherung der Zeitsperre oder der Versuchsbegrenzung zu umgehen, um so an die besonders geschützten Zugangsinformationen zu gelangen. Ein vorsätzliches Verhalten ist daher in der Regel gegeben und unproblematisch nachweisbar.

d)Teleologische Reduktion und Ergebnis

Vorläufig bleibt damit festzuhalten, dass sich der Verwender eines Trojanischen Pferdes nach § 202a Abs.1 StGB strafbar macht, wenn er durch sein Programm geschützte Zugangsdaten auskundschaften lässt und diese abruft.

Es stellt sich aber erneut die Frage, ob dieses Ergebnis mit dem Willen des Gesetzgebers vereinbar ist. Möglicherweise muss auch für die Verwendung von Trojanischen Pferden die Reichweite des Tatbestandes teleologisch reduziert werden. Dringt ein Hacker in ein fremdes System ein, ohne sich dort weiter umzusehen, so soll er nach der Auffassung des Gesetzgebers straflos bleiben.[218] Wenn schon das bloße Eindringen in einen Computer straflos ist, könnte dies erst recht für die Verwendung eines Trojanischen Pferdes gelten. Dessen Einsatz geht dem Eindringen in das System durch den Hacker zeitlich voraus. Erst wenn sich der Hacker durch die Verwendung des Programms in den Besitz der Zugangsdaten gebracht hat, kann er das fremde System betreten. Der Einsatz des Trojanischen Pferdes ist somit eine Art Vorbereitungshandlung für das spätere Eindringen in das System. Widersprüchlich wäre es, diese Vorbereitung unter Strafe zu stellen, das spätere Eindringen aber sanktionslos zu dulden.

Für eine Strafbarkeit käme es sonst nämlich allein darauf an, ob der Berechtigte seine Daten nur durch eine Zugangssperre schützt oder ob er eine Reihe von Zugangssperren hintereinander geschaltet hat.[219] Sowohl das Passwort selbst, als auch eine zusätzliche Sicherung, sind Vorkehrungen, die insgesamt dem gleichen Schutz-

[218] siehe oben: S.32; BT-Drs. 10/5058, S.28f.
[219] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.82.

ziel dienen, nämlich den Zugang zu einem System zu verhindern oder wenigstens zu erschweren. Die Gesamtheit der vorhandenen Zugangssperren ist daher auch als eine Einheit zum Schutz der Daten vor unberechtigtem Zugriff zu sehen.[220]
Soll der Wille des Gesetzgebers Berücksichtigung finden, so muss konsequenterweise auch das Ausspähen von Kennwörtern durch die Verwendung eines Trojanischen Pferdes straflos sein. Erst wenn der Hacker auch andere als die Zugangsdaten ausspäht, macht er sich nach § 202a Abs.1 StGB strafbar.

Die restriktive Auslegung des § 202a Abs.1 StGB führt also zur Straflosigkeit des Angreifers. Berücksichtigt man, dass der Täter tatsächlich nicht in ein fremdes System eindringt, sondern durch die Verwendung des Trojanischen Pferdes ein Eindringen allenfalls vorbereitet, kann man die Straflosigkeit des Angreifers akzeptieren. Zu berücksichtigen ist aber auch, dass der Hacker durch die Verwendung des Trojanischen Pferdes eine gesteigerte kriminelle Energie zum Ausdruck bringt. Er sucht den Zugang zum System nicht nur durch Ausprobieren von Passwörtern oder das Aufspüren von Schlupflöchern, sondern er spioniert gezielt nach Kennwörtern und Zugangsdaten. Der Berechtigte dieser Daten hat durch die zusätzliche Sicherung (zeitliche Beschränkung oder begrenzte Anzahl Versuche) unmissverständlich zum Ausdruck gebracht, dass er der Geheimhaltung der Zugangsdaten besondere Bedeutung beimisst. Durch den Angreifer wird diese Schranke nicht respektiert. Gerade bei Kennwörtern handelt es sich zudem um besonders schützenswerte Informationen. Gelangen sie in fremden Besitz, entsteht zwangsläufig die Gefahr des Missbrauchs. Zum Beispiel können die Daten auch an Dritte weitergegeben werden, die dann die Möglichkeit besitzen, in das System einzudringen.
Folgt man jedoch streng dem Willen des Gesetzgebers, so ist zu berücksichtigen, dass die bloße Gefahr eines tatsächlichen Ausspähens vertrauenswürdiger Daten gerade nicht unter Strafe

[220] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.82.

gestellt werden sollte. Konsequenterweise kann daher auch die Verwendung eines Trojanischen Pferdes, das nur Zugangsdaten ausspäht, nicht zu einer Strafbarkeit nach § 202a Abs.1 StGB führen.

2) Die Datenveränderung gemäß § 303a Abs.1 StGB

Durch die Installation eines Trojanischen Pferdes werden die Datenbestände auf dem betroffenen System verändert. In Betracht kommt daher auch eine Strafbarkeit nach § 303a Abs.1 StGB. Den Tatbestand erfüllt, „wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert." Installiert ein Hacker ein Trojanisches Pferd auf einem fremden Computer, kann es zu einer dahingehenden Beeinträchtigung des Systems kommen. Im Einzelfall ist es möglich, dass durch die Installation andere Daten überschrieben oder verändert werden. Ein Überschreiben der Daten kommt insbesondere dann in Betracht, wenn das eingeschleuste Programm nicht durch seine Dateigröße auffallen soll und deshalb den Platz anderer Daten einnimmt. Sofern die Installation des Trojanischen Pferdes die Löschung oder Veränderung von Daten bewirkt, ist der Tatbestand des § 303a Abs.1 StGB erfüllt.

Im Normalfall werden durch die Installation aber zunächst nur Daten hinzugefügt und vorhandene Daten weder gelöscht noch verändert. Fraglich ist daher, ob auch die Datenvermehrung eine strafbare Datenveränderung im Sinne des § 303a Abs.1 StGB darstellt.

Zu denken ist hier an ein „Unbrauchbarmachen" von Daten. Dies setzt voraus, dass die Gebrauchsfähigkeit der Ursprungsdaten so beeinträchtigt wird, dass sie ihrem ursprünglichen Zweck nicht mehr dienen können.[221] Allein durch das Hinzufügen von Daten ist ein solches Ergebnis jedoch höchst unwahrscheinlich. Eine Beeinträchtigung käme nur in Betracht, wenn durch die Arbeit des Trojanischen Pferdes andere Datenverarbeitungsprozesse so behindert würden, dass sie für den Benutzer nicht mehr verfügbar sind. Trojanische Pferde aber sind in der Regel so programmiert, dass sie möglichst unauffällig agieren. Dazu gehört auch, dass sie

[221] Stree, in: S/S, § 303a, Rn.4.

keine anderen Datenverarbeitungsprozesse stören und jede beeinträchtigende Wirkungen vermeiden.

Ebenso scheidet ein „Unterdrücken“ von Daten aus. Trojanische Pferde sind darauf ausgelegt, dass sie jedem Benutzer die Kommunikation mit den durch die Passwörter geschützten Daten ermöglichen. Ließe das Trojanische Pferd einen ungehinderten Zugang zu diesen Daten nicht zu, wäre ein Ausspähen der Kennwörter, die die rechtmäßigen Benutzer eingeben, nicht möglich.[222]

Die Wahrscheinlichkeit, dass die Verwendung eines Trojanischen Pferdes zu einer Strafbarkeit nach § 303a StGB führt, ist folglich gering, wenn auch nicht ausgeschlossen. Letztlich kommt es auf die Beurteilung des Einzelfalls an, ob durch die Verwendung des Trojanischen Pferdes Daten des fremden Systems beeinträchtigt werden.

3) Die Computersabotage nach § 303b Abs.1 Nr.1 StGB

Die Computersabotage setzt als Qualifikationstatbestand voraus, dass der Täter durch die Verwendung des Trojanischen Pferdes eine Datenveränderung im Sinne des § 303a StGB bewirkt hat.[223] Da der Hacker nicht durch eine Beeinträchtigung der Daten auffallen möchte, kommt es wie beschrieben nur im Ausnahmefall zu einer dahingehenden Beeinträchtigung der Daten. In den meisten Fällen scheidet daher auch eine Computersabotage von vornherein aus.

Sollte die Verwendung eines Trojanischen Pferdes im Einzelfall dennoch zu einer Datenveränderung führen, muss hierdurch auch eine Störung der Datenverarbeitung hervorgerufen werden. Das Verschaffen von Passwörtern führt regelmäßig noch nicht zu einer Störung der Funktionsfähigkeit von Rechenanlagen. Erst wenn der Hacker die Passwörter verwertet, kann es normalerweise zu einer Beeinträchtigung der Datenverarbeitung kommen.[224] Dann aber ist

---

[222] Binder, Strafbarkeit des Ausspähens von DV-Informationen, S.78.

[223] Eine physische Zerstörung der Hardware, wie sie § 303b Abs.1 Nr.2 StGB fordert, kann durch die Installation eines Trojanischen Pferdes nicht bewirkt werden. Insoweit kommt eine Strafbarkeit nur als Qualifikation zur Datenveränderung in Betracht.

[224] Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S.225.

nicht mehr die Verwendung des Trojanischen Pferdes für die Störung ursächlich, sondern die anschließende Verwertung durch den Angreifer.

Sollte anders als im Normalfall bereits die Installation des Trojanischen Pferdes zu einer Beeinträchtigung der Datenverarbeitung führen, wird es regelmäßig Probleme hinsichtlich des Vorsatznachweises geben. Der Verwender eines Trojanischen Pferdes will die Datenverarbeitungsvorgänge nicht behindern. Die Installation seines Trojanischen Pferdes soll unerkannt bleiben. Es ist daher nicht davon auszugehen, dass er eine Störung der Datenverarbeitung billigend in Kauf nimmt.

4) Ergebnis

Nach dem derzeitigen Stand ist die Verwendung Trojanischer Pferde daher in den meisten Fällen straflos. Zwar erfasst der Wortlaut des §202a Abs.1 StGB das Ausspähen von besonders geschützten Passwörtern mittels Trojanischer Pferde, Konsequenz der restriktiven Auslegung des § 202a StGB nach herrschender Meinung ist aber, dass gleich dem Eindringen in fremde Computer auch die Benutzung Trojanischer Pferde nicht bestraft werden darf. Dies führt zu dem bemerkenswerten Ergebnis, dass ein Hacker geheime, fremde Kennwörter auskundschaften darf und diese auch legal an Dritte weitergeben darf. Erst wenn die Passwörter dazu benutzt werden, weitere Daten auszuspähen, liegt ein strafbares Verhalten vor.

Die Tatbestände der Datenveränderung (§ 303a) und der Computersabotage (§ 303b) können durch die Installation eines Trojanischen Pferdes erfüllt werden. In der Praxis stellen diese Fälle aber die Ausnahme dar.

D. DENIAL OF SERVICE ANGRIFFE

Dieses Kapitel beschäftigt sich mit der Strafbarkeit von Denial of Service (DoS) Angriffen. Hierbei handelt es sich um eine Angriffsform, die erst in den letzten Jahren zu einer der größten Bedrohungen für Datenangebote im Internet geworden ist. Allein im vergangenen Jahr ist die Zahl der Denial of Service Angriffe um rund 250 Prozent gestiegen.[225]

Eine strafrechtliche Bewertung dieses Phänomens ist jedoch nicht nur aufgrund der Vielzahl der Angriffe interessant. DoS-Attacken unterscheiden sich in ihrer Funktion und Zielrichtung grundlegend von allen herkömmlichen Hackerangriffen. Die bisher beschriebenen Formen des Hacking richteten sich in erster Linie gegen die Vertraulichkeit und Integrität von Computerdaten. Hacker, die in fremde Systeme eindringen oder dort ein Trojanisches Pferd platzieren, verletzen das Geheimhaltungsinteresse des Verfügungsberechtigten an seinen Daten. Werden die Daten durch den Eingriff verändert, können Integrität und Authentizität der Daten beeinträchtigt werden.

Durch Denial of Service Angriffe werden Daten auf fremden Systemen weder zerstört, noch beschädigt oder verändert. Dem Angreifer kommt es auch nicht darauf an, bestimmte Informationen auszukundschaften. Ziel der Angriffe ist es lediglich, die Verfügbarkeit von Informationen zu stören und durch die Überlastung eines Systems das Datenangebot unerreichbar zu machen.[226]

I. Technischer Hintergrund und Funktionsweise

Denial of Service Angriffe nutzen eine der grundlegendsten Eigenschaften von offenen Netzwerken. Insbesondere das Internet beruht darauf, dass jeder Nutzer, der an das Netz angeschlossen ist, mit jedem beliebigen anderen Nutzer in Kontakt treten kann. Damit die Kommunikation mit allen Teilnehmern funktioniert, muss jedes

---

[225] vgl. Studie „2003 Computer Crime and Security Survey“ des Computer Security Institutes (CSI), San Francisco in Zusammenarbeit mit dem amerikanischen FBI, http://www.gocsi.com/press/20030528.jhtml.

[226] Rubin, Hackerabwehr und Datensicherheit, S.260.

angeschlossene System eingehende Anfragen akzeptieren. Die Verarbeitung der eingehenden Anfragen ist Grundlage für die Initialisierung einer Verbindung. Erst wenn eine Verbindung zwischen den teilnehmenden Computern hergestellt ist, kann der eigentliche Datenaustausch beginnen. Folglich kann auch eine Entscheidung darüber, ob überhaupt ein weitergehender Datenaustausch stattfinden soll erst nach diesem ersten Kontakt getroffen werden.
Auch wenn ein System nur einer geschlossenen Benutzergruppe zur Verfügung steht, kann ein Angreifer deshalb Anfragen an dieses System schicken. Denn der Webserver, der die Anfrage empfängt, kann erst nach deren Bearbeitung feststellen, ob es sich um eine ordnungsgemäße oder eine unzulässige Anfrage handelt. Von einem Angreifer kann diese Offenheit der Netzwerke für missbräuchliche Zwecke ausgenutzt werden. Sendet ein Angreifer so viele oder so komplexe Anfragen an ein System, dass dieses unter der Last der Verarbeitungsvorgänge zusammenbricht, führt dies letztlich dazu, dass gar keine Anfragen mehr bearbeitet werden können und das Datenangebot steht insgesamt nicht mehr zur Verfügung. Das Ergebnis des Angriffs ist also die Versagung jeglicher Dienstleistungen (Denial of Service).
Das einfache Prinzip der Denial of Service Attacken macht es sehr leicht die Angriffe auszuführen, ihre Abwehr bereitet jedoch große Schwierigkeiten.[227] Während die Installation von Firewalls und Scan-programmen ein System vor Einbrüchen oder der Infizierung mit Viren abschirmen kann, ist eine wirksame Verteidigung gegen DoS-Angriffe kaum möglich.

1) Die Angriffssoftware

Es gibt ein breites Spektrum frei erhältlicher Software, die Denial of Service Angriffe auch für wenig geschulte Anwender sehr leicht durchführbar machen. Im wesentlichen kann zwischen zwei unter-schiedlichen Programmarten unterschieden werden.

[227] Rubin, Hackerabwehr und Datensicherheit, S.273.

a) „Ping of Death“

Eine erste Art von Software zielt darauf ab, dem angegriffenen System derart komplexe Aufgaben zu stellen, dass deren Bearbeitung eine so hohe Rechenleistung beansprucht, dass eine Bewältigung weiterer Aufgaben nicht mehr möglich ist.[228]

Das bekannteste Angriffsprogramm dieser Kategorie heißt „Ping of Death“.[229] Hierbei handelt es sich um eine Software, die eine Sicherheitslücke des TCP/IP-Protokolls ausnutzt. Dieses für die Kommunikation im Internet unverzichtbare Protokoll organisiert den Datenverkehr innerhalb eines Netzwerkes. Es stellt Verbindungen zwischen den Systemen her und definiert die Aufteilung der Informationen, die vom Nutzer des Internets versandt und empfangen werden.[230] Wegen der limitierten Übertragungsraten werden im Internet Daten nicht am Stück übertragen, sondern in kleine Pakete aufgeteilt. Die Aufteilung und Zusammensetzung der Pakete werden von dem Protokoll überwacht. Für einen ordnungsgemäßen Ablauf enthält das Protokoll bestimmte Regeln, die unter anderem eine maximale Größe der einzelnen Pakete vorgeben. Das Angriffsprogramm „Ping of Death“ missachtet diese Regel und sendet größere Pakete an den angegriffenen Server. Dies führt dazu, dass der Server außerstande ist, die empfangenen Daten richtig zu interpretieren. Bei der Zusammensetzung der Datenpakete durch das Betriebssystem wird deshalb bei einigen internen Variablen ein Überlauf hervorgerufen.[231] Diese Unregelmäßigkeit beansprucht eine so große Rechenleistung, dass es schließlich zu dem beabsichtigten Zusammenbruch des Systems kommen kann.

---

[228] Rubin, Hackerabwehr und Datensicherheit, S.261.
[229] siehe auch: http://insecure.org/sploits/ping-o-death.html.
[230] Nolden/Franke, Das Internet Buch, S.155.
[231] Rubin, Hackerabwehr und Datensicherheit, S.261.

b) „SYN-Flooding“ und „LAND“

Programme der zweiten Software-Kategorie[232] zielen darauf ab, die begrenzten Ressourcen, die ein Computer für TCP-Verbindungen zur Verfügung stellt, dadurch zu erschöpfen, dass so viele Anfragen an ein System gesendet werden, bis dieses aufgrund der Flut von Arbeitsaufträgen keine weiteren Anfragen mehr akzeptiert.[233] Es werden also keine unverständlichen Befehle an das Zielsystem geschickt, sondern der angegriffene Server soll durch die Vielzahl der Anfragen überlastet und zum Absturz gebracht werden. Zu einer vorgegebenen Zeit wird das Zielsystem mit so vielen Anfragen wie möglich bombardiert. Normalerweise wird jede einzelne Anfrage mit einer gefälschten IP-Adresse, also einem falschen Absender, verschickt. Dies führt nicht nur dazu, dass der Angreifer später schwerer zu ermitteln ist, sondern eine gefälschte Absenderadresse bewirkt auch, dass der Server längere Zeit benötigt, um die Anfrage zu verarbeiten. Grund dafür ist ein Routine-Vorgang namens „Three-way-handshake“, mit dem jede Kommunikation unter dem TCP/IP-Protokoll beginnt.

Der „Three-way-handshake“ ist eine Art „Begrüßung“ der beteiligten Systeme, die dem eigentlichen Datenaustausch vorgeschaltet ist. Auf eine erste Anfrage des Benutzers reagiert der Server mit einer Bestätigung. Anschließend wartet der Server auf eine Antwort des Benutzers, dass er die Bestätigung erhalten hat. Erst danach kann die eigentliche Kommunikation beginnen. Sendet der Angreifer im Falle einer DoS-Attacke seine erste Anfrage mit einer gefälschten Absenderadresse, erreicht die Antwort des Servers nicht ihr Ziel und der Server wartet vergeblich auf eine Bestätigung.[234] In der Regel trennt der Server erst nach einer längeren Wartezeit automatisch die Verbindung. Bis dahin wird der für die Verbindung reservierte Teil

---

[232] Die bekannteste Software aus diesem Bereich sind die Programme „Syn-Flooding“ und „Land“, die sich nur dadurch unterscheiden, dass die Anfragen mit einer anderen Absenderadresse an das angegriffenen System gesandt werden.

[233] Rubin, Hackerabwehr und Datensicherheit, S.261.

[234] Auf diesem Prinzip beruht die Software „Syn-Flooding“. Bei dem Programm „Land“ entspricht die gefälschte Absenderadresse der IP-Adresse des angegriffenen Systems, was dazu führt, dass sich das Zielsystem sogar selbst mit zusätzlichen Anfragen überlastet.

des Systemspeichers blockiert. Werden genügend Anfragen an das System gesendet, kann durch diesen Effekt das gesamte Datenangebot für einige Zeit unerreichbar sein.

2) Distributed Denial of Service Angriffe (DDoS)

Leistungsstarke Server mit einer breitbandigen Netzverbindung verfügen über so große Ressourcen, dass ein einzelner Rechner nicht dazu in der Lage ist, das System mit genügend Anfragen zu überlasten. Angreifer bedienen sich daher immer häufiger einer neuen Methode, bei der mehrere Rechner einen Server gleichzeitig angreifen. Der Täter muss dafür aber nicht selbst im Besitz aller Angriffsrechner sein. Von einem einzelnen Rechner aus kann er mittels einer Software nach fremden Computern suchen, die sich als Angriffswerkzeuge eignen. Meist haben diese Systeme gewisse Sicherheitslücken, die eine Fernsteuerung der Anlagen durch den Angreifer ermöglichen. Der Eigentümer des betroffenen Computers muss von dem Missbrauch nicht einmal etwas bemerken.

Zu einem vom Täter bestimmten Zeitpunkt werden die Angriffe durch ein Kommando gleichzeitig von allen beteiligten Rechnern gestartet. Hierbei ist es sogar möglich, dass der Täter den Angriff so organisiert, dass er selbst zum Zeitpunkt der Durchführung nicht online ist, sondern der Angriff von manipulierten fremden Anlagen kontrolliert wird.[235] Eine Zurückverfolgung des Angriffs wird dadurch erheblich erschwert.

Durch die Verteilung der Aufgaben[236] auf mehrere Rechner und den gleichzeitigen Angriff wird die Intensität der Attacke um ein Vielfaches erhöht. DDoS-Attacken können deshalb innerhalb kurzer Zeit auch große Server überlasten und zum Absturz bringen.

Eines der spektakulärsten Beispiele für einen erfolgreichen Angriff auf leistungsstarke Systeme stammt aus dem Monat Februar 2000, als durch DDoS-Attacken die Server mehrerer bekannter Internet-seiten zum Absturz gebracht wurden. Innerhalb von nur zwei Tagen

[235] Diese Rechner nennt man auch Handler. Jene Computer, die unmittelbar das Zielsystem angreifen, bezeichnet man als Agents.
[236] Daher der Name „Distributed“ Denial of Service Attacks.

wurden die Server des Internetportals „Yahoo!“, des Nachrichtensenders „CNN“ und die Onlineshops von „Amazon.com“ und „Ebay“ lahm gelegt. Die Unerreichbarkeit des Datenangebots führt gerade bei den ausschließlich im Internet operierenden Unternehmen zwangsläufig zu hohen wirtschaftlichen Verlusten.

II. Strafbarkeit der Denial of Service Angriffe

(Distributed) Denial of Service Angriffe können erhebliche Schäden bei den Betroffenen verursachen. Im Unterschied zu den oben beschriebenen Formen des Hacking entstehen diese Schäden jedoch nicht durch das Eindringen in ein System und das Ausspionieren von Daten oder durch ein unmittelbares Einwirken auf die Datenbestände. Durch Denial of Service Angriffe werden die auf dem fremden System gespeicherten Daten weder gelöscht noch verändert. Die Besonderheit der Attacken besteht darin, dass allein durch die Verhinderung des Zugriffs auf das Datenangebot ein Schaden herbeigeführt wird.[237]

Es bedarf daher einer erneuten Prüfung der für das Hacking relevanten Straftatbestände, um festzustellen, ob das Strafrecht einen ausreichenden Schutz gegen Denial of Service Angriffe bietet.

1) Das Ausspähen von Daten nach § 202a Abs.1 StGB

Ein strafbares Ausspähen von Daten nach § 202a Abs.1 StGB setzt voraus, dass der Täter sich „Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, verschafft.“ Geschützt wird das Interesse des Verfügungsberechtigten, die in seinen Daten, Dateien oder Datenbanksystemen verkörperten Informationen vor unbefugtem Zugriff zu sichern.[238] Dieser Schutzbereich wird durch Denial of Service Angriffe nicht berührt. Bei dem betroffenen Datenangebot handelt es sich regelmäßig nicht um vertrauliche Informationen, sondern um Daten, die gerade der Allgemeinheit zur Verfügung gestellt werden und deshalb nicht durch eine

[237] Faßbender, Angriffe auf Datenangebote im Internet, S.49.
[238] T/F, § 202a, Rn.2.

Zugangssperre gesichert sind. Aber selbst wenn die Daten nicht für die Allgemeinheit bestimmt sind, scheitert eine Strafbarkeit nach §202a StGB daran, dass der Täter sich bei einer DoS-Attacke keine fremden Daten verschafft. Durch seinen Angriff blockiert er lediglich die Erreichbarkeit dieser Daten, ohne jedoch von deren Inhalt Kenntnis zu nehmen. Auch ist ein Eindringen in das angegriffene System für die Durchführung der Attacke nicht erforderlich. Anders als bei den zuvor beschriebenen Angriffen durch Hacker kommt bei DoS-Angriffen der Täter nicht mit den Daten des Betroffenen in Kontakt. Folglich wird die Vertraulichkeit der Daten durch Denial of Service Angriffe nicht gefährdet. Eine Strafbarkeit nach § 202a Abs.1 StGB scheidet deshalb im Hinblick auf Denial of Service Angriffe aus.

2) Die Datenveränderung nach § 303a StGB

Gemäß § 303a StGB macht sich strafbar, wer „rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert."

a) Geschütztes Rechtsgut

Nach herrschender Meinung schützt § 303a StGB das Interesse des Datenberechtigten an der unversehrten Verwendbarkeit der in den gespeicherten Daten enthaltenen Informationen.[239]

Bereits die Überschrift des Tatbestandes als „Datenveränderung" lässt jedoch vermuten, dass nicht jede Form der Beeinträchtigung auch zu einer Strafbarkeit führen soll. Denial of Service Angriffe haben wie festgestellt keine unmittelbare Wirkung auf die Daten selbst. Insbesondere werden die auf dem angegriffenen System gespeicherten Daten nicht verändert.[240] Beeinträchtigt wird nur die Verfügbarkeit der Daten. Dies könnte für eine Strafbarkeit deshalb nicht ausreichend sein, da keine Substanzverletzung an den Daten stattfindet.

Berücksichtigt man die systematische Stellung des § 303a StGB, so spricht einiges dafür, dass aufgrund der Einordnung des Tatbe-

[239] T/F, § 303a, Rn.2; Kühl, in: Lackner/Kühl, §303a, Rn.1.
[240] siehe oben: S.63.

standes als Sachbeschädigungsdelikt auch bei der Datenveränderung ein Substanzschutz beabsichtigt wird.[241] Dieser Substanzschutz führt bei der Sachbeschädigung nach § 303 StGB dazu, dass sich nur derjenige strafbar macht, der die körperliche Unversehrtheit einer Sache verletzt.[242] Ausgenommen ist also der Fall, in dem eine Sache lediglich unzugänglich gemacht wird. Denn durch eine solche Sachentziehung wird die Substanz der Sache nicht beeinträchtigt.[243]
Betrachtet man unter diesem Gesichtspunkt § 303a StGB als ein sachbeschädigungsähnliches Delikt,[244] so ist anzunehmen, dass die Datenveränderung keinen anderen Zweck hat, als den strafrechtlichen Substanzschutz auch auf unkörperliche Gegenstände, nämlich Daten, auszudehnen. Ausschlaggebend für die Einführung des § 303a StGB war unter anderem die Unklarheit, ob Daten als Sachen angesehen werden können und somit Schutzobjekte des §303 StGB sind.[245] Durch § 303a StGB wird folglich in erster Linie klargestellt, dass ein der Sachbeschädigung vergleichbarer Schutz auch für unkörperliche Daten gelten soll.
Die uneingeschränkte Verwendbarkeit von Daten wird folglich nicht umfassend geschützt. Strafbar macht sich nur, wer durch eine der genannten Tathandlungen auf die Daten selbst einwirkt und dadurch den Berechtigten von der uneingeschränkten Verwendung der Daten ausschließt.[246]

b) Tathandlungen

aa) Löschen oder Verändern

Das Löschen und Verändern von Daten sind Tathandlungen, die typischerweise zu einer Substanzverletzung bei den Daten führen. Gelöscht werden Daten, wenn sie vollständig und unwiederbringlich unkenntlich gemacht werden.[247] Verändert sind sie, wenn sie einen anderen Informationsgehalt oder Aussagewert erhalten und dadurch

[241] Faßbender, Angriffe auf Datenangebote im Internet, S.51.
[242] Stree, in: S/S, § 303, Rn.8.
[243] Zaczyk, in: NK, § 303, Rn.17.
[244] Arzt/Weber, Strafrecht BT, § 12, Rn.41.
[245] Arzt/Weber, Strafrecht BT, § 12, Rn.42.
[246] Faßbender, Angriffe auf Datenangebote im Internet, S.51.
[247] BT-Drs. 10/5058, S.34; v.Gravenreuth, NStZ 1989, 201 (206).

der ursprüngliche Verwendungszweck beeinträchtigt wird.[248] Bei Denial of Service Angriffen ist beides nicht der Fall. Die Daten werden weder gelöscht noch verändert, sondern sie sind auf dem Speichermedium des angegriffenen Systems während und nach dem Angriff unverändert vorhanden.

bb) Unbrauchbarmachen

Ein Unbrauchbarmachen von Daten ist dann gegeben, wenn die Daten in ihrer Gebrauchsfähigkeit so beeinträchtigt werden, dass sie den Zweck, für den sie vorgesehen sind, nicht mehr erfüllen können.[249] Es stellt sich also die Frage nach der Zweckbestimmung von Daten, die durch Denial of Service Angriffe betroffen sind.

Regelmäßig sind die angegriffenen Datenangebote auf einem an das Internet angeschlossenen Server gespeichert. Dieser Server ist permanent mit dem Internet verbunden und ermöglicht es deshalb, dass interessierte Nutzer das Datenangebot zu einer beliebigen Zeit abrufen können. Der Datenberechtigte bezweckt also durch die Bereitstellung der Daten, dass diese über das Internet jederzeit und unbeschränkt erreichbar sind.[250]

Wird durch eine Denial of Service Attacke die Zugriffsmöglichkeit auf einen Server blockiert, so stehen die dort gespeicherten Daten für diesen Zweck nicht mehr zur Verfügung. Insoweit könnte man davon ausgehen, dass die Daten durch den Angriff unbrauchbar gemacht werden. Zu berücksichtigen ist aber, dass auch die Tathandlung des Unbrauchbarmachens entsprechend des Schutzzweckes von § 303a StGB interpretiert werden muss. Folglich kann nicht jede Form der Beeinträchtigung von dem Begriff umfasst sein. Tatbestandsmäßig ist nur ein Verhalten, durch das eine Einwirkung auf die Daten selbst stattfindet. Der Täter muss also durch die Tathandlung unmittelbar auf den Datenbestand Einfluss nehmen. Auch bei einem Unbrauchbarmachen kommt daher vor allem eine Veränderung der Daten in Betracht. Diese bezieht sich jedoch anders als oben nicht

---

[248] Möhrenschlager, wistra 1986, 123 (141); Stree, in: S/S, § 303a, Rn.4.
[249] BT-Drs. 10/5058, S.35.
[250] Faßbender, Angriffe auf Datenangebote im Internet, S.64.

darauf, dass der Täter den Informationsgehalt der Daten ändert, sondern er bewirkt durch die Veränderung bestimmter technischer Parameter, dass die Verarbeitung der Daten gestört wird.[251]

Eine solche Störung rufen Denial of Service Angriffe jedoch nicht hervor. Die Daten sind nicht selbst Objekt des Angriffs, sondern nur die Kapazitäten des entsprechenden Servers, der im Falle einer Überlastung die gespeicherten Daten nicht mehr zur Verfügung stellen kann. Ist der Angriff jedoch beendet, so stehen alle Daten wieder unversehrt zur Verfügung, so dass es nicht einmal zu einer dauerhaften Beeinträchtigung kommt.[252]

Im Ergebnis ist daher festzustellen, dass mangels einer unmittelbaren Einflussnahme auf die Daten ein Unbrauchbarmachen von Daten im Sinne des § 303a StGB nicht gegeben ist.

cc) Unterdrücken

Ein Unterdrücken im Sinne des § 303a StGB liegt vor, wenn die Daten dem Zugriff des Verfügungsberechtigten auf Dauer oder zeitweilig entzogen werden und sie deshalb nicht mehr verwendet werden können.[253]

Diese Tathandlungsvariante geht über den vergleichbaren Anwendungsbereich der Sachbeschädigung nach § 303 StGB hinaus. Durch die Strafbarkeit der Datenunterdrückung wird der Anwendungsbereich des § 303a StGB auch auf die Fälle ausgedehnt, in denen auf andere Weise als durch eine Bestandsverletzung der Zugriff auf die Daten verhindert wird.[254] Folglich könnte auch das Blockieren eines Datenangebotes durch eine DoS-Attacke eine strafbare Datenunterdrückung im Sinne des § 303a StGB darstellen. Da durch Denial of Service Angriffe die Erreichbarkeit der Daten beeinträchtigt wird, stehen diese Daten wenigstens vorübergehend nicht zur Verfügung.

---

[251] Guder, Computersabotage, S.208.
[252] Faßbender, Angriffe auf Datenangebote im Internet, S.66.
[253] T/F, § 303a, Rn.6; Lenckner/Winkelbauer, CR 1986, 824 (829).
[254] Kühl, in Lackner/Kühl, § 303a, Rn.3, Arzt/Weber, Strafrecht BT, § 12, Rn.49.

Erforderlich ist aber, dass die Daten gerade dem Zugriff des Verfügungsberechtigten entzogen sind.[255] Denial of Service Angriffe verhindern in erster Linie den Zugriff durch Internetnutzer, die sich zum Zeitpunkt des Angriffs für das Datenangebot interessieren. Der Urheber der Daten oder die speichernde Stelle haben in aller Regel unverändert die Möglichkeit, alle Daten abzurufen, da sie anders als entfernte Benutzer nicht auf das Funktionieren der Datenfernübertragung angewiesen sind.

Fraglich ist daher, ob auch ein normaler Internetbenutzer als Verfügungsberechtigter im Hinblick auf ein im Internet bereit gestelltes Datenangebot angesehen werden kann. Zwar werden die Daten gerade für eine unbestimmte Zahl beliebiger Interessenten auf dem Server gespeichert, denn nur so kann derjenige, der die Daten zur Verfügung stellt gewährleisten, dass sie für die Allgemeinheit zugänglich sind. Aus dieser Bereitstellung der Daten ergibt sich im Umkehrschluss aber noch kein Recht der Nutzer darauf, diese Daten auch tatsächlich abrufen zu können. Im Ergebnis hätte dies nämlich zur Konsequenz, dass weltweit alle Internetnutzer potentiell als Verfügungsberechtigte hinsichtlich aller im Internet angebotener Daten anzusehen sind. Ein so weitreichender Schutzbereich ist vom Tatbestand der Datenveränderung zweifellos nicht beabsichtigt. Als sachbeschädigungsähnliches Delikt schützt die Datenveränderung eine dem Eigentum angenäherte Rechtsposition.[256] Erforderlich ist daher auch, dass die Daten als Schutzobjekt einer bestimmten Person oder einem Personenkreis zugeordnet werden können. Angesichts der unüberschaubaren Zahl von Internetnutzern ist eine solche Zuordnung völlig ausgeschlossen. Insbesondere ist es im Vorfeld nicht abzusehen, wer sich zum Zeitpunkt des Angriffs für das jeweilige Datenangebot interessieren wird. Der einzelne Internetnutzer kann daher auch nicht als Verfügungsberechtigter der Daten angesehen werden. Folglich werden durch Denial of Service Angriffe

[255] Stree, in:S/S, § 303a, Rn.4; Schulze-Heiming, Strafrechtlicher Schutz der Computerdaten, S.176.
[256] Arzt/Weber, Strafrecht BT, § 12, Rn.42.

Daten zwar unterdrückt, regelmäßig aber nicht gegenüber dem Verfügungsberechtigten.
Nach allen Tathandlungsvarianten ist das Ausführen eines Denial of Service Angriffes daher nicht gemäß § 303a Abs.1 StGB strafbar.

3) Die Computersabotage nach § 303b StGB

Eine Strafbarkeit wegen Computersabotage gemäß § 303b Abs.1 StGB setzt voraus, dass der Täter eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, dadurch stört, dass er entweder eine Tat nach § 303a Abs.1 begeht oder eine Datenverarbeitungsanlage oder einen Datenträger beschädigt.
Die Vorschrift schützt das Interesse von Wirtschaft und Verwaltung an einem störungsfreien Ablauf ihrer Datenverarbeitung.[257] Dieses Interesse kann durch Denial of Service Angriffe beeinträchtigt sein, denn typischerweise richten sich DoS-Angriffe gegen einen Betrieb oder ein Unternehmen. Da die entsprechende Firma ihr Datenangebot auf einem Server online zur Verfügung stellt, kann regelmäßig auch an der Bedeutung der Datenverarbeitung für das Unternehmen nicht gezweifelt werden.
Probleme ergeben sich aber im Hinblick auf die in Frage kommenden Tathandlungen. Nach § 303b Abs.1 Nr.2 StGB ist eine Beeinträchtigung der Hardware erforderlich. Bei Denial of Service Angriffen erleiden aber weder Datenträger noch die Datenverarbeitungsanlagen einen physischen Schaden. Die Hardware der Datenverarbeitungsanlage bleibt in ihrem ursprünglichen Zustand grundsätzlich voll funktionsfähig.[258] Die erhebliche Belastung, der ein Server während eines Denial of Service Angriffs ausgesetzt ist, wirkt sich lediglich auf Softwareebene aus.
Die softwareschützende Vorschrift des § 303b Abs.1 Nr.1 StGB verlangt als Qualifikationstatbestand zur Datenveränderung die Verwirklichung des Grunddelikts nach § 303a Abs.1 StGB. Ein

[257] BT-Drs. 10/5058, S.35; Stree, in S/S, § 303b, Rn.1.
[258] Faßbender, Angriffe auf Datenangebote im Internet, S.79.

tatbestandsmäßiges Verhalten scheitert hier jedoch fast immer daran, dass sich die Datenunterdrückung durch den Angriff nicht gegenüber dem Verfügungsberechtigten, sondern lediglich gegenüber den an dem Datenangebot interessierten Internetnutzern auswirkt.[259] Das Interesse des Verfügungsberechtigten daran, dass sein Datenangebot auch für andere erreichbar ist, wird nach dem Wortlaut des § 303a Abs.1 StGB aber nicht geschützt.

Ein Hacker, der einen Denial of Service Angriff auf einen Betrieb, ein Unternehmen oder eine Behörde verübt, macht sich folglich nicht nach § 303b Abs.1 StGB wegen einer Computersabotage strafbar. Dieses Ergebnis ist besonders bemerkenswert, da der Gesetzgeber durch die Einführung der Computersabotage mit dem 2. WiKG gerade eine umfassende Vorschrift zur Bekämpfung der Betriebssabotage schaffen wollte.[260] Hinsichtlich der Denial of Service Attacken ist dies nicht gelungen.

4) Ergebnis

Zusammenfassend ist somit festzustellen, dass das geltende deutsche Strafrecht keinen Schutz vor Denial of Service Attacken bietet. Durch die durch das 2.WiKG eingeführten Straftatbestände wird diese neuartige Angriffsform nicht erfasst. Eine Strafbarkeit nach § 202a StGB scheidet aus, da der Täter sich keine Daten verschafft, sondern lediglich den Zugang zu ihnen durch Dritte verhindert. Hierfür ist nicht einmal ein unmittelbares Einwirken auf Computerdaten erforderlich. Es kommt weder zu Eingriffen in die Software noch zu Störungen von Datenverarbeitungsanlagen oder sonstiger Hardware. Eine Strafbarkeit wegen Datenveränderung gemäß § 303a StGB oder Computersabotage gemäß § 303 b StGB scheidet daher ebenfalls aus.

---

[259] siehe oben: S.73.
[260] BT-Drs. 10/5058, S.35.

E. ZUSAMMENFASSUNG UND AUSBLICK

I. Die bestehende Rechtslage

Der technische Fortschritt in der Informationstechnologie hat für zahlreiche Veränderungen in unserer Gesellschaft gesorgt. Elektronische Kommunikationsnetze und Informationssysteme sind mittlerweile ein fester Bestandteil unseres Alltags und von grundlegender Bedeutung für den Erfolg der Wirtschaft. Auch für den privaten Anwender ergeben sich durch die globale Vernetzung von Computeranlagen zahlreiche Vorteile.

Die Entwicklungen in der Informationstechnologie haben jedoch auch viele Gefahren mit sich gebracht. Angriffe auf Datenangebote durch Hacker sind zu einer großen Bedrohung für Wirtschaft und Gesellschaft geworden. Angesichts der zunehmenden Bedeutung von Informationen wächst auch das Bedürfnis, die Interessen an einem ungestörten Umgang mit Informationen umfassend zu schützen. Diesem Erfordernis wird das geltende Strafrecht nur teilweise gerecht.

Für das Hacking in der Form eines unberechtigten Eindringens in fremde Computersysteme ist festzustellen, dass die geltenden Bestimmungen in einigen Fällen lückenhaft sind. Nach § 202a StGB ist ein Eindringen nur dann strafbar, wenn der Täter sich Daten des fremden Systems „verschafft“. Zwar verschafft sich ein Täter streng genommen schon durch seinen Einbruch solche Daten, der Gesetzgeber wollte jedoch das Hacking als bloßes Eindringen in ein Computersystem nicht bestrafen.[261] Sanktioniert werden sollte nur der unerwünschte Datendiebstahl. Die Tathandlung „verschaffen“ wird daher nach herrschender Meinung[262] teleologisch reduziert. Die Abgrenzungskriterien für diese teleologische Reduktion sind im einzelnen umstritten. Allen Ansätzen ist aber gemeinsam, dass das bloße Eindringen in einen fremden Computer nicht strafbar ist. In der

---

[261] BT-Drs. 10/5058, S.28.

[262] T/F, § 202a, Rn.9; Lackner, in: Lackner/Kühl, § 202a, Rn.5; Hilgendorf, JuS 1996, 702 (704); Haft, NStZ 1987, 6 (9); Zielinski, Strafrechtl. Schutz v. Software, S.120.

Praxis können hierdurch Strafbarkeitslücken entstehen. Bereits der schlichte Einbruch in eine Rechenanlage kann erhebliche Schäden verursachen. Neben einem unmittelbaren wirtschaftlichen Schaden droht dem Betroffenen vor allem ein Vertrauensverlust in Bezug auf die Sicherheit seines Systems. Eine Strafbarkeit des bloßen Eindringens wäre daher in vielen Fällen wünschenswert. Ein generelles Zutrittsverbot zu fremden Systemen würde auch zu Beweiserleichterungen führen. Rückblickend kann oft nicht nachvollzogen werden, ob und welche Daten ein Eindringling tatsächlich abgerufen hat.

Nach § 303a StGB macht sich ein Hacker strafbar, sofern er bei seinem Einbruch vorsätzlich Veränderungen an den Daten vornimmt. Keinen Schutz bietet das geltende Strafrecht aber für den Fall, dass ein Hacker gegen den Willen des Verfügungsberechtigten eine Zugangssperre überwindet und versehentlich Daten verändert.

Wird durch die Manipulation des Hackers die Datenverarbeitung eines fremden Betriebes, eines Unternehmens oder einer Behörde gestört, kommt eine Strafbarkeit nach § 303b StGB in Betracht, die ihrerseits aber die Verwirklichung des Grunddelikts nach § 303a erfordert.

Noch größere Strafbarkeitslücken tun sich hinsichtlich der Denial of Service Attacken auf.[263] Ein strafrechtlicher Schutz gegen diese Art der Angriffe ist derzeit nicht gewährleistet. Die relevanten Tatbestände des Strafgesetzbuches schützen allein die Unversehrtheit von Daten und Datenverarbeitungsanlagen. Denial of Service Angriffe richten sich aber gegen die Verfügbarkeit von Daten in einem Netzwerk. Das Recht auf ungehinderte Datenverbreitung und Datenbeschaffung wird durch das Strafrecht nicht geschützt. Gerade die uneingeschränkte Nutzbarkeit von Daten ist in der modernen Informationsgesellschaft jedoch von besonderer Bedeutung. Durch Denial of Service Angriffe können Hacker dieses Recht empfindlich

[263] siehe oben: S.75.

beeinträchtigen, ohne strafrechtliche Konsequenzen fürchten zu müssen.

Durch die Einführung des 2.WiKG ist es folglich nicht gelungen, einen umfassenden Schutz auch gegen die damals noch unbekannten Angriffsformen auf Daten zu gewährleisten.

II. Die „Cybercrime-Convention“ des Europarates

Eine Verschärfung des deutschen Strafrechts könnte sich schon sehr bald aus völkerrechtlichen Verpflichtungen ergeben. Der Europarat hat zusammen mit einigen weiteren Staaten, insbesondere den USA, Kanada und Japan, eine Konvention gegen Cybercrime ausgearbeitet.[264] Die Konvention ist das erste internationale Abkommen zur Bekämpfung von Straftaten, die über das Internet oder andere Computernetzwerke begangen werden. Sie enthält Regelungen, die eine international einheitliche Bestrafung von Internetstraftaten bezwecken.

Für das Inkrafttreten der „Cybercrime Convention“ ist nach Art. 36 Nr.3 die verbindliche Zustimmung von fünf Staaten, darunter mindestens drei Mitgliedsstaaten des Europarates, erforderlich. In Deutschland soll die Konvention noch in dieser Legislaturperiode in nationales Recht umgesetzt werden.[265]

Für das deutsche Strafrecht würde eine Umsetzung einige Änderungen mit sich bringen. Für die hier behandelten Fragen im Zusammenhang mit dem Hacking sind vor allem die Regelungen des ersten Titels in Kapitel zwei der Konvention von besonderem Interesse.

---

[264] Die „Convention on Cybercrime“ vom 23. November 2001 ist in engl. Fassung abrufbar unter: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

[265] vgl. Heise-Newsticker, Meldung v. 5.12.2002, abrufbar unter: http://www.heise.de/newsticker/data/anw-05.12.02-009/.

1) „Illegal Access“

Art.2 der Konvention beschäftigt sich unter der Überschrift „Illegal Access“ mit dem unerlaubten Zugang zu einem Computersystem.[266] Die Regelung sieht die Schaffung von nationalstaatlichen Normen vor, die einen vorsätzlichen, unerlaubten Zugriff auf ein Computersystem oder einen Teil dieses Systems unter Strafe stellen. Nach der Kommentierung des Vertragstextes[267] umfasst ein Zugang in diesem Sinne jede Form des Eindringens in ein System oder einen Teil dieses Systems. Erforderlich ist lediglich, dass der Zugang unberechtigt erfolgt. Grundsätzlich straffrei bleibt daher nur der genehmigte Zugang oder das Betreten eines für die Allgemeinheit frei zugänglichen Systems.

In der Kommentierung des Vertragstextes wird jedoch auch dem Umstand Rechnung getragen, dass ein solch umfassender Straftatbestand unter den beitretenden Staaten nicht unumstritten ist. Wie in Deutschland wird auch in einigen anderen Ländern das Hacking als bloßes Eindringen in ein Computersystem als nicht strafwürdig angesehen.[268] Die Konvention stellt es den beitretenden Staaten daher frei, ob sie einen so weitgehenden Tatbestand übernehmen wollen. Alternativ können die Mitgliedstaaten bestimmte weitere Voraussetzungen an eine Strafbarkeit knüpfen. Nach Art.2 Satz 2 der Konvention kann eine Strafbarkeit etwa von dem Überwinden einer Sicherungsvorkehrung abhängig gemacht werden. Eine Begrenzung kann auch dahingehend erfolgen, dass nur der Angreifer bestraft wird, der in der Absicht der Datenbeschaffung handelt oder sonst böswillige Zwecke verfolgt.

Auch nach der Cybercrime Konvention bleibt also erneut Spielraum für mögliche Einschränkungen der entsprechenden Straftatbestände.

---

[266] Art.2: „Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.“

[267] Explanatory Report v. 8.November 2001, Ziffer 46, abrufbar unter: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

[268] Explanatory Report, aaO., Ziffer 49.

Allerdings betont der Europarat in seiner Kommentierung auch das Bedürfnis für einen Strafrechtsschutz gegen das unerlaubte Eindringen in Computersysteme.[269] Sowohl für Unternehmen als auch für Privatpersonen soll ein ungestörter Umgang mit Rechenanlagen gewährleistet werden. Bereits das unautorisierte Eindringen eines Hackers in ein System könne zu Behinderungen für die rechtmäßigen Nutzer führen oder sogar Änderungen oder Zerstörungen an dem vorhandenen Datenbestand verursachen. Prinzipiell soll daher bereits das Eindringen selbst illegal sein.[270]
Welche konkrete Ausgestaltung die Umsetzung der Konvention im deutschen Recht erfahren wird, bleibt abzuwarten. In der Tendenz ist jedoch eine Verschärfung der strafrechtlichen Bestimmungen zu erwarten.

2) „System Interference“

Art.5 der Konvention verlangt von den beitretenden Staaten die Schaffung einer strafrechtlichen Regelung zum Schutz von Computersystemen.[271] Anders als in § 303a sind nicht die Computerdaten Schutzobjekt des einzuführenden Tatbestandes, sondern die Verursachung einer Systemstörung durch Einspeisung, Übertragung, Beschädigung, Löschung, Veränderung oder Unterdrückung von Daten soll unter Strafe gestellt werden. Geschützt wird das Interesse der Betreiber und Nutzer an einem ordnungsgemäßen Funktionieren von Computer- und Telekommunikationssystemen.[272] Bewusst wurde der Wortlaut des Artikels weit formuliert, um möglichst alle denkbaren Funktionsstörungen dem strafrechtlichen Schutz zu unterstellen.

---

[269] Explanatory Report, aaO., Ziffer 44.
[270] Explenatory Report, aaO., Ziffer 44.
[271] Art.5: „Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.”
[272] Explenatory Report, aaO., Ziffer 65.

Nach dem Wortlaut ist aber erforderlich, dass die Funktionsstörung schwerwiegend ist.[273] Hinsichtlich des verursachten Schadens können die beitretenden Staaten unterschiedliche Maßstäbe für die tatsächlichen Auswirkungen der Funktionsstörung entwickeln. Schwerwiegend sind nach der Kommentierung der Konvention aber in jedem Fall solche Angriffe, die eine Denial of Service Attacke oder das Versenden von Computerviren zum Gegenstand haben.[274]

Die „Cybercrime Convention“ verlangt also ausdrücklich eine Strafbarkeit für Denial of Service Angriffe. Mit der Umsetzung der Konvention in deutsches Recht muss der Gesetzgeber dieser Forderung nachkommen und entsprechende strafrechtliche Regelungen schaffen.

[273] Explenatory Report, aaO., Ziffer 67: „The hindering must furthermore be serious in order to give rise to criminal sanction.“
[274] Explenatory Report, aaO., Ziffer 67.