Rechtliche Qualifikation von Denial of Service Attacken

Johannes Öhlböck/Balazs Esztegar, Wien

Denial of Service (DoS) Attacken sind keine Erscheinung der letzten Jahre. Dennoch haben sie im Zusammenhang mit den Protestaktionen gegen den Gründer der Whistleblower[1] Plattform WikiLeaks, *Julian Assange*, an Aktualität gewonnen[2]. Wie auch die jüngsten Angriffe gegen die Websites der SPÖ und der FPÖ zeigen[3], werden DoS-Attacken zunehmend zum Instrument politischer Meinungsäußerung. Es stellt sich die Frage nach der Qualifikation derartiger Angriffe in strafrechtlicher und zivilrechtlicher Hinsicht.

Johannes Öhlböck

Balazs Esztegar

1. Begriff und Arten von DoS-Attacken

Unter „Denial of Service" versteht man den Ausfall einer EDV Anlage durch Überlastung[4]. Nicht jede derartige Dienstverweigerung ist auf einen gezielten Angriff zurückzuführen. Ein Systemausfall kann technische oder organisatorische Hintergründe haben, etwa bei einem Defekt eines Anlagenteiles oder einem wartungsbedingten Ausfall eines (Teil)Systems. Ein Computersystem kann aber auch Opfer eines Angriffes werden, sodass der Ausfall auf das vorsätzliche Handeln einer oder mehrerer Personen zurückzuführen ist.

Eine DoS-Attacke liegt vor, wenn die Rechenressourcen eines Computersystems bewusst und gezielt überbeansprucht werden, um letztlich eine Dienstverweigerung herbeizuführen. Das Computersystem wird dabei mit einer so großen Anzahl gleichzeitiger Anfragen konfrontiert, dass es nicht mehr in der Lage ist, alle Anfragen zu verarbeiten. Das kann im einfachen Fall zu einer bloßen Verlangsamung der Reaktionszeit des Dienstes führen. Wird die Attacke jedoch über einen längeren Zeitraum intensiv aufrecht erhalten, zwingt es das Computersystem möglicherweise in die Knie, sodass Anfragen gar nicht mehr beantwortet werden. Der Dienst kommt zum Erliegen, der Computer stürzt ab.

Bei der Distributed Denial of Service (DDoS) Attacke verwendet der Angreifer sog „Zombies", also zuvor gehackte Computer, um den Server lahmzulegen. Die DDoS-Attacke ist eine Weiterführung des eigentlichen DoS-Angriffes. Der Angreifer bringt im Vorfeld zunächst eine möglichst große Zahl an eigenständigen Computersystemen unter seine Kontrolle, indem er sog Backdoor-Programme[5] platziert. Dabei nützt er Sicherheitslücken der unzureichend geschützten Systeme aus. Diese Backdoor-Programme ermöglichen ihm eine Steuerung des Computersystems ohne Wissen des tatsächlichen Betreibers der Anlage. Im Jahr 2006 wurden in Österreich rund 3.600 Computer in dieser Weise über fremde Bot-Netzwerke[6] gesteuert[7]. Der eigentliche Angriff wird ausgeführt, indem diese „Zombies" zeitgleich Anfragen an das angegriffene Ziel schicken. Dadurch wird die Angriffslast dezentralisiert und auf verschiedene, unabhängig voneinander operierende Computersysteme verteilt.

Nicht jede absichtlich herbeigeführte Überlastung eines Netzwerks ist auf eine DoS-Attacke zurück-

1 Als „Whistleblower" (engl abgeleitet von „to blow the whistle" – „die Pfeife blasen") bezeichnet man einen Aufdecker bzw Hinweisgeber, der Missstände öffentlich macht.

2 Vgl etwa FAZ, Noch keine Entscheidung über *Assange,* 15.12.2010, http://www.faz.net/-01llyb; Der Standard, Internetuser als Rächer und Lebensversicherung von *Julian Assange,* 09.12.2010, http://derstandard.at/1291454635687/Operation-Payback-Internetuser-als-Raecher-und-Lebensversicherung-von-Julian-Assange.

3 Vgl etwa ORF.at, Websites von SPÖ und FPÖ angegriffen, 01.07.2011, http://oesterreich.orf.at/stories/524121/; Der Standard, Anonymous attackiert Seiten von SPÖ und FPÖ, 01.07.2011.

4 Vgl Wikipedia, Lema „Denial of Service".

5 Es handelt sich dabei um eine Software, die es einem Benutzer ermöglicht, unter Umgehung der Schutzmechanismen des betroffenen Computersystems Zugang zum Computer zu erlangen und dessen Funktionen zu steuern.

6 Als Bot wird eine Software bezeichnet, die selbstständig ohne Interaktion des Benutzers zuvor eingegebene Anweisungen ausführt.

7 Bundeskriminalamt, Cybercrime Report 2006, http://www.bmi.gv.at/cms/cs03documentsbmi/428.pdf (Stand: 31.12.2010).

zuführen. Zum einen besteht eine große Zahl an Anwendungen, die eine gezielte Netzwerkbelastung herbeiführen. Prominentestes Beispiel ist die Low Orbit Ion Cannon (LOIC), die entwickelt wurde, um das Verhalten eines angegriffenen Computersystems bei hoher Belastung bis zu dessen Versagen zu beobachten. Derartige Programme können natürlich aktiv missbräuchlich zur Durchführung von DoS-Attacken eingesetzt werden. Im Fall von LOIC ist das im Rahmen der „Operation Payback" passiert. In Chatforen[8] und über soziale Netzwerke wie Facebook[9] und Twitter[10] wurde gezielt zur Verwendung des Programms aufgerufen.

Zum anderen ist es gerade bei Katastrophen, Attentaten oder anderen unerwarteten Ereignissen von weitreichender Bedeutung denkbar, dass ein System aufgrund des weltweiten Nachrichtenbedarfes nicht mehr in der Lage ist, die plötzlich auftretende enorme Flut von Anfragen zu bearbeiten, wie das etwa mit Diensten der Nachrichtenagenturen CNN und BBC bei den Anschlägen vom 11. September 2001 der Fall war[11].

2. Bekannte DoS-Attacken

Gegenstand von DoS-Attacken sind in der Regel Websites und Online-Dienste bzw die dahinter stehenden Computersysteme. Die bekanntesten DoS-Attacken waren politisch motivierte Angriffe auf Server der estnischen Regierung im April/Mai 2007[12], auf die Website des georgischen Präsidenten *Micheil Saakaschwili* im August 2008[13] sowie auf südkoreanische und US-amerikanische Regierungsseiten im Juli 2009[14]. Im November bzw Dezember 2010 kam es zu einer Häufung von DoS-Attacken, die sich zunächst gegen die Whistleblower-Plattform WikiLeaks gerichtet haben, nachdem diese angekündigt hatte, geheime Dokumente der US-Regierung an die Öffentlichkeit zu bringen[15]. Nachdem in der Folge diverse Zahlungsdienstleister die Weiterleitung von Zahlungen an WikiLeaks eingestellt haben, wurden diese selbst Opfer von DoS-Angriffen, die von WikiLeaks-Anhängern unter dem medienwirksamen Projektnamen „Operation Payback" eingeleitet worden waren[16]. Neu an dieser Attacke gegenüber bisherigen war jedoch der bereits beschriebene Online-Aufruf an die breite Web-Öffentlichkeit, sich an der Attacke zu beteiligen.

3. Strafrechtliche Beurteilung

3.1 Störung der Funktionsfähigkeit eines fremden Computersystems

Bei einer DoS-Attacke liegt zumindest eine Störung der Funktionsfähigkeit eines fremden Computersystems vor. Es kommt daher in erster Linie die Anwendung von § 126b StGB in Betracht[17], der auf den internationalen Vorgaben des Art 5 der Cyber-Crime Konvention des Europarates (CyCC)[18] basiert und mit dem Strafrechtsänderungsgesetz 2002[19] umgesetzt wurde. Das erklärte Ziel dieser Bestimmung der CyCC ist es, DoS Attacken unter Strafe zu stellen[20].

3.1.1 Verfügungsbefugnis über das Computersystem

Es handelt sich um ein vorsätzliches (*dolus eventualis*) Begehungsdelikt, dessen Erfolg in der schweren Störung der Funktionsfähigkeit eines Computersystems besteht[21]. Der Täter muss die Herbeiführung einer schweren Störung ernstlich für möglich halten und sich damit abfinden. Der objektive Tatbestand knüpft an das Computersystem an, das in § 74 Abs 1 Z 8 StGB legal definiert wird. Demnach sind unter einem Computersystem sowohl einzelne als auch verbundene Vorrichtungen

8 Beispielsweise http://www.4chan.org/.
9 http://www.facebook.com/pages/Operation-Payback/163859246989155?ref=ts#!/pages/Operation-Payback/163859246989155?v=wall.
10 http://twitter.com/#!/Anon_Operationn.
11 *Conrad Longmore*, The Impact on the Internet of 9/11, http://www.dynamoo.com/diary/0109.htm (Stand: 12.01.2011).
12 Heise Online, DDoS-Attacke auf Estland: Keine Verbindung nach Moskau, 01.06.2007, http://www.heise.de/newsticker/meldung/DDoS-Attacke-auf-Estland-Keine-Verbindung-nach-Moskau-134693.html (Stand: 28.12.2010).
13 Spiegel Online, Hack-Attacke auf Georgien − Ehrenamtliche Angriffe, 14.08.2008, http://www.spiegel.de/netzwelt/web/0,1518,572033,00.html (Stand: 28.12.2010).
14 Die Presse Online, Hacker-Attacke auf Südkorea: Österreich unter Verdacht, 10.07.2009, http://diepresse.com/home/politik/aussenpolitik/493971/HackerAttacke-auf-Suedkorea_Oesterreich-unter-Verdacht?_vl_backlink=/home/politik/aussenpolitik/index.do (Stand: 28.12.2010).
15 Heise Online, DDoS-Attacke auf Wikileaks vor angekündigter Veröffentlichung [Update], 28.11.2010, http://www.heise.de/newsticker/meldung/DDoS-Attacke-auf-Wikileaks-vor-angekuendigter-Veroeffentlichung-Update-1143468.html (Stand: 28.12.2010).
16 Spiegel Online, Operation Payback. Hacker-Großangriff auf Mastercard, Visa & Co http://www.spiegel.de/netzwelt/web/0,1518,733520,00.html (Stand: 08.12.2010).
17 Vgl *Fabrizy*, StGB[9] § 126b Rz 2.
18 Budapester Konvention vom 23.11.2001.
19 BGBl I Nr. 134/2002.
20 Erläuternder Bericht zur CyCC vom 08.11.2001, Rz 65.
21 *Fabrizy*, StGB[9] § 126b Rz 2.

zu verstehen, die der automationsunterstützten Datenverarbeitung dienen. Das geschützte Rechtsgut ist nicht das Computersystem, sondern dessen ungestörte Verwendbarkeit, die selbst einen Vermögenswert darstellt[22]. Unzweifelhaft ist gerade bei Internetdiensten der Ausfall des Computersystems mit massiven wirtschaftlichen Einbußen verbunden, sodass die Annahme eines Vermögenswertes für den störungsfreien Betrieb gerechtfertigt ist. Tatbildlich ist nur die Störung eines Computersystems, über das der Täter nicht oder nicht allein verfügen darf. Die Störung eines eigenen Computersystems ist nicht strafbar. Fraglich ist freilich, wann jemand über ein Computersystem allein verfügungsberechtigt ist. Insbesondere im Hinblick auf den Computer am Arbeitsplatz ist dies fraglich, zumal das Eigentum im Regelfall dem Arbeitgeber zusteht, dieser aber de facto den Computer dem Arbeitnehmer – unter mehr oder weniger restriktiven Nutzungsbedingungen – zur Verfügung stellt. Als Maßstab könnte hier die tatsächlich eingeräumte Verfügungsbefugnis herangezogen werden, beispielsweise ob der Arbeitnehmer selbst Software installieren darf. In diesem Fall wäre er hinreichend verfügungsbefugt, um straffrei zu bleiben, freilich nur dann, wenn das Ziel seines Angriffs der selbst genutzte Computer ist[23]. Das bedeutet freilich keine Straffreiheit hinsichtlich eines von diesem Computer aus vorgenommenen Angriffes auf andere Computersysteme.

Bei DoS-Attacken, die von einem Computersystem initiiert werden, über das der Täter verfügen darf, ist daher bloß die Störung des Zielsystems tatbildlich. Hingegen ist bei der DDoS-Attacke, wo sich der Täter zunächst die Kontrolle über manipulierte Drittcomputer verschafft, die Qualifikation dieser Vorbereitungshandlung fraglich.

3.1.2 Schwere Störung

Die Störung muss schwerwiegend sein. Eine nähere Konkretisierung ist weder dem StGB noch der CyCC zu entnehmen. Der ursprüngliche Begutachtungsentwurf des StRÄG 2002 sah eine „Störung in erheblichem Ausmaß“ vor und orientierte sich an der vor allem bei Gewaltdelikten bestehenden Abstufung[24]. Als Beispiel kann etwa der minderschwere Raub nach § 142 Abs 2 StGB herangezogen werden, wo der Täter unter anderem keine erhebliche Gewalt angewendet haben darf. Eine solche wendet er an, wenn die Belastung des Opfers im Vergleich zu Durchschnittsfällen nicht als geringfügig einzustufen wäre. Anstelle dieser Formulierung fand letztlich aber der unbestimmte Gesetzesbegriff der „schweren Störung“ Eingang in das Gesetz.

Bei der Abgrenzung der schweren Störung erscheint eine Anknüpfung primär an die Dauer der Störung unangemessen, da im Strafrecht die Schwere des Delikts üblicherweise andere Faktoren, wie etwa der Höhe des verursachten Schadens[25], oder der Intensität der Tathandlung[26] gemessen wird. Da zudem § 126b Abs 2 ein zeitliches Qualifikationselement festlegt, wäre es verfehlt, die Schwere der Störung an der Zeitdauer zu messen. Es ist jedoch davon auszugehen, dass eine schwere Störung schon in dem Zeitpunkt vorliegt, in dem ein Computersystem aufgrund eines Angriffs für die Datenverarbeitung unbrauchbar gemacht wird[27].

Als schwer störend ist eine DoS-Attacke jedenfalls zu werten, wenn sie ein Computersystem vollständig lahm legt, was im kompletten Stillstand des Dienstes zum Ausdruck kommt. Dem ist eine gravierende Verlangsamung des Systems gleichzusetzen, wenn diese wirtschaftlich einem Stillstand gleichkommt, wenn also der verbleibende Gebrauchswert für den betroffenen Betreiber nicht wesentlich höher liegt, als bei einem kompletten Stillstand[28]. Umgekehrt ist eine Störung nicht tatbildlich, die den Betrieb des Computersystems nur geringfügig beeinträchtigt. Folglich wäre selbst ein kompletter Ausfall eines Dienstes infolge einer DoS-Attacke als schwer störend zu qualifizieren, selbst wenn dadurch gar kein Schaden entsteht, etwa weil die zu einem Zeitpunkt erfolgt, wo der Dienst nicht frequentiert wird. Die Beeinträchtigung einzelner Datenverarbeitungsvorgänge wird umgekehrt idR keine schwere Störung bedeuten, wenn sich diese ohne nennenswerten Aufwand wiederholen lassen[29]. Freilich ist das anders, wenn wenige oder gar eine einzige Transaktion vereitelt wird, wenn dadurch ein großer Vermögensschaden entsteht. Das wäre denkbar, wenn sich die Störung zwar nicht in der Breite, jedoch ausgerechnet auf

22 *Reindl-Krauskopf* in WK-StGB², § 126b Rz 5.
23 Vgl *Reindl-Krauskopf* in WK-StGB², § 126b Rz 8.
24 Vgl Materialien zum StRÄG 2002, 1166 dB, XXI. GP.
25 Vgl bspw §§ 125, 126 StGB.
26 Vgl bspw §§ 142, 143 StGB.
27 So auch *Heghmanns*, Computersabotage, in: *Joerden/Scheffler/Sinn* (Hg), Frankfurter Festschrift für Andrzej J. Szwarc zum 70. Geburtstag, 323.
28 Vgl Materialien zum StRÄG 2002, 1166 dB, XXI. GP.
29 Vgl zur deutschen Rechtslage ähnlich *Wolff* in *Laufhütte/Rissing-van Saan/Tiedemann* (Hg), Leipziger Kommentar zum StGB[12], Band 10, § 303b StGB Rz 26.

eine einzelne Transaktion von großem Wert auswirkt.

Das Ausmaß des Schadens, der vor allem auch im Wiederherstellungsaufwand besteht, kann aufgrund der systematischen Einordnung von § 126b StGB als Vermögensdelikt als ergänzendes Beurteilungskriterium herangezogen werden. Dennoch darf die Qualifikation als „schwer" nicht mit der sonst im StGB vorherrschenden ersten Wertgrenze von derzeit EUR 3.000,00 (vgl etwa § 126 Abs 1 Z 7 StGB) gleichgesetzt werden, da in diesem Fall die Einstufung „schwer" bereits für die Erfüllung des objektiven Tatbestandes des Grunddelikts vorausgesetzt wird und daran nicht bloß eine höhere Strafdrohung geknüpft ist[30].

Wenig hilfreich ist die Festlegung einer starren Wertgrenze für die Höhe des Schadens, da stets die Gesamtumstände des Einzelfalles zur Beurteilung herangezogen werden müssen. Die „schwere Störung" muss uE anhand eines beweglichen Systems mehrerer Kriterien beurteilt werden. Zu diesen Kriterien gehören einerseits die faktische Auswirkung der Störung auf die Erreichbarkeit des Computersystems, andererseits das wirtschaftliche Ausmaß und die Zeitdauer des Wiederherstellungsaufwandes, nicht jedoch die Zeitdauer der Störungshandlung.

Das Äquivalent zu § 126b StGB im deutschen Recht ist § 303b dStGB. Dort wird auf eine „erhebliche Störung" abgestellt. Nach der dt Lehre liegt eine unerhebliche Störung vor, wenn die Beeinträchtigung ohne großen Aufwand an Zeit und Kosten behoben werden kann[31]. Diese Ansicht wird zutreffend kritisiert[32], da die Strafbarkeit hier in hohem Maße davon abhängt, welche Vorkehrungen der Betroffene getroffen hat, um eine Störung rasch und effizient zu beheben. Hingegen vernachlässigt dieser Ansatz das Ausmaß der direkten Auswirkung des Angriffs.

3.1.3 Störung über einen längeren Zeitraum

Die zeitliche Komponente spielt in der Deliktsqualifikation nach § 126b Abs 2 StGB eine Rolle, der mit dem Strafrechtsänderungsgesetz 2008[33] eingeführt wurde. Dauert die Störung über einen längeren Zeitraum an, erhöht sich die Strafdrohung von Freiheitsstrafe bis zu sechs Monaten bzw Geldstrafe bis 360 Tagessätzen auf Freiheitsstrafe von sechs Monaten bis zu fünf Jahren. Offen bleibt die Frage, wann eine Störung über einen längeren Zeitraum andauert. Es wird hier wohl ein nicht bloß vorübergehender, zeitlich auf wenige Stunden beschränkter Ausfall eines Computersystems vorliegen müssen. Angesichts der gerade bei hochgradig spezialisierten Internetdiensten vorhandenen Infrastruktur wäre es verfehlt, einen Ausfall von mehreren Tagen zu fordern, da einerseits schon ein mehrstündiger Ausfall in der „Kernzeit" einen bedeutenden Vermögensnachteil hervorrufen wird, andererseits aber die Reaktionszeiten zur Beseitigung von Stillständen in der IT extrem kurz sind. Somit wäre uE eine über 24 Stunden dauernde Störung jedenfalls als über einen längeren Zeitraum andauernd anzusehen, wenn diese Zeitspanne nicht auf einem dem Diensteanbieter vorwerfbaren Versäumnis beruht.

3.2 Datenbeschädigung

§ 126b StGB ist gegenüber § 126a StGB subsidiär[34]. Wird also durch die Störungshandlung eine Datenbeschädigung herbeigeführt, und ist § 126a erfüllt, scheidet die Anwendung von § 126b aus. Als Datenbeschädigung ist das Verändern, Löschen oder sonst Unbrauchbarmachen bzw das Unterdrücken von Daten anzusehen. Die Bestimmung pönalisiert somit alle Verhaltensweisen, die zur Folge haben, dass der Berechtigte seine Daten nicht mehr bestimmungsgemäß verwenden kann, sei es auch nur vorübergehend[35]. Es handelt sich um ein Erfolgsdelikt, das mit der Unbrauchbarmachung oder Unterdrückung vollendet ist. Im Fall der Unterdrückung von Daten ist ein Dauerdelikt anzunehmen, an dem die Beteiligung bis zur Beseitigung des rechtswidrigen Zustandes möglich ist[36].

Der Schaden muss unmittelbar[37] durch die Tathandlung entstehen und bemisst sich aus dem Wiederbeschaffungswert der manipulierten Daten, die nicht mehr in der bisherigen Weise genutzt werden können. Ein Folgeschaden, der infolge der Datenbeschädigung dadurch entsteht, dass Daten

30 So auch *Reindl-Krauskopf* in WK-StGB², § 126b Rz 12.
31 *Stree* in *Schönke/Schröder* (Hg), StGB, § 303b, Rn 10; ebenso *Wolff* in *Laufhütte/Rissing-van Saan/Tiedemann* (Hg), Leipziger Kommentar zum StGB[12], Band 10, § 303b StGB Rz 26.
32 *Marberth-Kubicki,* Computer- und Internetstrafrecht², 82.
33 BGBl I Nr. 109/2007 in Umsetzung des Rahmenbeschlusses 2005/222/JI des Rates vom 24. Februar 2005 über Angriffe auf Informationssysteme.
34 Kraft gesetzlicher Anordnung in § 126b Abs 1 StGB.
35 *Bertel* in WK-StGB², § 126a Rz 3.
36 *Triffterer* in SbgK § 126a Rz 19, 108.
37 *Triffterer* in SbgK § 126a Rz 84 f.

nicht in der beabsichtigten Weise genutzt oder nicht fristgerecht weiterverarbeitet werden können, ist nicht vom Schadensbegriff des § 126a StGB umfasst. Einen solchen Folgeschaden könnte etwa eine Lieferverzögerung darstellen, die dadurch hervorgerufen wird, dass die manipulierten Daten erst wiederhergestellt werden müssen.

Werden daher im Zuge eines DoS-Angriffes Daten beschädigt oder sind sie, sei es auch nur vorübergehend, nicht verfügbar, liegt der Schaden im Wiederbeschaffungswert der Daten, also in dem Aufwand, der getragen werden müsste, um die ersatzweise Beschaffung oder neuerliche Verarbeitung der Daten zu erwirken. Der Folgeschaden, den etwa der Stillstand eines Dienstes verursacht, weil die zum Betrieb notwendigen Daten eben nicht verfügbar sind, fällt nicht darunter.

3.3 Vorbereitungshandlungen

3.3.1 Eindringen in fremde Computersysteme

Im Fall einer DDoS-Attacke ist es erforderlich, dass sich der Angreifer zuvor Zugang zu anderen Computersystemen verschafft. Dabei wird er in aller Regel nicht allein über das System verfügungsbefugt sein. Erfolgt das Zugang-Verschaffen durch das Überwinden spezifischer Sicherheitsvorkehrungen im Computersystem, ist § 118a StGB erfüllt. Die Regelung pönalisiert das widerrechtliche Eindringen in ein fremdes[38] Computersystem, indem der Täter einen Sicherungsmechanismus umgeht oder außer Funktion setzt. Derartige Sicherungsmechanismen können bereits Passwortabfragen sein, sofern sie individualisiert sind. Beim Verwenden von Standardpasswörtern für die jeweilige Software, die allgemein bekannt oder herausfindbar sind, liegt hingegen keine spezifische Sicherung vor[39]. Spezifität ist daher anzunehmen, wenn die Beschränkung dazu führt, dass der Zugang nur einem eingeschränkten Personenkreis möglich ist.

Der Täter „überwindet" eine Sicherungsmaßnahme, wenn er einen nicht bloß geringfügigen Aufwand setzen muss, um Zugang zu erlangen. Das ist etwa der Fall, wenn er eine vom Programm vorgesehene Passwortabfrage in einer nicht vom System vorgesehenen Weise umgeht[40]. Dazu gehört auch das widerrechtliche Erlangen von Passwörtern, etwa durch Sniffing[41], Phishing[42] oder im Wege einer Brute-Force-Attacke[43]. Hingegen überwindet der Täter keine Sicherungsmaßnahme, wenn er offenkundige oder offensichtliche Programmfehler ausnützt, mögen sie auch dazu führen, dass unberechtigt auf das System zugegriffen werden kann. Das Delikt nach § 118a StGB kann aber dennoch erfüllt sein, wenn schädliche Software installiert wird, um in der Folge unter Umgehung eines Passwortschutzes Zugriff auf das System zu erlangen.

3.3.2 Verbreitung von Software zur Durchführung von DoS-Attacken

Die Beschaffung von Software, die einen DoS-Angriff ermöglicht, ist im Hinblick auf die Delikte nach §§ 126a und 126b StGB eine Vorbereitungshandlung[44], die durch § 126c StGB unter Strafe gestellt wird. Die Tat begeht, wer ein Computerprogramm, das zur Verwirklichung der in den §§ 118a, 126a und 126b StGB beschriebenen Tathandlungen geeignet ist, herstellt, einführt, vertreibt, veräußert, oder sonst zugänglich macht, sich verschafft oder besitzt. Computerprogrammen sind Passwörter, Zugangsdaten und sonstige Daten wie etwa Programmcodeteile, gleichgestellt, wenn sie zur Erfüllung der genannten Delikte geeignet sind. Es geht also um die Verbreitung und den Besitz sog „Hacker-Tools".

Allerdings sind die beschriebenen Handlungsweisen nur strafbar, wenn sie der Täter mit dem Vorsatz setzt, eines der genannten Delikte zu begehen. Wer ein Computerprogramm, das zur Ausführung einer DoS-Attacke geeignet ist, online zum Download bereit stellt, hat zunächst den Vorsatz, das Programm zu vertreiben oder sonst zugänglich zu machen. Zur Erfüllung des Delikts nach § 126c StGB muss er es darüber hinaus zumindest ernst-

38 Zur Frage der Verfügungsbefugnis des Angreifers siehe oben 3.1.

39 *Reindl-Krauskopf* in WK- StGB² § 118a Rz 25.

40 *Reindl-Krauskopf* in WK-StGB² § 118a Rz 26.

41 Unter „Sniffing" (von engl to sniff – schnüffeln) wird das Abfangen von Datenverkehr und die Auswertung seines Inhaltes verstanden. Sniffer-Programme können ua dazu eingesetzt werden, Passwörter und Benutzerdaten zu „erschnüffeln".

42 Bei „Phishing" wird ein Benutzer auf eine Website geführt, die der vertrauenswürdigen Seite, die er tatsächlich aufrufen wollte, im Design bis zur Verwechslung nachempfunden ist. Ziel des Phishing ist, den Benutzer zur Eingabe von Zugangsdaten bzw. Passwörtern zu verleiten und sie derart zu erlangen.

43 Bei einer „Brute-Force-Attacke" werden Zugangsdaten dadurch ermittelt, dass der Computer so lange nach einer Kombination sucht, bis die richtige gefunden ist. Man spricht auch von einem Wörterbuchangriff, wenn der Angreifer die Software alle Wörter eines Wörterbuches durchprobieren lässt.

44 *Fabrizy*, StGB⁹ § 126c Rz 1.

lich für möglich halten und sich damit abfinden, dass sich jemand das Programm zu dem Zweck beschafft, damit eines der genannten Delikte zu verwirklichen. Diese Möglichkeit wird man bei einer Anwendung nicht ausschließen können, die bekanntermaßen zur Ausführung von DoS-Attacken geeignet ist. Unter diesem Gesichtspunkt ist folglich das Bereitstellen des oben beschriebenen Programms LOIC zu sehen. Wer einen Download-Link zu einer derartigen Software per E-Mail, auf einer Website oder in einem sozialen Netzwerk wie Facebook verbreitet, macht die Anwendung ebenfalls zugänglich. Geschieht das zumindest mit dem Eventualvorsatz, dass dadurch eine DoS-oder DDoS-Attacke ausgeführt werden soll, macht sich der Täter nach § 126c StGB strafbar.

3.4 Begehung als Mitglied einer kriminellen Vereinigung

Sowohl die Störung der Funktionsfähigkeit eines Computersystems nach § 126b als auch die Datenbeschädigung nach § 126a StGB kann der Täter als Mitglied einer kriminellen Vereinigung begehen und sich dadurch einer höheren Strafdrohung von bis zu fünf Jahren aussetzen. Fraglich ist, wann eine kriminelle Vereinigung anzunehmen ist. Diese wird in § 278 Abs 2 StGB definiert. Demnach ist sie ein auf längere Zeit angelegter Zusammenschluss von mehr als zwei Personen mit dem Ziel, eines der genannten Delikte zu begehen. Es reicht damit auch schon die Begehung einer einzigen beabsichtigten Straftat aus, wenn diese aufwändige Planung und Vorbereitung erfordert, sodass das Zusammenwirken der Täter über einen längeren Zeitraum andauert[45]. Das ist bei einer lange geplanten DoS-Attacke durchaus möglich, zumal sich die Täter hier zur Erreichung eines bestimmten Ziels, nämlich dem Ausführen der Attacke, zusammenschließen.

Hingegen ist die kriminelle Vereinigung dort nicht anzunehmen, wo sich Internetnutzer aufgrund eines Aufrufes in Chatforen oder sozialen Netzwerken relativ spontan zur Beteiligung an einer geplanten DoS-Attacke entschließen. Die Spontanität des Entschlusses steht dem von § 278 StGB geforderten längerfristigen Zusammenschluss entgegen[46], da die Attacke selbst kaum über die geforderte längere Zeit aufrecht erhalten werden könnte und es somit an der bereits erwähnten Mindestdauer fehlt.

4. Zivilrechtliche Betrachtung

4.1 Schadenersatz durch den Angreifer

4.1.1 Schaden

Abseits der Strafbarkeit löst eine DoS-Attacke im Regelfall auch zivilrechtliche Folgen aus, erleidet doch derjenige, der den angegriffenen Dienst anbietet, durch den Ausfall einen wirtschaftlichen Schaden. Der Schaden des unmittelbar Geschädigten wird in der Regel ein reiner Vermögensschaden sein. Dieser wird sich einerseits als positiver Schaden darstellen, und zwar in Form jener Kosten, die der Geschädigte aufwenden muss, um die Attacke abzuwehren und den Dienst wieder zum Laufen zu bringen. Ein großer Teil des Schadens kann andererseits entgangener Gewinn sein, der durch den Stillstand des Systems selbst verursacht wird. Nur wenn der Angriff zu einem Hardware Defekt führt, ist eine faktische Beschädigung des Computersystems gegeben. Diese Unterscheidung spielt freilich im hier interessierenden Fall einer DoS-Attacke keine tragende Rolle. Nach § 1324 ABGB ist der Schädiger ja bei vorsätzlicher Schädigung dazu verpflichtet, volle Genugtuung zu leisten, also sowohl den positiven Schaden aus auch den entgangenen Gewinn zu ersetzen.

Die Nichterreichbarkeit eines Dienstes infolge eines DoS-Angriffes kann schließlich einen ideellen Schaden für den Geschädigten erzeugen. Dies etwa dadurch, dass das Ansehen eines Unternehmens, einer Marke oder der Website an sich in der Öffentlichkeit herabgesetzt wird. In Lehre[47] und Rsp[48] wird der Ersatz immaterieller Schäden für juristische Personen etwa auf Grundlage von § 16 Abs 2 UWG als Ausgleich einer erlittenen Kränkung als legitim erachtet. Freilich wird diese Schadenskategorie schon deshalb eine untergeordnete Rolle spielen, weil zumindest in jenen Fällen, in denen das Opfer, dessen Dienst attackiert wird, als börsennotierte Gesellschaft über einen Kurswert verfügt, sich der Schaden regelmäßig monetär im Kurswertverlust niederschlagen und sich als Vermögensschaden manifestieren wird[49].

45 *Fabrizy*, StGB[9] § 126c Rz 1.
46 Vgl auch *Plöchl* in WK-StGB[2] § 278 Rz 8.
47 *Fellner*, Persönlichkeitsschutz juristischer Personen, 200 ff.
48 Vgl etwa OGH vom 10.10.1995, 4 Ob 49/95, SZ 68/10.
49 Zum Schaden durch Kursverluste von Aktien vgl. etwa *Größ*, Kursverluste und Schadenersatz im Übernahmerecht, ÖBA 2003, Heft 2, 95; *Kalss*, Konkurrenzangebot und Rücktritt bei der Unternehmensübernahme, RdW 1999, 269 FN 48; Zur Ersatzfähigkeit des Schadens für den Aktionär siehe OGH 22.12.1994, 2 Ob 591/94.

4.1.2 Schadenminderungs- und Vorsorgepflichten

Fraglich ist, inwieweit den Betroffenen eine Schadenminderungspflicht bzw. den Inhaber eines betroffenen Computersystems, dessen sich der Angreifer durch Durchführung des Angriffs bedient, eine Verpflichtung für Sicherheitsvorkehrungen trifft. Was dem Geschädigten im Rahmen der Schadenminderungspflicht zumutbar ist, bestimmt sich nach den Interessen beider Teile und den Grundsätzen des redlichen Verkehrs[50]. Es kommt daher wesentlich auf den Einzelfall an. Zumutbar werden jedenfalls die Implementierung üblicher Sicherheitssysteme sowie die regelmäßige Wartung des Computersystems sein. So haftet jemand, der ein ungesichertes WLAN Netzwerk betreibt, als Störer, wenn Dritte diesen Anschluss missbräuchlich nutzen. Allerdings wird hier ein Schadenersatz des Inhabers nicht zum Tragen kommen, er könnte lediglich auf Unterlassung in Anspruch genommen werden[51].

4.1.3 Kausalität

DoS-Angriffe können von einem oder mehreren Tätern ausgeführt werden. Im Fall eines einzelnen Schädigers bereitet die Kausalitätsfrage keine Schwierigkeiten. Bei mehreren Tätern wird man davon ausgehen müssen, dass jeder zumindest einen Teil des Schadens verursacht hat, weil jede Anfrage, die an das angegriffene Computersystem geschickt wird, conditio sine qua non für den letztlich eintretenden Erfolg, die Überlastung, ist. Bei vorsätzlichem Zusammenwirken ist Mittäterschaft iSd §§ 1301, 1302 ABGB anzunehmen, die eine Solidarhaftung der Teilnehmer zur Folge hat[52].

Geht man jedoch davon aus, dass jeder Mittäter nur einen vergleichsweise geringen Teil zum Erfolg beiträgt und sich der Erfolg der DoS-Attacke erst in der Summe aller einzelnen Anfragen als Überlastung des Systems zeigt, müsste man von minimaler Kausalität ausgehen. Ein Fall minimaler Kausalität liegt vor, wenn viele Schädiger (zB über 1.000) zusammen einen Schaden herbeigeführt haben, aber niemand von ihnen den gesamten Schaden verursacht, sondern lediglich jeweils nur einen kleinen Teilbeitrag leistet[53]. Dies wird für jene Fälle gelten, in denen die Attacke sehr breit ausgeführt wird, dh viele Personen daran teilnehmen, die aber alle jeweils nur eine geringe Zahl von Anfragen an das Computersystem übermitteln und der Anteil des Einzelnen am Gesamterfolg damit gering ist. Die Theorie von der minimalen Kausalität wandte die Rsp bereits in den 1930er Jahren auf die Beteiligung an Streiks an[54] und gelangte zu einer Solidarhaftung der Beteiligten.

4.2 Haftung des Internetproviders

Neben der Schadenersatzpflicht des unmittelbaren Schädigers stellt sich die Frage nach der Providerhaftung. §§ 13 bis 17 ECG legen eine horizontale Haftungsbefreiung[55] fest. Liegen die Voraussetzungen vor, wird der Provider von jeglicher Haftung – zivilrechtlich wie strafrechtlich – befreit. Umgekehrt bedeutet das nicht automatisch eine Haftung des Providers. Diese ist anhand der zivil- und strafrechtlichen Haftungstatbestände zu prüfen ist.

Der Access Provider ist nach § 13 ECG ein Diensteanbieter, der von einem Nutzer eingegebene Informationen in einem Kommunikationsnetz übermittelt bzw einen Zugang zu einem solchen Kommunikationsnetz bereitstellt. Er ist von einer Haftung befreit, wenn er die Übermittlung nicht veranlasst den Empfänger der übermittelten Information nicht ausgewählt und die übermittelten Informationen weder ausgewählt noch verändert hat. Gemeint ist damit eine reine Durchleitung der Information des Nutzers, ohne diese inhaltlich zu kennen oder sonst wie Einfluss auf den Inhalt oder den Empfänger auszuüben. Es ist im Regelfall anzunehmen, dass der Internet-Service-Provider, über dessen Zugang eine DoS-Attacke ausgeführt wird, die Übermittlung weder veranlasst, noch den Empfänger auswählt hat. Er leitet sie lediglich weiter, allenfalls mit einer kurzzeitigen automatischen Zwischenspeicherung (Caching), die nach § 13 Abs 2 ECG zum Vorgang der Übermittlung zählt. Das hat zur Folge, dass der Access-Provider selbst dann von der Haftung befreit ist, wenn er Kenntnis von der Rechtswidrigkeit der übermittelten Daten hat, also wenn ihm bewusst ist, dass über seinen Dienst eine DoS-Attacke vorgenommen wird[56].

5. Zusammenfassung

Die Durchführung von DoS-Attacken kann in strafrechtlicher Hinsicht je nach Ausgestaltung des An-

50 RIS RS0027787.
51 Vgl BGH, Urteil vom 12. 5. 2010 - I ZR 121/08.
52 Vgl *Schacherreiter* in *Kletecka/Schauer*, ABGB-ON, §§ 1301, 1302 Rz 6 ff.
53 *Schacherreiter* in *Kletecka/Schauer*, ABGB-ON, §§ 1301, 1302 Rz 6 ff.
54 Vgl etwa JBl 1931, 81.
55 *Zankl*, ECG, § 13 Rz 187.
56 Vgl dazu *Zankl*, ECG, § 13 Rz 199.

griffes die Delikte nach §§ 126a und 126b StGB erfüllen. Der Missbrauch von Computerprogrammen nach § 126c StGB ist als Vorbereitungshandlung zu diesen Delikten zu sehen und selbst unter Strafe gestellt. Bei der Störung der Funktionsfähigkeit eines Computersystems nach § 126b StGB kommt es in erster Linie auf das Vorliegen einer schweren Störung an. Neben dem kompletten Stillstand des Systems ist auch eine dem gleichzusetzende gravierende Verlangsamung der Antwortzeiten als schwere Störung zu beurteilen. Die zeitliche Komponente der Störung, die über einen längeren Zeitraum andauern muss, bildet eine eigenständige Deliktsqualifikation. Die Delikte nach §§ 126a und 126b StGB können als Mitglied einer kriminellen Vereinigung begangen werden. Diese setzt ein gezieltes Zusammenwirken über einen längeren Zeitraum voraus.

Zivilrechtlich richtet sich der Ersatz des verursachten Schadens nach allgemeinem Schadenersatzrecht. Eine Haftung des Internetproviders wird in der Regel aufgrund der horizontalen Haftungsbefreiung nach § 13 ECG selbst bei Kenntnis von der Ausführung des Angriffes nicht vorliegen.

Kontakt:
RA Dr. Johannes Öhlböck LL.M.
RAA Mag. Balazs Esztegar LL.M.
office@raoe.at
www.raoe.at