Rechtliche Betrachtung von Desinfektionsmaßnahmen zur Botnetzbekämpfung durch Internet-Service-Provider

Philipp Roos / Philipp Schumacher[1]

Till Elsner / Michael Meier / Matthias Wübbeling[2]

Botnetze stellen eine große Gefahr für die IT-Sicherheit dar, an deren Bekämpfung ein gesellschaftliches Interesse besteht. Auch die Bekämpfung dieser Botnetze beinhaltet rechtliche Risiken und Gefahren, die in dem vorliegenden Beitrag[3] beleuchtet werden. Nach einer kurzen Einführung erfolgen zunächst technische Erläuterungen zur Funktionsweise von Botnetzen. Daneben wird erörtert, wie und wo Botnetze eingesetzt werden und welche Maßnahmen zur Bekämpfung von Botnetzen ergriffen werden können. Anschließend setzt sich der Beitrag mit den rechtlichen Risiken auseinander, die bei der Durchführung von Desinfektionsmaßnahmen bestehen. Hierbei werden zivilrechtliche und strafrechtliche Haftungsrisiken aufgezeigt und untersucht. Kommt es bei der Durchführung von Desinfektionsmaßnahmen zu Schäden, so kann sich eine Schadensersatzpflicht des Internet-Service-Providers ergeben. Zudem können Desinfektionsmaßnahmen auch strafrechtlich relevante Handlungen darstellen. Eine fehlende Schadenszurechnung, das Fehlen von Vorsatz oder das Eingreifen von Rechtfertigungsgründen kann jedoch eine Haftung im Einzelfall ausschließen.

1. Einführung in die Thematik

Dem Internet kommt in der heutigen Gesellschaft eine immer größer werdende und bedeutendere Rolle zu. Dies spiegelt sich in nahezu allen Lebensbereichen wider: Der wirtschaftliche Verkehr ist dabei ebenso wie die staatlichen Einrichtungen oder der Privatnutzer auf das Internet angewiesen. Vor dem Hintergrund dieser wachsenden Bedeutung, die mit einer Abhängigkeit korreliert, steigen auch die Risiken bei der Nutzung, sodass sich die Kriminalität mehr und mehr auf den Cyber-Raum fokussiert. So belief sich der vom Bundeskriminalamt ermittelte Schaden durch Internetkriminalität im Jahr 2011 auf 71,2 Millionen Euro, was einer Zunahme von 16 % im Vergleich zum Vorjahr entspricht.[4] Zudem wird von einem großen Dunkelfeld ausgegangen, das seine Ursache u.a. in der fehlenden Kenntnis der Betroffenen von einer Infektion des Computers haben kann oder dadurch entsteht, dass geschädigte Unternehmen die erkannten Straftaten nicht anzeigen, um einen Reputationsverlust bei Kundschaft und Öffentlichkeit zu vermeiden.[5]

---

1 Institut für Informations-, Telekommunikations- und Medienrecht (ITM) – Zivilrechtliche Abteilung – an der Westfälischen Wilhelms-Universität Münster. Verantwortlich für den rechtlichen Inhalt.

2 Arbeitsgruppe IT-Sicherheit der Abteilung für Informatik IV der Rheinischen Friedrich-Wilhelms-Universität Bonn und Forschungsbereich Cyber Security am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE). Verantwortlich für den technischen Inhalt.

3 Der Artikel entstand im Rahmen des durch das BMBF im Förderschwerpunkt IT-Sicherheitsforschung geförderten Forschungsprojektes MonIKA.

4 Bundeskriminalamt, Cybercrime Bundeslagebild 2011, S. 8.

5 Bundeskriminalamt, Cybercrime Bundeslagebild 2011, S. 9.

Eine der größten Bedrohungen stellt die Existenz von Botnetzen dar. Diese bestehen aus einer in der Regel großen Anzahl von mit Malware infizierten Computersystemen. Über die Malware lassen sich diese Systeme von einem sog. Botmaster fernsteuern, der somit über eine enorme Menge an Ressourcen verfügt. Je größer ein solches Botnetz ist, umso größer ist auch das Gefahrenpotential, das von ihm ausgeht. Die durch das Botnetz verfügbaren Ressourcen nutzt der Botmaster zur Ausführung von Angriffen wie DDoS-Attacken oder Spam-Kampagnen. Bei DDoS-Attacken (verteilte Attacken zur Verhinderung von Diensterbringung) werden die ferngesteuerten Systeme genutzt, um große Mengen von Anfragen an Webserver oder andere Internetdienste zu stellen und diese damit zu überlasten, so dass die angebotenen Dienste von legitimen Nutzern nicht mehr in Anspruch genommen werden können. Bei Spamkampagnen kommen die Rechner des Botnetzes zum verteilten Versand von E-Mails zum Einsatz, was die Filterung dieser (in aller Regel unerwünschter) E-Mails anhand des sendenden Systems deutlich erschwert.

Eine bestmögliche Sicherheit der Internetinfrastruktur ist daher ein von allen Seiten erstrebenswertes Ziel. Damit kommt der Forschung zur Abwehr und Bekämpfung von Botnetzen ein besonders hoher Stellenwert zu, da sämtliche Lebensbereiche betroffen sind und ein legitimes Interesse an sicherer Kommunikation im Internet besteht. Die rasante Entwicklung auf diesem Gebiet und die schnellen Reaktionen der entsprechenden kriminellen Kreise auf technische Neuerungen machen die Bekämpfung zu einer besonderen Herausforderung. Die technischen Verfahren, die Botnetzen entgegen gebracht werden, müssen dabei jedoch selbst rechtskonform ausgestaltet sein. Die rechtlichen Rahmenbedingungen für die Internet-Service-Provider (ISP), denen bei der Bekämpfung eine besonders wichtige Rolle zukommen kann, und die effektivste reaktive Methode in Form der Desinfektion beleuchtet der folgende Beitrag. Es werden sowohl technische als auch rechtliche Hintergründe untersucht.

2. Bedrohung durch Botnetze

Um die Desinfektion als Maßnahme zur Botnetzbekämpfung rechtlich bewerten zu können, ist es notwendig, zu verstehen, wie diese technisch funktioniert und welche Alternativen existieren. Dies setzt die Kenntnis der Funktionsweise von Botnetzen sowie deren Einsatzfelder voraus.

2.1. Funktionsweise eines Botnetzes

Schadsoftware, die durch Ausnutzung von Sicherheitslücken oder als versteckter Anhang an vom Nutzer installierter Software auf einem Computersystem installiert wird, kann Funktionen enthalten, die sich zum Aufbau eines Botnetzes durch einen Botmaster eignen. Der Botmaster erlangt durch Kommunikation mit dem Schadprogramm teilweise Kontrolle über das infizierte System. Durch diese Hintertür ist es möglich, den Computer des Opfers vollständig zu verwenden. Durch nachträgliche Änderungen der installierten Schadsoftware lässt sich die Funktionalität eines Bots erweitern.

Da ein Botmaster die Kontrolle über viele Systeme hat, findet die Kommunikation und Befehlsausführung hauptsächlich automatisiert statt. Es entsteht ein Verbund von verschiedenen Systemen, die alle gemeinsam kontrolliert werden. Ein Kommando wird dann von einem Command-&-Control-System an alle Bots versandt und von diesen ausgeführt. Es gibt verschiedene Verbreitungswege für solche Kommandos, die sowohl die Entdeckung von Botnetzen als auch die Gegenmaßnahmen erschweren sollen.
In einigen Fällen war es möglich, Botnetze zu deaktivieren, indem der zentrale Command-&-Control-Server (C&C-Server) durch Behörden oder ISPs vom Internet getrennt wurde und somit eine Kommunikation mit den Bots nicht mehr möglich war. Die Entwickler von Botnetzen reagierten auf diese Maßnahmen mit der Entwicklung verschiedener Techniken zur Verschleierung oder zur Steigerung der Robustheit der Kommunikationskanäle. Um die Abschaltung des C&C-Servers und damit des gesamten Botnetzes zu erschweren, kommen häufig mehrere C&C-Server zum Einsatz, zwischen denen die Bots in regelmäßigen Abständen wechseln. Oft wird der C&C-Server von den Bots auch nicht direkt kontaktiert, sondern kommuniziert mit diesem durch eine hierarchische Struktur innerhalb des Botnetzes. Dies dient der Ausfallsicherheit der Kommandostruktur und ist außerdem geeignet, Quellen von Kommandos oder Angriffen unkenntlich zu machen. Bei Peer-to-Peer-Botnetzen werden Kommandos des Botmasters von einem benachbarten Knoten an alle anderen benachbarten Knoten weiterverteilt. Der C&C-Server entfällt hier ganz, der Botmaster selbst kann sich innerhalb des Netzes als ebenfalls infizierter Hosts ausgeben und ist nicht eindeutig erkennbar. Bei der Nutzung von Anonymisierungsdiensten ist auch die Identifikation von üblichen C&C-Servern kaum möglich.

2.2. Einsatzmöglichkeiten

Botnetze eignen sich für verschiedene Einsatzszenarien, von denen vorliegen die wichtigsten aufgezeigt werden. Grundsätzlich erfolgt der Einsatz mit krimineller Motivation. Zu den Einsatzmöglichkeiten gehören insbesondere die bereits erwähnten DDoS-Angriffe, die sich meist gegen große Firmen, Banken und Medien-Dienstleister richten. Motive derartiger Angriffe sind in der Regel der Versuch einer Erpressung, Vergeltungsaktionen oder die gezielte Ausschaltung von Diensten, z.B. zur Unterdrückung von Informationen.
Viele Botnetze werden auch zum Versand von E-Mail-Werbung (SPAM) verwendet. Durch die Vielzahl vorhandener Systeme und daraus resultierend verschiedener IP-Adressen ist es möglich, Systeme zur Spambekämpfung zu umgehen. E-Mail-Provider nutzen in vielen Fällen sog. Blacklists, auf denen IP-Adressen von bekannten SPAM-Versendern gesammelt werden. Da vielen privaten Computersystemen bei der Interneteinwahl dynamisch IP-Adressen zugewiesen werden, tauchen diese nicht in den Blacklisten auf bzw. lassen sich nur nachträglich und unzuverlässig dort einpflegen.
Ein weiterer häufiger Einsatz von Botnetzen besteht in der Entwendung sensibler Daten. Hierbei wird die auf dem infizierten System installierte

Malware genutzt, um Benutzernamen und Passwörter, Bankdaten, E-Mails und ähnlich vertrauliche Informationen vom infizierten System zu entwenden.
Da durch den kriminellen Einsatzen von Botnetzen die IP-Adressen der Opfer in Netzwerk-Logs auftauchen können, drohen diesen unter Umständen weitere Folgen.

2.3. Bekämpfung von Botnetzen

Zur effektiven Bekämpfung von Botnetzen ist eine umfassende Informationslage über das zu bekämpfende Botnetz nötig. Verschiedene Einrichtungen wie Honeypots oder Spam-Traps sammeln gezielt Informationen, die sich mit Botnetzen in Zusammenhang bringen lassen. Eine weitere Möglichkeit zur Gewinnung von Informationen ist die Enumeration von Botnetzen, bei der Bots mit dem Botnetz eigenen Methoden nacheinander erfasst und katalogisiert werden.
Maßnahmen zur tatsächlichen Bekämpfung von Botnetzen unterscheiden sich in Umfang und Invasivität. Im praktischen Einsatz befinden sich meist Maßnahmen hemmenden Charakters. Hier sind verschiedene Formen des Blacklistings zu nennen: Die Auflösung von durch Botnetze genutzte Domainnamen wird durch die zuständigen DNS-Server verweigert, Firewalls bzw. Mailserver trennen Verbindungen zu IP-Adressen von zum Botnetz gehörenden Hosts. Eine Möglichkeit, DDoS-Attacken zu begegnen, ist das sog. Null-Routing, bei dem Datenverkehr, der von einem Botnetz zur Erzeugung einer Überlastsituation erzeugt wird, direkt an einem zwischen Angreifer und Opfer liegenden Router verworfen wird.
All diese hemmenden Maßnahmen haben gemeinsam, dass sie zwar geeignet sind, den Wirkungsgrad eines Botnetzes zu verringern. Das Botnetz besteht dadurch aber nach wie vor und ist in der Lage, auf die getroffenen Maßnahmen zu reagieren. Der Bestand des Botnetzes selbst kann bspw. durch den lokalen Einsatz von Anti-Virus-Software auf den infizierten Geräten angegangen werden, welche die das System kontrollierende Malware beseitigt. Dieses Vorgehen ist allerdings langwierig und umständlich, da zunächst alle Betroffenen identifiziert werden müssen, was im ersten Schritt der kompletten Enumeration der beteiligten Rechner, im zweiten Schritt der Identifikation der entsprechenden Besitzer bedarf. Darüber hinaus ist diese Maßnahme von der Mitarbeit der Betroffenen abhängig. Wird das Botnetz dabei nicht komplett entfernt, besteht die Gefahr einer erneuten Ausbreitung.
Die wohl effektivste Maßnahme zur Entfernung von Botnetzen ist die automatische Desinfektion. Hierbei sollen Mechanismen des Botnetzes zur Bekämpfung desselben genutzt werden: Über die Update-Funktionalität, mit deren Hilfe der Botmaster normalerweise Aktualisierungen für die Malware verteilt, wird durch Malware-Analysten ein speziell gefertigtes Update in das Botnetz eingespielt, welches die Malware dazu veranlasst, sich selbst vom infizierten System zu entfernen. Dies stellt die umfassende Beseitigung des Botnetzes sicher.

Trotz ihrer Effizienz ist die Desinfektion eine in der Praxis schwierig anzuwendende Maßnahme: Die hohe Invasivität sowie die größflächige Wirkung machen die Folgen einer Desinfektion schwer abschätzbar. Die Heterogenität der in der Regel von einem Botnetz betroffenen Systeme macht alle Eventualitäten berücksichtigende Testläufe desinfizierender Updates praktisch unmöglich. Aufgrund dieser Unsicherheit besteht die erhöhte Gefahr, Schäden an unbekannten Systemen mit nicht absehbaren Folgen zu verursachen, was auch die möglichen Konsequenzen für den die Desinfektion Durchführenden unabsehbar macht. Dies macht die hier vorgenommene Beleuchtung der rechtlichen Situation solcher Desinfektionsmaßnahmen notwendig.

3. Verpflichtung der Internet-Service-Provider zur Botnetzbekämpfung?

Von erhöhter Relevanz ist zunächst die Frage, ob den ISPs eine Pflicht zur Botnetz-bekämpfung zukommt. Eine derartige Pflicht könnte sich sowohl aus öffentlich-rechtlichen Normen als auch aus dem Vertrag mit dem jeweiligen Kunden ergeben.

3.1. Öffentlich-rechtliche Rahmenbedingungen

Die öffentlich-rechtlichen Rahmenbedingungen werden durch das Telekommunikationsgesetz (TKG) vorgegeben. Hier sind die §§ 88 ff. TKG, die sich dem Fernmeldegeheimnis, dem Datenschutz und der Öffentlichen Sicherheit widmen, von besonderer Bedeutung. § 109 TKG bezweckt die Sicherstellung, dass Telekommunikationsdienstleister angemessene Vorkehrungen zum Schutz vor unbefugten Zugriffen auf Daten und vor äußeren Störungen treffen. Zu diesen Störungen zählt auch die Infektion mit Malware als ein systemwidriger Eingriff[6]. Insbesondere § 109 Abs. 2 TKG definiert Sicherheitsanforderungen, denen Betreiber eines öffentlichen Telekommunikationsnetzes nachkommen müssen. Als Betrieb eines Telekommunikationsdienstes für die Öffentlichkeit gilt das gewerbliche Angebot von Übertragungswegen für beliebige natürliche und juristische Personen, also wenn nicht lediglich geschlossene Nutzergruppen den Telekommunikationsdienst nutzen können.[7] Somit unterliegen die ISPs den Pflichten aus § 109 Abs. 2 TKG. Entscheidend ist, dass eine Einrichtung oder ein System betroffen ist, das zum Angebot des Telekommunikationsdienstes genutzt wird.[8] Eine Pflicht zur Unterbindung jedweder Bedrohung, die mit Hilfe des Telekommunikationsnetzwerks verbreitet wird, ergibt sich aus der Norm hingegen nicht. Da Botnetze die Telekommunikationsanlagen und den durch sie gewährleisteten Datenfluss durch eine gezielte Überlastung des Netzes hemmen

6 Zum Begriff des systemwidrigen Eingriffs *Bock,* in: Beck'scher TKG-Kommentar, 4. Aufl. (2013), § 109 Rn. 33.
7 Ebd., § 109 Rn. 31.
8 *Graulich,* in: Arndt/Fetzer/Scherer, TKG: Telekommunikationsgesetz Kommentar, 2008, § 109 Rn. 9.

können, muss eine Pflicht zur Bekämpfung von Botnetzen aus § 109 Abs. 2 TKG abgeleitet werden.

3.2. Vertragsrechtliche Aspekte

Fraglich ist, inwiefern sich aus dem zwischen ISP und Kunden bestehenden Access-Provider-Vertrag, der nach h.M. in Rechtsprechung und Literatur als Dienstvertrag im Sinne der §§ 611 ff. BGB einzuordnen ist,[9] eine Pflicht zur Bekämpfung von Botnetzen ergibt. Als jeweilige Hauptleistungspflicht stehen die Zugangsgewährung zum Internet entsprechend den vertraglichen Bestimmungen durch den ISP und die (in der Regel monatliche) Zahlung des vereinbarten Entgelts durch den Kunden im Synallagma.[10] § 241 Abs. 2 BGB statuiert im vertraglichen Bereich Neben- und Schutzpflichten für die Vertragsparteien. Anerkannt ist, dass den ISP die Schutzpflicht zur Gewährleistung einer ausreichenden Datensicherheit gegenüber seinen Vertragskunden trifft.[11] Das bedeutet, dass der ISP dem Stand der Technik entsprechende Vorkehrungen gegenüber Gefahrenquellen durch die Zugangsgewährung zum Internet auf die er Einfluss hat, treffen muss. Hierzu zählen insbesondere die Abwehr von Hacker-Angriffen und DDoS-Attacken sowie der Einsatz von Spamfiltern.[12] Entsprechend den Einsatzmöglichkeiten von Botnetzen und dem Streben nach präventiven Maßnahmen ergibt sich daraus, dass ebenfalls Maßnahmen gegen Botnetze zu treffen sind, da über Botnetze DDoS-Attacken und Spamkampagnen gesteuert werden können. In Ausnahmefällen kann der ISP im Rahmen von Sicherheitsmaßnahmen den Kunden vom Zugang zum Internet trennen, ohne sich schadensersatzpflichtig zu machen. Derartige Einschränkungen der Hauptleistungspflicht können über die in den Allgemeinen Geschäftsbedingungen enthaltenen Verfügbarkeits- sowie Störungsbeseitigungsklauseln gerechtfertigt werden.[13]

Zu beachten ist, dass den Kunden im Gegenzug die Nebenpflicht trifft, rechtswidrige Nutzungen des ihm zur Verfügung gestellten Internetzugangs zu unterlassen und den Anbieter nicht zu schädigen.[14] Unter einer solchen Schädigung ist auch die Verbreitung von Malware zum Ausbau eines Botnetzes zu fassen. Um Maßnahmen gegen den aktiven Störer, der bewusst Malware verbreitet und/oder aktiver Teil eines Botnetzes ist, zu ermöglichen, sehen die

9 Für die Praxis entschieden durch *BGH*, NJW 2005, 2076.

10 *Hoeren,* in: Graf von Westphalen, Vertragsrecht und AGB-Klauselwerke, 31. Aufl. (2012), Kapitel: E-Commerce-Verträge, Rn. 10 ff.

11 *Schmitz/von Netzer,* in: Schuster, Vertragshandbuch Telemedia, 2001, Kapitel 12 Rn. 21.

12 *Redeker*, in: Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, 32. Aufl. (2012), Teil 12 Rn. 102; *Spindler*, Vertragsrecht der Internetprovider, 2. Aufl. (2004), Teil IV Rn. 81.

13 Siehe dazu *Hoeren,* in: Graf von Westphalen, (o. Fußn. 10), Kapitel: E-Commerce-Verträge, Rn. 11 ff. Diese müssen freilich den allgemeinen Anforderungen der §§ 305 ff. BGB genügen.

14 *Schmitz/von Netzer,* in: Schuster, (o. Fußn. 11), Kapitel 12 Rn. 24.

Allgemeinen Geschäftsbedingungen der Access-Provider häufig Sperr- und Verdachtsklauseln vor.[15]

4. Haftungsrisiken bei der Botnetzbekämpfung durch Desinfektion

Als wohl effektivste Methode zur Bekämpfung eines entdeckten Botnetzwerkes ist die (automatische) Desinfektion infizierter Systeme anzuführen. Bei Desinfektionsmaßnahmen ergeben sich zwei maßgebliche Problemfelder: Zunächst kann durch die Verbreitung des Botnetzes auf Systemen unterschiedlichster Beschaffenheit die genaue Wirkung des desinfizierenden Updates nicht mit absoluter Sicherheit vorhergesagt werden. Erschwerend tritt hinzu, dass auch Bestandteile kritischer Infrastrukturen in das Botnetz integriert sein könnten.

4.1. Zivilrechtliche Risiken

In zivilrechtlicher Hinsicht sähe sich der ISP im Fall des Schadenseintritts Schadensersatzansprüchen ausgesetzt. Es ist danach zu unterscheiden, ob der ISP mit dem Geschädigten in einem vertraglichen Verhältnis steht oder nicht. Im Falle des Bestehens eines Access-Provider-Vertrages ergibt sich ein Anspruch aus §§ 280 Abs. 1, 241 Abs. 2 BGB. Gegenüber Geschädigten, zu denen der ISP kein vertragliches Verhältnis pflegt, erwachsen dem Betroffenen Ansprüche deliktsrechtlicher Natur, insbesondere also aus § 823 Abs. 1 BGB sowie aus § 823 Abs. 2 BGB i.V.m. einem (strafrechtlichen) Schutzgesetz.

4.1.1. Betroffene Rechtsgüter und Zurechnung

Welche Rechtsgüter durch eine Desinfektion tangiert sind, spielt eine wichtige Rolle für die Frage, ob der Schutzbereich des § 823 Abs. 1 BGB mit den umfassten absoluten und ihnen gleichzustellenden Rechten betroffen ist. Auch auf Rechtsfolgenseite erscheint es maßgeblich, welche Rechtsgüter betroffen sein können, um eine effektive Risikoanalyse durchzuführen. Als problematischer Faktor stellt sich vor allem die Unvorhersehbarkeit der Folgen dar, die durch eine Desinfektionsmaßnahme ausgelöst werden können.

Denkbar sind insbesondere Hard- und Softwareschäden, aber auch die Beschädigung von Daten, die in dem betroffenen System gespeichert sind. Möglich sind auch Folgeschäden. Bei Betroffenheit einer Anlage, über die kritische Infrastrukturen kontrolliert werden, kann sogar die Tötung von Menschen nicht ausgeschlossen werden.

Das weite Spektrum an betroffenen Rechtsgütern bedingt, dass mehrere absolute Rechtsgüter berührt sein können. In erster Linie kann es zu Beeinträchtigungen des Rechtsguts Eigentum kommen, von dem sowohl Einwirkungen auf die Sachsubstanz als auch die bloße Beeinträchtigung der

15 Ein Beispiel findet sich in den Allgemeinen Geschäftsbedingungen für Access-Verträge der Unitymedia NRW GmbH unter 3.2.

Nutzungsmöglichkeit erfasst sind.[16] Die Veränderung oder Löschung von Daten, die durch die Magnetisierung auf Speichermedien wie etwa einer Festplatte gespeichert sind, wird weit überwiegend als Eigentumsverletzung – und damit als von § 823 Abs. 1 BGB erfasst – angesehen.[17] Die Verletzung der Rechtsgüter Leben, Körper und Gesundheit in Folge einer (fehlerhaften) Desinfektion kann ebenfalls nicht ausgeschlossen werden. In Erwägung zu ziehen sind auch das als „sonstiges Recht" anerkannte Recht am eingerichteten und ausgeübten Gewerbebetrieb und das allgemeine Persönlichkeitsrecht. Ein Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb wird allerdings an dem Erfordernis der Betriebsbezogenheit scheitern. Dazu müsste die Maßnahme nämlich die Zielrichtung inne haben, gerade in den Betrieb und seine Organisation einzugreifen. Der ISP – in der Regel auch ohne Kenntnis darüber, wer betroffen sein könnte – würde jedoch die Desinfektion vornehmen, um die Risiken durch ein bestehendes Botnetz einzudämmen, aber nicht um ein von Malware betroffenes Unternehmen zu beeinträchtigen. Das allgemeine Persönlichkeitsrecht steht neben natürlichen auch juristischen Personen zu.[18] Daten und deren Offenlegung sind von dem Schutz erfasst: Entsteht also infolge der Desinfektion ein Datenleck, bei dem sensible persönliche Daten von Individuen oder kritische Unternehmensinterna an die Öffentlichkeit gelangen, liegt zumindest ein Eingriff vor. Ob dieser dann allerdings rechtswidrig ist, muss in einem weiteren Schritt auf der Ebene der Widerrechtlichkeit ermittelt werden. Diese Güter- und Interessenabwägung kann allerdings nur anhand des Einzelfalls vorgenommen werden, wobei dem Gefahrengrad, der durch das Botnetz ausgeht, und der Rechtssphäre der betroffenen Daten besondere Berücksichtigung zugemessen werden muss.

Fraglich ist, inwieweit eine Zurechnung im Fall des Schadenseintritts reicht. Die Rechtsprechung wendet dabei die Adäquanztheorie an, nach der die Ursache im Allgemeinen und nicht nur unter besonders eigenartigen, unwahrscheinlichen und nach dem gewöhnlichen Verlauf der Dinge außer Betracht zu lassenden Umständen geeignet sein muss, einen Erfolg dieser Art herbeizuführen.[19] Da sogar bekannt ist, dass selbst kritische Infrastrukturen betroffen sein könnten, ist eine enorm hohe Anzahl an Szenarien und Schadensfolgen denkbar. Im Einzelfall kann sich der schädigende ISP u.U. auf eine hypothetische Kausalität berufen, also einwenden, dass der Schaden auch auf Grund des Botnetzes eingetreten wäre. Rechtssicherheit bietet dies aber nicht.

16 *Schiemann*, in: Erman, BGB, 13. Aufl. (2011), § 823 Rn. 25.

17 Zuletzt *OLG Oldenburg*, ZD 2012, 177. Ferner *OLG Karlsruhe*, NJW 1996, 200, 201; *LG Kaiserslautern*, DAR 2001, 225; *Bartsch*, CR 2000, 721, 723; *Koch*, NJW 2004, 801, 802; *Leible/Sosnitza*, K&R 2002, 51, 52; *Libertus*, MMR 2005, 507, 508; *Meier/Wehlau*, NJW 1998, 1585, 1588.

18 *Sprau*, in: Palandt, BGB, 71. Aufl. (2012), § 823 Rn. 87 - 92.

19 Ständige Rechtsprechung: *BGH*, NJW 1953, 700; 1972, 36; 1995, 126, 127; 1998, 138; 2002, 2232, 2233.

4.1.2. Verschulden des ISP

Der ISP muss die Nebenpflichtverletzung bzw. die Verletzung eines Rechtsguts zu vertreten haben. Dabei gilt nach § 276 Abs. 1 Satz 1 BGB, dass der Schuldner Vorsatz und Fahrlässigkeit zu vertreten hat. Im Rahmen von vertraglichen Schadensersatzansprüchen ordnet § 280 Abs. 1 Satz 2 BGB eine gesetzliche Vermutung dahingehend an, dass der Schuldner die Pflichtverletzung zu vertreten hat, sodass sich der ISP exkulpieren müsste.[20] Gleiches gilt für § 831 Abs. 1 Satz 1 BGB, aus dem sich ebenfalls eine Haftung ergeben kann. Bei dem deliktischen Anspruch aus § 823 Abs. 1 BGB ist das Verschulden hingegen nachzuweisen. Da der ISP als juristische Person selber nicht handeln kann, findet jeweils eine Zurechnung statt, die sich für vertragliche Ansprüche aus § 278 BGB und § 31 BGB analog bzw. bei deliktischen Ansprüchen aus § 31 BGB analog oder durch § 831 Abs. 1 Satz 1 BGB ergibt.[21]

Nachgegangen werden muss der Frage, ob Fahrlässigkeit oder Vorsatz vorlagen. Vor allem im Verhältnis des ISP zu seinen Kunden spielt dies eine Rolle, da dem Vertrag Allgemeine Geschäftsbedingungen zugrunde liegen, die regelmäßig eine Haftungsbegrenzung auf Vorsatz und grobe Fahrlässigkeit in den Grenzen des § 309 Nr. 7 lit. b BGB im Fall eines etwaigen Schadenseintritts vorsehen.[22]
Ein vorsätzliches Handeln verlangt das Wissen und Wollen des Eintritts der objektiven Tatbestandsmerkmale.[23] Das Wissenselement gilt dabei dann als erfüllt, wenn der Handelnde den Eintritt des Erfolges auf Grund seines eigenen Verhaltens für möglich hält.[24] Ein Schadenseintritt wird dabei selbst dann als erkannt und gewollt qualifiziert, wenn der Kausalverlauf zwar vom intendierten abweicht, sich jedoch noch im Rahmen des Denkbaren hält und keine andere Bewertung der Tat angezeigt ist.[25] Sofern der Desinfizierende darum weiß, dass sein Handeln zu einem Schadenseintritt führen kann, ist das Wissenselement zu bejahen. Lediglich völlig unabsehbare Folgen würden das Wissenselement ausscheiden lassen. Da aber die Gefährdung kritischer Infrastrukturen nach derzeitigem Stand der Forschung ebenfalls nicht ausgeschlossen werden kann, dürfte selbst dieses Ausschlusskriterium nicht greifen. Das Willenselement verlangt, dass die handelnde Person mit dem für möglich gehaltenen Schadenseintritt einverstanden sein oder ihn wenigstens billigend in Kauf nehmen muss, wobei schon Gleichgültigkeit gegenüber dem nicht für

20 Dazu *Ernst,* in: Münchener Kommentar BGB II, 6. Aufl. (2012), § 280 Rn. 31.

21 Auf eine genaue Abgrenzung und Beleuchtung der Unterschiede innerhalb der Hierarchie eines Unternehmens muss an dieser Stelle verzichtet werden.

22 Siehe nur Allgemeine Geschäftsbedingungen der Telekom Deutschland GmbH „Call & Surf Basic, Comfort und Comfort Plus“ unter 10.

23 *BGH*, NJW 1965, 962, 963.

24 *Grundmann,* in: Münchener Kommentar, (o. Fußn. 20), § 276 Rn. 155 f.

25 *BGH*, NJW 1951, 596, 597; 1963, 148, 150; 1971, 459, 461.

unwahrscheinlich gehaltenen Erfolg genügt.[26] An diesem Punkt verläuft die Grenze zur bewussten Fahrlässigkeit, die gegeben ist, wenn auf den Nichteintritt des Schadens und die Möglichkeit der Abwendung berechtigterweise vertraut wurde. Damit ist festzuhalten, dass eine Maßnahme nur im Einzelfall unter Berücksichtigung der realistischen Erfolgschancen abschließend beurteilt werden kann. Kann allerdings überhaupt keine Risikoanalyse der Desinfektionsmaßnahme vorgenommen werden, kann auch kein Worst-Case-Szenario ausgeschlossen werden. Damit dürfte regelmäßig Vorsatz gegeben sein.

In technischer Hinsicht sollte also an Lösungen gearbeitet werden, mit deren Hilfe das Gefahrenpotenzial überschaubarer gemacht werden kann. Bei der Möglichkeit einer gewissenhaften Prüfung und ihrem positiven Ergebnis können Vorsatz und grobe Fahrlässigkeit dann u.U. entfallen.

4.1.3. Mitverschulden

Eine andere rechtliche Frage besteht darin, ob dem von der Desinfektion Betroffenen unter bestimmten Umständen im Fall des Schadenseintritts ein Mitverschulden nach § 254 Abs. 1 BGB angelastet werden muss. Verschulden i.S.d. § 254 Abs. 1 BGB bedeutet, dass eine vorwerfbarer Verstoß gegen Gebote des eigenen Interesses besteht, mithin ein „Verschulden gegen sich selbst“[27].[28] Bei der Infektion mit einem Bot ist der Anknüpfungspunkt das Unterlassen der Einrichtung und Nutzung abwehrender Mittel wie etwa von Anti-Viren-Programmen, Firewalls oder sicheren Browsern. Festgestellt werden muss jedenfalls, dass jedem Nutzer bekannt sein sollte, dass das Internet kein gefahrenfreier Raum ist.[29] Konsequenterweise ist damit auch zu verlangen, dass mittlerweile jeder Nutzer ein Anti-Viren-Programm auf seinem Computer installiert hat, das er in angemessenen Abständen auf seine Aktualität hin überprüft. Ferner erwartet werden darf, dass sich der Nutzer in gewissem Maße informiert, also aktuelles Tagesgeschehen zumindest nicht ignoriert. Wird medienwirksam vor bestimmten Sicherheitslücken gewarnt, infiziert sich ein Nutzer über einen solchen Verbreitungsweg und findet in der Folge eine Desinfektion mit Schadensfolgen statt, die diese gefährliche Malware beseitigen will, kann ein Mitverschulden des Nutzers angenommen werden. Dennoch dürften Beweisschwierigkeiten bestehen, wann und wie sich der Nutzer mit der Malware infiziert hat. Der *BGH* hat sich bis dato lediglich in der sog. Dialer-

26 *Grundmann,* in: Münchener Kommentar (o. Fußn. 20), § 276 Rn. 161 m.w.N. aus der Rechtsprechung des BGH.

27 Zuletzt *BGH*, NJW 2009, 582, 585.

28 *Grüneberg*, in: Palandt, (o. Fußn. 18), § 254 Rn. 1.

29 Man denke nur an die umfangreiche Berichterstattung über die Sicherheitslücke des Windows Internet Explorers im September 2012.

Entscheidung[30] mit Selbstschutzpflichten im Internet befasst. Hierbei kam er zu der nutzerfreundlichen These, dass auf ein Ausbleiben des Angriffs durch einen Dialer vertraut werden dürfe. Ob sich dies auf andere Gefahren bei der Nutzung des Internets und im Übrigen auch ein Jahrzehnt später noch vertreten lässt, erscheint fraglich und vom jeweiligen Einzelfall abhängig. Bei einem Datenverlust kann zudem ein Mitverschulden in der Tatsache gesehen werden, dass über einen unverhältnismäßig langen Zeitraum keine Datensicherung erfolgte.[31] Im Falle des Schadenseintritts kann es also unter bestimmten Umständen durch ein Mitverschulden des Nutzers zu einer Minderung der Anspruchshöhe kommen.

4.2. Strafrechtliche Risiken

Bei der Durchführung von Desinfektionsmaßnahmen stellt sich für die ISPs und deren Mitarbeiter neben der Frage einer zivilrechtlichen Haftung auch die Frage nach einer strafrechtlichen Haftung. Entscheidend für eine strafrechtliche Beurteilung ist der im Rahmen der Desinfektion entstandene Schaden und dessen Entstehung. Auch ist für eine strafrechtliche Bewertung bedeutend, bei wem Schäden oder Rechtsgutverletzungen auftreten. Als mögliche Opfer kommen zum einen die Inhaber der infizierten IT-Systeme in Betracht, bei denen die Desinfektionsmaßnahmen durchgeführt werden. Unter Umständen können aber auch unbeteiligte Dritte durch die Desinfektionsmaßnahmen betroffen sein. Werden z.B. Desinfektionsmaßnahmen an kritischen Infrastrukturen vorgenommen, können Schäden an IT-Systemen Dritter und deren Rechtsgütern entstehen. Nachfolgend werden nun mögliche Tatbestände erläutert, die bei der Durchführung von Desinfektionsmaßnahmen von Bedeutung sein könnten. Der Schwerpunkt der Untersuchung liegt hierbei auf computerstrafrechtlichen Tatbeständen.

4.2.1. Relevante Straftatbestände

Zunächst ist an eine Strafbarkeit aus § 202a StGB (Ausspähen von Daten) zu denken. Im Strafrecht ist von einem weiten Datenbegriff auszugehen, der von § 202a Abs. 2 StGB eingeschränkt wird.[32] Daten im Sinne des § 202a Abs. 1 StGB sind danach nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

Nicht unmittelbar wahrnehmbar bedeutet, dass die Daten erst nach einer entsprechenden technischen Umformung sichtbar oder hörbar sein dürfen.[33] Die rechtliche Hürde, die für eine Strafbarkeit nach § 202a StGB besteht und

30 *BGH*, MMR 2004, 308. Dialer sind Einwahlprogramme, die eine Wählverbindung mit dem Internet oder Rechnernetzen herstellen können und durch ihren vom Anschlussinhaber ungewollten und unbemerkten Einsatz in der Lage sind, Schädigungen herbeizuführen.

31 Eingehend zu Datensicherungspflichten *Hoeren,* in: Graf von Westphalen, (o. Fußn. 10), Kapitel: IT-Verträge, Rn. 84 ff. Ebenfalls beachtenswert *OLG Karlsruhe*, NJW 1996, 200, 201 f.

32 *Fischer*, Strafgesetzbuch: StGB, 60. Aufl. (2013), § 202a Rn. 3; *Lenckner/Eisele* in: Schönke/Schröder, Strafgesetzbuch: StGB Kommentar, 28. Aufl. (2010), § 202a Rn. 3.

33 *Lenckner/Eisele,* in: Schönke/Schröder, (o. Fußn. 32), § 202a Rn. 4.

vom Täter überwunden werden muss, ist recht niedrig: Bereits das Verschaffen des bloßen Zugangs zu den Daten reicht aus, um eine Strafbarkeit nach dieser Norm zu begründen. Es genügt, dass der Täter bestehende Sicherheitseinrichtungen überwindet. Eine Kenntnisnahme der Daten durch den Täter ist nicht notwendig.[34] Dies bedeutet, dass auch das „reine Hacking" von § 202a StGB erfasst wird.[35] Hierzu zählt etwa der Einsatz von Trojanern, Sniffern oder Backdoorprogrammen, die der Aufzeichnung von Vorgängen auf dem Rechner, dem Ausspähen von Daten oder gar der gezielten Steuerungen des infizierten Rechners dienen.[36] Auf Grund dieser niedrigen Hürde liegt eine Erfüllung des objektiven Tatbestandes von § 202a StGB bei der Durchführung von Desinfektionsmaßnahmen nahe. In bestimmten Fällen kann eine Desinfektion so durchgeführt werden, dass der Anwender der Desinfektionsmaßnahme selbst keine Zugangssicherung überwinden muss, um Zugriff auf fremde Rechnersysteme zu erhalten. Stattdessen wird der Zugang, den der Angreifer mit dem Bot geschaffen hat, genutzt, um den Bot zu beobachten und zu bekämpfen. Eine Strafbarkeit nach § 202a StGB dürfte daher in diesen Fällen ausscheiden, da die Zugangssicherung auf Grund des eingeschleusten Bots bereits überwunden ist und der Zugang zu fremden Daten durch den Anwender nicht unter Überwindung der Zugangssicherung erfolgt. Die Überwindung der Zugangssicherung muss für die Verschaffung des Zugangs jedoch ursächlich sein, um eine Strafbarkeit nach § 202a StGB begründen zu können.[37] Außerdem muss die Zugangssicherung zum Zeitpunkt der Tathandlung wirksam sein.[38] An diesen Erfordernissen dürfte es in dem aufgegriffenen Szenario fehlen.

Bei der Durchführung von Desinfektionsmaßnahmen besteht zudem die Gefahr einer Verwirklichung von § 202b StGB (Abfangen von Daten). Entscheidend für eine Strafbarkeit nach § 202b StGB ist die konkrete Maßnahme und deren technische Vorgehensweise. Werden bei der Durchführung z.B. Dateien kopiert oder umgeleitet, so kann eine Strafbarkeit aus § 202b StGB bestehen. In den Anwendungsbereich von § 202b StGB fallen nur Daten, die sich zum Zeitpunkt der Tat in einem Übertragungsvorgang befinden.[39] Gespeicherte Daten, die früher übermittelt wurden, werden hingegen nicht von § 202b StGB erfasst.[40]

Ferner liegt bei der Durchführung von Desinfektionsmaßnahmen die Verwirklichung des Tatbestandes aus § 303a Abs. 1 StGB (Datenveränderung) nahe. Diese Gefahr besteht insbesondere dann, wenn durch die Maßnahme

34 *Lenckner/Eisele,* in: Schönke/Schröder, (o. Fußn. 32), § 202a Rn. 10.

35 *Ernst*, NJW 2007, 2661.

36 *Fischer*, (o. Fußn. 32), § 202a Rn. 10; *Lenckner/Eisele* in: Schönke/Schröder, (o. Fußn. 32), § 202a Rn. 3.

37 *Fischer*, (o. Fußn. 32), § 202a Rn. 11b; *Lenckner/Eisele* in: Schönke/Schröder, (o. Fußn. 32), § 202a Rn. 10a.

38 *Lenckner/Eisele* in: Schönke/Schröder, (o. Fußn. 32), § 202a Rn. 10a.

39 *Eisele,* in: Schönke/Schröder, (o. Fußn. 32), § 202b Rn. 3.

40 *Eisele,* in: Schönke/Schröder, (o. Fußn. 32), § 202b Rn. 3.

Daten gelöscht werden sollten. Eine besondere Zugangssicherung ist für die Erfüllung von § 303a StGB nicht notwendig. § 303a StGB erfasst die „virtuelle Sachbeschädigung“ und dient dem Schutz des Interesses des Verfügungsberechtigten am Zustand seiner Daten, deren unversehrte Verwendungsmöglichkeit und der in ihnen enthaltenen Informationen.[41]

Auch besteht die Möglichkeit einer Strafbarkeit nach § 303b Abs. 1 StGB (Computersabotage). Neben dem Qualifikationstatbestand aus § 303b Abs. 1 Nr. 1 StGB zu § 303a StGB kommt als Verletzungshandlung auch eine Tathandlung nach § 303b Abs. 1 Nr. 3 StGB in Betracht, wenn es im Rahmen der Desinfektionsmaßnahme zu Hardwareschäden kommen sollte. § 303b Abs. 1 Nr. 3 StGB erfasst Fälle, in denen eine erhebliche Störung der Datenverarbeitung durch das Zerstören, Beschädigen, Unbrauchbarmachen, Beseitigen oder Verändern einer Datenverarbeitungsanlage oder eines Datenträgers erfolgt. Als Datenträger kommen insbesondere Magnetbänder, Festplatten, CD-ROMs und Disketten in Betracht.[42] Eine Strafbarkeit aus § 303b Abs. 1 Nr. 2 StGB dürfte jedoch bei der Durchführung von Desinfektionsmaßnahmen zu verneinen sein, da der Täter in diesen Fällen nicht in Nachteilszufügungsabsicht handeln wird. Eine Strafbarkeit nach § 303b Abs. 1 StGB setzt eine erhebliche Störung der Datenverarbeitung voraus. Für eine erhebliche Störung ist bereits ausreichend, wenn ein einziger sonst möglicher Datenverarbeitungsvorgang nicht in bisheriger Form durchführbar ist.[43] Lässt sich hingegen eine Beeinträchtigung ohne großen Aufwand an Zeit, Mühe und Kosten beheben, so liegt lediglich eine unerhebliche Störung vor.[44] Durch die Beschränkung des § 303b Abs. 1 StGB auf Fälle „von wesentlicher Bedeutung“ sollen Bagatellfälle von der Norm ausgeschlossen werden.[45]

Die Erfüllung weiterer Straftatbestände ist ebenfalls denkbar. So könnte es durch den Ausfall von IT-System zu Personenschäden kommen, sodass Straftatbestände, die den Schutz des Lebens bzw. der körperlichen Unversehrtheit bezwecken, einschlägig sein können. Sollten durch die Desinfektionsmaßnahmen bspw. E-Mails gelöscht werden, ist auch eine Strafbarkeit wegen Verletzung des Post- oder Fernmeldegeheimnisses aus § 206 Abs. 2 Nr. 2 StGB möglich.

4.2.2. Kausalität und objetive Zurechnung

Neben der Erfüllung der Tatbestandsmerkmale erfordert eine Strafbarkeit auch, dass der Täter den tatbestandlichen Erfolg durch die Handlung verursacht hat

41 *Ernst*, NJW 2007, 2661, 2664.

42 *Fischer*, (o. Fußn. 32), § 303b Rn. 13.

43 *Stree/Hecker,* in: Schönke/Schröder, (o. Fußn. 32), § 303b Rn. 9.

44 *Stree/Hecker,* in: Schönke/Schröder, (o. Fußn. 32), § 303b Rn. 9.

45 *Kühl,* in: Lackner/Kühl, Strafgesetzbuch: StGB Kommentar, 27. Aufl. (2011), § 303b Rn. 2.

und ihm der Erfolg zuzurechnen ist. Im Einzelfall kann eine objektive Zurechnung ausscheiden, wenn Desinfektionsmaßnahmen durchgeführt werden. So ist der Erfolg dann nicht zurechenbar, wenn der Täter diesen durch das Eingreifen in den Kausalablauf in seiner konkreten Gestalt zwar beeinflusst, jedoch dabei den drohenden (schwereren) Erfolg abmildert oder ein zeitliches Hinausschieben seines Eintritts bewirkt.[46] Wird durch die Desinfektionsmaßnahme ein größerer Schaden für den Betroffenen verhindert, so kann es an einer solchen Zurechnung mangeln. In diesem Falle können ggf. auch Rechtfertigungsgründe zugunsten des Täters eingreifen und eine Strafbarkeit ausschließen. Eine Zurechnung des tatbestandlichen Erfolges liegt aber dann vor, wenn der Täter zwar durch sein Handeln eine konkrete Gefahr abwendet, dabei jedoch eine neue eigenständige (rechtlich relevante) Gefahr begründet, die sich in dem von ihm verursachten Verletzungserfolg niederschlägt.[47]

4.2.3. Vorsatz

Eine weitere bedeutsame Frage im Zusammenhang mit einer strafrechtlichen Haftung ist die Frage nach dem Bestehen des Vorsatzes. Eine Strafbarkeit wegen Fahrlässigkeit muss in der Strafnorm ausdrücklich festgelegt sein (vgl. § 15 StGB). So ist für bestimmte Straftatbestände – so auch für die erwähnten §§ 202a, 202b, 303a, 303b StGB – ein vorsätzliches Handeln für eine Strafbarkeit erforderlich. Bei der Durchführung von Desinfektionsmaßnahmen kann die Abgrenzung des bedingten Vorsatzes von der bewussten Fahrlässigkeit entscheidend für eine Strafbarkeit sein. Denn derjenige, der eine Desinfektion durchführt, wird nicht in Schädigungsabsicht handeln und auch keine Schäden an fremden Rechtsgütern verursachen wollen. Bzgl. der Anforderungen, die zur Annahme eines Vorsatzes erfüllt sein müssen, kann auf die Ausführungen unter 4.1.2. zu den zivilrechtlichen Haftungsrisiken verwiesen werden.

Kriterien zur Abgrenzung des bedingten Vorsatzes von der bewussten Fahrlässigkeit können die Offensichtlichkeit der Tatbestandsverwirklichung, die Gefährlichkeit oder auch die getroffenen Vorkehrungen zur Gefahrvermeidung sein.[48] Daher sollte vor einer Anwendung der Desinfektionsmaßnahmen geprüft werden, wie anfällig das Verfahren bei Probedurchläufen war und welche Schäden hierbei aufgetreten sind. Insgesamt dürfte Vorsatz bei der Anwendung von Desinfektionsmaßnahmen naheliegen, wenn die Verletzung fremder Rechtsgüter nicht ausgeschlossen werden kann. Hält der Täter die Wahrscheinlichkeit eines strafbaren Erfolgseintritts für gering, weil er etwa Vorsichtsmaßnahmen getroffen hat und deshalb davon ausgeht, dass „schon

46 *Lenckner/Eisele,* in: Schönke/Schröder, (o. Fußn. 32), Vorbem. § 13 Rn. 94.

47 *Lenckner/Eisele,* in: Schönke/Schröder, (o. Fußn. 32), Vorbem. § 13 Rn. 94.

48 *Sieber,* in: Hoeren/Sieber/Holznagel, (o. Fußn. 12), Teil 19 Rn. 83.

alles gut gehen werde“, liegt in der Regel aber nur bewusste Fahrlässigkeit vor.[49]

4.2.4. Ergebnis

Insgesamt ist festzuhalten, dass die Durchführung von Desinfektionsmaßnahmen die Gefahr einer strafrechtlichen Haftung in sich birgt. Die Frage nach einem möglichen Vorsatz spielt hierbei eine wichtige Rolle. Um die Gefahr einer strafrechtlichen Inanspruchnahme zu minimieren, sollte daher im Vorfeld, bspw. durch Testläufe, geprüft werden, ob Schäden an Rechtsgütern eintreten werden und wie hoch das entsprechende Riskio des Eintritts einer Rechtsgutverletzung ist. Eine Strafbarkeit kann zudem in Ausnahmefällen ausscheiden, falls Rechtfertigungsgründe eingreifen sollten.

4.3. Rechtfertigung im Fall des Schadenseintritts

Die hohen haftungsrechtlichen Risiken in zivil- und strafrechtlicher Sicht eröffnen die Frage, ob eine Desinfektionsmaßnahme einer Rechtfertigung zugänglich ist. So entfiele im Falle der Rechtfertigung im Rahmen der deliktischen Ansprüche die Rechtswidrigkeit ebenso wie die Rechtswidrigkeit etwaiger verwirklichter Straftatbestände. Die aus dem Strafrecht bekannten Rechtfertigungsgründe sind auch im Zivilrecht anerkannt[50] und umgekehrt. Betont werden muss allerdings, dass vertragliche Schadensersatzansprüche nicht gerechtfertigt werden können, sodass Kunden des ISP – im Falle des Schadenseintritts – stets der vertragliche Anspruch bliebe. Bei Dritten, denen keine vertraglichen Ansprüche zustehen, wäre dies dann anders.

4.3.1. Nothilfe

Zunächst ist an den Rechtfertigungsgrund der Notwehr bzw. Nothilfe zu denken. Eine Desinfektionsmaßnahme könnte eine Nothilfe darstellen, da sie dazu dient, dass der befallene Rechner von dem Botnetz befreit und somit nicht mehr rechtswidrig missbraucht wird sowie lokale Daten gesichert werden. Jedoch kann über § 32 StGB lediglich eine Handlung gerechtfertigt werden, die sich gegen den Angreifer richtet. Eingriffe in die Rechte Dritter sind nicht umfasst. Im Fall der Nutzung fremder Gegenstände, kann eine Beschädigung vielmehr über die §§ 228, 904 BGB gerechtfertigt werden.[51]

4.3.2. Regeln des rechtfertigenden Notstands

Eigentumsschäden, die bei der Desinfektion entstehen, könnten möglicherweise auch durch § 228 BGB oder § 904 BGB gerechtfertigt werden, die als Spezialvorschriften der allgemeinen Regelung des rechtfertigenden Notstands in § 34 StGB vorgehen.[52] Für Schäden, die nicht bloß fremde Sachen betreffen,

---

49 *Sieber,* in: Hoeren/Sieber/Holznagel, (o. Fußn. 12), Teil 19 Rn. 83.

50 *Wagner,* in: Münchener Kommentar BGB V, 6. Aufl. (2013), § 823 Rn. 314.

51 *Fischer*, (o. Fußn. 32), § 32 Rn. 24.

52 Ganz h.M., siehe *Erb,* in Münchener Kommentar StGB I, 2. Aufl. (2011), § 34 Rn. 14; *Fischer*, (o. Fußn. 32), § 34 Rn. 22; *Günther,* in: Wolter, Systematischer Kommentar zum Strafgesetzbuch: SK-StGB, 2012, § 34 Rn.

bleibt § 34 StGB anwendbar. Richtigerweise muss unterschieden werden, ob die Gefahr von der Sache selbst im Sinne einer unmittelbaren Kausalität ausgeht (dann § 228 BGB) oder die Gefährdung nur mittelbar von der Sache ausgeht (dann § 904 BGB).[53] Die infizierten Computersysteme stellen selbst nicht den Ursprung der Gefahr dar, sondern vielmehr das Verhalten desjenigen, der das Botnetz unterhält und steuert. Er ist in der Lage, den infizierten Rechner als Teil des Botnetzes einzusetzen. Somit ist § 904 BGB anwendbar, der inhaltlich eine Duldungspflicht des Eigentümers begründet, obwohl von ihm selbst kein rechtswidriger Angriff ausgeht.[54]

§ 904 BGB verlangt zunächst, dass eine Notstandslage besteht, also eine gegenwärtige Gefahr vorliegt. Für eine Gefahr muss aus objektiver Sicht (ex ante) der Eintritt eines Schadens nicht nur als möglich, sondern als nahe liegend erscheinen.[55] Zu den Schäden, die durch Botnetze verursacht werden können, sind insbesondere Vermögensschäden durch mögliche DDoS-Attacken, Spamkampagnen oder die unbefugte Nutzung ausspionierter Daten und Eigentumsschäden durch die Löschung lokaler Daten[56] zu zählen. Ist der Rechner erst einmal mit Malware infiziert, lässt er sich bei bestehender Internetverbindung jederzeit zu missbräuchlichen Zwecken einsetzen oder lassen sich die in seinem System abgelegten sensiblen Daten ausspionieren. Damit ist sofortige Abhilfe notwendig und auch die Gegenwärtigkeit zu bejahen. Es liegt dann eine dauerhafte Gefahr vor. Auf ein Verschulden oder die Vorhersehbarkeit der Gefahr kommt es bei § 904 BGB nicht an.[57] Die Notstandshandlung muss sodann auch geeignet und erforderlich sein. Zweifel bestehen an der Erforderlichkeit, wenn es technisch möglich sein sollte, den Betroffenen zu informieren und selber zu einer Desinfektionsmaßnahme aufzufordern. Dies an sich erscheint schon technisch kaum möglich. Nutzer könnten jedoch zudem den Hinweis ignorieren, wodurch eine Erforderlichkeit begründet werden könnte. Außerdem kann eine derart schnelle Desinfektion erforderlich sein, um akute Gefahren abzuwehren. Es muss ferner angedacht werden, ob tatsächlich ausschließlich die Desinfektion des Einzelnen technisch möglich ist oder ob an Verfahren gearbeitet werden kann, mit deren Hilfe gegen den Ursprung des Botnetzes vorgegangen werden kann. Letztlich ist eine Interessenabwägung durchzuführen, bei der die gefährdeten Rechtsgüter miteinander abzuwägen sind: Überwiegt das geschützte das beeinträchtigte

57; *Kühl,* in: Lackner/Kühl, (o. Fußn. 45), § 34 Rn. 14; *Beulke,* in: *Wessels*/Beulke, Strafrecht Allgemeiner Teil, 42. Aufl. (2012), Rn. 287.

53 Palandt/*Ellenberger*, (o. Fußn. 18), § 228 Rn. 6; *Fahse*, in: Soergel, Bürgerliches Gesetzbuch II, 13. Aufl. (1999), § 228 Rn. 13 f.; *Repgen*, in: Staudinger, BGB, Buch 1: Allgemeiner Teil, §§ 164-240 (Allgemeiner Teil 5), 2009, § 228 Rn. 16.

54 *Schulte-Nölke*, in: Schulze u.a., BGB Handkommentar, 7. Aufl. (2011), § 904 Rn. 1.

55 *BGH*, NJW 1963, 1069; 1964, 1911; 1969, 939.

56 Daten können unter den Eigentumsbegriff gefasst werden, siehe *Wiek-Noodt,*in: Münchener Kommentar StGB V, 1. Aufl. (2006), § 303 Rn. 33.

57 *Seiler*, in: Staudinger, BGB, Buch 3: Sachenrecht, §§ 903 - 924 (Eigentum 1), 14. Aufl. (2002), § 904 Rn. 13.

Interesse wesentlich, kann eine Rechtfertigung erfolgen. Zu wessen Seite die Interessenabwägung dabei ausschlägt, hängt von den Umständen des Einzelfalls und den entsprechend bedrohten Rechtsgütern ab: Sollte das Botnetz bspw. gezielt angelegt sein, um kritische Infrastrukturen und Menschenleben zu gefährden, wären mögliche Vermögensschäden zu rechtfertigen. Allerdings gilt umgekehrt, dass eine Desinfektion nicht zu rechtfertigen wäre, wenn Desinfektionsmaßnahmen kritische Infrastrukturen gefährden und „nur" Vermögensschäden durch das Botnetz möglich erscheinen. Drohen qualititativ gleichartige Verluste, kann es gerechtfertigt sein, den quantitativ größeren Verlust abzuwenden.[58]

Im Ergebnis ist also auf den Einzelfall und die konkret gefährdeten Rechtsgüter zu verweisen. Bei Vorliegen der Voraussetzungen des § 904 BGB erwächst dem Duldungspflichtigen jedoch aus § 904 Satz 2 BGB ein verschuldensunabhängiger Schadensersatzanspruch, sofern er die Notstandslage nicht schuldhaft verursacht hat. § 254 BGB kann bei diesem Anspruch ebenfalls herangezogen werden.

Die Erwägungen gelten auch für die Rechtfertigung anderer Rechtsgüter außer Eigentum, die durch § 34 StGB möglich ist.

4.3.3. Mögliche weitere Rechtfertigungsgründe

Die Regeln der Geschäftsführung ohne Auftrag (§§ 677 ff. BGB) werden zumindest im Zivilrecht auch als Rechtfertigungsgrund für unerlaubte Handlungen angesehen. Allerdings liegen die Voraussetzungen einer Geschäftsführung ohne Auftrag des ISP im Verhältnis zu Kunden schon nicht vor, da der Vertrag zwischen ISP und Kunden eine Abwehrpflicht beinhaltet. Im Verhältnis zu Dritten besteht zwar kein Auftrag, aber im Ergebnis kann eine Beurteilung offen bleiben. Der ISP haftet regelmäßig – sollte ein deliktischer Anspruch ausscheiden – aus einem vertraglichen Anspruch (die Geschäftsführung ohne Auftrag als Schuldverhältnis und eine entsprechende Sorgfaltspflichtverletzung, die im Fall des – wenn auch nur bedingten – Vorsatzes nicht durch die Privilegierung des § 680 BGB legitimiert würde) oder dem Anspruch aus § 678 BGB, also einem Übernahmeverschulden, durch die dann nicht vorhandene verkehrserforderliche Sorgfalt.

Es kann ferner angedacht werden, § 109 Abs. 2 TKG, der die Erhaltung der Verfügbarkeit von Telekommunikationssystemen als zentraler Infrastruktur bezweckt,[59] als Rechtfertigungsgrund fruchtbar zu machen. Dieser schreibt den Betreibern öffentlicher Telekommunikationsnetze u.a. vor, Maßnahmen gegen Störungen durch äußere Eingriffe zu treffen. Allerdings wird weder aus dem Wortlaut noch aus dem Telos ersichtlich, dass eine Rechtfertigung schädigender Maßnahmen gewollt ist. Insbesondere vor dem Hintergrund des

58 So *Fischer*, wenn auch zu § 34 StGB: *Fischer*, (o. Fußn. 32), § 34 Rn. 13.

59 *Klesczewski,* in: Säcker, Berliner Kommentar zum Telekommunikationsgesetz, 2006, § 109 Rn. 17.

Rechtsstaatsprinzips und des ansonsten verbundenen Eingriffs in hochrangige Grundrechte wie u.a. Eigentum, ist eine andere Deutung nicht möglich.

4.4. Ergebnis

Die Desinfektion als effektivstes individuelles Mittel der Bekämpfung von Botnetzen birgt hohe rechtliche Risiken in zivil- als auch in strafrechtlicher Hinsicht. In gewissen Konstellationen ist eine Rechtfertigung zwar möglich, insgesamt muss den ISPs aber unter der aktuellen Rechtslage und den bestehenden Risiken abgeraten werden, Desinfektionen vorzunehmen. Dies gilt zumindest solange, wie kritische Infrastrukturen gefährdet sind. Gearbeitet werden sollte an Verfahren, die ein höheres Maß an Überschaubarkeit etwaiger Gegenmaßnahmen gewährleisten.

5. Fazit und Ausblick

Die Untersuchungen zeigen, dass vermehrt an präventiven Lösungen gearbeitet werden sollte, da eine reaktive Desinfektion als Mittel zur Bekämpfung von Botnetzstrukturen unter den derzeitigen Gegebenheiten hohe rechtliche, nahezu unüberschaubare Risiken mit sich bringt. Ansatzpunkte sind zum einen eine Sensibilisierung der Bevölkerung für die Thematik der IT-Sicherheit. So existiert mit der Website *www.botfrei.de* bereits ein Beispiel, wie diese Sensibilisierung erfolgen kann, auch wenn die Website wohl noch keine ausreichende Bekanntheit besitzt. Derartige Maßnahmen können sich allerdings lohnen, da das Problem der IT-Kriminalität wachsend ist. Zum anderen sind Forschungsprojekte, die sich der Thematik der Bekämpfung von Botnetzstrukturen widmen, zu befürworten und wichtig. Die Forschung kann der Praxis dabei wesentlich unter die Arme greifen und gemeinsam können adäquate Lösungen entwickelt werden. Ein Beispiel stellt das interdisziplinäre Forschungsprojekt MonIKA (Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung) dar, an dem die Verfasser dieses Beitrags partizipieren.[60]

[60] Nähere Informationen unter http://www.vdivde-it.de/KIS/sichere-ikt/it-sicherheitsforschung/monika.