Computerwürmer – eine Gemeingefährdung?

Christian Bergauer

Karl-Franzens-Universität Graz
Institut für Rechtsphilosophie, Rechtssoziologie und Rechtsinformatik
Universitätsstraße 15, 8010 Graz
christian.bergauer@uni-graz.at

Schlagworte: Computerstrafrecht, Malware, Gemeingefährdung
Abstract: Neben der Anwendbarkeit der speziellen Computerdelikte des StGB (§ 126a, § 126b, § 126c) könnte möglicherweise im Zusammenhang mit der explosionsartigen und vom Täter unkontrollierbaren Verbreitung von Computerwürmern über das Internet auch der Tatbestand der vorsätzlichen Gemeingefährdung gem § 176 StGB für eine strafrechtliche Beurteilung herangezogen werden. Untersucht wird, ob sich diese „alte" Strafbestimmung auch auf derartig „neue" Sachverhalte anwenden lässt.

1. Einleitung

Computerwürmer gibt es bereits seit vielen Jahren. Einer der ersten Vertreter war der Morris-Wurm[1], der bereits im Jahr 1988 einige Netzwerke durch Mehrfachbefall lahmgelegt hat. Zum Unterschied von Computerviren, sind Computerwürmer selbständige, sich selbst reproduzierende Programme, die kein Träger- bzw Wirtsprogramm benötigen und sich explosionsartig über Netzwerke verbreiten.[2] Dabei dient ein einzelner Computer lediglich als Mittel zum Zweck, nämlich dem Zweck, ganze Computernetzwerke zu attackieren.[3] Auch führen die meisten Computerwürmer eine schädigende Funktion mit sich, die die infizierten Computersysteme beeinträchtigen soll. Neben diesem „Payload"[4] besitzen Würmer auch einen Infektionsmechanismus[5], der die Verbreitung und Reproduktion steuert. In sehr vie-

1 *Winterer*, Viren, Würmer & Trojanische Pferde (2002) 140 ff; siehe auch *Harley/Slade/Gattiker*, Das Anti-Viren-Buch (2002) 405.
2 *Harley/Slade/Gattiker*, Anti-Viren-Buch, 100.
3 *Winterer*, Viren, 131.
4 *Harley/Slade/Gattiker*, Anti-Viren-Buch, 131 f.
5 *Harley/Slade/Gattiker*, Anti-Viren-Buch, 129 f.

len Fällen verbreiten sich Würmer per E-Mail – über E-Mail-Adressbücher der befallenen Opfer-Computersysteme. Einige Wurm-Gattungen besitzen – analog zu Computerviren – auch eine sog „Trigger-Funktion“[6], die an einen Bedingungseintritt geknüpft ist. Dieser Auslösemechanismus bestimmt letztendlich, wann der Payload am befallenen Computer ausgeführt werden soll. Weiters gibt es auch selbststartende Würmer[7], wie etwa den „Sasser-Wurm“, bei denen das Opfer selbst keine Interaktion mehr setzen muss, um das Wurmprogramm auszuführen. Eine aktive Internetverbindung ist für eine Schädigung und Verbreitung dabei völlig ausreichend.

Hinsichtlich der unterschiedlichen Ebenen, auf denen der Wurm aktiv ist, unterscheidet man zwischen der Computer- und Netzwerkebene. Auf der Computerebene befällt der Wurm einen einzelnen Computerarbeitsplatz, weshalb man von einem Befall durch ein „Wurmsegment“ spricht. Das Zusammenspiel und die Vereinigung sämtlicher Wurmsegmente führt letztendlich zum Computerwurm bzw Internetwurm auf Netzwerkebene.[8]

2. Computerstrafrecht

Mit Einführung des § 126 a durch das StRÄG 1987[9], gibt es eine spezielle Bestimmung im Strafgesetzbuch, die Datenbeschädigungshandlungen pönalisiert. § 126a[10] ist daher sehr eng an die Sachbeschädigung nach § 125 angelehnt, wobei – im Gegensatz zu § 125 – unkörperliche Sachen, wie elektronisch verarbeitbare Daten, vor Beeinträchtigungen geschützt werden. Unter dem Begriff „Daten“ werden gem § 74 Abs 2 personenbezogene und nicht personenbezogene Daten, sowie Programme verstanden.

Tathandlungen sind das Verändern, Löschen, sonst Unbrauchbarmachen oder Unterdrücken von Daten.

Auch hat sich der Gesetzgeber an internationalen Vorgaben[11] orientiert und weitere spezielle Computerdelikte mit dem StRÄG 2002[12] ins StGB ein-

6 *Harley/Slade/Gattiker*, Anti-Viren-Buch, 130 f.
7 *Harley/Slade/Gattiker*, Anti-Viren-Buch, 101.
8 *Gleißner*, Manipulation in Rechnern und Netzen: Risiken, Bedrohungen und Gegenmaßnahmen (1990), 23.
9 Strafrechtsänderungsgesetz 1987, BGBl I 1987/605.
10 Paragrafenangaben ohne Nennung des Gesetzes beziehen sich auf das StGB.
11 Convention on Cybercrime (ETS 185), http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (19. 03. 2007).
12 Strafrechtsänderungsgesetz 2002, BGBl I 2002/134.

geführt. Dabei handelt es sich ua um die „Störung der Funktionsfähigkeit eines Computersystems“ gem § 126 b und um das Vorbereitungsdelikt des § 126c[13] (Missbrauch von Computerprogrammen oder Zugangsdaten).

Diese speziellen Strafbestimmungen sind bei der kernstrafrechtlichen Beurteilung von Angriffen auf Daten bzw Systeme mittels Computerwürmern jedenfalls zur Prüfung heranzuziehen. Sollte zudem Hardware – als körperliche Sache – von einem Computerwurm beschädigt werden, so könnte auch die klassische Sachbeschädigung nach § 125 mit der Datenbeschädigung konkurrieren.

Die genannten Bestimmungen sind im Vermögensstrafrecht angesiedelt, weshalb die Datenbeschädigung (§ 126a) und auch die dazu subsidiäre Störung der Funktionsfähigkeit eines Computersystems (§ 126b) einen nachteiligen, vermögensschädigenden Charakter haben müssen. Das Schadensausmaß orientiert sich grundsätzlich an den Wiederherstellungs- bzw Beschaffungskosten, also an jenem finanziellen Aufwand, der zur Rekonstruktion der Daten erbracht werden muss und für vernünftig denkende Menschen bereits ins Gewicht fällt.[14]

Unter „Vermögen“ versteht das Strafrecht ganz allgemein, sämtliche Aktiva, also auch Forderungen und vermögenswerte Rechte.[15] Mit anderen Worten sind davon alle wirtschaftlich ins Gewicht fallenden und rechnerisch feststellbaren Werte erfasst.[16] Es kommt dabei auf eine rein wirtschaftliche und nicht auf eine formaljuristische Betrachtung an.[17]

Geschütztes Rechtsgut der Datenbeschädigung ist neben dem „Vermögen“ auch das Interesse am Fortbestand und der Verfügbarkeit von Daten.[18]

ME sind die genannten Bestimmungen auch ausreichend, um derartige Sachverhalte zu erfassen. Betrachtet man gleichwohl die Funktionsweise eines Computerwurms, der sich explosionsartig über Netzwerke verbreitet und vom Täter unkontrollierbar Daten und Systeme schädigt, so könnte möglicherweise auch die vorsätzliche Gemeingefährdung gem § 176 ins Treffen geführt werden.

---

13 Novelliert durch das Strafrechtsänderungsgesetz 2004, BGBl I 2004/15.

14 *Reindl*, Computerstrafrecht im Überblick (2004) 21; vgl auch *Bertel/Schwaighofer*, Österreichisches Strafrecht – Besonderer Teil I §§ 75 bis 168b StGB[9] (2006), 154.

15 *Triffterer* in Triffterer-Komm § 126 a Rz 82.

16 *Kienapfel*, Grundriss des österreichischen Strafrechts – Besonderer Teil II[3] (1993) § 144 Rz 42 und § 146 Rz 119.

17 *Venier*, „Kunsterpressung“ – ein vermögensstrafrechtliches Paradoxon?, JSt 2004, 73.

18 *Triffterer* in Triffterer-Komm § 126 a Rz 21.

3. Die vorsätzliche Gemeingefährdung

§ 176 pönalisiert die vorsätzliche „Herbeiführung" einer Gemeingefahr. Tathandlung kann jede Handlung oder Unterlassung sein, die an den geschützten Rechtsgütern Leben, Gesundheit, körperliche Sicherheit, aber auch fremdes Eigentum eine konkrete Gefährdung herbeiführt.[19] Auf der subjektiven Tatseite wird ein (bedingter) Gefährdungsvorsatz gefordert.

Das Wesen der Gemeingefahr liegt in erster Linie in der Unberechenbarkeit ihres Wachstums und in der Machtlosigkeit des Täters gegenüber den Folgen seiner Handlung.[20] Zudem zeichnet sie sich durch einen unbestimmten Gefahrenradius und ihre Unbeherrschbarkeit aus.[21] Von Gemeingefahr spricht man, wenn eine Verletzung von Leib oder Leben einer größeren Zahl von Menschen oder für fremdes Eigentum im großem Ausmaß mit großer Wahrscheinlichkeit zu erwarten ist. Auf die tatsächliche Verletzung kommt es hingegen nicht an. Die „drohende" Verletzung eines der taxativ genannten Rechtsgüter reicht aus.[22] Die Gefährdung der Rechtsgüter muss „konkret" sein. Das heißt, dass Personen oder Objekte jedenfalls tatsächlich in den Gefahrenbereich geraten müssen.[23]

Bei der Gefährdung einer größeren Zahl von Menschen geht die Rsp und Lehre von einem Richtwert ab etwa 10 Personen aus.[24] Eine Gemeingefahr für Eigentum im großem Ausmaß liegt vor, wenn ein Schaden von mehr als € 500 000,-[25] bzw € 50 000,-[26] zu erwarten ist.

Die Verbreitung eines Computerwurms erfüllt prinzipiell exakt das gesetzliche Tatbild der Gemeingefährdung, zumal der Täter nach dem Versenden seiner Malware[27] nicht mehr Eingreifen kann und auch die Unberechenbarkeit der Verbreitung keinesfalls abzuschätzen vermag. Die Situation ist einem „Lauffeuer" gleich, nur mit der Erweiterung, dass der Gefahrenradius ein viel größerer ist, man denke an das weltumspannende Internet. Computerwürmer, die sich „selbsttätig" über Sicherheitslücken bzw Websites oder über die „Mitwirkung" eines E-Mail-Empfängers durch

---

19 *Mayerhofer* in WK² § 176 Rz 6; vgl auch *Triffterer* in Triffterer-Komm § 176 Rz 3.

20 *Fabrizy*, StGB und ausgewählte Nebengesetze⁹ (2006) § 176 Rz 2.

21 *Triffterer* in Triffterer-Komm § 176 Rz 9 mwN.

22 *Triffterer* in Triffterer-Komm § 176 Rz 7.

23 *Mayerhofer* in WK² § 176 Rz 7.

24 *Bertel/Schwaighofer*, Österreichisches Strafrecht – Besonderer Teil II §§ 169 bis 321 StGB⁷ (2006), 7; *Fabrizy*, StGB⁹ § 176 Rz 3; *Mayerhofer* in WK² § 176 Rz 8 mwN.

25 *Bertel/Schwaighofer*, Strafrecht – BT III⁷, 8.

26 *Fabrizy*, StGB⁹ § 176 Rz 3; vgl auch *Mayerhofer* in WK² § 176 Rz 8 und *Triffterer* in Triffterer-Komm § 176 Rz 21, die von über ATS 500.000,- als Schaden ausgehen.

27 Steht für „Malicious Software" (boshafte Software).

Aufruf des Attachements über Adressbücher verbreiten, können in wenigen Sekunden Internetarbeitsplätze aller Kontinente befallen.

In erster Linie wird bei Computerwürmern an die Gefährdung von Eigentum in großem Ausmaß zu denken sein, da wie oben erwähnt der Payload des Wurms in den meisten Fällen auf Datenbeschädigungen gerichtet ist. Eine Gefährdung für Leib oder Leben kann jedoch dann realisiert sein, wenn zB Verkehrsregelungssoftware oder Computersysteme der Luftraumüberwachung betroffen sind. Bereits im Fall „Sasser-Wurm" hat das entscheidende deutsche Gericht festgestellt, dass der Angeklagte durch die Verbreitung seines Internetwurms Notrufanlagen und ähnliche Einrichtungen vorübergehend funktionsunfähig gemacht hat. Aus diesem Grund seien auch Gefahren für Leib und Leben anderer herbeigeführt worden.[28]

In welchem Ausmaß Schäden durch Computerwürmer zu erwarten sind, lässt sich sehr gut am Beispiel des „VBS/Loveletter"- und „Sasser"-Wurms erkennen. Der „Loveletter"-Wurm richtete im Jahr 2000 einen auf 10 Milliarden Euro geschätzten Schaden an.[29] Auch im Fall „Sasser" hat die Staatsanwaltschaft einen Schaden iHv € 130.000,– ermittelt, wobei davon ausgegangen werden kann, dass der Schaden weltweit mehr als eine Million Euro betrug.[30]

Prüft man nunmehr die Gefährdung von Eigentum, so muss man sich fragen, von welchem „Eigentumsbegriff" das Strafrecht überhaupt ausgeht.

Einig ist sich die Lehre darüber, dass sich der strafrechtliche Eigentumsbegriff grundsätzlich an dem des Zivilrechts orientiert.[31]

Expressis verbis ist in der Definition der Norm vom „Eigentum" die Rede, was impliziert, dass das Vermögen als der weitere Begriff nicht von der Gemeingefährdung erfasst ist. Folglich muss es sich um körperliche Gegenstände handeln.[32]

Kein Problem ergibt sich aus der Subsumtion, wenn der Computerwurm in der Lage ist „Hardware", als körperliche Sache, zu schädigen. Man denke etwa an Überlastung der Festplatten-Schreib- bzw -Leseköpfe, die zu einem

28 Pressemitteilung des Landgerichts Verden, Urteil im Sasser-Prozess, http://www.landgericht-verden.niedersachsen.de/master/C11833164_N6377361_L20_D0_I4799562.html (19. 3. 2007).

29 *Reischl*, Gefährliche Netze (2001), 32.

30 Heise online, Entwickler des Wurms Sasser steht vor Gericht, http://www.heise.de/news ticker/meldung/61392 (19. 3. 2007).

31 *Seiler* in Triffterer-Komm § 125 Rz 5; ebenso *Bertel* in WK² § 125 Rz 3. (Beachte, dass im Strafrecht bei einem Liegenschaftskauf jedoch bereits außerbücherliches Eigentum zB hinsichtlich einer Sachbeschädigung als maßgebend angesehen wird).

32 *Triffterer* in Triffterer-Komm § 176 Rz 21.

„Headcrash“[33] führt. Durch die enorme Ausbreitung eines neuen, den Virenschutzfirmen unbekannten, Computerwurms und Schädigung unzähliger Festplatten kann durchaus eine Gefährdung von Eigentum in großem Ausmaß vorliegen, auch wenn die tatsächliche Schädigung in einzelnen Fällen ausbleibt.

Problematisch ist jedoch der Sachverhalt, wenn der Computerwurm „lediglich“ unkörperliche Software löscht. Auch im Zivilrecht geht die hL[34] davon aus, dass die sachenrechtlichen Bestimmungen des ABGB grundsätzlich nur auf körperliche Sachen abzielen, weshalb an unkörperlichen Sachen kein Eigentum begründet werden kann.

Da im Strafrecht hinsichtlich des Eigentumsbegriffs Zivilrechtsakzessorietät herrscht und zudem das Analogieverbot gilt, wird derzeit die Gefährdung von Software durch einen Computerwurm, auch wenn mittlerweile der wirtschaftliche Wert von Software idR über dem der Hardware steht, nicht als Gemeingefährdung an Eigentum in großem Ausmaß zu inkriminieren sein.

4. Exkurs: Terroristische Vereinigung – Cyberterrorismus

Haben sich auf längere Zeit mehr als zwei Personen zu einer terroristischen Vereinigung zusammengeschlossen, um zumindest eine terroristische Straftat iSd § 278 c Abs 1 zu begehen, so könnte auch § 278 c Anwendung finden. § 278 c Abs 1 Z 6 erfasst als terroristische Straftat ua die Datenbeschädigung nach § 126a, wenn dadurch eine Gefahr für das Leben eines anderen oder für fremdes Eigentum in großem Ausmaß entstehen kann. Zudem muss die Tat auch geeignet sein, eine schwere oder längere Zeit anhaltende Störung des öffentlichen Lebens oder eine schwere Schädigung des Wirtschaftslebens herbeizuführen (Eignung und Zielsetzung als terroristische Straftat).[35]

Auf der subjektiven Seite wird neben dem Tatvorsatz auch der erweiterte Vorsatz verlangt, die Bevölkerung auf schwerwiegende Weise einzuschüchtern, öffentliche Stellen oder eine internationale Organisation zu einer

33 Ein grundsätzlich auf einem Luftpolster über der rotierenden Plattenoberfläche schwebender Schreib- bzw Lesekopf berührt die Oberfläche.

34 *Klang* in *Klang* (Hrsg), Kommentar zum ABGB II² (1950) 131; vgl auch *Spielbüchler* in *Rummel,* ABGB-Kommentar I³ § 292 Rz 2; vgl auch *P. Bydlinski*, Grundzüge des Privatrechts für Ausbildung und Praxis⁶ (2005) 103.

35 *Plöchl* in WK² § 278 c Rz 1.

Handlung, Duldung oder Unterlassung zu nötigen oder die politischen, verfassungsrechtlichen, wirtschaftlichen und sozialen Grundstrukturen eines Staates oder einer internationalen Organisation ernsthaft zu erschüttern oder zu zerstören.

Im diesbezüglichen Zusammenhang mit § 126a, gilt es nun ähnliche Überlegungen anzustellen wie im Falle der vorsätzlichen Gemeingefährdung, da auch hier Eigentum in großem Ausmaß gefährdet sein muss. Der Gesetzgeber räumt zumindest in dieser Strafbestimmung durch die ausdrückliche Normierung dieser Wortfolge ein, dass es durch eine Datenbeschädigung auch möglich sein muss Eigentum zu verletzen. Im EU-Rahmenbeschluss[36], der ua als Grundlage für die Einführung des § 278 c fungierte, wird idZ von „Zerstörungen an Privateigentum" gesprochen, die „zu erheblichen wirtschaftlichen Verlusten führen können". § 278 a wiederum, der die Gründung einer bzw Beteiligung an einer kriminellen Organisation pönalisiert, zählt in Z 1 strafbare Handlungen auf, die eine „kriminelle Organisation" näher beschreiben. Eine kriminelle Zielsetzung der Organisation wäre demnach ua die Bedrohung von „Vermögen" (nicht Eigentum). In den Gesetzesmaterialien[37] findet sich kein Hinweis dazu, warum § 278 a von „Vermögen" und die konkretisierende taxative Aufzählung der terroristischen Straftaten in § 278 c Abs 1 Z 6 von zB der Gefährdung von fremden „Eigentum" im großen Ausmaß spricht. Warum soll nunmehr – entgegen der grundsätzlich geübten Zivilrechtsakzessorietät iZm dem Eigentumsbegriff – eine Eigentumsbegründung an Daten, als unkörperliche Sachen, möglich sein? Denn wie bereits erwähnt ist eines der von § 126 a geschützten Rechtsgüter das „Vermögen". § 278 c Abs 1 Z 6 bringt jedoch nun erstmals den viel engeren Begriff des „Eigentums" mit der Datenbeschädigung in Verbindung.

ME gibt es unterschiedliche Ansätze, wie es zu diesen Unstimmigkeiten gekommen ist:

Es könnte einerseits ein Redaktionsversehen vorliegen oder einfach unbedarft die gegenständliche Wortfolge von den Formulierungen der bestehenden Gemeingefährdungsdelikte (iSd §§ 169 ff) übernommen worden sein.

Oder andererseits ist möglicherweise lediglich eine Datenbeschädigung (iSd § 126a) gemeint, die durch die Manipulation von Daten zusätzlich

36 EU-Rahmenbeschluss vom 13. Juni 2002 zur Terrorismusbekämpfung (2002/475/JI), ABl 2002 L 164, 4.

37 Vgl ErläutRV zum StRÄG 2002, 1166 BlgNR 21.GP 37.

auch körperliche Gegenstände, an denen (zivilrechtlich) Eigentum bestehen kann, in großem Ausmaß „gefährdet".

Eine andere Interpretation würde eine Vermengung wesentlicher Begrifflichkeiten zur Folge haben, die die herkömmlichen strafrechtlichen Definitionen der Begriffe „Eigentum" und „Vermögen" entscheidend verändern würde.

5. Fazit

Die bestehenden kernstrafrechtlichen speziellen Computerdelikte (§ 126a, § 126b, § 126c) erscheinen grundsätzlich bei Daten- bzw System-Angriffen mittels Computerwurm zweckmäßig und ausreichend. Würde man die vorsätzliche Gemeingefährdung ins Treffen führen wollen, so stellt sich jedenfalls das Problem hinsichtlich des Eigentumsbegriffs im Strafrecht, da § 176 ua „Eigentum" in großem Ausmaß schützt. Aufgrund des prinzipiellen Verweises auf das „zivilrechtliche Eigentum" und der damit verbundenen Ablehnung von Eigentum an unkörperlichen Sachen, kann aufgrund des Analogieverbots im Strafrecht keine Gemeingefährdung an (unkörperlicher) Software vorliegen. Dasselbe muss mE auch im Zusammenhang mit der Bestimmung des § 278 c Abs 1 Z 6 gelten, in der expressis verbis unter bestimmten Voraussetzungen eine Datenbeschädigung nach § 126 a als terroristische Straftat in Frage kommt, wenn dadurch ua eine Gefahr für Eigentum im großem Ausmaß entstehen kann. Die ausdrückliche Normierung dieser Wortfolge eröffnet jedoch unterschiedliche Interpretationsmöglichkeiten, die zu einer Vielzahl an Ergebnissen führen können.