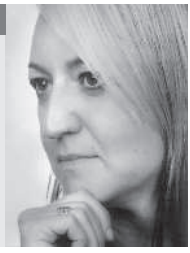
Aleksandra Sowa/Jan Mönikes

Programmier- und Exportverbote für Software?

Nach dem Bekanntwerden der sogenannten »Staatstrojaner« muss man folgende Fragen stellen: Sind neue Gesetze notwendig, um die Programmierung, Nutzung und Verbreitung »gefährlicher« Software – also v.a. von »Schnüffelsoftware«, die die Privatsphäre von Menschen betreffen und auch gegen Regimekritiker in undemokratischen Staaten eingesetzt werden können – zu verbieten oder mindestens zu reglementieren? Oder ist eine endgültige Lösung des Problems durch (neue) Gesetze gar nicht möglich?

Aleksandra Sowa

leitete zusammen mit dem deutschen Kryptologen Hans Dobbertin das Horst Görtz Institut für Sicherheit in der Informationstechnik. Sie ist Autorin zahlreicher Fachpublikationen und aktuell in einem großen Telekommunikationskonzern tätig.



Jan Mönikes

ist als Rechtsanwalt vor allem in den Bereichen Datenschutz, Internet- und Medienrecht tätig. Er ist u.a. Mitglied des Vorstandes des Managerkreises der FES und der deutschen Abteilung des »Internet-Aufsichtsrates« ISOC.

info@moenikes.de

Drei Jahre lang war Philip Zimmermann, der Erfinder der populären Verschlüsselungssoftware *Pretty Good Privacy* (PGP), Ziel polizeilicher Ermittlungen. Die US-Regierung legte ihm die Verletzung von Exportbeschränkungen für Kryptografie, welche in den 90er Jahren in den Vereinigten Staaten galten, zur Last. Als Hilfsmittel zum Schutz der Meinungsfreiheit entwickelt, ermöglicht PGP u.a. vertrauliche E-Mail-Korrespondenz. Die Verschlüsselung von Informationen erfolgte mit Hilfe eines Schlüsselpaares, dessen öffentlicher Teil in einem zentralen Verzeichnis im Internet abgelegt war. Der zweite, private Schlüssel sollte nur für denjenigen verfügbar sein, für den die Information bestimmt ist.

Indem er im Jahr 1991 PGP als Freeware im Internet veröffentlichte, stellte Zimmermann als erster der Allgemeinheit asymmetrische Verschlüsselungsverfahren zur Verfügung, die so wirksam nie zuvor für Private verfügbar, sondern allein staatlichen Institutionen vorbehalten waren.

Noch bis circa 1998 war es in den USA – anders als beispielsweise in Deutschland – nur Banken und anderen Finanzinstitutionen erlaubt, Kryptografiesysteme mit mehr als 128-Bit-Schlüssellängen einzusetzen. Mit Zunahme des E-Commerce wurde das Exportverbot für solche Systeme jedoch auch in den USA schrittweise gelockert, da eine weitere Beschränkung einen negativen Einfluss auf die Wettbewerbsfähigkeit von US-Unternehmen v.a. Softwarefirmen gehabt hätte. Heute wären Internetbanking oder -shopping ohne den Schutz wirksamer Kryptografie gar nicht mehr denkbar. Im Gegenteil verlangt selbst der Bundesgerichtshof heute von jedem Inhaber eines WLAN eine ausreichende Sicherung seines Internetzugangs durch hinreichend sichere Verschlüsselung und Schlüssel.

Software als Kriegswaffe?

Exportbeschränkungen für Software sind allerdings keine US-amerikanische Spezialität. In Deutschland hat man Überlegungen, die Nutzer zum Deponieren eines »privaten« Schlüssels bei einer »vertrauenswürdigen Behörde« per Gesetz zu verpflichten, zwar schon Mitte der 90er Jahre zu den Akten gelegt. Dennoch gilt auch heute Kryptografie weiterhin als »Waffe«, wie die Journalistin Christiane Schulzki-Haddouti den Abschluss des sog. Wassenaar-Abkommens zwischen 33 Staaten, zu denen auch Deutschland gehört, im Dezember 1998 zusammenfasste. Die dort vereinbarten Exportkontrollen gelten heute in der EU. Daher gilt in Deutschland für den Export solcher Software die Genehmigungspflicht von »Dual-Use-Gütern«. Bei der Prüfung, ob gegebenenfalls eine Genehmigung erteilt werden kann, beachtet die Bundesregierung die »Politischen Grundsätze der Bundesregierung für den Export von Kriegswaffen und sonstigen Rüstungsgütern« von 2000 und den »Gemeinsamen Standpunkt 2008/944/GASP des Rates der Europäischen Union vom 8. Dezember 2008 betreffend gemeinsame Regeln für die Kontrolle der Ausfuhr von Militärtechnologie und Militärgütern». Danach werden Exportgenehmigungen bei dem hinreichenden Verdacht des Missbrauchs zur inneren Repression oder zu sonstigen fortdauernden und systematischen Menschenrechtsverletzungen von der Bundesregierung grundsätzlich nicht erteilt. Andererseits ist hochwirksame Verschlüsselungssoftware weiterhin frei im Internet verfügbar, soll dieses auch bleiben und kann selbstverständlich auch von Nutzern in solchen Ländern frei heruntergeladen werden, in die ein offizieller Export nicht genehmigungsfähig wäre. Staatlichen Stellen dort ist es damit aber ein leichtes, solche »zivilen« Produkte dann auch für militärische oder andere staatliche Zwecke zu verwenden. Das Exportverbot für Software hat sich damit aber als in der Praxis wirkungslos erwiesen.

Programmierverbote für Schnüffelsoftware?

Wesentlich weiter geht daher der, wenn auch wenig gelungene, so genannte »Hackertoolparagraf«, der Ende Mai 2007 neu eingefügte §202c StGB, der das Vorbereiten des Ausspähens und Abfangens von Daten unter Strafe stellt und grundsätzlich auch Programme wie den »Staatstrojaner« und andere sogenannte »Remote Forensic Software« umfasst. Denn, wie die im Oktober 2011 vom Chaos Computer Club (CCC) veröffentlichte Analyse des sich heimlich installierenden Programmes ergab, handelt es sich bei den Trojanern um Software, die, ähnlich der im Internet verbreiteten Hacker- und Schadsoftware, heimlich die Daten von Computern ausspäht. Unbemerkt und ohne Spuren zu hinterlassen können damit zudem Dateien auf fremden Rechnern hinterlegt und ferngesteuert sogar weitere Schadsoftware nachgeladen werden. Damit kann auch Zugriff auf »höchst intime« und zugangsgeschützte Daten genommen werden. Strafbar ist nach der StGB-Regel jedoch nicht nur die Beschaffung und Verbreitung von Zugangscodes zu zugangsgeschützten Daten, sondern bereits die Herstellung von Werkzeugen, die diesem Zweck dienlich sind, jedenfalls wenn dies in Vorbereitung einer Straftat geschieht. Juristen gehen wegen dieser Einschränkung davon aus, dass Schnüffelprogramme im Dienste des Staates oder auch der IT-Sicherheit aufgrund legitimer Zweckbestimmung grundsätzlich nicht strafbar sind. Jedoch bleibt die Frage des konkreten Vorsatzes am Ende stets der individuellen Überzeugung eines Staatsanwaltes oder Richters vorbehalten. Schon die Programmierung, die Verbreitung (über das Internet) oder der

Download einer entsprechenden »Schnüffelsoftware« birgt für alle Beteiligten die Gefahr von Strafverfolgung und Verurteilung.

Zweckbestimmungen lassen sich aber nur aus den individuellen Motiven und dem Handeln des jeweiligen Täters ableiten. Ein »legales« und ein »illegales« Programm kann man dann aber eben nicht allein auf Grund rein objektiver Merkmale voneinander unterscheiden, sondern muss dazu mindestens auch die Frage beantworten, ob eine Software hauptsächlich für eine deliktische Verwendung programmiert, verbreitet oder besessen wird. Die abstrakte Gefahr durch ein Programm reicht dagegen nicht aus, Verbot und Strafe zu begründen, weil sonst auch solche Tools strafbar wären, die zwingend zur Überprüfung und Verbesserung der Sicherheit und Integrität informationstechnischer Systeme – gerade zu Zwecken der Verbesserung der Datensicherheit – benötigt werden.

Wenn aber die abstrakte Gefährdung durch »Schnüffelsoftware« kein Verbot begründet, bleibt diese grundsätzlich frei programmier- und auch vertreibbar. Und damit sowohl für inländische, als auch für ausländische Nutzer und fremde Staaten weiterhin zugänglich, da ihnen ja im Zweifel stets das Argument zur Verfügung steht, die Software nur für (mindestens nach ihren nationalen Gesetzen) legale Zwecke der Verbrechensbekämpfung einzusetzen. Denn auch der »Staatstrojaner« ist technisch nichts anderes als die übliche Schnüffelsoftware, wie sie gut- oder eben auch böswillige Hacker aus unterschiedlichen Motiven nutzen – nur dass sie hier in staatlichem Auftrag entwickelt worden ist.

Insoweit ist die Auskunft der Bundesregierung nur konsequent, wenn vielleicht auch politisch nicht befriedigend, dass der Verkauf und die Ausfuhr von Spähsoftware deutscher Hersteller zum Eindringen in fremde Rechnersysteme an andere Regierungen »grundsätzlich keiner Genehmigungspflicht« unterliegt. Nur auf den ersten Blick konsequent erscheint demgegenüber die Kritik beispielsweise von Evgeny Morozov, dass mit dem Verkauf von Spionage-Software westliche Staaten die Repressionen autoritärer Regime unterstützen würden. Überwachungs-Software wäre wie eine Waffe. Ein Exportverbot funktioniere daher nur, wenn es global gelte. Er plädiere daher für eine Außenpolitik, die den Einsatz von Überwachungs-Programmen berücksichtigt. Auf den zweiten Blick wird aber am Beispiel von PGP klar, dass Exportverbote keine Lösung des Problems bieten können. Denn durch das Internet bleibt mindestens die Information über die Funktionsweisen solcher Programme, wenn nicht schon die fertigen Bausteine zu ihrer Entwicklung, immer weltweit und grenzüberschreitend verfügbar. Soweit mit »weltweitem Exportverbot« jedoch in Wirklichkeit ein »globales Verbot« von Hackertools gemeint ist, steht man wieder vor dem gleichen Problem, das schon der deutsche Gesetzgeber mit § 202c StGB nicht überzeugend lösen konnte. Nicht die Verfügbarkeit einer »Dual-Use«-Software ist das Problem, sondern das jeweilige Motiv macht daraus erst eine Waffe.

»Remote Forensic Software« in Deutschland unzulässig?

Wenn das Problem des »Dual-Use« sich aber weder durch ein generelles Verbot entsprechender Programme, noch durch Exportbeschränkungen grundsätzlich lösen lässt, stellt sich die Frage, ob nicht zumindest die Nutzung stärker reglementiert werden kann. Denn zumindest nach Ansicht des CCC liegt die Funktionalität des »Staatstrojaners« weit über dem, was das Bundesverfassungsgericht in einem Urteil von 2008 dem Staat als Grenzen seiner Online-Ermittlungen gesetzt habe. Soweit nicht schon die Möglichkeit der »Quel-

len-TKÜ«, also der Überwachung des Anschlusses bzw. Computers eines Verdächtigen, generell kritisiert wird, steht besonders die in dem staatlichen Trojaner gefundene »Nachladefunktion« in der Kritik.

Das vom Bundesverfassungsgericht entwickelte »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme« lässt nämlich Eingriffe sowohl zu präventiven Zwecken als auch zu Zwecken der Strafverfolgung zu, allerdings nur soweit Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen und wenn das den Eingriff erlaubende Gesetz Vorkehrungen enthält, den Kernbereich privater Lebensführung zu schützen. Überragend wichtige Rechtsgüter sind vor allem Leben, Freiheit und die Gesundheit von Menschen, sowie der Bestand des Staates und seiner Einrichtungen. Einsätze des Trojaners beispielsweise zur Bekämpfung illegalen Zigarettenschmuggels wären somit nicht gestattet. Ebenso nicht Totalüberwachungen, die über die zur Ermittlung einer Straftat nötige Maß hinaus den grundrechtlich geschützten Kernbereich privater Lebensführung betreffen.

Einsatz von »Staatstrojanern« zulässig?

Selbst wenn also eine Nachladefunktion aus irgendwelchen Gründen technisch nötig sein sollte, so muss durch eine noch zu schaffende Rechtsgrundlage sichergestellt werden, dass diese nicht für eine Totalüberwachung genutzt wird. Die Existenz einer solchen Software dagegen ist nicht schon per se verfassungswidrig. Soweit der Gesetzgeber hier für den gesetzlich nötigen Rahmen sorgt, der die Vorgaben des Bundesverfassungsgerichtes beachtet, bleibt der Einsatz von »Staatstrojanern« also zulässig. Die Weiterleitung von ausgespähten Daten auf amerikanische Server oder der Umstand, dass laut CCC auch unberechtigte Dritte sich leichten Zugriff auf die vom Trojaner »infizierten« Rechner verschaffen könnten, widersprechen dabei selbstverständlich aber heute schon geltendem Recht.

Das Grundgesetz, wie auch bestehende und noch zu schaffende gesetzliche Beschränkungen der Verwendung von Schnüffelsoftware durch staatliche Stellen, binden aber nur den deutschen Staat und können nicht auf andere souveräne Staaten ausstrahlen. Denn selbst das generelle Verbot von »Hackertools« und »Schüffelsoftware« kann, genauso wenig wie ein Exportverbot, die Probleme der Verbreitung von »Dual-Use«-Software im Internet lösen, wenn die Nutzung zu »ethischen« Zwecken möglich bleiben muss und die Daten im Internet nicht an Staatsgrenzen angehalten werden sollen.

Zusammenfassend lässt sich sagen, dass sich im Hinblick auf die Verbreitung von »Hacktools« und »Schnüffelprogrammen« Exportbeschränkungen als lediglich symbolisch wirksam erweisen.

Weitergehende Verbote von »Dual-Use«-Software wären nicht wünschenswert, denn es ist im Interesse der Allgemeinheit, wenn wirksame Verschlüsselung jedem Menschen zur Verfügung steht und »Hacktools« jedenfalls zu Zwecken der IT-Sicherheit grundsätzlich frei verfügbar bleiben. Missbrauch durch Kriminelle im Einzelfall ist hinzunehmen und lässt sich auch nur polizeilich, nicht aber grundsätzlich durch Gesetze lösen. Erst recht nicht gegenüber fremden Mächten. Sie hätten bestenfalls symbolische, ansonsten aber nur negative Wirkung.

Davon zu unterscheiden sind nationale Regeln hinsichtlich des Einsatzes solcher Software durch staatliche Stellen innerhalb eines jeweiligen Staates. Das Bundesverfassungsgericht hat für Deutschland den Rahmen abgesteckt. Die Frage, was einem Staat letztlich legal gestattet sein soll, kann dabei nur durch politische Entscheidungen beantwortet werden. ■