Verfassungsmäßigkeit des § 202c StGB

Stellungnahme der Gesellschaft für Informatik e.V. (GI) zur Strafbarkeit der Prüfung des Sicherheitsniveaus von IT-Systemen

Hartmut Pohl

Gemäß dem 2007 in Kraft getretenen § 202c StGB wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, „Wer eine Straftat nach § 202a oder § 202b (Ausspähen und Abfangen von Daten) vorbereitet, indem er ... Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht ...".

Dagegen hat der Geschäftsführer eines Sicherheitsberatungsunternehmens beim Bundesverfassungsgericht Verfassungsbeschwerde eingelegt wg. Unvereinbarkeit mit Art. 12 Abs. 1 GG (Freiheit der Berufsausübung). Der Beschwerdeführer führt aus, auf Wunsch seiner Kunden Penetrationstests in möglichst allen Systembestandteilen und Anwendungen eines Netzwerkssystems durchzuführen. Durch die Strafbarkeit der in § 202c bezeichneten Handlungen sieht er seine wirtschaftliche Existenz in Frage gestellt.

Die Gesellschaft für Informatik e.V. (GI) sieht weitergehende Folgen für den Bereich Datenschutz und generell für die Forschung, Entwicklung und Lehre sowie auch Auswirkungen auf die Praxis.

Im Folgenden wird entsprechend der im Schreiben vom 17. April 2008 formulierten Anregung des Bundesverfassungsgerichts aus der Sicht der Gesellschaft für Informatik e.V. (GI) zu den gestellten Fragen Stellung genommen. Im Anhang 2 wird ein einfacher Änderungsvorschlag zu § 202c vorgelegt.

Zweck von Software

Frage: Inwieweit lässt sich aus informationstechnischer Sicht definieren, welchen „Zweck" eine Software verfolgt? Lassen sich hierfür objektive Kriterien in der Beschaffenheit des jeweiligen Programms angeben oder erfordert dies notwendig oder typischerweise einen Rückgriff auf außerhalb des Programms liegende Umstände?

Zu Beginn werden die Eigenarten von Software und ihre Entwicklung erläutert, um den „Zweck" von Software darzustellen.

Zum Begriff Software

Der Begriff „Software" kennzeichnet Programme für IT-Systeme und wird synonym mit dem Begriff „Programm" benutzt. Aktivitäten von Computern werden grundsätzlich durch Programme gesteuert; Programme stellen eine Folge von Befehlen (Code) dar, die von einem Computer ausgeführt (bearbeitet) werden (sollen). Der Zweck von Software ist daher die Steuerung von Computern.

Software Engineering bezeichnet den Prozess der Softwareerstellung und meint die zielorientierte Bereitstellung und systematische Verwendung von Prinzipien, Methoden und Werkzeugen für die arbeitsteilige, ingenieurmäßige Entwicklung und Anwendung von umfangreichen Softwaresystemen.

DOI 10.1007/s00287-008-0277-6

Prof. Dr. Hartmut Pohl
Informationssicherheit, Fachbereich Informatik,
Fachhochschule Bonn-Rhein-Sieg,
Sprecher des Präsidiumsarbeitskreises „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik e.V. (GI),
Grantham-Allee 20, 53757 Sankt Augustin
E-Mail: Hartmut.Pohl@sang.net

Funktionen, Eigenschaften und Wirkungen sowie Zweck von Software

Funktionen. Das grundsätzliche Verfahrensergebnis der Ausführung eines Programms (seiner Befehle) wird als Funktion bezeichnet. Im Rahmen des Software Engineering werden bei der Erstellung eines Programms regelmäßig die Soll-Funktionen (Requirements) formuliert. Danach wird ein Design (Entwurf) erstellt, das Design in Befehle umgesetzt (Implementierung) und das Programm (Gesamtmenge der Befehle) hinsichtlich seiner Funktionsfähigkeit und Korrektheit überprüft; danach wird das Programm freigegeben und an die Nutzer verteilt.

Da weder die Soll-Funktionen insbesondere umfangreicher Programme oder Programmkombinationen (wie häufig „Malware") unter Sicherheitsaspekten vollständig korrekt erstellt werden können, noch das Programm-Design exakt entsprechend den Soll-Funktionen und auch die Überprüfung des erstellten Codes nicht vollständig sein kann, bleiben – auch sicherheitsrelevante – Fehler in Programmen, die erst im Betrieb oder auch nie bemerkt werden.

Sind z.B. bei einem Produkt die Soll-Funktionen nicht oder nicht vollständig bekannt oder liegen Informationen zum Design nicht vor, so kann allein aus dem Code eines Programms nicht vollständig auf die Funktionen geschlossen werden (Source Code Analysis). Dies gelingt im Gegenteil nur, wenn die Anzahl der Befehle des Programms gering ist und ihre Bedeutung dokumentiert (beschrieben) ist. Wegen der meist vielen Funktionen eines Programms ist die Anzahl von Befehlen häufig groß; so umfasst ein Programm wie ein marktübliches Betriebssystem größenordnungsmäßig 50 Millionen Programmzeilen mit jeweils meist mehreren Befehlen. Derartige Programme sind wegen ihres Umfangs und ihrer komplexen Struktur nicht mehr überschaubar; so sind zwar die wesentlichen Funktionen dokumentiert und anhand der Wirkungen des Programms erkennbar – allerdings sind meist nicht alle Funktionen vollständig dokumentiert und einige können auch unbekannt bleiben.

Eigenschaften und Wirkungen. Ein Programm hat – u.a. entsprechend seinen Funktionen oder seiner Codierungsweise – Eigenschaften wie: Geschwindigkeit der Datenverarbeitung, Benutzerfreundlichkeit (z.B. leichte Benutzbarkeit ohne weitere Ausbildung), großer Speicherbedarf oder unsicherer Betrieb (bricht bei der Eingabe unerwarteter Zeichen ab).

Ein Programm wirkt sich – entsprechend seinen Eigenschaften und Funktionen – auf seine Umgebung aus und kann z.B. Dateien des Betriebssystems ändern, Ressourcen wie Speicher- und Prozessorkapazität konsumieren.

Dual-Use Programme. Soweit bekannt, können alle Angriffsprogramme („Malware") sowohl für schlechte als auch für gute Zwecke (Informationssicherheits-Prüfprogramme) genutzt werden.

1. Beispiel So benutzen Angreifer Passwort-Crackprogramme, um Passworte auszuspähen. Für Sicherheitsbeauftragte in Unternehmen und Behörden ist dasselbe Programm unverzichtbar zur Überprüfung der im Unternehmen benutzten Passworte auf korrekte Einhaltung der Unternehmens-internen Passwort-Richtlinie (z.B. Mindestlänge des Passworts, Wechselhäufigkeit, Verwendung von Buchstaben, Ziffern und Sonderzeichen).

Im Anhang 1 sind eine Reihe von Programmen aufgelistet, die von Unternehmen zur Prüfung des Sicherheitsniveaus ihrer IT-Systeme (Informationssicherheits-Prüfprogramme), aber gleichermaßen auch von Angreifern genutzt werden, um unberechtigt in IT-Systeme einzudringen; u.a. BOSS, das im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zusammengestellt wurde und angeboten wird. Diese Informationssicherheits-Prüfprogramme können durchweg für gute und schlechte Zwecke verwendet werden. Es kommt allein auf die Person des Handelnden und seine Absichten an.

Selbst auf den ersten Blick nur mit gutem Zweck einsetzbare Programme wie Anti-Virenprogramme werden von Angreifern dazu benutzt herauszufinden, welche Anti-Virenprogramme auf einem IT-System laufen, um dann von diesen Programmen nicht erkennbare Viren zu platzieren.

Zusammenfassung zum Zweck von Software. Computerprogramme haben typischerweise keinen eindeutigen „Zweck". Selbst wenn der Entwickler

(Programmierer) einen bestimmten – positiven – Zweck intendiert, können sie immer missbraucht werden.

Die Funktion eines Computerprogramms, eine Sicherheitslücke auf einem Computer (oder in einem Netz) zu erkennen, unterscheidet sich aus technischer Perspektive nicht von der Funktion, einen Angriff gegen einen Computer (oder ein Netz) auszuführen. Aus Sicht der GI kann deshalb ein Straftatbestand nicht am Zweck oder der Art des Programms festgemacht werden, sondern ausschließlich an der Art der Verwendung durch einen Nutzer.

⇒ **Aus informationstechnischer Sicht lässt sich nicht definieren, welchen „Zweck" eine Software verfolgt. Hierfür lassen sich auch keine objektiven Kriterien in der Beschaffenheit des jeweiligen Programms angeben. Eine Unterscheidung von Software für Anwendungen, die zur Begehung von Straftaten hergestellt und eingesetzt wird und Software, die ausschließlich für legale Zwecke hergestellt und eingesetzt wird, ist nicht möglich.**
Dies kann allenfalls für den einzelnen Anwendungsfall durch einen Rückgriff auf außerhalb des Programms liegende Umstände erfolgen: Es liegt im Belieben des Anwenders, eine Software für gute oder schlechte Zwecke einzusetzen.

Sachdienlichkeit von Malware

Frage: Inwieweit sind aus informationstechnischer Sicht der Besitz und die Analyse von Software, die ausschließlich oder weit überwiegend für nicht autorisierte Zugriffe auf informationstechnischen Systemen eingesetzt wird („Malware"), sachdienlich oder notwendig, um mögliche Schwachstellen der Systeme auffinden und beheben zu können?

Nach dem Stand der Technik (z.B. ISO/IEC 27000-Familie und entsprechend IT-Grundschutzkataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI)) [2] ist Software (Informationssicherheits-Prüfprogramme – „Malware") zur Prüfung des Sicherheitsniveaus von unternehmensinternen IT-Systemen (mit Anwendungsprogrammen, Betriebssystemen etc.) ein unverzichtbarer Bestandteil von Sicherheitsprüfungen im IT-Bereich. Mit diesen Informationssicherheits-Prüfprogrammen werden von Herstellern und Anwendern Sicherheitslücken in Programmen gesucht. Im Rahmen des Secure Software Development Lifecycle (SDL) geschieht dies bereits in der Designphase von Programmen mit Verfahren wie Threat Modeling; weiterhin wird z.B. der generierte Code auf Sicherheitslücken mit Programmen zur Source Code Analysis überprüft und es werden bekannte Angriffsverfahren z.B. zur Erkennung von Pufferüberläufen eingesetzt (Exploiting Frameworks).

Software zur Prüfung des Sicherheitsniveaus wird so lange für größere Programme unverzichtbar bleiben, wie es nicht möglich ist, ihr Design als korrekt im Sinne der Sicherheitsforderungen mathematisch zu beweisen und (anschließend) den Programmcode als dem Design entsprechend mathematisch zu beweisen und damit nachzuweisen, dass ein Programm sicher ist.

Programme können keine Unterscheidungen zwischen Anwendungen zur Begehung von Straftaten und solchen ausschließlich für legale Zwecke treffen. Die heute verwendeten Informationssicherheits-Prüfprogramme zur Aufdeckung von Sicherheitslücken in IT-Systemen werden deshalb auch für Angriffe auf IT-Systeme verwendet.

Tatsächlich werden weit überwiegend ursprünglich als „Malware" für Angriffszwecke entwickelte Programme von Herstellern und Anwendern zum Aufspüren von Sicherheitslücken als Informationssicherheits-Prüfprogramme in den Bereichen IT-Sicherheit und Datenschutz genutzt – in Anhang 1 sind dazu Web-Seiten aufgelistet mit „Malware" aus Bereichen wie Cracking, Exploiting, Footprinting, Fuzzing, Scanning, Sniffing, Source Code Analysis, Spoofing etc.

Vor dem Einsatz von Informationssicherheits-Prüfprogrammen muss vom Anwender wie dem IT-Sicherheitsbeauftragten oder Datenschutzbeauftragten der funktionale Umfang analysiert werden, um über die gewünschte Art der Ergebnisse und damit den konkreten Einsatz im Unternehmen (Zeitpunkt, IT-System) entscheiden zu können.

⇒ **Besitz und Analyse von Informationssicherheits-Prüfprogrammen („Malware") ist zur Feststellung und Behebung von Schwachstellen von IT-Systemen in den Bereichen IT-Sicherheit und Datenschutz unverzichtbar.**

Auswirkungen auf Forschung, Entwicklung und Lehre an Hochschulen

Frage: Liegen Ihrer Organisation Erkenntnisse darüber vor, wie sich das Inkrafttreten der angegriffenen Norm – namentlich des Abs. 1 Satz 2 – auf die universitäre Forschung und Lehre zur Sicherheit von Informationssystemen tatsächlich ausgewirkt hat? Wurden insbesondere Lehrveranstaltungen modifiziert oder nicht mehr angeboten? Lassen sich – gegebenenfalls – Aussagen darüber treffen, inwieweit sich die etwaigen Änderungen in der Lehre auf die Sicherheit der Informationstechnik auswirken?

Auswirkungen auf Forschung und Lehre

Eine nicht-repräsentative Umfrage bei Mitgliedern der Gesellschaft für Informatik an Informatiklehrstühlen ergab, dass das Inkrafttreten der angegriffenen Norm im Lehrbereich vielfach starke Verunsicherung hervorgerufen hat. Als Reaktion auf den § 202c wurden die Inhalte von Lehrveranstaltungen modifiziert. Dies gilt auch für Lehrveranstaltungen zur Praxis des Datenschutzes.

Es ist einhellige Meinung, dass für eine qualifizierte Lehre in Informationssicherheit an Hochschulen die fundierte Vermittlung der theoretischen Funktionsweise von „Malware", ihr exemplarischer praktischer Einsatz und auch die beispielhafte Entwicklung derartiger „Malware" an Hochschulen unverzichtbar sind. Ziele der Hochschulen in diesem Bereich sind

1. sachkundige Informationssicherheits-Fachleute auszubilden und
2. den Entwicklern zukünftiger sicherer Systeme eine wissenschaftlich fundierte Kompetenz zu vermitteln.

In Forschung, Lehre und Entwicklung müssen vielmehr auch die zur Verfügung stehenden Sicherheits-Prüfprogramme hinsichtlich ihrer Funktionen untersucht, bewertet und weiterentwickelt werden.

Diese Auffassung teilen auch die von der Gesellschaft für Informatik e.V. befragten Datenschutzbeauftragten.

Es kann regelmäßig davon ausgegangen werden, dass weder die Informatik-Professoren noch die Studierenden konkrete Taten planen oder auch nur vor Augen haben noch generell in Forschung, Entwicklung und Lehre Straftaten vorsätzlich oder im Wege des Eventualvorsatzes vorbereitet werden. Vielmehr kann davon ausgegangen werden, dass im Rahmen des Lehrbetriebs berechtigt und befugt gehandelt wird, sowie nur auf Daten zugegriffen wird, die für die Studierenden bestimmt und ggf. für sie so gesichert sind, damit diese die Zugangssicherung überwinden lernen.

2. Beispiel Kryptoanalyse: Im Bereich der Informationssicherheit wendet die Kryptoanalyse als Teilgebiet der Wissenschaft der Kryptologie Methoden und Techniken an, um Informationen aus verschlüsselten Texten zu gewinnen oder allgemeiner die Analyse kryptographischer Verfahren mit dem Ziel, die Verschlüsselung entweder zu „brechen", d.h. ihre Schutzfunktion aufzuheben bzw. zu umgehen oder ihre Sicherheit nachzuweisen und zu quantifizieren.
   Eine Beschäftigung mit diesem Wissenschaftsbereich wäre gleichermaßen nicht mehr möglich.

Aus Sicht der Gesellschaft für Informatik ist dies nicht nur zur Förderung der Informationssicherheit dringend geboten, sondern ist auch Ausfluss der Freiheit von Forschung und Lehre gemäß Art. 5 Abs. 3 GG. Dazu sollte zur Klarstellung jedenfalls ausdrücklich auf die auch hier geltende Wissenschaftsfreiheit gemäß Art. 5 Abs. 3 GG hingewiesen werden.

Auswirkungen auf die Entwicklung

Die Ausweitung der Strafandrohung auch auf die Forschung und Entwicklung kann dazu führen, dass die notwendige Forschung und Entwicklung in diesem Bereich entscheidend gebremst wird, was wiederum die Gefahr von Angriffen aus dem globalen Internet erhöhen wird. Eine gezielte und ständige Verbesserung von Informationssicherheits-Prüfprogrammen kann nicht durch die Beschränkung der Entwicklung erreicht werden, sondern im Gegenteil ausschließlich durch einen breiten Zugang von Forschung und Lehre in diesem Bereich und darauf aufbauenden eigenen Arbeiten. So müssen bei der Evaluierung eines Systems unter Sicherheitsaspekten alle Komponenten eingehend analysiert werden.

Ein Computersystem wird nicht dadurch unsicher, dass ein Angriffswerkzeug entwickelt wird. Das Angriffswerkzeug nutzt nur in der Software

vorhandene Schwachstellen, zeigt sie auf oder deutet zumindest auf sie hin – ermöglicht aber dadurch auch, die erkannten Schwachstellen zu schließen. Ein Verbot von Werkzeugen fördert somit direkt die Verbreitung unsicherer IT-Systeme, da die Schwachstellen nicht mehr offen zu Tage treten.

3. Beispiel Anti-Virenprogramme: Angriffe mit Computerviren lassen sich nur erkennen und abwehren, wenn der benutzte Virus oder zumindest seine Funktionsweise bekannt sind. Im betrieblichen Einsatz müssen die Randbedingungen (z.B.: nicht alle Viren werden von allen Produkten erkannt) und die Funktionsweise (z.B. Vergleich bekannter Vireneigenschaften mit dem aktuellen Datenstrom) dem Entwickler (Hersteller) bekannt sein; neue Viren müssen sowohl hinsichtlich ihres Aufbaus als auch ihrer Funktion detailliert analysiert werden.

Sollte auch die Beschäftigung mit Sicherungscodes und Computerprogrammen verboten sein, dürfte insgesamt nicht nur die (international erhebliche) deutsche IT-Sicherheitsforschung sondern auch die deutsche IT-Sicherheitsindustrie einen erheblichen Rückschlag erleiden. Damit würden einige Tausend Arbeitsplätze wegfallen. Weiterhin würde ein entscheidender Anteil der Informationssicherheits-Ausbildung an Hochschulen wegfallen und damit der Informationsfluss neuester Sicherheitstechnologien an Unternehmen durch die Absolventen unterbrochen. Deutsche Unternehmen könnten sich dann im internationalen Vergleich nur unzureichend schützen, es sei denn, sie werben an ausländischen Hochschulen ausgebildete Informatiker an.

Damit entstünde eine Wettbewerbsverzerrung gegenüber anderen EU-Mitgliedsstaaten und auch international (Israel, Russland, USA etc.). Die gesamte deutsche IT-Sicherheitsbranche wäre benachteiligt, weil Informationssicherheits-Prüfprogramme ausschließlich nur noch in anderen Staaten entwickelt würden.

⇒ **Durch die Strafnorm ist in Wissenschaftskreisen (Forschung, Lehre und Entwicklung) an Hochschulen und Forschungseinrichtungen eine erhebliche Unsicherheit zu erkennen; Lehrveranstaltungen wurden modifiziert. Sollten keine wissenschaftlichen Aktivitäten im Bereich der Informationssicherheits-Prüfprogramme mehr möglich sein, könnten entsprechende Fachleute in Deutschland nur unzureichend ausgebildet werden; damit ständen deutschen Anwendern (Unternehmen, Hersteller von Informationssicherheits-Prüfprogrammen und Sicherheitsbehörden) keine wissenschaftlich ausgebildeten Nachwuchskräfte mehr zur Verfügung – diese Mitarbeiter müssten ggf. im Ausland akquiriert werden; die Qualität der in Deutschland entwickelten Produkte dürfte erheblich leiden.**
Dürfen Informationssicherheits-Prüfprogramme nicht mehr eingesetzt werden, wird das Informationssicherheitsniveau von Unternehmen und Behörden sehr stark absinken und Unternehmen und Behörden werden IT-Angriffen hilflos ausgeliefert sein.
Schließlich müssten sich viele Wissenschaftler an Hochschulen und Forschungseinrichtungen, die im Bereich der IT-Sicherheit tätig sind, bei einem Verbot der Verwendung von Informationssicherheits-Prüfprogrammen in ihrer persönlichen Arbeit neu ausrichten; bestehende Forschungsaktivitäten und -projekte könnten nicht fortgeführt werden. Die gesamte Wissenschaftsdisziplin Informationssicherheit sowie die benachbarte Disziplin Praxis des Datenschutzes müsste eingestellt werden.

Auswirkungen auf die Praxis

Auswirkungen auf Behörden und Unternehmen

IT-Sicherheitsbeauftragte. IT-Sicherheitsbeauftragte in Unternehmen und Behörden müssen u.a. zur Erfüllung ihrer gesetzlichen Verpflichtungen im Rahmen der IT-Compliance die Sicherheit ihrer IT-Systeme wirkungsvoll überprüfen; dabei kommen die Beauftragten nach dem Stand der Technik (z.B. ISO/IEC 27000-Familie und IT-Grundschutzkataloge des BSI) nicht ohne Informationssicherheits-Prüfprogramme aus.

Dies gilt gleichermaßen für von IT-Sicherheitsbeauftragten für ihre Unternehmen beauftragte Sicherheitsberater und Sicherheitsberatungsunternehmen.

Aus dem Ausland werden Informationssicherheits-Prüfprogramme bereits seit Ende 2007 unter Hinweis auf die neue Strafnorm nicht mehr oder

nur zögerlich nach Deutschland exportiert; dadurch dürfte das Sicherheitsniveau deutscher Unternehmen zukünftig drastisch sinken.

Datenschutzbeauftragte. Für den Datenschutzbeauftragten in öffentlichen und nicht-öffentlichen Stellen sind Informationssicherheits-Prüfprogramme zur Überprüfung der Wirksamkeit der nach der Anlage zu § 9 BDSG ergriffenen technischen Maßnahmen nach dem Stand der Technik (z.B. ISO/IEC 27000-Familie und IT-Grundschutzkataloge des BSI) unverzichtbar.

Sicherheitsunternehmen, Sicherheits- und Datenschutzberater. Die Strafnorm trifft auch die Hersteller sowie die Anbieter von Sicherheitslösungen und der entsprechenden Informationssicherheits-Prüfprogramme sowie Security-Spezialisten und -Berater. Die gesamte IT-Sicherheitsbranche ist aber auf solche Computerprogramme angewiesen, mit denen nicht nur die eigenen Systeme überprüft werden können, sondern auch Straftaten im Sinne der Strafnorm begangen werden könnten. Insbesondere die Hersteller dieser Computerprogramme sind darauf angewiesen, dass ihnen gute Absicht und guter Wille unterstellt werden, wenn sie Informationssicherheits-Prüfprogramme herstellen oder zugänglich machen, mit denen Dritte eine Straftat begehen können.

Risiken aus dem Internet

Da Angriffe im weltweiten Internet auch aus Regionen und Bereichen durchgeführt werden, die den Einsatz von Informationssicherheits-Prüfprogrammen (noch) nicht reglementieren, überwachen oder unter Strafe stellen, muss IT-Anwendern die Möglichkeit gegeben sein, im Vorgriff auf solche Angriffe die Sicherheit ihrer eigenen IT-Systeme überprüfen zu können.

Ohne die Informationssicherheits-Prüfprogramme ist die Identifizierung von Sicherheitslücken aber nicht oder kaum möglich und würde dadurch zur „Informations-Unsicherheit“ in Unternehmen und Behörden führen. Dies wäre auch aus der Sicht des Datenschutzes bedenklich.

Zusammenfassung

Angesichts der großen Zahl bekannter, unbekannter und unveröffentlichter Sicherheitslücken in Software muss das Sicherheitsniveau von IT-Systemen kontinuierlich erhöht werden. Dazu sind aus Sicht der Gesellschaft für Informatik die beiden folgenden Punkte unverzichtbar:

1. Alle sicherheitsrelevanten Aspekte von Software müssen allgemein bekannt gemacht werden und sie müssen frei untersucht werden können.
2. Insbesondere müssen erkannte Sicherheitslücken allgemein bekannt gemacht werden und untersucht werden können, um sie beheben zu können.

⇒ **Der Einsatz von Informationssicherheits-Prüfprogrammen („Malware“) und eine breite öffentlich geführte Fachdiskussion ist für Unternehmen, Behörden und Private und insbesondere für Techniker und Informatiker wie auch Fachjuristen in Forschung, Lehre, Entwicklung und Anwendung unverzichtbar.**

Anhänge

Anhang 1: Web-Seiten und E-Mail Dienste

Im Folgenden werden – ohne einen Anspruch auf Vollständigkeit – einige wenige öffentlich zugängliche Webseiten im Internet beispielhaft aufgeführt, auf denen sich mehr als 1.000 Informationssicherheitsprüfprogramme, Angriffsprogramme sowie Sicherheitslücken finden.

Webseiten mit Informationssicherheitsprüfprogrammen und Angriffsprogrammen. Webseiten zum Download von Informationssicherheits-prüfprogrammen und Angriffsprogrammen gegen IT-Systeme (letzter Zugriff: 15. August 2008):

- http://board.kanzleramt.ca/showthread.php?t=3343
- http://www.bsi.bund.de/produkte/boss/index.htm des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- http://www.crackstore.com./
- http://www.foundstone.com/us/resources-free-tools.asp
- http://freeworld.thc.org/releases.php
- http://www.hacken-lernen.de/hacker-programme.php
- http://insecure.org/ mit mehr als 100 Scannern, Crack-Programmen und Sniffern
- http://www.netzwelt.de/software/6924-metasploit-framework-.html

Webseiten mit Informationen zu aktuellen Sicherheitslücken.

- http://www.cve.mitre.org/
- http://www.milworm.com/
- http://www.securityfocus.com/archive/1
- http://www.vulnwatch.org/index.html
- http://www.zerodayinitiative.com/

Informationsservice über Sicherheitslücken mit E-Maillisten.

- http://www.bsi.de/certbund/infodienst/ des Bundesamtes für Sicherheit in der Informationstechnik (BSI): „Warn- und Informationsdienst (WID)"

Anhang 2: Änderungsvorschlag zu § 202c

Aus Sicht der Gesellschaft für Informatik bleibt anzumerken, dass der Gesetzgeber die bestehenden Unsicherheiten um die Reichweite der Strafbarkeit nach § 202c StGB, die daraus resultierenden Verunsicherungen der Wissenschaftler und Anwender im Bereich der IT-Sicherheit sowie die verfassungsrechtlichen Probleme des vorliegenden Verfahrens durch leichte Korrekturen im Gesetzgebungsverfahren weithin hätte vermeiden können. Sowohl aus den technischen wie den juristischen Wissenschaften lagen entsprechende Stellungnahmen vor; auch die GI hat auf die Probleme der aktuellen Gesetzesfassung hingewiesen [3].

Der § 202c StGB ließe sich auf zwei Arten entschärfen. Zum einen könnte eine Bezugnahme auf eine konkrete Tat erfolgen, sodass nicht im Sinne eines abstrakten Gefährdungsdeliktes bereits der bloße Besitz strafbar wäre. Dagegen wird zwar eingewandt, dass dem die Cybercrime-Convention entgegenstehe, die in Art. 6 vorsieht, „den Besitz eines unter Buchstabe a Ziffer i oder ii bezeichneten Mittels mit dem Vorsatz, es zur Begehung einer nach den Artikeln 2 bis 5 umschriebenen Straftat zu verwenden", zu bestrafen. Es wird deshalb sogar vorgeschlagen [1], explizit schon den Besitz zu bestrafen. Dagegen ließe sich einwenden, dass die Formulierung der Konvention jedenfalls enger ist als der Gesetzeswortlaut, weil sie wohl auf eine konkrete Straftat hindeutet.

Zum anderen hätte der Gesetzgeber auch den Eventualvorsatz streichen können: Das hätte es zumindest ausgeschlossen, Wissenschaftler zu bestrafen, die lediglich billigend in Kauf nehmen, dass die von ihnen in Forschung und Lehre verwendeten Programme auch zu schädlichen Zwecken benutzt werden. Die entstehenden Strafbarkeitslücken wären aus Sicht der Gesellschaft für Informatik angesichts der ohnehin weiten Vorverlagerung des Tatbestandes vertretbar gewesen. Man hätte etwa in Anlehnung an [1] die Formulierung in „Wer [Nr. 1 und Nr. 2, Text bis zugänglich macht], mit dem Wissen oder in der Absicht, dass sie zur Begehung einer konkreten Straftat nach § 202a oder § 202b gebraucht werden, wird … bestraft." ändern können.

Danksagung

Die Stellungnahme wurde vom Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik erarbeitet. Besonderer Dank gebührt den Herren Dr. Bernd Beier, Prof. Dr. Dr. Herbert Fiedler, Dr. Gerrit Hornung, LL.M., Prof. Dr. Klaus-Peter Löhr, Prof. Dr. Andreas Pfitzmann und Prof. Dr. Alexander Roßnagel.

Literatur

1. Borges G, Stuckenberg C-F, Wegener C (2007) Bekämpfung der Computerkriminalität – Zum Entwurf eines Strafrechtsänderungsgesetzes zur Bekämpfung der Computerkriminalität. D u D 275–278
2. Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.bund.de/gshb/deutsch/index.htm
3. Gesellschaft für Informatik e.V. (GI) (2007) Entwurfsfassung des § 202c StGB droht Informatiker/innen zu kriminialisieren. http://www.gi-ev.de/aktuelles/meldungsdetails/meldung/159/ (3. Juli 2007)